

Web UI Reference Guide

Product Model : DGS-3130-30TS
Layer 3 Stackable Managed Switch
Release 1.00

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

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

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

© 2017 D-Link Corporation. All rights reserved.

Table of Contents

Table of Contents	i
1. Introduction	1
Audience	1
Other Documentation	1
Conventions	1
Notes, Notices, and Cautions	1
2. Web-based Switch Configuration	3
Management Options	3
Logging into the Web UI	3
Web User Interface (Web UI)	4
Areas of the User Interface.....	4
3. System	6
Device Information	6
System Information Settings	6
Peripheral Settings	7
Port Configuration	8
Port Settings	8
Port Status	10
Port GBIC	11
Port Auto Negotiation	11
Error Disable Settings.....	12
Jumbo Frame	13
System Log	14
System Log Settings.....	14
System Log Discriminator Settings	16
System Log Server Settings	16
System Log.....	18
System Attack Log.....	18
Time and SNTP	19
Clock Settings.....	19
Time Zone Settings	19
SNTP Settings	21
Time Range	22
4. Management	24
Command Logging	24
User Accounts Settings	24
Password Encryption	25
Password Recovery	26
Login Method	26
SNMP.....	28
SNMP Global Settings.....	29
SNMP Linkchange Trap Settings	30
SNMP View Table Settings	31
SNMP Community Table Settings	31
SNMP Group Table Settings	32
SNMP Engine ID Local Settings.....	33
SNMP User Table Settings.....	34
SNMP Host Table Settings.....	35
RMON	37

RMON Global Settings	37
RMON Statistics Settings	37
RMON History Settings	38
RMON Alarm Settings	39
RMON Event Settings	40
Telnet/Web.....	41
Session Timeout	42
DHCP	42
Service DHCP	42
DHCP Class Settings	43
DHCP Server	44
DHCPv6 Server	51
DHCP Relay	56
DHCPv6 Relay	64
DHCP Auto Configuration	72
DNS	72
DNS Global Settings.....	73
DNS Name Server Settings.....	73
DNS Host Settings.....	74
IP Source Interface	75
File System	75
Stacking	77
Physical Stacking	80
Stacking Bandwidth	81
Virtual Stacking (SIM)	82
Single IP Settings	83
SMTP Settings	84
PPPoE Circuit ID Insertion Global Settings	86
5. Layer 2 Features	87
FDB.....	87
Static FDB.....	87
MAC Address Table Settings	88
MAC Address Table	90
MAC Notification	91
VLAN.....	92
802.1Q VLAN	92
802.1v Protocol VLAN	93
GVRP.....	94
Asymmetric VLAN	97
MAC VLAN	98
VLAN Interface	98
Super VLAN.....	104
Auto Surveillance VLAN	105
Voice VLAN	108
Private VLAN	111
VLAN Tunnel	113
Dot1q Tunnel	113
VLAN Mapping	115
VLAN Mapping Profile	116
STP	121
STP Global Settings	123
STP Port Settings	124

MST Configuration Identification	126
STP Instance	127
MSTP Port Information	128
ERPS (G.8032)	129
ERPS	129
ERPS Profile	133
Loopback Detection	134
Link Aggregation	136
L2 Protocol Tunnel	138
L2 Multicast Control	140
IGMP Snooping	140
MLD Snooping	145
Multicast VLAN	152
Multicast Filtering	155
LLDP	156
LLDP Global Settings	156
LLDP Port Settings	158
LLDP Management Address List	159
LLDP Basic TLVs Settings	159
LLDP Dot1 TLVs Settings	160
LLDP Dot3 TLVs Settings	161
LLDP-MED Port Settings	162
LLDP Statistics Information	162
LLDP Local Port Information	163
LLDP Neighbor Port Information	165
6. Layer 3 Features	166
ARP	166
ARP Aging Time	166
Static ARP	166
Proxy ARP	167
ARP Table	168
Gratuitous ARP	168
IPv6 Neighbor	169
Interface	170
IPv4 Interface	170
IPv6 Interface	172
Loopback Interface	175
Null Interface	177
UDP Helper	177
IP Forward Protocol	177
IP Helper Address	178
IPv4 Static/Default Route	178
IPv4 Route Table	179
IPv6 Static/Default Route	180
IPv6 Route Table	181
Route Preference	181
ECMP Settings	182
IPv6 General Prefix	183
RIP	183
RIP Settings	183
RIP Distribute List	185
RIP Interface Settings	186

RIP Database	186
RIPng	187
RIPng Settings	187
RIPng Interface Settings	188
RIPng Database	189
IPMC	189
IP Route Filter	190
Route Map	190
Policy Route	193
VRRP Settings	194
7. Quality of Service (QoS)	196
Basic Settings	196
Port Default CoS	196
Port Scheduler Method	196
Queue Settings	198
CoS to Queue Mapping	198
Port Rate Limiting	199
Queue Rate Limiting	200
Advanced Settings	201
DSCP Mutation Map	201
Port Trust State and Mutation Binding	202
DSCP CoS Mapping	202
CoS Color Mapping	203
DSCP Color Mapping	204
Class Map	205
Aggregate Policer	206
Policy Map	210
Policy Binding	213
WRED	214
WRED Profile	214
WRED Queue	215
8. Access Control List (ACL)	217
ACL Configuration Wizard	217
Step 1 - Create/Update	217
Step 2 - Select Packet Type	218
Step 3 - Add Rule	218
Step 4 - Apply Port	226
ACL Access List	227
Standard IP ACL	229
Extended IP ACL	230
Standard IPv6 ACL	232
Extended IPv6 ACL	233
Extended MAC ACL	236
ACL Interface Access Group	237
ACL VLAN Access Map	238
ACL VLAN Filter	240
CPU ACL	241
9. Security	244
Port Security	244
Port Security Global Settings	244
Port Security Port Settings	245

Port Security Address Entries.....	247
802.1X.....	247
802.1X Global Settings.....	252
802.1X Port Settings.....	252
Authentication Sessions Information	253
Authenticator Statistics	254
Authenticator Session Statistics	255
Authenticator Diagnostics.....	255
AAA.....	256
AAA Global Settings	256
Application Authentication Settings	257
Application Accounting Settings	257
Authentication Settings.....	259
Accounting Settings.....	261
RADIUS	263
RADIUS Global Settings.....	263
RADIUS Server Settings	264
RADIUS Group Server Settings	265
RADIUS Statistic	266
TACACS	267
TACACS Global Settings.....	267
TACACS Server Settings	267
TACACS Group Server Settings	268
TACACS Statistic	269
IMPB	269
IPv4.....	270
IPv6.....	282
DHCP Server Screening.....	287
DHCP Server Screening Global Settings	288
DHCP Server Screening Port Settings.....	289
ARP Spoofing Prevention	289
BPDU Attack Protection.....	290
MAC Authentication	291
Web-based Access Control	293
Web Authentication	295
WAC Port Settings.....	295
WAC Customize Page.....	296
Network Access Authentication	297
Guest VLAN.....	297
Network Access Authentication Global Settings	297
Network Access Authentication Port Settings	299
Network Access Authentication Sessions Information	300
Safeguard Engine	301
Safeguard Engine Settings.....	302
CPU Protect Counters	303
CPU Protect Sub-Interface	303
CPU Protect Type.....	304
Trusted Host	305
Traffic Segmentation Settings.....	305
Storm Control.....	306
DoS Attack Prevention Settings	308
SSH.....	309

SSH Global Settings	310
Host Key	310
SSH Server Connection	311
SSH User Settings	312
SSL	312
SSL Global Settings	313
Crypto PKI Trustpoint	314
SSL Service Policy	315
SFTP Server Settings	315
10. OAM	317
Cable Diagnostics	317
Ethernet OAM	318
Ethernet OAM Settings	318
Ethernet OAM Configuration Settings	319
Ethernet OAM Event Log Table	322
Ethernet OAM Statistics Table	322
DDM	323
DDM Settings	323
DDM Temperature Threshold Settings	324
DDM Voltage Threshold Settings	325
DDM Bias Current Threshold Settings	326
DDM TX Power Threshold Settings	326
DDM RX Power Threshold Settings	327
DDM Status Table	328
11. Monitoring	329
Utilization	329
Port Utilization	329
Statistics	329
Port	329
Interface Counters	331
Counters	333
Mirror Settings	334
sFlow	336
sFlow Agent Information	336
sFlow Receiver Settings	337
sFlow Sampler Settings	337
sFlow Poller Settings	338
Device Environment	339
12. Green	340
Power Saving	340
EEE	341
13. Save and Tools	343
Save Configuration	343
Firmware Upgrade & Backup	343
Firmware Upgrade from HTTP	343
Firmware Upgrade from TFTP	344
Firmware Backup to HTTP	344
Firmware Backup to TFTP	345
Configuration Restore & Backup	345
Configuration Restore from HTTP	345
Configuration Restore from TFTP	346

Configuration Backup to HTTP	347
Configuration Backup to TFTP	347
Log Backup	348
Log Backup to HTTP	348
Log Backup to TFTP.....	348
Ping.....	349
Trace Route	351
Reset.....	353
Reboot System	354
Appendix A - Password Recovery Procedure.....	355
Appendix B - System Log Entries	356
802.1X.....	356
AAA.....	356
ARP.....	358
Auto-save.....	358
BPDU Protection.....	359
Configuration/Firmware	359
DAD	361
DDM.....	361
DHCPv6 Client.....	362
DHCPv6 Relay.....	364
DHCPv6 Server	364
DoS Prevention.....	364
Dynamic ARP Inspection	365
ERPS	365
Ethernet OAM	366
Interface	367
IP Directed Broadcast.....	367
IPSG	367
LACP.....	368
LBD	368
LLDP-MED.....	369
Login/Logout	370
MAC	372
MSTP Debug Enhancement.....	373
Peripheral.....	374
Port	375
Port Security	376
Reboot Schedule	376
Safeguard	376
SNMP.....	376
SSH.....	376
SSL	377
Stacking	377
Storm Control.....	378
Telnet.....	379
Traffic Control	379
VRRP Debug Enhancement.....	380
WAC.....	383
Web.....	383
Appendix C - Trap Entries	385

802.1X.....	385
802.3ah OAM.....	385
Authentication Fail	386
BPDU Protection.....	386
DDM.....	386
DHCP Server Screen Prevention	386
DoS Prevention.....	387
ERPS	387
ErrDisable	387
External Alarm	387
Gratuitous ARP	388
IP-MAC-Port Binding	388
LACP	388
LBD	389
LLDP-MED.....	389
MAC-based Access Control.....	389
MAC Notification	390
MSTP	390
Peripheral.....	390
Port Security	391
Port	391
RMON	391
Safeguard	392
SIM.....	392
Stacking	393
Start	394
Storm Control.....	394
System File	394
Upload/Download	394
VRRP	395
WAC.....	395
Appendix D - RADIUS Attributes Assignment	396
Appendix E - IETF RADIUS Attributes Support.....	399

1. Introduction

This manual's feature descriptions are based on the software release **1.00**. The features listed here are the subset of features that are supported by the DGS-3130-30TS Switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the Switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DGS-3130-30TS Switch, which will be generally be referred to simply as the “**Switch**” within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

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

- *DGS-3130-30TS Hardware Installation Guide*
- *DGS-3130-30TS CLI Reference Guide*

Conventions

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

Notes, Notices, and Cautions

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



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



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



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

2. Web-based Switch Configuration

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

Management Options

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

Command Line Interface (CLI)

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

For more detailed information about the CLI, refer to the *DGS-3130-30TS CLI Reference Guide*.

SNMP-based Management

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

Web User Interface (Web UI)

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

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



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

Logging into the Web UI

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



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



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

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

A screenshot of a web browser displaying a login window titled 'Connect to 192.168.70.123'. The window has a blue header with a key icon. Below the header, there are two input fields: 'User Name' and 'Password'. At the bottom of the form, there are two buttons: 'Login' and 'Reset'.

Figure 2-2 Web UI Login Window

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



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

Web User Interface (Web UI)

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

Areas of the User Interface

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

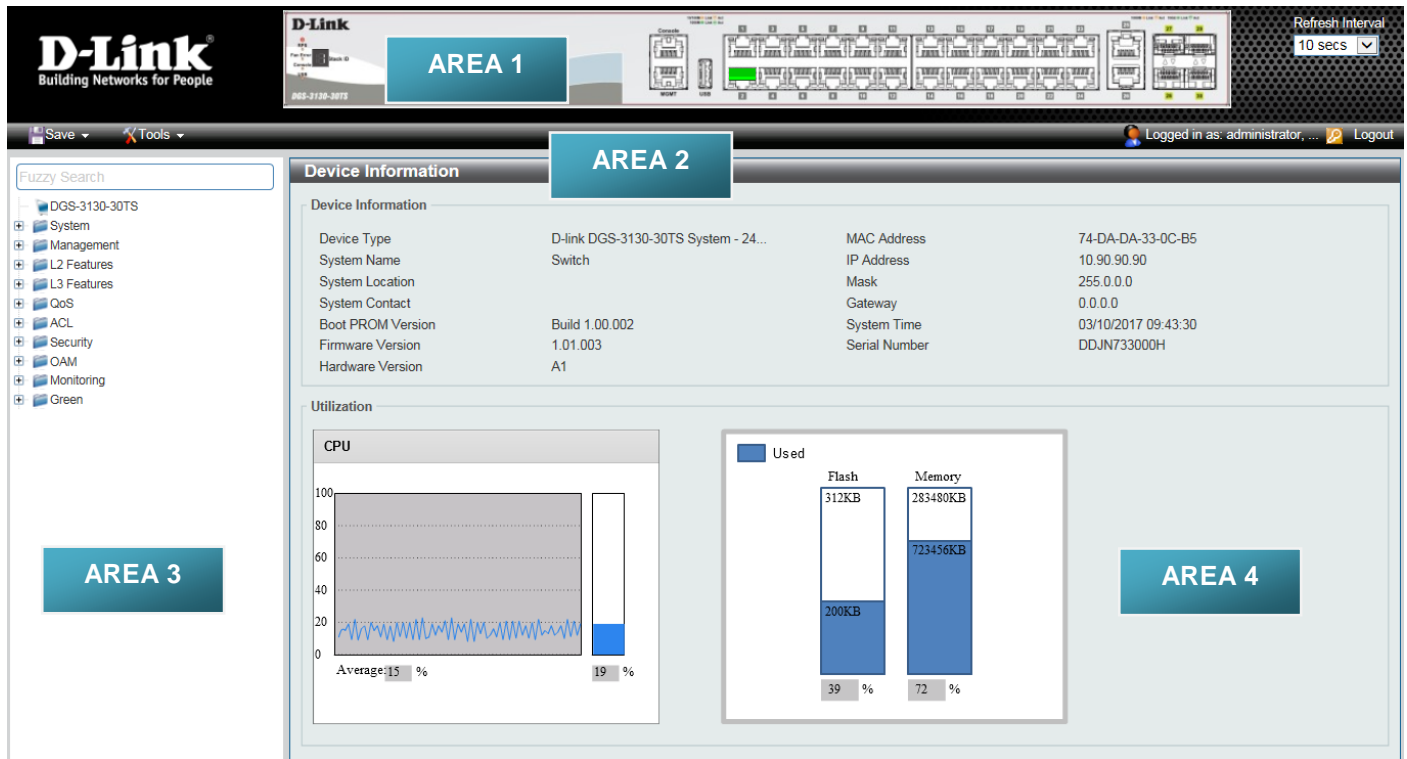


Figure 2-3 Main Web UI Window

Area Number	Description
AREA 1	This area displays a graphical, near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules. It also shows port activity based on a specific mode. Some management functions, including port monitoring, are accessible from here. Click the D-Link logo to go to the D-Link website.
AREA 2	This area displays a toolbar used to access Save and Tools menus.
AREA 3	This area displays a file explorer-type menu tree with all configurable options. Select the folder or window to display. Open folders and click the hyperlinked window buttons and subfolders contained within them to display information pertaining to that category.
AREA 4	In this area, the Switch's configuration page can be found, based on the selection made in AREA 3 .



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



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

3. System

[Device Information](#)
[System Information Settings](#)
[Peripheral Settings](#)
[Port Configuration](#)
[System Log](#)
[Time and SNTP](#)
[Time Range](#)

Device Information

In the Device Information section, the user can view a list of basic information regarding the Switch. It appears automatically when you log on to the Switch. To return to the Device Information window after viewing other windows, click the **DGS-3130-30TS** link.

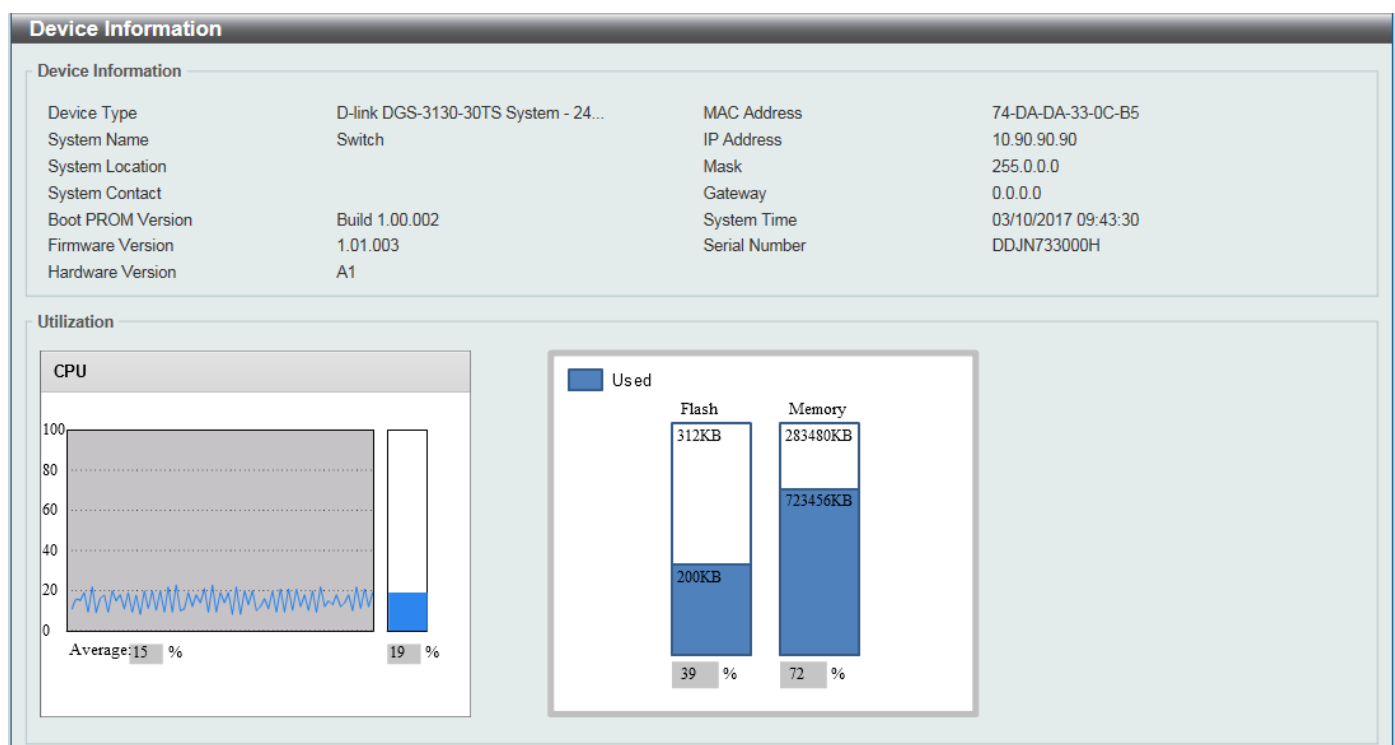


Figure 3-1 Device Information Window

System Information Settings

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

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

System Information Settings

System Information Settings

System Name: Switch

System Location: 255 chars

System Contact: 255 chars

Apply

Management Interface

Interface Name: mgmt_ipif

State: Enabled

IPv4 Address: 192 - 168 - 0 - 1

Subnet Mask: 255 - 255 - 255 - 0

Gateway: 0 - 0 - 0 - 0

Description: 64 chars

Link Status: Link Down

Apply

Figure 3-2 System Information Settings Window

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

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

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

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

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

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

Peripheral Settings

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

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

Figure 3-3 Peripheral Settings Window

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

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

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

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

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

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

Port Configuration

Port Settings

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



NOTE: The **10M** and **100M** speed options are only applicable when connecting to the **Management Port** (Mgmt 0).

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

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

Figure 3-4 Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Medium Selecting	Select the port medium type here. Options to choose from are Auto , RJ45 and SFP . Note: Selecting the SFP option, includes the use of SFP+ transceivers for 10G connectivity.
Medium Type	Select the port medium type here. Options to choose from are RJ45 and SFP . Note: Selecting the SFP option, includes the use of SFP+ transceivers for 10G connectivity.
State	Select this option to enable or disabled the physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are Auto, Normal, and Cross. <ul style="list-style-type: none"> • Auto - Select this option for auto-sensing of the optimal type of cabling. • Normal - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC NIC using a straight-through cable or a port (in the MDI mode) on another Switch through a cross-over cable. • Cross - Select this option for cross-over cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another Switch through a straight cable.
Auto Downgrade	Select to enable or disable the feature to automatically downgrade the advertised speed in the event that a link cannot be established at the available speed.
Flow Control	Select to either turn flow control On or Off here. Ports configured for full-duplex use 802.3x flow control and Auto ports use an automatic selection of the two. Note: This feature will not work through Switches that are physically stacked.
Duplex	Select the duplex mode used here. Options to choose from are Auto and Full .
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to only connect at the speed specified here.

Parameter	Description
	<p>Options to choose from are Auto, 10M, 100M, 1000M, 1000M Master, 1000M Slave, and 10G.</p> <p>The Master setting will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source.</p> <p>The Slave setting uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for master, the other side of the connection must be set for slave. Any other configuration will result in a 'link down' status for both ports.</p> <ul style="list-style-type: none"> • Auto - Specifies that for copper ports, auto-negotiation will start to negotiate the speed and flow control with its link partner. For fiber ports, auto-negotiation will start to negotiate the clock and flow control with its link partner. • 10M - Specifies to force the port speed to 10Mbps. This option is only available for 10Mbps copper connections. • 100M - Specifies to force the port speed to 100Mbps. This option is only available for 100Mbps copper connections. • 1000M - Specifies to force the port speed to 1Gbps. This option is only available for 1Gbps fiber connections. • 1000M Master - Specifies to force the port speed to 1Gbps and operates as the master, to facilitate the timing of transmit and receive operations. This option is only available for 1Gbps copper connections. • 1000M Slave - Specifies to force the port speed to 1Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. This option is only available for 1Gbps copper connections. • 10G - Specifies to force the port speed to 10Gbps. This option is only available for 10Gbps copper or fiber connections.
Capability Advertised	When the Speed is set to Auto , these capabilities are advertised during auto-negotiation.
Description	Enter a description for the corresponding port here. This can be up to 64 characters.

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

Port Status

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

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

Port Status								
Port Status								
Unit <input type="text" value="1"/>								
Unit 1 Settings								
Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	F0-7D-68-36-31-00	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
eth1/0/2	Not-Connected	F0-7D-68-36-31-01	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/3	Not-Connected	F0-7D-68-36-31-02	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/4	Not-Connected	F0-7D-68-36-31-03	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/5	Not-Connected	F0-7D-68-36-31-04	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/6	Not-Connected	F0-7D-68-36-31-05	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/7	Not-Connected	F0-7D-68-36-31-06	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/8	Not-Connected	F0-7D-68-36-31-07	1	Off	Off	Auto	Auto	1000BASE-T

Figure 3-5 Port Status Window

The fields that can be configured are described below:

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

Port GBIC

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

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

Port GBIC	
Port GBIC	
Unit <input type="text" value="1"/>	
Unit 1 Settings	
eth1/0/1	Interface Type 1000BASE-T
eth1/0/2	Interface Type 1000BASE-T
eth1/0/3	Interface Type 1000BASE-T
eth1/0/4	Interface Type 1000BASE-T
eth1/0/5	Interface Type 1000BASE-T
eth1/0/6	Interface Type 1000BASE-T
eth1/0/7	Interface Type 1000BASE-T
eth1/0/8	Interface Type 1000BASE-T

Figure 3-6 Port GBIC Window

The fields that can be configured are described below:

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

Port Auto Negotiation

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

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

Port Auto Negotiation

Port Auto Negotiation

Unit:

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

Unit 1 Settings

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

Figure 3-7 Port Auto Negotiation Window

The fields that can be configured are described below:

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

Error Disable Settings

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

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

Error Disable Settings

Error Disable Trap Settings

Asserted:

Cleared:

Notification Rate (0-1000):

Error Disable Recovery Settings

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

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

Interfaces that will be recovered at the next timeout:

Interface	VLAN	ErrDisable Cause	Time Left (sec)
-----------	------	------------------	-----------------

Figure 3-8 Error Disable Settings Window

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

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

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

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

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

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

Jumbo Frame

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

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

Jumbo Frame

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Maximum Receive Frame Size (64-12288): 1536 bytes Apply

Unit 1 Settings

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

Figure 3-9 Jumbo Frame Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Parameter	Description
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 12288 bytes. By default, this value is 1536 bytes.

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

System Log

System Log Settings

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

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

Figure 3-10 System Log Settings Window

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

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

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

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

Parameter	Description
Source Interface State	Select this option to enable or disable the global source interface state.

Parameter	Description
Type	Select the type of interface that will be used. Options to choose from are Loopback , Mgmt , and VLAN .
VID	Enter the interface VID used here. For loopback interfaces this ID can be from 1 to 8. For the management (Mgmt) interface this value is always 0. For VLAN interfaces this value is from 1 to 4094.

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

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

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

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

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

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

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

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

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

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

System Log Discriminator Settings

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

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

Name	Action	Facility List	Severity	Severity List	
Discriminato...	drop	DHCP,DHCPV6,SNMP,VRR...	drop	7	Delete

Figure 3-11 System Log Discriminator Settings Window

The fields that can be configured are described below:

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

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

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

System Log Server Settings

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

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

System Log Server Settings

Log Server

☒ Host IPv4 Address
☐ Host IPv6 Address

UDP Port (514, 1024-65535)
 Severity

Facility
 Discriminator Name

Apply

Total Entries: 5

Server IP	Severity	Facility	Discriminator Name	UDP Port	
1.1.1.1	0(Emergencies)	21	attack	1035	Delete
1.1.1.2	0(Emergencies)	21	through	1035	Delete
1.1.1.3	0(Emergencies)	21	attack	1035	Delete
2233::1	3(Errors)	21	attack	2300	Delete
2233::1	Emergencies	1	21	514	Delete

Figure 3-12 System Log Server Settings Window

The fields that can be configured are described below:

Parameter	Description		
Host IPv4 Address	Enter the system log server IPv4 address here.		
Host IPv6 Address	Enter the system log server IPv6 address here.		
UDP Port	Enter the system log server UDP port number here. This value must be either 514 or between 1024 and 65535. By default, this value is 514.		
Severity	Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) .		
Facility	Select the facility number that will be logged here. The range is from 0 to 23 . Each facility number is associated with a specific facility. See the table below:		
	Facility Number	Facility Name	Facility Description
	0	kern	Kernel messages
	1	user	User-level messages
	2	mail	Mail system
	3	daemon	System daemons
	4	auth1	Security/authorization messages
	5	syslog	Messages generated internally by the SYSLOG
	6	lpr	Line printer sub-system
	7	news	Network news sub-system
	8	uucp	UUCP sub-system
	9	clock1	Clock daemon
	10	auth2	Security/authorization messages
	11	ftp	FTP daemon
	12	ntp	NTP subsystem
	13	logaudit	Log audit
	14	logalert	Log alert
	15	clock2	Clock daemon
	16	local0	Local use 0 (local0)
17	local1	Local use 1 (local1)	

Parameter	Description		
	18	local2	Local use 2 (local2)
	19	local3	Local use 3 (local3)
	20	local4	Local use 4 (local4)
	21	local5	Local use 5 (local5)
	22	local6	Local use 6 (local6)
	23	local7	Local use 7 (local7)
Discriminator Name	Enter the name of the discriminator that will be used to filter messages sent to the log server here. This name can be up to 15 characters long.		

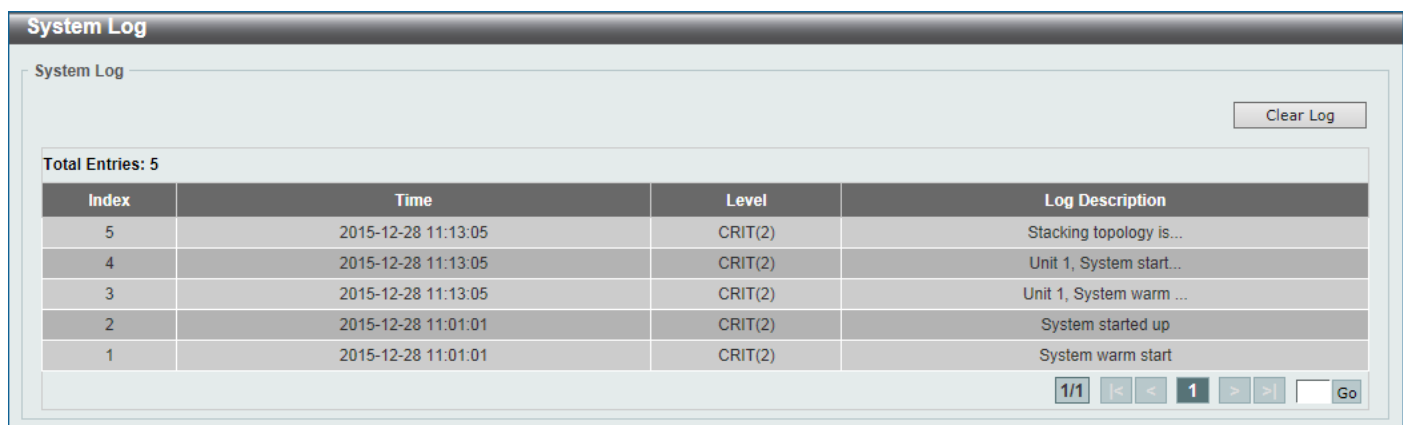
Click the **Apply** button to accept the changes made.

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

System Log

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

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



The screenshot shows the 'System Log' window. At the top right is a 'Clear Log' button. Below it, a summary bar indicates 'Total Entries: 5'. The main area contains a table with the following data:

Index	Time	Level	Log Description
5	2015-12-28 11:13:05	CRIT(2)	Stacking topology is...
4	2015-12-28 11:13:05	CRIT(2)	Unit 1, System start...
3	2015-12-28 11:13:05	CRIT(2)	Unit 1, System warm ...
2	2015-12-28 11:01:01	CRIT(2)	System started up
1	2015-12-28 11:01:01	CRIT(2)	System warm start

At the bottom right of the table, there are navigation controls: a page indicator '1/1', buttons for previous/next page, a text input field containing '1', and a 'Go' button.

Figure 3-13 System Log Window

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

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

System Attack Log

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

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



The screenshot shows the 'System Attack Log' window. At the top is a header bar with the title 'System Attack Log'. Below the header, there is a sub-header 'System Attack Log'. Underneath, there is a 'Unit' dropdown menu currently set to '1', and a 'Clear Attack Log' button to its right. Below this is a section titled 'Unit 1 Settings' which contains a 'Total Entries: 0' label. At the bottom of the window is a table with four columns: 'Index', 'Time', 'Level', and 'Log Description'.

Figure 3-14 System Attack Log Window

The fields that can be configured are described below:

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

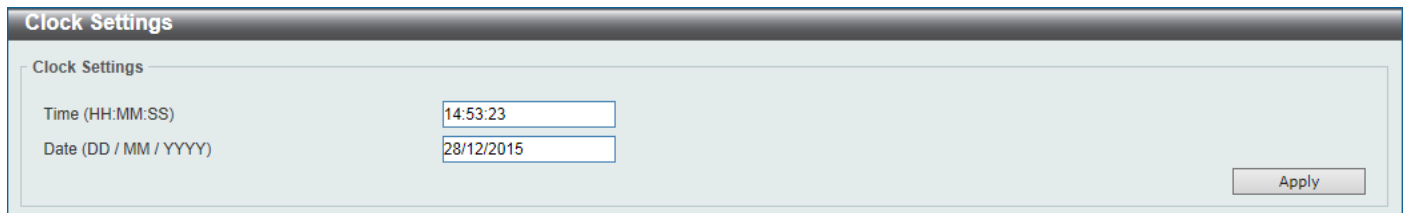
Click the **Clear Attack Log** button to clear the system attack log entries displayed in the table.

Time and SNTP

Clock Settings

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

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



The screenshot shows the 'Clock Settings' window. It has a header bar with the title 'Clock Settings'. Below the header, there is a sub-header 'Clock Settings'. Underneath, there are two input fields: 'Time (HH:MM:SS)' with the value '14:53:23' and 'Date (DD / MM / YYYY)' with the value '28/12/2015'. An 'Apply' button is located at the bottom right of the window.

Figure 3-15 Clock Settings Window

The fields that can be configured are described below:

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

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

Time Zone Settings

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

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

Time Zone Settings

Summer Time State

Disabled

Time Zone

+

0

0

Recurring Setting

From: Week of the Month

Last

From: Day of the Week

Sun

From: Month

Jan

From: Time (HH:MM)

00

00

To: Week of the Month

Last

To: Day of the Week

Sun

To: Month

Jan

To: Time (HH:MM)

00

00

Offset

60

Date Setting

From: Date of the Month

01

From: Month

Jan

From: Year

From: Time (HH:MM)

00

00

To: Date of the Month

01

To: Month

Jan

To: Year

To: Time (HH:MM)

00

00

Offset

60

Apply

Figure 3-16 Time Zone Settings Window

The fields that can be configured are described below:

Parameter	Description
Summer Time State	Select the summer time setting. Options to choose from are Disabled , Recurring Setting , and Date Setting . <ul style="list-style-type: none"> • Disabled - Select to disable the summer time setting. • Recurring Setting - Select to configure the summer time that should start and end on the specified week day of the specified month. • Date Setting - Select to configure the summer time that should start and end on the specified date of the specified month.
Time Zone	Select to specify your local time zone offset from Coordinated Universal Time (UTC).

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

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

Parameter	Description
To: Week of the Month	Select week of the month that summer time will end.
To: Day of the Week	Select the day of the week that summer time will end.
To: Month	Select the month that summer time will end.
To: Time	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

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

Parameter	Description
From: Date of the Month	Select date of the month that summer time will start.
From: Month	Select the month that summer time will start.
From: Year	Enter the year that the summer time will start.
From: Time	Select the time of the day that summer time will start.
To: Date of the Month	Select date of the month that summer time will end.
To: Month	Select the month that summer time will end.
To: Year	Enter the year that the summer time will end.
To: Time	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

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

SNTP Settings

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

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

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

Figure 3-17 SNTP Settings Window

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

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

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

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

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

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

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

Time Range

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

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

Figure 3-18 Time Range Window

The fields that can be configured are described below:

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

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

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

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

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

4. Management

[Command Logging](#)
[User Accounts Settings](#)
[Password Encryption](#)
[Password Recovery](#)
[Login Method](#)
[SNMP](#)
[RMON](#)
[Telnet/Web](#)
[Session Timeout](#)
[DHCP](#)
[DHCP Auto Configuration](#)
[DNS](#)
[IP Source Interface](#)
[File System](#)
[Stacking](#)
[SMTP Settings](#)

Command Logging

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

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

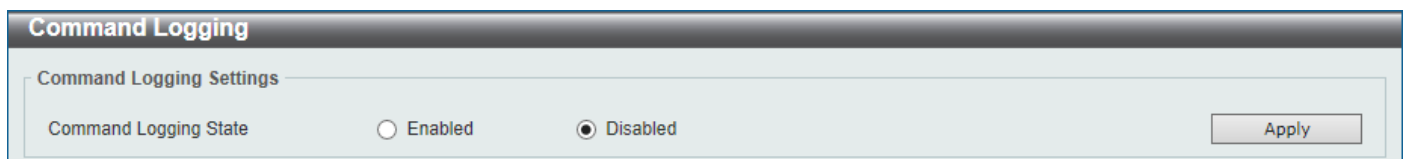


Figure 4-1 Command Logging Window

The fields that can be configured are described below:

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

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

User Accounts Settings

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

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



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

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

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

Figure 4-2 User Accounts Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.
Privilege	Enter the privilege level for this account here. The range is from 1 to 15.
Password Type	Select the password type for this user account here. Options to choose from are None , Plain Text , Encrypted-SHA1 , and Encrypted-MD5 .
Password	After selecting Plain Text , Encrypted-SHA1 , or Encrypted-MD5 as the password type, enter the password for this user account here.

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

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

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

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

Figure 4-3 Session Table Window

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

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

Password Encryption

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

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

Figure 4-4 Password Encryption Window

The fields that can be configured are described below:

Parameter	Description
Password Encryption State	Select this option to enable or disable the encryption of the password before being stored in the configuration file.
Password Type	When the state is enabled, select the password encryption type here. Options to choose from are: <ul style="list-style-type: none"> Encrypted-SHA1 - Specifies that the password is encrypted using SHA-1. Encrypted-MD5 - Specifies that the password is encrypted using MD5.

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

Password Recovery

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

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

Figure 4-5 Password Recovery Window

The fields that can be configured are described below:

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

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

Login Method

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

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

Login Method

Enable Password

Level: 15 Password Type: Plain Text Password: 32 chars Apply

Login Method

Application	Login Method	
Console	No Login	Edit
Telnet	Login	Edit
SSH	Login	Edit

Login Password

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

Application	Password	
SSH	*****	Delete

Figure 4-6 Login Method Window

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

Parameter	Description
Level	Select the privilege level for the user here. The range is from 1 to 15.
Password Type	Select the password type for the user here. Options to choose from are: <ul style="list-style-type: none"> • Plain Text - Specifies that the password will be in plain text. This is the default option. • Encrypted - Specifies that the password will be encrypted based on SHA-1. • Encrypted-MD5 - Specifies that the password will be encrypted based on MD5.
Password	Enter the password for the user account here. In the plain-text form, the password can be up to 32 characters long, is case-sensitive, and can contain spaces. In the encrypted form, the password must be 35 bytes long and is case-sensitive. In the encrypted MD5 form, the password must be 31 bytes long and is case-sensitive.

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

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

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

Parameter	Description
Login Method	After clicking the Edit button, this parameter can be configured. Select the login method for the specified application here. Options to choose from are No Login , Login and Login Local . <ul style="list-style-type: none"> • No Login requires no login authentication to access the specified application. • Login will require the user to at least enter a password when trying to access the application specified. • Login Local requires the user to enter a username and a password to access the specified application.

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

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

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

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

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

SNMP

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

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

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

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

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

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

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

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

MIBs

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

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

Traps

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

SNMP Global Settings

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

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

Figure 4-7 SNMP Global Settings Window

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

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

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

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

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

SNMP Linkchange Trap Settings

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

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

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

Figure 4-8 SNMP Linkchange Trap Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Trap Sending	Select this option to enable or disable the sending of the SNMP notification traps that are generated by the system.
Trap State	Select this option to enable or disable the SNMP <i>linkChange</i> trap.

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

SNMP View Table Settings

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

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

SNMP View Table Settings

SNMP View Settings

View Name *

Subtree OID *

View Type

* Mandatory Field Add

Total Entries: 8

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

Figure 4-9 SNMP View Table Settings Window

The fields that can be configured are described below:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) sub-tree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select the view type here. Options to choose from are Included and Excluded . <ul style="list-style-type: none"> Included - Select to include this object in the list of objects that an SNMP manager can access. Excluded - Select to exclude this object from the list of objects that an SNMP manager can access.

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

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

SNMP Community Table Settings

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

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

- Read-write or read-only level permissions for the MIB objects accessible to the SNMP community.

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

The screenshot shows the 'SNMP Community Table Settings' window. It has a header bar with the title. Below it, the 'SNMP Community Settings' section contains five fields: 'Key Type' (a dropdown menu set to 'Plain Text'), 'Community Name' (a text box with '32 chars' placeholder), 'View Name' (a text box with '32 chars' placeholder), 'Access Right' (a dropdown menu set to 'Read Only'), and 'IP Access-List Name' (a text box with '32 chars' placeholder). An 'Add' button is located to the right of these fields. Below the form is a section titled 'Total Entries: 2' containing a table with two rows of existing entries. Each row has a 'Delete' button to its right.

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

Figure 4-10 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Key Type	Select the key type for the SNMP community. Options to choose from are Plain Text , and Encrypted .
Community Name	Enter an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Enter an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	Select the access right here. Options to choose from are Read Only and Read Write . <ul style="list-style-type: none"> • Read Only - SNMP community members using the community string created can only read the contents of the MIBs on the Switch. • Read Write - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.
IP Access-List Name	Enter the name of the standard access list to restrict the users that can use this community string to access to the SNMP agent.

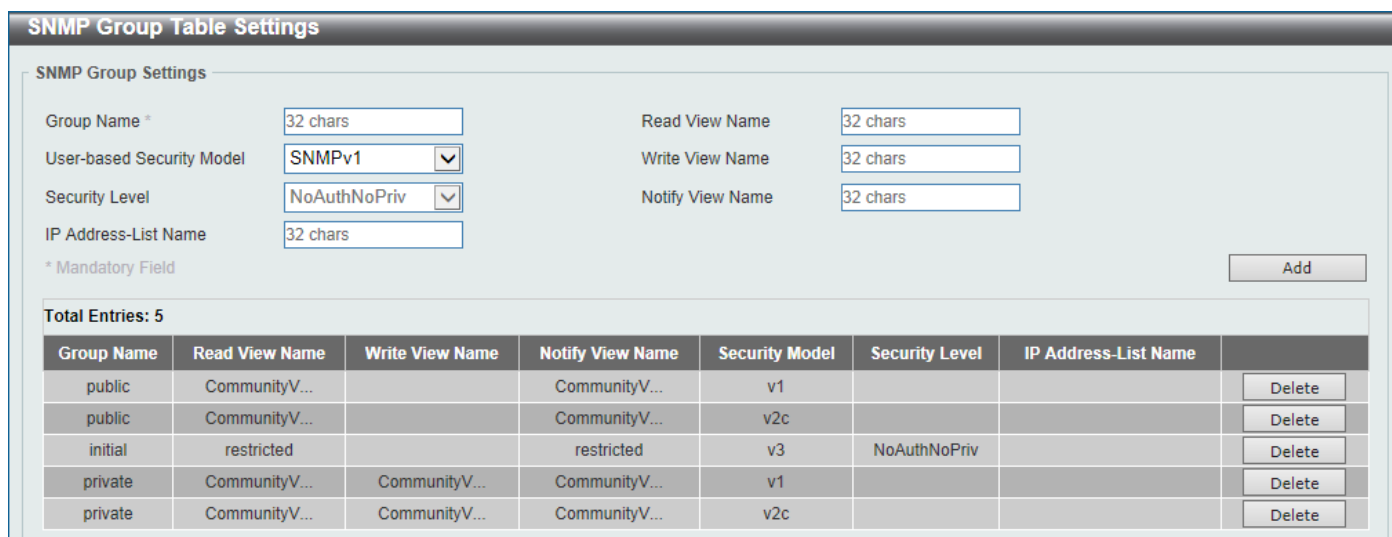
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Group Table Settings

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

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



SNMP Group Table Settings

SNMP Group Settings

Group Name * Read View Name

User-based Security Model Write View Name

Security Level Notify View Name

IP Address-List Name

* Mandatory Field Add

Total Entries: 5

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

Figure 4-11 SNMP Group Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the SNMP group name here. This name can be up to 32 characters long. Spaces are not allowed.
Read View Name	Enter the read view name that users of the group can access.
User-based Security Model	<p>Select the security model here. Options to choose from are SNMPv1, SNMPv2c, and SNMPv3.</p> <ul style="list-style-type: none"> • SNMPv1 - Select to allow the group to use the SNMPv1 security model. • SNMPv2c - Select to allow the group to use the SNMPv2c security model. • SNMPv3 - Select to allow the group to use the SNMPv3 security model.
Write View Name	Enter the write view name that the users of the group can access.
Security Level	<p>When selecting SNMPv3 in the User-based Security Model drop-down list, this option is available.</p> <ul style="list-style-type: none"> • NoAuthNoPriv - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • AuthNoPriv - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • AuthPriv - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
Notify View Name	Enter the notify view name that users of the group can access. The notify view describes the object that can be reported its status via trap packets to the group user.
IP Address-List Name	Enter the standard IP access control list (ACL) to associate with the group.

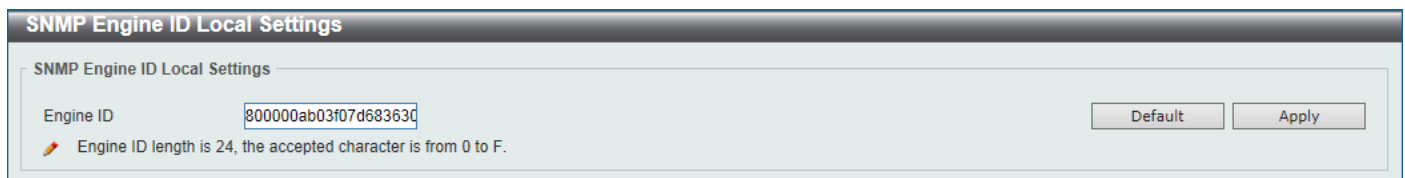
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Engine ID Local Settings

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

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



The window titled "SNMP Engine ID Local Settings" contains a section "SNMP Engine ID Local Settings". Inside this section, there is a label "Engine ID" followed by a text input field containing the value "800000ab03f07d683630". To the right of the input field are two buttons: "Default" and "Apply". Below the input field, a note states: "Engine ID length is 24, the accepted character is from 0 to F."

Figure 4-12 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

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

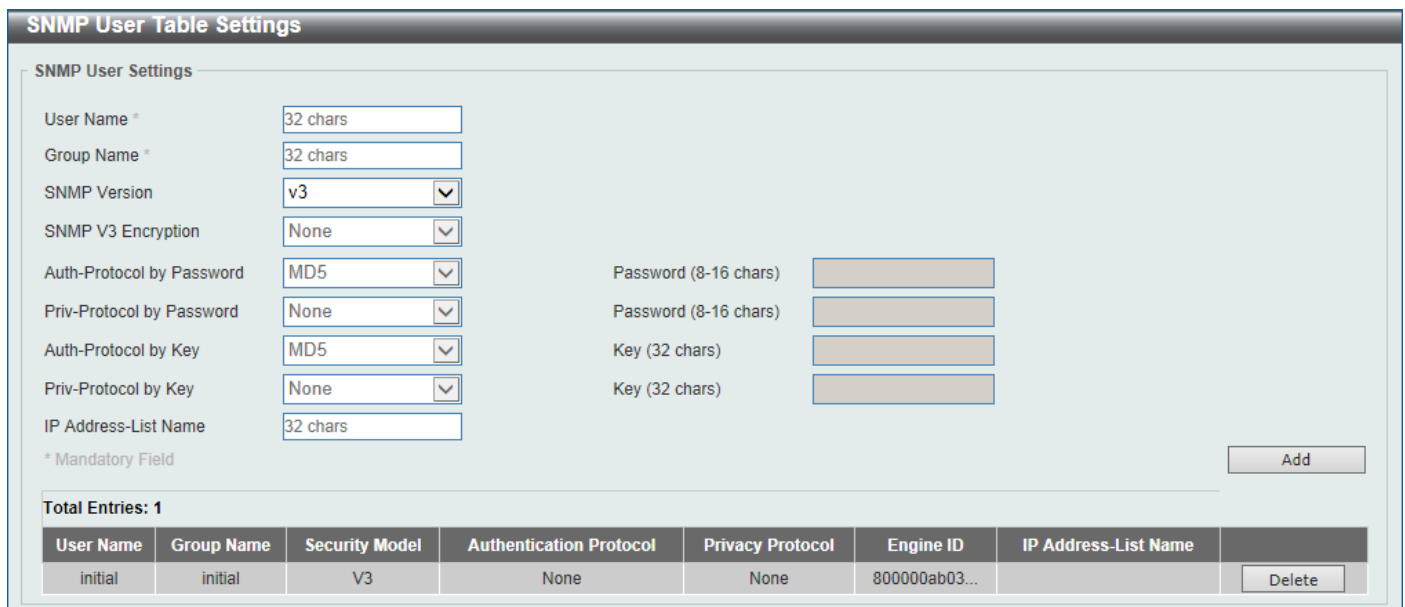
Click the **Default** button to revert the engine ID to the default.

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

SNMP User Table Settings

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

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



The window titled "SNMP User Table Settings" contains a section "SNMP User Settings". Inside this section, there are several configuration fields:

- User Name *: 32 chars
- Group Name *: 32 chars
- SNMP Version: v3 (dropdown)
- SNMP V3 Encryption: None (dropdown)
- Auth-Protocol by Password: MD5 (dropdown)
- Priv-Protocol by Password: None (dropdown)
- Auth-Protocol by Key: MD5 (dropdown)
- Priv-Protocol by Key: None (dropdown)
- IP Address-List Name: 32 chars

 To the right of these fields, there are four password/key input fields, each labeled "Password (8-16 chars)" or "Key (32 chars)". At the bottom right of the settings section is an "Add" button. Below the settings section, it says "Total Entries: 1". At the bottom of the window is a table with the following data:

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

Figure 4-13 SNMP User Table Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter SNMP user name here. This name can be up to 32 characters long. This is used to identify the SNMP user.
Group Name	Enter the SNMP group name to which the user belongs. This name can be up to 32 characters long. Spaces are not allowed.
SNMP Version	Select the SNMP version. Options to choose from are v1 , v2c , and v3 .
SNMP V3 Encryption	When selecting v3 in the SNMP Version drop-down list, this option is available. Options to choose from are None , Password , and Key .

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

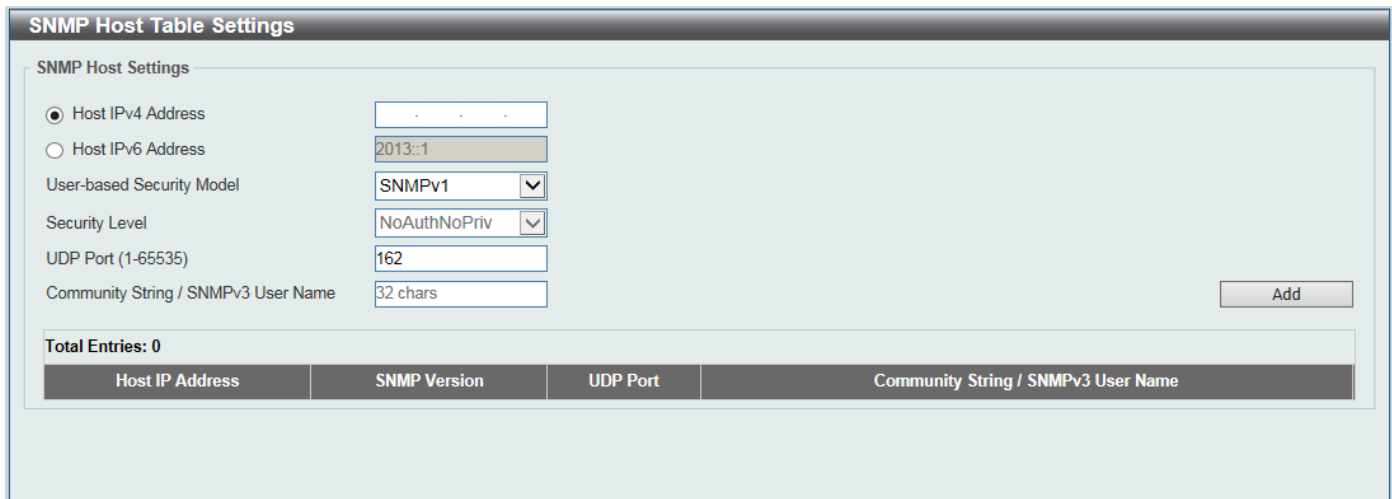
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Host Table Settings

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

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



The image shows the 'SNMP Host Table Settings' window. It has a title bar and a main content area. The content area is divided into two sections. The top section, 'SNMP Host Settings', contains several configuration fields: 'Host IPv4 Address' (radio button), 'Host IPv6 Address' (radio button), 'User-based Security Model' (dropdown menu), 'Security Level' (dropdown menu), 'UDP Port (1-65535)' (text input), and 'Community String / SNMPv3 User Name' (text input). Below these fields is an 'Add' button. The bottom section, 'Total Entries: 0', contains a table with four columns: 'Host IP Address', 'SNMP Version', 'UDP Port', and 'Community String / SNMPv3 User Name'.

Figure 4-14 SNMP Host Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	<p>Select the security model here. Options to choose from are SNMPv1, SNMPv2c, and SNMPv3.</p> <ul style="list-style-type: none"> • SNMPv1 - Select to allow the group user to use the SNMPv1 security model. • SNMPv2c - Select to allow the group user to use the SNMPv2c security model. • SNMPv3 - Select to allow the group user to use the SNMPv3 security model.
Security Level	<p>When selecting SNMPv3 in the User-based Security Model drop-down list, this option is available.</p> <ul style="list-style-type: none"> • NoAuthNoPriv - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • AuthNoPriv - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • AuthPriv - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
UDP Port	Enter the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string to be sent with the notification packet.

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

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

RMON

RMON Global Settings

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

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

Figure 4-15 RMON Global Settings Window

The fields that can be configured are described below:

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

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

RMON Statistics Settings

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

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

Figure 4-16 RMON Statistics Settings Window

The fields that can be configured are described below:

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

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

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

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

RMON Statistics Table																		
RMON Statistics Table																		
Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
1	eth1/0/1	1245946	8212	364	211	0	0	0	0	0	0	0	5763	585	0	1646	218	0

Back

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

This window is used to display and configure RMON MIB history statistics gathered on the specified port. To view the following window, click **Management > RMON > RMON History Settings**, as shown below:

RMON History Settings

RMON History Settings

Unit * Port * Index (1-65535) * Bucket Number (1-65535) Interval (1-3600) sec Owner

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	
1	eth1/0/1	50	50	1800		<input type="button" value="Delete"/> <input type="button" value="Show Detail"/>

The fields that can be configured are described below:

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

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

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

RMON History Table

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

Back

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

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

RMON Alarm Settings

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

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

RMON Alarm Settings

RMON Alarm Settings

Index (1-65535) * Interval (1-2147483647) * sec

Variable * N.N.N...N Type Absolute

Rising Threshold (0-2147483647) * Falling Threshold (0-2147483647) *

Rising Event Number (1-65535) Falling Event Number (1-65535)

Owner 1-127 chars

Total Entries: 0

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

Figure 4-20 RMON Alarm Settings Window

The fields that can be configured are described below:

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

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

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

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

RMON Event Settings

This window is used to display and configure event entries.

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

RMON Event Settings

RMON Event Settings

Index (1-65535) *

Description

Type ▼

Community

Owner

Total Entries: 1

Index	Description	Community	Event Trigger	Owner	Last Trigger Time	
1	description	community		owner	0d:0h:0m:0s	<input type="button" value="Delete"/> <input type="button" value="View Logs"/>

1/1 < < 1 > >

Figure 4-21 RMON Event Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

Event Logs Table

Event Logs Table

Event Index: 1

Total Entries: 0

Log Index	Log Time	Log Description
-----------	----------	-----------------

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

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

Telnet/Web

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

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

Figure 4-23 Telnet/Web Window

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

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

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

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

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

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

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

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

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

Session Timeout

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

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

Session Timeout			
Session Timeout			
Web Session Timeout (60-36000)	180	sec	<input checked="" type="checkbox"/> Default
Console Session Timeout (0-1439)	3	min	<input checked="" type="checkbox"/> Default
Telnet Session Timeout (0-1439)	3	min	<input checked="" type="checkbox"/> Default
SSH Session Timeout (0-1439)	3	min	<input checked="" type="checkbox"/> Default
			Apply

Figure 4-24 Session Timeout Window

The fields that can be configured are described below:

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

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

DHCP

Service DHCP

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

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

Service DHCP	
Service DHCP	
Service DHCP State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Apply	
Service IPv6 DHCP	
Service IPv6 DHCP State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Apply	

Figure 4-25 Service DHCP Window

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

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

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

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

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

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

DHCP Class Settings

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

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

Figure 4-26 DHCP Class Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

Figure 4-27 DHCP Class Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Option	Enter the DHCP option number. The range is from 1 to 255.
Hex	Enter the hex pattern of the specified DHCP option. Tick the * check box not to match the remaining bits of the option.
Bitmask	Enter the hex bit mask for masking of the pattern. The masked pattern bits will be matched. If not specified, all bits entered in the Hex field will be checked.

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

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

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

DHCP Server

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

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

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

DHCP Server Global Settings

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

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

Figure 4-28 DHCP Server Global Settings Window

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

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

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

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

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

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

DHCP Server Pool Settings

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

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

Figure 4-29 DHCP Server Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

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

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

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

The fields that can be configured are described below:

Parameter	Description
Class Name	Select an existing DHCP class name here that will be associated with this DHCP pool.
Start Address	Enter the starting IPv4 address that will be associated with the DHCP class in the DHCP pool here.
End Address	Enter the ending IPv4 address that will be associated with the DHCP class in the DHCP pool here.

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

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

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

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

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

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

The fields that can be configured are described below:

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

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

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

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

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

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

The fields that can be configured are described below:

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

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

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

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

DHCP Server Exclude Address

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

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

Begin Address	End Address

Figure 4-33 DHCP Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
VRF Name	Enter the name of the VRF instance here. This name can be up to 12 characters long.
Begin Address	Enter the first IPv4 address of a range of addresses to be excluded here.
End Address	Enter the last IPv4 address of a range of addresses to be excluded here.

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

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

DHCP Server Manual Binding

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

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

Pool Name	Host	Mask	Hardware Address	Client Identifier	
pool	192.168.70.220	255.55.55.0	00-11-22-33-44-55	-	Delete

Figure 4-34 DHCP Server Manual Binding Window

The fields that can be configured are described below:

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

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

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

DHCP Server Dynamic Binding

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

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

IP Address	Client-ID/Hardware Address	Lease Expiration	Type
192.168.1.2	0100b7443dc224	Oct 23 2009 09:12 AM	Automatic
192.168.1.3	0100b810863213	Oct 23 2009 09:12 AM	Automatic
10.1.9.10	0100b810863213	Oct 23 2009 09:12 AM	Automatic
10.1.1.1	0100b810863213	Oct 23 2009 09:12 AM	Automatic
10.1.9.1	0100b810863213	Oct 23 2009 09:12 AM	Automatic
10.1.9.10	0100b810863213	Oct 23 2009 09:12 AM	Automatic
10.1.1.1	0100b810863213	Oct 23 2009 09:12 AM	Automatic
10.1.9.1	0100b810863213	Oct 23 2009 09:12 AM	Automatic

Figure 4-35 DHCP Server Dynamic Binding Window

The fields that can be configured are described below:

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

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

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

DHCP Server IP Conflict

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

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

DHCP Server IP Conflict

DHCP Server IP Conflict

IP Address

Pool Name ☒ All

IP Address

Total Entries: 7

IP Address	Detection Method	Detection Time
192.168.12.1	Ping	Oct 21 2009 09:13 PM
192.168.12.2	Ping	Oct 22 2009 09:14 AM
192.168.12.3	Ping	Oct 23 2009 09:15 AM
192.168.12.4	Ping	Oct 24 2009 09:16 AM
192.168.12.5	Ping	Oct 25 2009 19:12 AM
192.168.12.6	Ping	Oct 26 2009 19:12 AM
192.168.12.110	Ping	Oct 27 2009 09:22 AM

1/1 < < 1 > >

Figure 4-36 DHCP Server IP Conflict Window

The fields that can be configured are described below:

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

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

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

DHCP Server Statistic

This window is used to display DHCP server statistics.

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

DHCP Server Statistic	
<input type="button" value="Clear"/>	
DHCP Server Statistic	
Address Pools	1
Automatic bindings	0
Manual binding	1
Malformed messages	0
Renew messages	0
Message Received	
BOOTREQUEST	0
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Message Sent	
BOOTREPLY	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

Figure 4-37 DHCP Server Statistic Window

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

DHCPv6 Server

DHCPv6 Server Pool Settings

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

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

DHCPv6 Server Pool Settings	
DHCPv6 Server Pool	
Pool Name <input type="text" value="12 chars"/>	<input type="button" value="Apply"/>
Total Entries: 1	
Pool Name	
Pool	<input type="button" value="Configure"/> <input type="button" value="Delete"/>
1/1 < < 1 > > <input type="button" value="Go"/>	

Figure 4-38 DHCPv6 Server Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

DHCPv6 Server Pool Configure

DHCPv6 Server Pool Configure

Pool Name
☐ Address Prefix
☒ Prefix Delegation Pool

Pool
 2001:0DB8::0/64
 12 chars

Valid Lifetime (60-4294967295) [] sec
 Preferred Lifetime (60-4294967295) [] sec

DNS Server [2013::1]
 DNS Server [2013::1]
 Domain Name []

Static Bindings

☒ Static Bindings Address [2001:0DB8::0]
☐ Static Bindings Prefix [2001:0DB8::0/64]

Client DUID [28 chars]
 IAID []

Valid Lifetime (60-4294967295) [2592000] sec
 Preferred Lifetime (60-4294967295) [604800] sec

Total Entries: 0

Apply Back Apply

Figure 4-39 DHCPv6 Server Pool Settings (Configure) Window

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

Parameter	Description
Address Prefix	Select and enter the DHCPv6 server pool IPv6 network address and prefix length here. For example, 2015::0/64.
Prefix Delegation Pool	Select and enter the DHCPv6 server pool prefix delegation name here. This name can be up to 12 characters long.
Valid Lifetime	Enter the valid lifetime value here. The range is from 60 to 4294967295 seconds. The valid lifetime should be greater than preferred lifetime. If this value is not specified, then the default valid lifetime will be 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. If this value is not specified, then the default preferred lifetime will be 604800 seconds (7 days).
DNS Server	Enter the DNS server IPv6 address to be assigned to requesting DHCPv6 clients here.
Domain Name	Enter the domain name to be assigned to requesting DHCPv6 clients here.

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

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

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

Parameter	Description
Static Bindings Address	Enter the static binding IPv6 address assign to the specific client here.
Static Bindings Prefix	Enter the static binding IPv6 network address and prefix length here.
Client DUID	Enter the client DHCP Unique Identifier (DUID) here. This string can be up to 28 characters long.

Parameter	Description
IAID	Enter the Identity Association Identifier (IAID) here. The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client.
Valid Lifetime	Enter the valid lifetime value here. The valid lifetime should be greater than the preferred lifetime. The range is from 60 to 4294967295 seconds. By default, this value is 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. By default, this value is 604800 seconds (7 days).

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

DHCPv6 Server Local Pool Settings

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

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

Figure 4-40 DHCPv6 Server Local Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

DHCPv6 Server Exclude Address

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

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

DHCPv6 Server Exclude Address

DHCPv6 Server Exclude Address

Low IPv6 Address: 2013::1

High IPv6 Address: 2013::1

Apply

Total Entries: 1

Range	Low IPv6 Address	High IPv6 Address	
1	2015::12	2015::15	Delete

Figure 4-41 DHCPv6 Server Exclude Address Window

The fields that can be configured are described below:

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

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

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

DHCPv6 Server Binding

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

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

DHCPv6 Server Binding

DHCPv6 Server Binding

IPv6 Address: 2013::1 ☐ All

Find Clear

Total Entries: 0

Client DUID	IPv6 Address	Preferred Lifetime	Valid Lifetime
-------------	--------------	--------------------	----------------

Figure 4-42 DHCPv6 Server Binding Window

The fields that can be configured are described below:

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

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

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

DHCPv6 Server Interface Settings

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

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

Figure 4-43 DHCPv6 Server Interface Settings Window

The fields that can be configured are described below:

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

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

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

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

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

DHCPv6 Server Operational Information

This window is used to display the DHCPv6 server operational information.

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

Figure 4-44 DHCPv6 Server Operational Information Window

DHCP Relay

DHCP Relay Global Settings

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

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

Figure 4-45 DHCP Relay Global Settings Window

The fields that can be configured are described below:

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

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

DHCP Relay Pool Settings

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

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

Figure 4-46 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

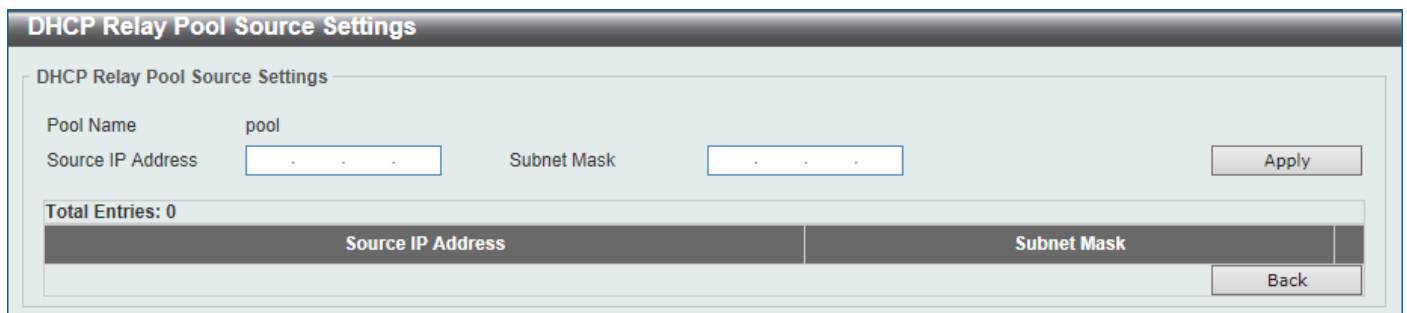
Click the **Apply** button to accept the changes made.

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

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

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

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



DHCP Relay Pool Source Settings

DHCP Relay Pool Source Settings

Pool Name: pool

Source IP Address: Subnet Mask:

Apply

Total Entries: 0

Source IP Address	Subnet Mask

Back

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

The fields that can be configured are described below:

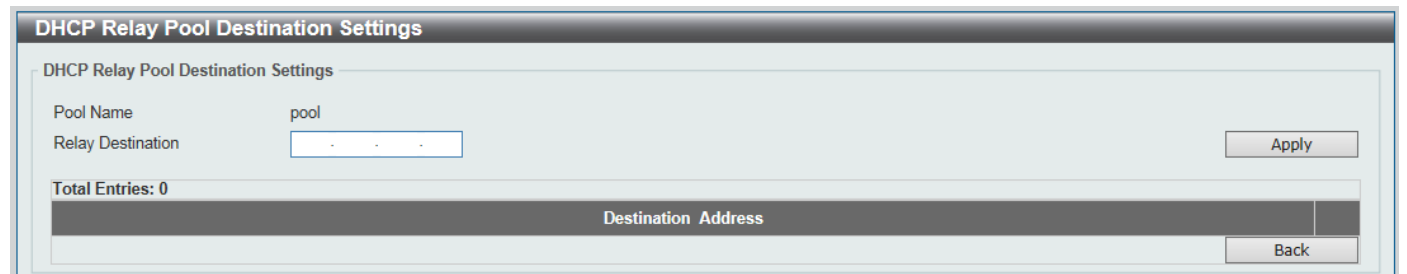
Parameter	Description
Source IP Address	Enter the source subnet of client packets.
Subnet Mask	Enter the network mask of the source subnet.

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

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

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

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



DHCP Relay Pool Destination Settings

DHCP Relay Pool Destination Settings

Pool Name: pool

Relay Destination:

Apply

Total Entries: 0

Destination Address

Back

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

The fields that can be configured are described below:

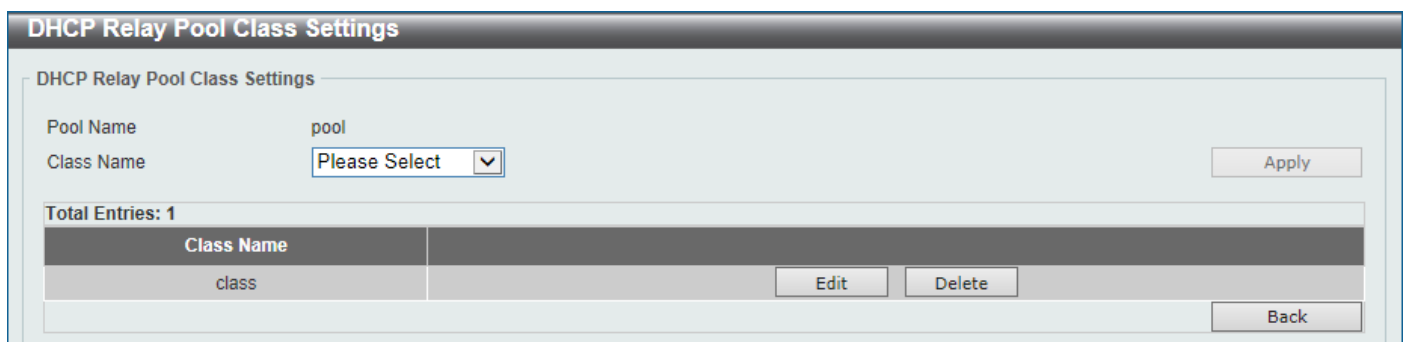
Parameter	Description
Relay Destination	Enter the relay destination DHCP server IP address.

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

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

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

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



DHCP Relay Pool Class Settings

DHCP Relay Pool Class Settings

Pool Name: pool

Class Name:

Apply

Total Entries: 1

Class Name	
class	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Back

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

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

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

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

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

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

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

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

The fields that can be configured are described below:

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

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

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

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

DHCP Relay Information Settings

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

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

Figure 4-51 DHCP Relay Information Settings Window

The fields that can be configured are described below:

Parameter	Description
Information Trust All	Select this option to enable or disable the DHCP relay agent to trust the IP DHCP relay information for all interfaces.
information Check	Select this option to enable or disable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet.
Information Policy	Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are Keep , Drop , and Replace . <ul style="list-style-type: none"> • Keep - Select to keep the packet that already has the relay option. The packet is left unchanged and directly relayed to the DHCP server. • Drop - Select to discard the packet that already has the relay option. • Replace - Select to replace the packet that already has the relay option. The packet will be replaced with a new option.
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets.

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

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

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

DHCP Relay Information Option Format Settings

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

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

Figure 4-52 DHCP Relay Information Option Format Settings Window

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

Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are Default , User Define , and Vendor2 . <ul style="list-style-type: none"> • Default - Select to use the Switch's system MAC address as the remote ID.

Parameter	Description
	<ul style="list-style-type: none"> • 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	<p>Select the DHCP information circuit ID sub-option. Options to choose from are Default, User Define, and Vendor1.</p> <ul style="list-style-type: none"> • Default - Select to use the default circuit ID sub-option. • User Define - Select to use a user-defined circuit ID. Enter the user-defined string with the maximum of 32 characters in the text box. • Vendor1 - Select to use vendor 1 as the circuit ID. • Expert UDF - Select to use the expert UDF circuit ID. Select the stand-alone unit format after this selection here.

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

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

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

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

DHCP Relay Information Profile Settings

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

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

DHCP Relay Information Profile Settings

DHCP Relay Information Option MAC Format

Case: Uppercase

Delimiter: None

Delimiter Number: 2

Example: AABBCCDDEEFF

Apply

DHCP Relay Information Profile Settings

Profile Name: 32 chars

Apply Find

Total Entries: 1

Profile Name	Format String
profile	

Edit Delete

1/1 < > 1 > > Go

Figure 4-53 DHCP Relay Information Profile Settings Window

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

Parameter	Description
Case	<p>Select the case that will be used here. Options to choose from are:</p> <ul style="list-style-type: none"> • Lowercase - Specifies that when using the lowercase format, the Option 82 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff. • Uppercase - Specifies that when using the uppercase format, the Option 82 MAC address for the user-defined profile username will be formatted as: AA-BB-CC-DD-EE-FF.
Delimiter	<p>Select the delimiter that will be used here. Options to choose from are:</p> <ul style="list-style-type: none"> • Hyphen - Specifies that the format will be AA-BB-CC-DD-EE-FF. • Colon - Specifies that the format will be AA:BB:CC:DD:EE:FF. • Dot - Specifies that the format will be AA.BB.CC.DD.EE.FF. • None - Specifies that when not using any delimiter, the format will be AABBCCDDEEFF.
Delimiter Number	<p>Select the delimiter number here. Options to choose from are:</p> <ul style="list-style-type: none"> • 1 - Single delimiter, the format is: AABBCC.DDEEFF. • 2 - Double delimiters, the format is: AABB.CCDD.EEFF. • 5 - Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF.

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

The fields that can be configured in **DHCP Relay Information Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the Option 82 profile name here. The profile can be used to define the flexible, user-defined Option 82 entry.
Format String	<p>After clicking the Edit button, enter the user-defined DHCP Option 82 format string here. This string can be up to 251 characters long.</p> <p>The following rules need to be considered:</p> <ul style="list-style-type: none"> • This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks (""), like "Ethernet". Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "%" + "\$" + "1~32" + "keyword" + ":". <ul style="list-style-type: none"> ○ % - Indicates that the string that follows this character is a formatted key string. ○ "\$" or "0" - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either "\$" or "0", and cannot be specified as both at the same time. <ul style="list-style-type: none"> ▪ "\$" - Indicates to fill the leading space (0x20). ▪ "0" - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting. ○ 1~32 - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the

Parameter	Description
	<p>actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly.</p> <ul style="list-style-type: none"> ○ keyword - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: <ul style="list-style-type: none"> ▪ devtype - The model name of the device. Only an ASCII string is allowed. ▪ sysname - Indicates the System name of the Switch. Only an ASCII string is allowed. ▪ ifdescr - Derived from <i>ifDescr</i> (IF-MIB). Only an ASCII string is allowed. ▪ portmac - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands. When in the format of a hexadecimal value, the MAC address will be encapsulated in order in hexadecimal. ▪ sysmac - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal. ▪ unit - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0. ▪ module - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value. ▪ port - Indicates the local port number. This can be either an ASCII string or a hexadecimal value. ▪ svlan - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. ▪ cvlan - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value. ○ : - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#\$%^&*()_+ =\\[]{};"/?.,<>`, and space characters. "\\" is the escape character. The special character after "\\" is the character itself, for example, "\\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

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

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

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

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

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:

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

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

Figure 4-54 DHCP Relay Port Settings Window

The fields that can be configured are described below:

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

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

DHCP Local Relay VLAN

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

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

Figure 4-55 DHCP Local Relay VLAN Window

The fields that can be configured are described below:

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

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



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

DHCPv6 Relay

DHCPv6 Relay Global Settings

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

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

DHCPv6 Relay Global Settings

DHCPv6 Relay Remote ID Settings

IPv6 DHCP Relay Remote ID Format: Expert UDF

IPv6 DHCP Relay Remote ID UDF: ASCII (128 chars)

IPv6 DHCP Relay Remote ID Policy: Keep

IPv6 DHCP Relay Remote ID Option: Disabled

DHCPv6 Relay Interface ID Settings

IPv6 DHCP Relay Interface ID Format: Expert UDF

IPv6 DHCP Relay Interface ID Policy: Keep

IPv6 DHCP Relay Interface ID Option: Enabled

DHCPv6 Relay Information Option MAC Format

Case: Uppercase

Delimiter: None

Delimiter Number: 1

Example: AABCCDDEEFF

Figure 4-56 DHCPv6 Relay Global Settings Window

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

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are Default , CID with User Define , User Define , and Expert UDF .
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 . <ul style="list-style-type: none"> 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 . <ul style="list-style-type: none"> 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.

Parameter	Description
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.

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

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

Parameter	Description
IPv6 DHCP Relay Interface ID Format	Select the IPv6 DHCP relay interface ID format that will be used here. Options to choose from are Default , CID , Vendor1 , and Expert UDF .
IPv6 DHCP Relay Interface ID Policy	Select the Option 18 re-forwarding policy for the DHCPv6 relay agent here. Options to choose from are: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 1 - Specifies to use a single delimiter. For example: AABBCC.DDEEFF. • 2 - Specifies to use two delimiters. For example: AABB.CCDD.EEFF • 5 - Specifies to use multiple delimiters. For example: AA.BB.CC.DD.EE.FF

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

DHCPv6 Relay Interface Settings

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

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

Figure 4-57 DHCPv6 Relay Interface Settings Window

The fields that can be configured are described below:

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

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

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

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

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

DHCPv6 Relay Remote ID Profile Settings

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

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

Figure 4-58 DHCPv6 Relay Remote ID Profile Settings Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the profile name here. This string can be up to 32 characters long.
Format String	<p>After clicking the Edit button, enter the Option 82 format string here. This string can be up to 251 characters long.</p> <p>The following rules need to be considered:</p> <ul style="list-style-type: none"> This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks ("") like "Ethernet". Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "% " + "\$ " + "1~32" + "keyword" + ":" : <ul style="list-style-type: none"> % - Indicates that the string that follows this character is a formatted key string. "\$ " or "0 " - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either "\$ " or "0 ", and cannot be specified as both at the same time. <ul style="list-style-type: none"> "\$ " - Indicates to fill the leading space (0x20). "0 " - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting. 1~32 - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. keyword - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: <ul style="list-style-type: none"> devtype - The model name of the device. Only an ASCII string is allowed. sysname - Indicates the System name of the Switch. Only an ASCII string is allowed. ifdescr - Derived from ifDescr (IF-MIB). Only an ASCII string is allowed. portmac - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands. When in the format of a hexadecimal value, the MAC address will be encapsulated in order in hexadecimal. sysmac - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal. unit - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0. module - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value.

Parameter	Description
	<ul style="list-style-type: none"> ▪ port - Indicates the local port number. This can be either an ASCII string or a hexadecimal value. ▪ svlan - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. ▪ cvlan - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value. ○ : - Indicates the end of the formatted key string. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#\$%^&*()_+ =\\[]{};"/?.,<>', and space characters. "\\" is the escape character. The special character after "\\" is the character itself, for example, "\\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

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

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

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

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

DHCPv6 Relay Interface ID Profile Settings

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

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

Figure 4-59 DHCPv6 Relay Interface ID Profile Settings Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the profile name here. This string can be up to 32 characters long.
Format String	<p>After clicking the Edit button, enter the Option 82 format string here. This string can be up to 251 characters long.</p> <p>The following rules need to be considered:</p> <ul style="list-style-type: none"> • This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string

Parameter	Description
	<p>needs to be enclosed with quotation marks (") like "Ethernet". Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values.</p> <ul style="list-style-type: none"> • A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "%" + "\$" + "1~32" + "keyword" + ":": <ul style="list-style-type: none"> ○ % - Indicates that the string that follows this character is a formatted key string. ○ "\$" or "0" - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either "\$" or "0", and cannot be specified as both at the same time. <ul style="list-style-type: none"> ▪ "\$" - Indicates to fill the leading space (0x20). ▪ "0" - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting. ○ 1~32 - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. ○ keyword - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: <ul style="list-style-type: none"> ▪ devtype - The model name of the device. Only an ASCII string is allowed. ▪ sysname - Indicates the System name of the Switch. Only an ASCII string is allowed. ▪ ifdescr - Derived from <i>ifDescr</i> (IF-MIB). Only an ASCII string is allowed. ▪ portmac - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands. When in the format of a hexadecimal value, the MAC address will be encapsulated in order in hexadecimal. ▪ sysmac - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal. ▪ unit - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0. ▪ module - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value. ▪ port - Indicates the local port number. This can be either an ASCII string or a hexadecimal value. ▪ svlan - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. ▪ cvlan - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value.

Parameter	Description
	<ul style="list-style-type: none"> ○ : - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#\$%^&*()_+ =\\[]{};:'"/?.,<>`, and space characters. "\\" is the escape character. The special character after "\" is the character itself, for example, "\\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

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

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

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

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

DHCPv6 Relay Format Type Settings

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

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

Figure 4-60 DHCPv6 Relay Format Type Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Type	Select the type here. Options to choose from are: <ul style="list-style-type: none"> • Remote ID - Specifies to configure the Expert UDF format type string for DHCPv6 Option 37.

Parameter	Description
	<ul style="list-style-type: none"> Interface ID - Specifies to configure the Expert UDF format type string for DHCPv6 Option 18.
Format Type Expert UDF	Enter the format type expert UDF string that will be used on the specified port(s) here.

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

DHCPv6 Relay Port Settings

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

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

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

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

Figure 4-61 DHCPv6 Relay Port Settings Window

The fields that can be configured are described below:

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

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

DHCPv6 Local Relay VLAN

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

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

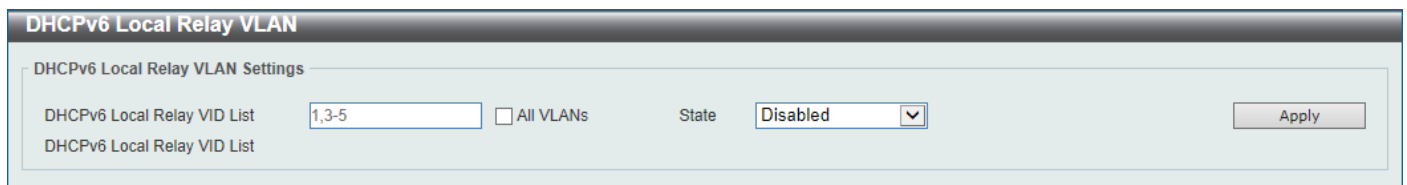


Figure 4-62 DHCPv6 Local Relay VLAN Window

The fields that can be configured are described below:

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

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



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

DHCP Auto Configuration

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

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

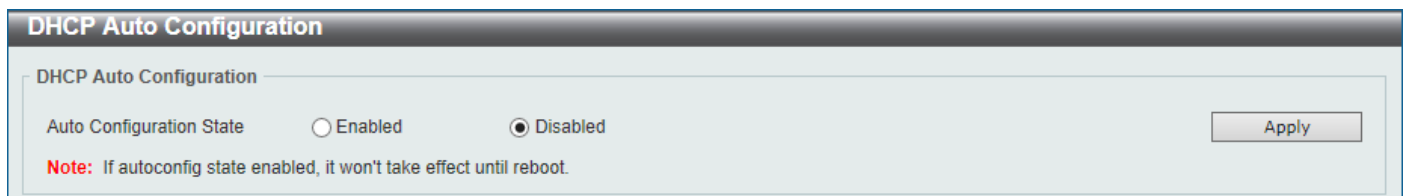


Figure 4-63 DHCP Auto Configuration Window

The fields that can be configured are described below:

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

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

DNS

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

DNS Global Settings

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

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

Figure 4-64 DNS Global Settings Window

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

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

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

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

Parameter	Description
Source Interface State	Select to enable or disable the source interface state here.
Interface Type	Select the source interface type here. Options to choose from are Loopback , Mgmt , and VLAN .
VID	Enter the VLAN ID of the source interface here.

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

DNS Name Server Settings

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

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

Figure 4-65 DNS Name Server Settings Window

The fields that can be configured are described below:

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

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

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

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

DNS Host Settings

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

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

Figure 4-66 DNS Host Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

IP Source Interface

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

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

Figure 4-67 IP Source Interface Window

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

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

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

File System

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

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

Drive	Media Type	Size (MB)	File System Type	Label
C:	Flash	1015	FFS	

Figure 4-68 File System Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Path	Enter the path string.

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

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

Click the [C:](#) hyperlink to navigate the C: drive

After clicking the [C:](#) hyperlink, the following window will appear:

Figure 4-69 File System (Drive) Window

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

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

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

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

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

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

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



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



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

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

Figure 4-70 File System (Copy) Window

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

Parameter	Description
Source	Select the source Switch Unit ID and type of source file that will be copied here. Options to choose from are startup-config and Source File . Only after selecting the Source File option can the source file path and filename be entered in the space provided.

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

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

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

Stacking

The Switch supports stacking 9 Switches together while being managed by one console connection to any one of the console ports on the master Switch, or by an IP address through the MGMT port, or by multiple IP addresses through any of the RJ45/SFP/SFP+ ports using Telnet, the Web User Interface, and SNMP. This cost effective Switch provides an affordable solution for administrators to upgrade their networks using the 10GBase-T/SFP+ ports to scale and stack the Switches. This increases overall reliability, serviceability, and availability of the network.

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

Switches in the series can be physically stacked using optical fiber cables connected to SFP+ transceivers or Direct Attached Cables (DAC) with SFP+ connectors or RJ-45 cables with 10GBase-T connectors. Only the last 6 ports can be used for physical stacking.



NOTE: When stacking is enabled, the last 2 10GBase-T and/or 4 SFP+ ports are dedicated stacking ports and cannot be used for any other purpose. These ports are only able to perform stacking when stacking is enabled.



NOTE: Using Duplex Ring topology is strongly recommended.

Physical stacking needs to be enabled and can be configured to support either a **2-port** or a **4-port** stacking configuration. When the **2-port** stacking configuration is used, a full-duplex speed of up to 40Gbps will be available between two Switches. When the **4-port** stacking configuration is used, a full-duplex speed of up to 80Gbps will be available between two Switches.

The figure below illustrates how switches can be stacked in a Duplex Ring formation using RJ45 cables, optical fiber cables connected to SFP+ transceivers or DAC with SFP+ connectors where the 2-port or 4-port stacking configuration is used.

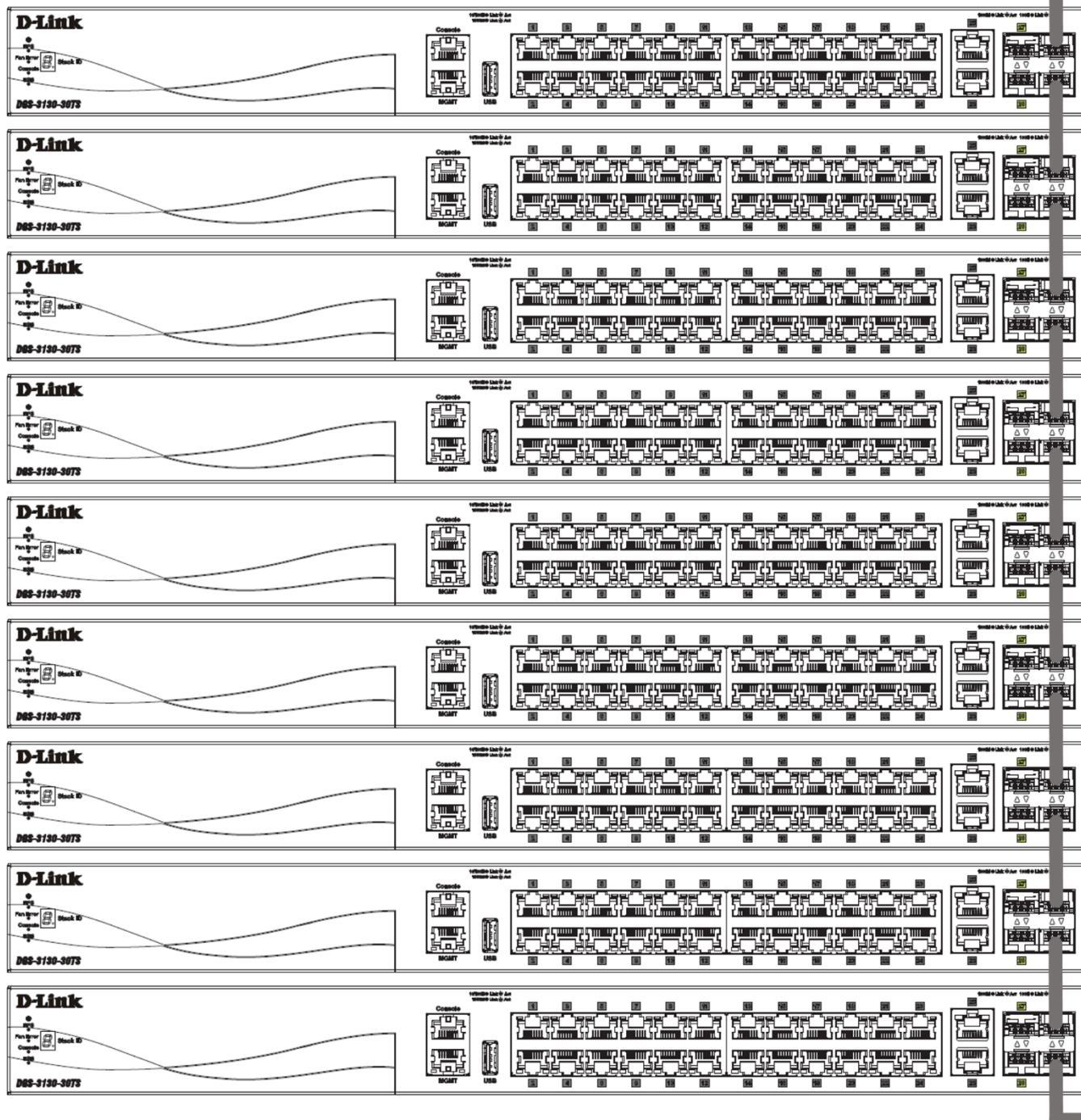


Figure 4-71 Duplex Ring stacking topology (SFP+)



NOTE: For more stacking topologies, please refer to Switch Stacking section in DGS-3130-30TS HW Installation Guide.

Switch Roles in a Stack

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

Primary Master - The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This Switch will also assign Stack Unit IDs, synchronize configurations and transmit commands to remaining Switches in the Switch stack. The Primary Master can be manually set by assigning this Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process. This determines the lowest MAC address

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

Backup Master - The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring Switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process. This determines the second lowest MAC address and then will assign that Switch as the Backup Master if all priorities are the same. The Backup master is physically displayed by the seven segment LED to the far right on the front panel of the Switch where the LED will flash between its given Box ID and 'h'.

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

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

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

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

Stack Switch Swapping

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

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

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

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

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

If the Primary Master is removed, the Backup Master will assume the Primary Master's role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configuration of the unit removed, and

dynamically learned databases, such as ARP, will also be cleared. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

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



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



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

Physical Stacking

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

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

Physical Stacking

Physical Stacking

Stacking Mode ☒ Enabled ☐ Disabled Apply

Stack ID

Current Unit ID ▼ New Box ID ▼ Apply

Current Unit ID ▼ Priority ▼ Apply

My Box ID: 1 BK Master ID: -
Master ID: 1 Box Count: 1

Box ID	Module Name	Priority	MAC	PROM/Runtime Version	H/W Version	Switch Status
1	DGS-3130-30TS	Unassigned	74-DA-DA-33-B8-36	1.00.003/1.01.025	A1	OK
2	--	-	--	--	-	Not Present
3	--	-	--	--	-	Not Present
4	--	-	--	--	-	Not Present
5	--	-	--	--	-	Not Present
6	--	-	--	--	-	Not Present
7	--	-	--	--	-	Not Present
8	--	-	--	--	-	Not Present
9	--	-	--	--	-	Not Present

Figure 4-72 Physical Stacking Window

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

Parameter	Description
Stacking Mode	Select this option to enable or disable the stacking mode.

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

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

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

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

Stacking Bandwidth

This window is used to display and configure the stacking bandwidth settings. Physical stacking needs to be enabled and can be configured to support either a **2-port** or a **4-port** stacking configuration.

- When the **2-port-SFP+** or **2-port-10GBaseT** stacking configuration is used, a full-duplex speed of up to 40Gbps will be used between two Switches.
 - The **DGS-3130-30TS** will use physical ports 25 and 26 for 2-port stacking.
 - The **DGS-3130-30TS** will use physical ports 29 and 30 for 2-port stacking.
- When the **4-port-SFP+** or **4-port-Hybrid** stacking configuration is used, a full-duplex speed of up to 80Gbps will be used between two Switches using four physical ports aggregated into two virtual stacking ports.
 - The **DGS-3130-30TS** will use physical ports 25, 26, 29, and 30 for 4-port stacking.
 - The **DGS-3130-30TS** will use physical ports 27, 28, 29, and 30 for 4-port stacking.



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

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

Box ID	Interface	Link Status	Link Speed (Gb/s)	Link Partner Box ID
1	0/53	Down	10	-
1	0/54	Down	10	-

Figure 4-73 Stacking Bandwidth Window

The fields that can be configured are described below:

Parameter	Description
Stack Bandwidth	<p>Select the stacking bandwidth here. Option to choose from are:</p> <ul style="list-style-type: none"> 2-port-10GBaseT - Specifies 2 10GBase-T switch ports to be used for stacking. 2-port-SFP+ - Specifies 2 SFP+ switch ports to be used for stacking. 4-port-Hybrid - Specifies 2 10GBase-T and 2 SFP+ switch ports to be used for stacking.

Parameter	Description
	<ul style="list-style-type: none"> • 4-port-SFP+ - Specifies 4 SFP+ switch ports to be used for stacking.

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

Virtual Stacking (SIM)

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

- SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
- SIM can reduce the number of IP address needed in your network.
- SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

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

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

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

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

The following rules also apply to the above roles:

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

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

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

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

Single IP Settings

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

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

Figure 4-74 Single IP Settings Window

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

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

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

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

Parameter	Description
Role State	<p>Select to change the SIM role of the Switch. Options to choose from are Candidate, and Commander.</p> <ul style="list-style-type: none"> • Candidate - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the Switch. • Commander - Select to make the Switch a Commander Switch (CS). The user may join other Switches to this Switch, over Ethernet, to be part of the SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	Enter a group name. This is optional. This name is used to segment Switches into different SIM groups.

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

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

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

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

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

SMTP Settings

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

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

SMTP Settings

SMTP Global Settings

SMTP IP: IPv4 (dropdown)

SMTP IPv4 Server Address: 0.0.0.0

SMTP IPv4 Server Port (1-65535): 25

Self Mail Address: 254 chars

Send Interval (0-65535): 30 min

SMTP Mail Receiver Address

Add A Mail Receiver: 254 chars

Send a Test Mail to All

Subject: 128 chars

Content: 512 chars

Total Entries: 8

Index	Mail Receiver Address	
1		Delete
2		Delete
3		Delete
4		Delete
5		Delete

Figure 4-75 SMTP Settings Window

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

Parameter	Description
SMTP IP	Select the SMTP server IP address type here. Options to choose from are IPv4 and IPv6 .
SMTP IPv4 Server Address	After selecting IPv4 as the SMTP IP type enter the SMTP server IPv4 address here.
SMTP IPv6 Server Address	After selecting IPv6 as the SMTP IP type enter the SMTP server IPv6 address here.
SMTP IPv4 Server Port	After selecting IPv4 as the SMTP IP type enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
SMTP IPv6 Server Port	After selecting IPv6 as the SMTP IP type enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
Self Mail Address	Enter the email address that represents the Switch here. This string can be up to 254 characters long.
Send Interval	Enter the sending interval value here. The range is from 0 to 65535 minutes. By default, this value is 30 minutes.

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

The fields that can be configured in **SMTP Mail Receiver Address** are described below:

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

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

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

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

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

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

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

PPPoE Circuit ID Insertion Global Settings

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

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

PPPoE Circuit ID Insertion Settings

PPPoE Circuit ID Insertion Global Settings

Global PPPoE State ☐ Enabled ☒ Disabled Apply

PPPoE Circuit ID Insertion Port Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 State: Disabled Circuit ID Type: IP Apply

Unit 1 Settings

Port	State	Circuit ID Type	User Defined String
eth1/0/1	Disabled	Switch IP	
eth1/0/2	Disabled	Switch IP	
eth1/0/3	Disabled	Switch IP	
eth1/0/4	Disabled	Switch IP	
eth1/0/5	Disabled	Switch IP	
eth1/0/6	Disabled	Switch IP	

Figure 4-76 PPPoE Circuit ID Insertion Global Settings Window

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

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

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

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

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

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

5. Layer 2 Features

FDB
 VLAN
 VLAN Tunnel
 STP
 ERPS (G.8032)
 Loopback Detection
 Link Aggregation
 L2 Protocol Tunnel
 L2 Multicast Control
 LLDP

FDB

Static FDB

Unicast Static FDB

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

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

Unicast Static FDB

Unicast Static FDB

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

Total Entries: 1

VID	MAC Address	Port
1	00-12-34-56-79-81	eth1/0/19

1/1

Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

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

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

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

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

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

Multicast Static FDB

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

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

Figure 5-2 Multicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
VID	Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX-XX.

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

Click the **Delete All** button to remove all the entries.

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

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

MAC Address Table Settings

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

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

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

The fields that can be configured are described below:

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

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

After selecting the **MAC Address Port Learning Settings** tab option, at the top of the page, the following page will be available.

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

Unit 1 Settings	
Port	Status
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled

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

The fields that can be configured are described below:

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

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

After selecting the **MAC Address VLAN Learning Settings** tab option, at the top of the page, the following page will be available.

VID	Status
1	Enabled

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

The fields that can be configured are described below:

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

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

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

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

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

MAC Address Table

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

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

VID	MAC Address	Type	Port
1	00-12-34-56-79-81	Static	eth1/0/19
1	00-23-7D-BC-08-44	Dynamic	eth1/0/5
1	00-23-7D-BC-2E-18	Dynamic	eth1/0/1
1	00-FF-47-77-70-B8	Dynamic	eth1/0/5
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/5
1	24-24-0E-E5-96-DE	Dynamic	eth1/0/5
1	40-B8-37-B1-06-9A	Dynamic	eth1/0/5
1	5C-33-8E-43-B3-68	Dynamic	eth1/0/5
1	CC-B2-55-8B-27-79	Dynamic	eth1/0/5
1	F0-7D-68-34-00-10	Static	CPU

Figure 5-6 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the stacking unit ID and the port number of the Switch that will be configured here.
VID	Enter the VLAN ID that will be used for this configuration here.
MAC Address	Enter the MAC address that will be used for this configuration here.

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

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

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

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

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

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

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

MAC Notification

This window is used to display and configure MAC notification.

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

Figure 5-7 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
Trap Type	Select the trap type here. Options to choose from are: <ul style="list-style-type: none"> Without VID - Specifies the trap information without the VLAN ID. With VID - Specifies the trap information with the VLAN ID.
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Added Trap	Select to enable or disable the added trap for the port(s) selected.
Removed Trap	Select to enable or disable the removed trap for the port(s) selected.

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

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

Figure 5-8 MAC Notification (MAC Notification History) Window

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

VLAN

802.1Q VLAN

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

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

Figure 5-9 802.1Q VLAN Window

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

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

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

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

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

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

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

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

Click the **Edit** button to 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.

802.1v Protocol VLAN

Protocol VLAN Profile

This window is used to display and configure 802.1v protocol VLAN profiles. The 802.1v Protocol VLAN group settings support multiple VLANs for each protocol and allow the user to configure untagged ports of different protocols on the same physical port. For example, it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port.

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

Figure 5-10 Protocol VLAN Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the 802.1v protocol VLAN profile ID here. This value must be between 1 and 16.
Frame Type	Select the frame type option here. This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Options to choose from are Ethernet 2 , SNAP , and LLC .
Ether Type	Enter the Ethernet type value for the group here. The protocol value is used to identify a protocol of the frame type specified. The range of values are 0x0 to 0xFFFF. Depending on the frame type, the octet string will have one of the following values: <ul style="list-style-type: none"> For Ethernet 2, this is a 16-bit (2-octet) hex value. For example, IPv4 is 0800, IPv6 is 86DD, ARP is 0806, etc. For IEEE802.3 SNAP, this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is a 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

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

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

Protocol VLAN Profile Interface

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

To view the following window, click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface**, as shown below:

Protocol VLAN Profile Interface

Add New Protocol VLAN Interface

Port: Profile ID: VID (1-4094): Priority:

Unit 1 Settings

Port	Profile ID	VID	Priority	
eth1/0/18	1	1	0	<input type="button" value="Delete"/>

Figure 5-11 Protocol VLAN Profile Interface Window

The fields that can be configured are described below:

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

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

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

GVRP

GVRP Global

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

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

GVRP Global

GVRP Global

Global GVRP State: ☐ Enabled ☒ Disabled

Dynamic VLAN Creation: ☒ Enabled ☐ Disabled

NNI BPDU Address:

Figure 5-12 GVRP Global Window

The fields that can be configured are described below:

Parameter	Description
Global GVRP State	Select to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select to enable or disable the dynamic VLAN creation function here.
NNI BPDU Address	Select the NNI BPDU address option here. This option is used to determine the BPDU protocol address for GVRP in customer networks. It can use 802.1d GVRP address or 802.1ad service provider GVRP address. Options to choose from are Dot1d and Dot1ad .

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

GVRP Port

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

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

GVRP Port

GVRP Port

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 GVRP Status: Disabled Join Time (10-10000): 20 centiseconds Leave Time (10-10000): 60 centiseconds Leave All Time (10-10000): 1000 centiseconds

Note:
The Leave Time should be no less than 3 * Join Time.
Leave All Time should be greater than Leave Time.

Apply

Unit 1 Settings

Port	GVRP Status	Join Time	Leave Time	Leave All Time
eth1/0/1	Disabled	20	60	1000
eth1/0/2	Disabled	20	60	1000
eth1/0/3	Disabled	20	60	1000
eth1/0/4	Disabled	20	60	1000
eth1/0/5	Disabled	20	60	1000
eth1/0/6	Disabled	20	60	1000

Figure 5-13 GVRP Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
GVRP Status	Select the enable or disable the GVRP port status. This enables the port to dynamically become a member of a VLAN. By default, this option is disabled.
Join Time	Enter the Join Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 1000 centiseconds.

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

GVRP Advertise VLAN

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

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

Figure 5-14 GVRP Advertise VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Action	Select the advertised VLAN to port mapping action here. Options to choose from are All , Add , Remove , and Replace . When selecting All , all the advertised VLANs will be used.
Advertise VID List	Enter the advertised VLAN ID list here.

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

GVRP Forbidden VLAN

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

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

Figure 5-15 GVRP Forbidden VLAN Window

The fields that can be configured are described below:

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

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are All , Add , and Remove . When selecting All , all the forbidden VLANs will be used.
Forbidden VID List	Enter the forbidden VLAN ID list here.

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

GVRP Statistics Table

This window is used to view GVRP statistics information.

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

Port		JoinEmpty	JoinIn	LeaveEmpty	LeaveIn	LeaveAll	Empty
eth1/0/1	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/2	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/3	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/4	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0

Figure 5-16 GVRP Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit to be displayed here.
Port	Select the port number to display GVRP statistic information for here.

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

Click the **Clear** button to clear all the information for the specific port.

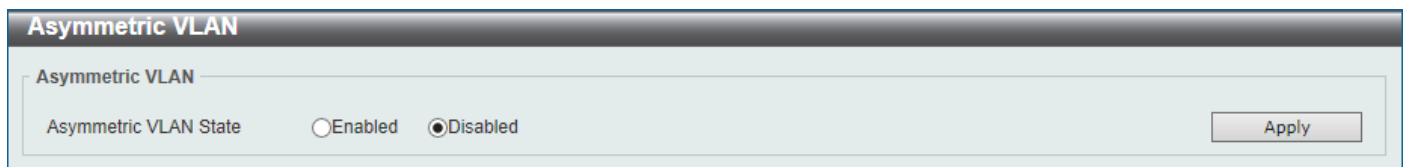
Click the **Show All** button to view all GVRP statistic information.

Click the **Clear All** button to clear all the information in this table.

Asymmetric VLAN

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

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



The screenshot shows the 'Asymmetric VLAN' configuration window. It has a title bar 'Asymmetric VLAN' and a sub-header 'Asymmetric VLAN'. Below the sub-header, there is a section 'Asymmetric VLAN State' with two radio buttons: 'Enabled' and 'Disabled'. The 'Disabled' radio button is selected. To the right of these options is an 'Apply' button.

Figure 5-17 Asymmetric VLAN Window

The fields that can be configured are described below:

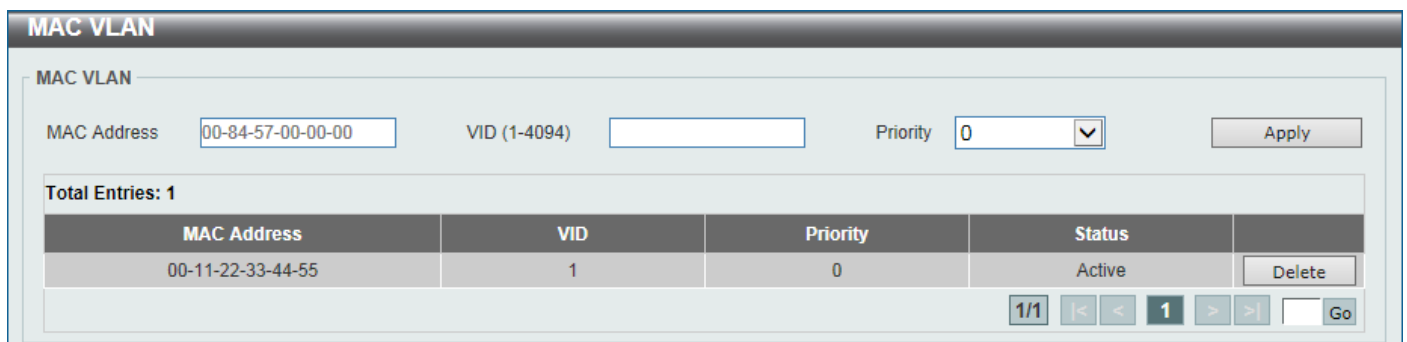
Parameter	Description
Asymmetric VLAN State	Select to enable or disable the asymmetric VLAN feature here.

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

MAC VLAN

This window is used to display and configure the MAC-based VLAN information. When a static MAC-based VLAN entry is configured, the VLAN operating on the port will be changed.

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



The screenshot shows the 'MAC VLAN' configuration window. It has a title bar 'MAC VLAN' and a sub-header 'MAC VLAN'. Below the sub-header, there are three input fields: 'MAC Address' with the value '00-84-57-00-00-00', 'VID (1-4094)' which is empty, and 'Priority' with a dropdown menu showing '0'. To the right of these fields is an 'Apply' button. Below these fields, there is a section 'Total Entries: 1' containing a table with the following data:

MAC Address	VID	Priority	Status
00-11-22-33-44-55	1	0	Active

To the right of the table is a 'Delete' button. At the bottom right of the window, there is a pagination control showing '1/1' and navigation buttons, with '1' selected.

Figure 5-18 MAC VLAN Window

The fields that can be configured are described below:

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

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

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

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

VLAN Interface

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

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

VLAN Interface

VLAN Interface

Unit

Unit 1 Settings

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

Figure 5-19 VLAN Interface Window

The fields that can be configured are described below:

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

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

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

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

VLAN Interface Information

VLAN Interface Information

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

Back

Figure 5-20 VLAN Interface (VLAN Detail) Window

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

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

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

Figure 5-21 VLAN Interface (Access) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , Host , Trunk Promiscuous , and Trunk Secondary .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN ID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

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

Figure 5-22 VLAN Interface (Hybrid) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , Host , Trunk Promiscuous , and Trunk Secondary .

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

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

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

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

Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/1

VLAN Mode: Trunk

Acceptable Frame: Admit All

Ingress Checking: ☒ Enabled ☐ Disabled

Native VLAN: ☒ Native VLAN ☐ Untagged ☒ Tagged

VID (1-4094): 1

Action: None

Allowed VLAN Range:

Current Allowed VLAN Range:

☐ Clone

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

Back Apply

Figure 5-23 VLAN Interface (Trunk) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , Host , Trunk Promiscuous , and Trunk Secondary .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	After selecting Trunk as the VLAN Mode the following parameter will be available. Select to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function. Also select if this VLAN supports Untagged or Tagged frames.
VID	After ticking the Native VLAN option the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are All , Add , Remove , Except , and Replace .
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

When **802.1Q-Tunnel** was selected as the **VLAN Mode**, the following page will appear.

The screenshot shows the 'Configure VLAN Interface' window. The title bar says 'Configure VLAN Interface'. Inside, there's a sub-header 'Configure VLAN Interface'. The form has the following fields and values:

- Port: eth1/0/1
- VLAN Mode: 802.1Q-Tunnel (dropdown)
- Acceptable Frame: Admit All (dropdown)
- Ingress Checking: ☒ Enabled ☐ Disabled
- VID (1-4094): 1
- Action: Add (dropdown)
- Add Mode: ☒ Untagged ☐ Tagged
- Allowed VLAN Range: (empty text box)
- Current Hybrid untagged VLAN Range: 1
- ☐ Clone
- From Port: eth1/0/1 (dropdown)
- To Port: eth1/0/1 (dropdown)
- Buttons: Back, Apply

Figure 5-24 VLAN Interface (802.1Q-Tunnel) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , Host , Trunk Promiscuous , and Trunk Secondary .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select Add to add a new entry based in the information entered. Select Remove to remove an entry based in the information entered.
Add Mode	Select to add an Untagged parameter.
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

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

The screenshot shows the 'Configure VLAN Interface' window. The 'Port' is set to 'eth1/0/1'. The 'VLAN Mode' is set to 'Promiscuous'. The 'Acceptable Frame' is set to 'Admit All'. The 'Ingress Checking' is set to 'Enabled'. The 'Clone' checkbox is unchecked. The 'From Port' and 'To Port' are both set to 'eth1/0/1'. There are 'Back' and 'Apply' buttons at the bottom right.

Figure 5-25 VLAN Interface (Promiscuous) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , Host , Trunk Promiscuous , and Trunk Secondary .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

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

The screenshot shows the 'Configure VLAN Interface' window. The 'Port' is set to 'eth1/0/1'. The 'VLAN Mode' is set to 'Host'. The 'Acceptable Frame' is set to 'Admit All'. The 'Ingress Checking' is set to 'Enabled'. The 'Clone' checkbox is unchecked. The 'From Port' and 'To Port' are both set to 'eth1/0/1'. There are 'Back' and 'Apply' buttons at the bottom right.

Figure 5-26 VLAN Interface (Host) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , Trunk , 802.1Q-Tunnel , Promiscuous , Host , Trunk Promiscuous , and Trunk Secondary .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

Super VLAN

This window is used to display and configure the super VLAN settings. This is used to specify a VLAN as a super VLAN. Super VLANs are used to aggregate multiple sub-VLANs (Layer 2 broadcast domains) into an IP subnet. A super VLAN cannot have any physical member port. A super VLAN cannot be a sub-VLAN at the same time. Once an IP interface is bound to a super VLAN, the proxy ARP will be enabled automatically on the interface for communication between its sub-VLANs. Multiple super VLANs can be configured and each super VLAN can consist of multiple sub-VLANs.

Private VLAN and super VLAN are mutually exclusive. A private VLAN cannot be configured as a super VLAN. Layer 3 routing protocols, multicast protocols, and the IPv6 protocol cannot run on a super VLAN interface.

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

Figure 5-27 Super VLAN Window

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

Parameter	Description
Super VID List	Enter the super VLAN ID(s) that will be created here.

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

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

Parameter	Description
Super VID	Enter the super VLAN ID that will be associated with the sub-VLAN(s) here. The range is from 1 to 4094.
Sub VID List	Enter the sub-VLAN ID(s) that will be associated with the super VLAN here.

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

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

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

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

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

Click the **Delete** button to remove the specific entry or to remove the sub-VLAN from the super VLAN.

Click the [IP Range List](#) link to add an IP range to the sub-VLAN.

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

After clicking the [IP Range List](#) link, the following page will be available.

Sub VLAN	
Sub VLAN	3
Action	Add
Start IP Address	- - -
End IP Address	- - -
<input type="button" value="Back"/> <input type="button" value="Apply"/>	
Total Entries: 1	
NO.	SubVLAN IP Address Range
1	192.168.70.33-192.168.70.35

Figure 5-28 Super VLAN (IP Range List) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Add and Remove .
Start IP Address	Enter the starting IP address in the range of this sub-VLAN here.
End IP Address	Enter the ending IP address in the range of this sub-VLAN here.

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

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

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to display and configure the auto surveillance VLAN properties.

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

The screenshot shows the 'Auto Surveillance Properties' window. It is divided into two main sections: 'Global Settings' and 'Port Settings'.

Global Settings:

- Surveillance VLAN:** Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected.
- Surveillance VLAN ID (2-4094):** A text input field.
- Surveillance VLAN CoS:** A dropdown menu showing '5'.
- Aging Time (1-65535):** A text input field showing '720' with a 'min' label.
- Apply:** A button.

Port Settings:

- Unit:** A dropdown menu showing '1'.
- From Port:** A dropdown menu showing 'eth1/0/1'.
- To Port:** A dropdown menu showing 'eth1/0/1'.
- State:** A dropdown menu showing 'Disabled'.
- Apply:** A button.

Unit 1 Settings:

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

Figure 5-29 Auto Surveillance Properties Window

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

Parameter	Description
Surveillance VLAN	Select to enable or disable the surveillance VLAN feature here.
Surveillance VLAN ID	Enter the VLAN ID of the surveillance VLAN here. The range is from 2 to 4094. A normal VLAN needs to be created before assigning the VLAN as a surveillance VLAN.
Surveillance VLAN CoS	Enter the Class of Service (CoS) value for the surveillance VLAN here. The surveillance packets arriving at the surveillance VLAN enabled port are marked with the CoS specified here. The remarking of CoS allows the surveillance VLAN traffic to be distinguished from data traffic in quality of service. The range is from 0 to 7.
Aging Time	Enter the aging time value here. This is used to configure the aging time for aging out the surveillance VLAN dynamic member ports. The range is from 1 to 65535 minutes. When the last surveillance device connected to the port stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be cancelled.

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

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

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

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

MAC Settings and Surveillance Device

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

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

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

Figure 5-30 MAC Settings and Surveillance Device Window

The fields that can be configured are described below:

Parameter	Description
Component Type	<p>Select the component type here. Option to choose from are:</p> <ul style="list-style-type: none"> • Video Management server - Specifies the surveillance device type as Video Management Server (VMS). • VMS Client/Remote Viewer - Specifies the surveillance device type as VMS client. • Video Encoder - Specifies the surveillance device type as Video Encoder. • Network Storage - Specifies the surveillance device type as Network Storage. • Other IP Surveillance Device - Specifies the surveillance device type as other IP Surveillance Devices.
Description	Enter the description for the user-defined OUI here. This string can be up to 32 characters long.
MAC Address	Enter the OUI MAC address here. If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.
Mask	Enter the matching bitmask for the OUI MAC address here.

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

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

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

Figure 5-31 MAC Settings and Surveillance Device (Auto Surveillance VLAN Summary) Window

The fields that can be configured are described below:

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

Voice VLAN

Voice VLAN Global

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

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

Figure 5-32 Voice VLAN Global Window

The fields that can be configured are described below:

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

Parameter	Description
	aging time, the aging timer will be cancelled. The range is from 1 to 65535 minutes.

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

Voice VLAN Port

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

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

Voice VLAN Port

Voice VLAN Port

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

Unit 1 Settings

Port	State	Mode
eth1/0/1	Disabled	Auto/Untag
eth1/0/2	Disabled	Auto/Untag
eth1/0/3	Disabled	Auto/Untag
eth1/0/4	Disabled	Auto/Untag
eth1/0/5	Disabled	Auto/Untag

Figure 5-33 Voice VLAN Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the voice VLAN feature on the specified port(s) here. When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets complies with the OUI addresses.
Mode	<p>Select the mode here. Options to choose from are:</p> <ul style="list-style-type: none"> Auto Untagged - Specifies that voice VLAN untagged membership will be automatically learned. Auto Tagged - Specifies that voice VLAN tagged membership will be automatically learned. Manual - Specifies that voice VLAN membership will be manually configured. <p>If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will automatically be aged out. When the port is working in the auto-tagged mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the Port VLAN ID (PVID).</p> <p>When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the voice VLAN.</p>

Parameter	Description
	When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.

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

Voice VLAN OUI

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

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

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

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

Figure 5-34 Voice VLAN OUI Window

The fields that can be configured are described below:

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

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

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

Voice VLAN Device

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

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

Voice VLAN Device

Voice VLAN Device Table

Unit: ▼

Total Entries: 0

Port	Voice Device Address	Start Time	Status
------	----------------------	------------	--------

Figure 5-35 Voice VLAN Device Window

The fields that can be configured are described below:

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

Voice VLAN LLDP-MED Device

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

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

Voice VLAN LLDP-MED Device

Voice VLAN LLDP-MED Device Table

Total Entries: 0

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

Figure 5-36 Voice VLAN LLDP-MED Device Window

Private VLAN

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

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

Figure 5-37 Private VLAN Window

The fields that can be configured for **Private VLAN** are described below:

Parameter	Description
VID List	Enter the private VLAN ID list here.
State	Select to enable or disable the private VLAN state here.
Type	Select the type of private VLAN that will be created here. Options to choose from are Community , Isolated , and Primary .

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

The fields that can be configured for **Private VLAN Association** are described below:

Parameter	Description
VID List	Enter the private VLAN ID list here.
Action	Select the action that will be taken for the private VLAN here. Options to choose from are Add , Remove , and Disabled .
Secondary VID List	Enter the secondary private VLAN ID here.

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

The fields that can be configured for **Private VLAN Host Association** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here. Select the Trunk option to specify that the trunk port will be associated with the private VLAN host association.
Primary VID	Enter the primary private VLAN ID here.
Secondary VID	Enter the secondary private VLAN ID here. When ticking the Remove Association option, specifies that this configuration will not be enabled.

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

The fields that can be configured for **Private VLAN Mapping** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here. Select the Trunk option to specify that the trunk port will be associated with the private VLAN map.
Primary VID	Enter the primary private VLAN ID here.
Action	Select Add to add a new entry based in the information entered. Select Remove to remove an entry based in the information entered.
Secondary VID List	Enter the secondary private VLAN ID here. When ticking the Remove Mapping option, this specifies that this configuration will not be enabled.

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

VLAN Tunnel

Dot1q Tunnel

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

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

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

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

Port	Outer TPID
eth1/0/1	0x8100
eth1/0/2	0x8100
eth1/0/3	0x8100
eth1/0/4	0x8100
eth1/0/5	0x8100

Figure 5-38 Dot1q Tunnel Window

The fields that can be configured are described below:

Parameter	Description
Inner TPID	Enter the inner TPID value here. This value is in the hexadecimal form. The range is from 0x1 to 0xFFFF. The inner TPID is used to decide if the ingress packet is C-tagged. The inner TPID can be configured per system.

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

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

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

Figure 5-39 Dot1q Tunnel Settings (Dot1q Tunnel Port Settings) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the port range that will be used here.
Trust Inner Priority	Select to enable or disable the 802.1Q Inner Trust Priority feature here. When the trusting priority option is enabled on an 802.1Q tunnel port, the priority of the VLAN tag in the received packets will be copied to the service VLAN tag.
Miss Drop	Select to enable or disable the Miss Drop feature here. If the VLAN mapping Miss Drop option is enabled on the receiving port, when the original VLAN of the received packets cannot match the VLAN mapping entries or rules on this port, the received packets will be dropped.
Insert Dot1q Tag	Enter the 802.1Q VLAN ID that is inserted to the untagged packets which are received on the 802.1Q tunnel port(s) here. The range is from 1 to 4094.
VLAN Mapping Profile	Enter the ID of the VLAN mapping profile here. A lower ID has a higher priority. The ID range is from 1 to 1000.
Action	Select Add to add a new entry based in the information entered. Select Remove to remove an entry based in the information entered.

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

VLAN Mapping

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

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

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

Figure 5-40 VLAN Mapping Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
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 . <ul style="list-style-type: none"> Translate - Specifies that the outer-VID will replace the outer-VID of the matched packets. Dot1q-tunnel - Specifies that the outer-VID will be added for matched packets.
VID	Enter the VLAN ID here. The range is from 1 to 4094.
Inner VID	Enter the inner VLAN ID here. The range is from 1 to 4094.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A lower value has a higher priority.

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

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

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

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

VLAN Mapping Profile

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

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

VLAN Mapping Profile

VLAN Mapping Profile

Profile ID (1-1000) Type Ethernet

Profile ID (1-1000)

Total Entries: 1

Profile ID	Type	
1	Ethernet	<input type="button" value="Add Rule"/> <input type="button" value="Delete"/>

1/1 |< < 1 > >|

Profile 1 Rules

Rule ID	Match	Action	802.1P Priority	New Inner VID	
2	inner-vid: 1 ether-t...	dot1q-tunnel outer-v...	0	1	<input type="button" value="Delete"/>

1/1 |< < 1 > >|

Figure 5-41 VLAN Mapping Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the ID of the VLAN mapping profile here. A lower ID has a higher priority. The ID range is from 1 to 1000.
Type	<p>Select the profile type here. Different profiles can match different fields. Options to choose from are Ethernet, IP, IPv6, and Ethernet-IP.</p> <ul style="list-style-type: none"> • Ethernet - The profile can match Layer 2 fields. • IP - The profile can match Layer 3 IP fields. • IPv6 - The profile can match IPv6 destination or source addresses. • Ethernet-IP - The profile can match Layer 2 and Layer 3 IP fields.

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

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

Click the **Add Rule** button to create a new rule.

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

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

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

Figure 5-42 VLAN Mapping Profile (Ethernet, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000.
Src-MAC Address	Enter the source MAC address here.
Dst-MAC Address	Enter the destination MAC address here.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A lower 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 . <ul style="list-style-type: none"> 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 lower 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.

Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID: 2

Type: IP

Rule ID (1-10000): 2

Src-IP Address (IP/Mask): [] []

Dst-IP Address (IP/Mask): [] []

DSCP (0-63): 21

Source Port (1-65535): 65535

Destination Port (1-65535): 65535

IP Protocol (0-255): 1

Action: Dot1q-Tunnel [] (1-4094)

802.1P Priority: None []

New Inner VID (1-4094): []

Back Apply

Figure 5-43 VLAN Mapping Profile (IP, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-IP Address (IP/Mask)	Enter the source IPv4 address and subnet mask here.
Dst-IP Address (IP/Mask)	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the 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	<p>Select the action that will be taken here. Options to choose from are Dot1q-Tunnel and Translate.</p> <ul style="list-style-type: none"> • 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 lower 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.

Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID: 3

Type: IPv6

Rule ID (1-10000): 2

Src-IPv6 Address: 2013::1/16

Dst-IPv6 Address: 3333::1/8

Action: Dot1q-Tunnel (1-4094)

802.1P Priority: None

New Inner VID (1-4094):

Back Apply

Figure 5-44 VLAN Mapping Profile (IPv6, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-IPv6 Address	Enter the source IPv6 address and prefix length here.
Dst-IPv6 Address	Enter the destination IPv6 address and prefix length here.
Action	<p>Select the action that will be taken here. Options to choose from are Dot1q-Tunnel and Translate.</p> <ul style="list-style-type: none"> 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 lower 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.

Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID: 4

Type: Ethernet-IP

Rule ID (1-10000):

Src-MAC Address:

Dst-MAC Address:

Priority:

Inner VID (1-4094):

Ethernet Type (0x0-0xffff):

Src-IP Address (IP/Mask):

Dst-IP Address (IP/Mask):

DSCP (0-63):

Source Port (1-65535):

Destination Port (1-65535):

IP Protocol (0-255):

Action: (1-4094)

802.1P Priority:

New Inner VID (1-4094):

Figure 5-45 VLAN Mapping Profile (Ethernet-IP, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-MAC Address	Enter the source MAC address here.
Dst-MAC Address	Enter the destination MAC address here.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A lower value has a higher priority.
Inner VID	Enter the inner VLAN ID here. The range is from 1 to 4094.
Ethernet Type	Enter the Ethernet type value here. The range is from 0x0 to 0xFFFF.
Src-IP Address	Enter the source IPv4 address and subnet mask here.
Dst-IP Address	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the 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 . <ul style="list-style-type: none"> 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 lower value has a higher priority.

Parameter	Description
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel was selected as the action.

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

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

STP

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

802.1Q-2005 MSTP

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

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

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

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

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

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

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

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by IEEE 802.1D-2004 and a

version compatible with IEEE 802.1D-1998. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998, however the advantages of using RSTP will be lost. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

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

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently, with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and therefore faster topology adjustment. A drawback of IEEE 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Blocking</i>	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Listening</i>	No	No
<i>Learning</i>	<i>Learning</i>	<i>Learning</i>	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

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

Edge Port

A port can be configured as an Edge Port if it is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the Listening and Learning states. An Edge Port loses its status if it receives a BPDU packet, after which it immediately becomes a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and are capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also includes a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

- On the Switch level, the settings are globally implemented.
- On the port level, the settings are implemented on a user-defined group of ports.

STP Global Settings

This window is used to display and configure the global STP settings.

To view the following window, click **L2 Features > STP > STP Global Settings**, as shown below:

The screenshot shows the 'STP Global Settings' window with the following configuration:

- STP State:** Radio buttons for 'Disabled' (selected) and 'Enabled'. An 'Apply' button is on the right.
- STP Traps:** Two rows of radio buttons. 'STP New Root Trap' has 'Disabled' selected. 'STP Topology Change Trap' has 'Disabled' selected. An 'Apply' button is on the right.
- STP Mode:** A dropdown menu showing 'RSTP'. An 'Apply' button is on the right.
- STP Priority:** A dropdown menu showing '32768'. An 'Apply' button is on the right.
- STP Configuration:** A grid of input fields. 'Bridge Max Age (6-40)' is 20 sec. 'Bridge Hello Time (1-2)' is 2 sec. 'Bridge Forward Time (4-30)' is 15 sec. 'TX Hold Count (1-10)' is 6 times. 'Max Hops (6-40)' is 20 times. 'NNI BPDU Address' is 'Dot1d'. An 'Apply' button is on the right.

Figure 5-46 STP Global Settings Window

The field that can be configured for **STP State** is described below:

Parameter	Description
STP State	Select to enable or disable the global STP state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select to enable or disable the STP New Root Trap option here.
STP Topology Change Trap	Select to enable or disable the STP Topology Change Trap option here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Mode** are described below:

Parameter	Description
STP Mode	Select the STP mode used here. Options to choose from are MSTP , RSTP , and STP .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Priority** are described below:

Parameter	Description
Priority	Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Configuration** are described below:

Parameter	Description
Bridge Max Age	Enter the bridge Maximum Age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting RSTP/STP as the Spanning Tree Mode , this parameter will be available. Enter the bridge Hello Time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP version. For MSTP, the Hello Time must be set on a port per-port basis.
Bridge Forward Time	Enter the bridge Forwarding Time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
TX Hold Count	Enter the Transmit Hold Count value here. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. This value must be between 6 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out.
NNI BPDU Address	Select the NNI BPDU Address option here. Options to choose from are Dot1d and Dot1ad . By default, this option is Dot1d . This parameter is used to determine the BPDU protocol address for STP in the service provider network. It can use an 802.1d STP address and an 802.1ad service provider STP address.

Click the **Apply** button to accept the changes made.

STP Port Settings

This window is used to display and configure the STP port settings.

To view the following window, click **L2 Features > STP > STP Port Settings**, as shown below:

STP Port Settings

STP Port Settings

Unit From Port To Port

Cost (1-200000000, 0=Auto) State Guard Root

Link Type Port Fast TCN Filter

BPDU Forward Priority Hello Time (1-2) sec

Loop Guard

Unit 1 Settings

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority	Loop Guard
eth1/0/1	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled
eth1/0/2	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled
eth1/0/3	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled
eth1/0/4	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled
eth1/0/5	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled
eth1/0/6	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled
eth1/0/7	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128	Disabled

Figure 5-47 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Cost	Enter the cost value here. This value must be between 1 and 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000, a Gigabit port is 20000, and a 10 Gigabit port is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.
Link Type	Select the Link Type option here. Options to choose from are Auto , P2P , and Shared . A full-duplex port is considered to have a Point-to-Point (P2P) connection. Alternatively, a half-duplex port is considered to have a Shared connection. The port cannot transit into the forwarding state rapidly by setting the link type to Shared . By default this option is Auto .
Port Fast	<p>Select the Port Fast option here. Options to choose from are Network, Disabled, and Edge.</p> <ul style="list-style-type: none"> In the Network mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the Disable mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. <p>By default, this option is Network.</p>

Parameter	Description
TCN Filter	Select to enable or disable the TCN Filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is Disabled .
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is Disabled .
Priority	Select the priority value here. Options to choose from are 0 to 240 . By default this option is 0 . A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between 1 and 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.
Loop Guard	<p>Select to enable or disable the Loop Guard feature on the specified port(s) here.</p> <p>The STP Loop Guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the Forwarding state. This usually happens because one of the ports in a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs.</p> <p>When one of the ports in a physically redundant topology no longer receives BPDUs, the STP considers the topology to be loop free. Eventually, an alternate port that was previously a Blocking or Backup port becomes Designated and moves to a Forwarding state. This situation creates a loop.</p>

Click the **Apply** button to accept the changes made.

MST Configuration Identification

This window is used to display and configure the MST configuration identification settings. These settings will uniquely identify an MSTI configured on the Switch. The Switch initially possesses one Common Internal Spanning Tree (CIST) of which the user may modify the parameters for but cannot change or delete the MSTI ID.

To view the following window, click **L2 Features > STP > MST Configuration Identification**, as shown below:

MST Configuration Identification

MST Configuration Identification

Configuration Name: F0:7D:68:34:00:10

Revision Level (0-65535): 0

Digest: AC36177F50283CD4B83821D8AB26DE62

Apply

Private VLAN Synchronize

Private VLAN Synchronize

Apply

Instance ID Settings

Instance ID (1-64):

Action: Add VID

VID List: 1 or 3-5

Apply

Total Entries: 1

Instance ID	VID List	
CIST	1-4094	Edit Delete

1/1 < < 1 > > Go

Figure 5-48 MST Configuration Identification Window

The fields that can be configured for **MST Configuration Identification** are described below:

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	Enter the revision level value here. This value must be between 0 and 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

Click the **Apply** button to accept the changes made.

In the **Private VLAN Synchronize** section, the user can click the **Apply** button to synchronize the private VLANs.

The fields that can be configured for **Instance ID Settings** are described below:

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 64.
Action	Select the action that will be taken here. Options to choose from are Add VID and Remove VID .
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

STP Instance

This window is used to display and configure the STP instance settings.

To view the following window, click **L2 Features > STP > STP Instance**, as shown below:

Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	<input type="button" value="Edit"/>

1/1 < < 1 > >

Instance CIST

CIST Global Info[Mode RSTP]	
Bridge Address	F0-7D-68-34-00-10
Designated Root Address / Priority	00-00-00-00-00-00 / 0
Regional Root Bridge Address / Priority	00-00-00-00-00-00 / 0
Designated Bridge Address / Priority	00-00-00-00-00-00 / 0

Figure 5-49 STP Instance Window

The fields that can be configured are described below:

Parameter	Description
Instance Priority	After clicking the Edit button, enter the Instance Priority value here. The range is from 0 to 61440.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MSTP Port Information

This window is used to display and configure the MSTP port information settings.

To view the following window, click **L2 Features > STP > MSTP Port Information**, as shown below:

MSTP Port Information

MSTP Port Information

Unit Port

eth1/0/1 Settings

Instance ID	Cost	Priority	Status	Role	
CIST	200000	128	Forwarding	NonStp	<input type="button" value="Edit"/>

1/1 < < 1 > >

Figure 5-50 MSTP Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here.
Port	Select the port number that will be cleared here.
Cost	After clicking the Edit button, enter the cost value here. This value must be between 1 and 200000000.
Priority	After clicking the Edit button, select the priority value here. Options to choose from are 0 to 240 . By default this option is 0 . A lower value has higher priority.

Click the **Clear Detected Protocol** button to clear the detected protocol settings for the port selected.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ERPS (G.8032)

Ethernet Ring Protection Switching (ERPS) (ITU-T G.8032) integrates mature Ethernet Operations, Administration, and Maintenance (OAM) functions and a simple Automatic Protection Switching (APS) protocol to provide sub-50ms protection for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

One link within a ring will be blocked to avoid a Loop (RPL, Ring Protection Link). When the failure happens, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

ERPS

This window is used to display and configure the Ethernet Ring Protection Switching (ERPS) settings. STP and Loopback Detection (LBD) should be disabled on the ring ports before enabling ERPS. The ERPS cannot be enabled before the R-APS VLAN ring ports, RPL port, and RPL owner are configured.



NOTE: Be aware that changing the ERPS version will lead to the restart of the running protocol.

To view the following window, click **L2 Features > ERPS (G.8032) > ERPS**, as shown below:

Ethernet Ring	Admin Port0	Admin Port1	Ring Type	Ring ID	Instance
---------------	-------------	-------------	-----------	---------	----------

Figure 5-51 ERPS Window

The fields that can be configured in **ERPS Version Settings** are described below:

Parameter	Description
ERPS Version	<p>G.8032v2 provides the following functions:</p> <ul style="list-style-type: none"> • Supports multi-instance in a physical ring. • Supports operation commands: manual, force, and clear. • Supports to configure the sending of the R-APS PDU destination address with the RING-ID of the physical ring. <p>If Ethernet ring nodes running ITU-T G.8032v1 and ITU-T G.8032v2 co-exist on an Ethernet ring, the following configurations should be made on the G.8032v2 device:</p> <ul style="list-style-type: none"> • All physical ring IDs must have the default value of 1.

Parameter	Description
	<ul style="list-style-type: none"> The major ring instance and sub-ring instance of the interconnection node must have different R-APS VLAN IDs. Manual switch or force switch command must not exist. The physical ring must have only one instance.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Ethernet Ring G.8032** are described below:

Parameter	Description
Ring Name	Enter the Ethernet Ring Protection (ERP) instance name here. This name can be up to 32 characters long.

Click the **Apply** button to create an ITU-T G.8032 ERP physical ring.

Click the **Edit Ring** button to modify an ITU-T G.8032 ERP physical ring.

Click the **Show Detail** button to view the ITU-T G.8032 ERP physical ring status information.

Click the **Delete** button to delete the specified ITU-T G.8032 ERP physical ring.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After click the **Edit Ring** button, the following window will appear.

The screenshot shows the 'Edit Ethernet Ring' window with the following fields and options:

- Ethernet Ring Name:** ring
- Instance ID (1-32):** [text box] ☐ None ☒ Specify
- Sub Ring Name:** 32 chars ☐ None ☒ Specify
- Port0:** [1] [eth1/0/1] ☐ None ☒ Specify
- Port1:** [1] [None] ☐ None ☒ Specify
- Ring ID:** [text box] ☐ None ☒ Specify
- Ring Type:** Major ring ☐

Buttons: Back, Apply

Figure 5-52 ERPS (Edit Ring) Window

The fields that can be configured are described below:

Parameter	Description
Instance ID	Select the checkbox and enter the ERP instance number here. This value must be between 1 and 32. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Sub Ring Name	Select the checkbox and enter the physical ring's sub-ring name here. This name can be up to 32 characters long. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Port0	Select the checkbox and then select the Switch unit ID and the port number that will be the first ring port of the physical ring. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Port1	Select the checkbox and then select the Switch unit ID and the port number that will be the second ring port of the physical ring. Select the None option, from the drop-down menu, specifies that the inter-connected node is a local

Parameter	Description
	node endpoint of an open ring. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Ring ID	Select the checkbox and enter the ring ID here. The range is from 1 to 239. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Ring Type	Select the checkbox and then select the ring type here. Options to choose from are Major Ring and Sub Ring .

Click the **Back** button to discard the changes made and return to the previous window.

Click the **Apply** button to accept the changes made.

After click the **Show Detail** button, the following window will appear.

ERPS Status Information	
Ethernet Ring	Ring
Admin Port0	eth1/0/10
Admin Port1	eth1/0/11
Ring Type	Major ring
Ring ID	1
Instance ID	1
Instance Status	Deactivated
R-APS Channel	0
Protected VLANs	
Port0	eth1/0/10, Forwarding
Port1	eth1/0/11, Forwarding
Profile	
Description	
Guard Timer	500 ms
Hold-Off Timer	0 ms
WTR Timer	5 min
Revertive	Enabled
MEL	1
RPL Role	None
RPL Port	-
Sub Ring Instance	none

Back

Figure 5-53 ERPS (View Detail) Window

Click the **Back** button to return to the previous window.

After selecting the **ERPS Brief** tab option, at the top of the page, the following page will be available.

ERPS				
ERPS Status		ERPS Brief		
Total Entries: 1				
Ethernet Ring	Instance ID	Status	Port State	
Ring	1	Deactivated	P0:eth1/0/10,Forwarding P1:eth1/0/12,Forwarding	Edit Instance

1/1 < < 1 > > Go

Figure 5-54 ERPS (ERPS Brief) Window

Click the **Edit Instance** button to configure the ERP instance.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After click the **Edit Instance** button, the following window will appear.

The screenshot shows the 'Edit Ethernet Instance' window with the following fields and values:

- Ethernet Ring Name: Ring
- Instance ID: 1
- Description: 64 chars ☐ None ☒ Specify
- R-APS Channel VLAN (1-4094): ☐ None ☒ Specify
- Inclusion VLAN List: 1,3-5 ☐ None ☒ Specify
- MEL (0-7): 1 ☐ None ☒ Specify
- Profile Name: 32 chars ☐ None ☒ Specify
- RPL Port: Port0 ☐
- RPL Role: Owner ☐ None ☒ Specify
- Activate: Disabled ☐
- Sub Ring Instance (1-32): ☐ None ☒ Specify
- Force Ring Port Block: Port0 ☐
- Manual Ring Port Block: Port0 ☐

Buttons at the bottom: Back, Apply, Clear.

Figure 5-55 ERPS (ERPS Brief, Edit Instance) Window

The fields that can be configured are described below:

Parameter	Description
Description	Select the checkbox and enter the ERP instance description here. This description can be up to 64 characters long. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
R-APS Channel VLAN	Select the checkbox and enter the R-APS channel VLAN ID for the ERP instance here. The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring. This value must be between 1 and 4094. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Inclusion VLAN List	Select the checkbox and enter the inclusion VLAN list here. A range is identified when a hyphen (-) is used. For example VLANs 1 to 5 can be entered as 1-5. A list is identified when commas (,) are used. For example, use VLANs 1,3,5. The VLANs specified here will be protected by the ERP mechanism. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
MEL	Select the checkbox and enter the ring MEL value of the ERP instance here. This value must be between 0 and 7. The configured MEL value of all ring nodes that participate in the same ERP instance should be identical. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Profile Name	Select the checkbox and enter the G.8032 profile name here that will be associated with this ERP instance. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance. This name can be up to 32 characters long. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
RPL Port	Select the checkbox and then select the RPL port option here. Options to choose from are Port0 and Port1 . The option selected will be configured as the RPL port.

Parameter	Description
RPL Role	Select the checkbox and then select whether this node is the RPL owner or neighbor. Options to choose from are Owner and Neighbor . Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Activate	Select the checkbox and then select whether or not to active this ERP instance. Options to choose from are Enabled and Disabled . Enabling this option will active this ERP instance.
Sub Ring Instance	Select the checkbox and enter the identifier of the ERP instance here. This is used to specify the sub-ring instance of a physical ring instance. The range is from 1 to 32. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Force Ring Port Block	Select the checkbox and select the ERP instance port that will be blocked here. This forcibly blocks an instance port immediately after force is configured, irrespective of whether link failures have occurred. Options to choose from are Port0 and Port1 .
Manual Ring Port Block	Select the checkbox and select the ERP instance port that will be blocked here. This forcibly blocks a port on which MS is configured when link failures and FS conditions are absent. Options to choose from are Port0 and Port1 .

Click the **Back** button to discard the changes made and return to the previous window.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear the forced or manual configuration associated with this entry.

ERPS Profile

This window is used to display and configure the Ethernet Ring G.8032 Profile settings.

To view the following window, click **L2 Features > ERPS (G.8032) > ERPS Profile**, as shown below:

Figure 5-56 ERPS Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the G.8032 profile name here. This name can be up to 32 characters long. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance.

Click the **Apply** button to associate the G.8032 profile with the ERP instance created.

Click the **Edit** button to modify the specified G.8032 profile.

Click the **Delete** button to disassociate the G.8032 profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After click the **Edit** button, the following window will appear.

Figure 5-57 ERPS Profile (Edit) Window

The fields that can be configured are described below:

Parameter	Description
TCN Propagation	Select the checkbox and then select the TCN propagation state. Options to choose from are Enable and Disabled . This function is used to enable the propagation of the topology change notifications from the sub-ERP instance to the major instance.
Revertive	Select the checkbox and then select the revertive state. Options to choose from are Enable and Disabled . This function is used to revert back to the working transport entity, for example, when the RPL is blocked.
Guard Timer	Select the checkbox and enter the guard timer value here. This value must be between 10 and 2000 milliseconds. By default, this value is 500 milliseconds.
Hold-Off Timer	Select the checkbox and enter hold-off timer value here. This value must be between 0 and 10 seconds. By default, this value is 0 seconds.
WTR Timer	Select the checkbox and enter the Wait To Restore (WTR) timer value here. This value must be between 1 and 12 minutes. By default, this value is 5 minutes.

Click the **Back** button to discard the changes made and return to the previous window.

Click the **Apply** button to accept the changes made.

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:

Port	Loopback Detection State	Result	Time Left (sec)
eth1/0/1	Disabled	Normal	-
eth1/0/2	Disabled	Normal	-
eth1/0/3	Disabled	Normal	-
eth1/0/4	Disabled	Normal	-
eth1/0/5	Disabled	Normal	-
eth1/0/6	Disabled	Normal	-
eth1/0/7	Disabled	Normal	-
eth1/0/8	Disabled	Normal	-

Figure 5-58 Loopback Detection Window

The fields that can be configured in **Loopback Detection Global Settings** are described below:

Parameter	Description
Loopback Detection State	Select to enable or disable loopback detection. The default is Disabled .
Mode	Select the loopback detection mode. Options to choose from are Port-based and VLAN-based .
Enabled VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when VLAN-based is selected in the Mode drop-down list.
Interval	Enter the interval in seconds that the device will use to transmit Configuration Test Protocol (CTP) packets to detect a loopback event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.
Trap State	Select to enable or disable the loopback detection trap state.
Action Mode	Select the action mode here. Option to choose from are: <ul style="list-style-type: none"> • Shutdown - Specifies to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected. • None - Specifies not to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected.
Address Type	Select the address type here. Options to choose from are Multicast and Broadcast .

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Loopback Detection Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

Click the **Apply** button to accept the changes made.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 32 port trunk groups with up to 8 ports in each group.

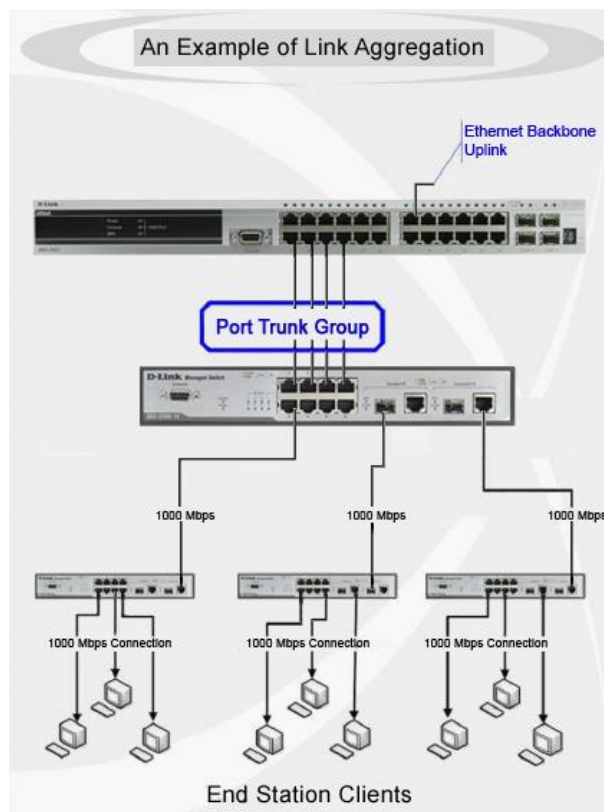


Figure 5-59 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This results in a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link bandwidth intensive network devices, such as servers, to the backbone of a network.

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of up to 8 links (ports). Each port can only belong to a single link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

This window is used to display and configure the link aggregation settings. To view the following window, click **L2 Features > Link Aggregation**, as shown below:

Figure 5-60 Link Aggregation Window

The fields that can be configured for **Link Aggregation** are described below:

Parameter	Description
System Priority	Enter the system priority value used here. This value must be between 1 and 65535 . By default, this value is 32768 . The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load balancing algorithm that will be used here. Options to choose from are Source MAC , Destination MAC , Source Destination MAC , Source IP , Destination IP , Source Destination IP , Source L4 Port , Destination L4 Port , and Source Destination L4 Port . By default, this option is Source Destination MAC .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Channel Group Information** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the list of ports that will be associated with this configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 32 . The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are On , Active , and Passive . If the mode On is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

Click the **Add** button to add a new channel group.

Click the **Delete Member Port** button, to delete the member port(s) specified from the group.

Click the **Delete Channel** button to delete the specified channel group.

Click the **Show Detail** button to view more detailed information about the channel.

After clicking the **Show Detail** button, the following page will be available.

Port Channel

Port Channel Description Information

Port Channel1
Description64 chars

Apply

Port	Status	Administrative	Description	
Port-channel1	down	enabled		<div>Delete Description</div>

Port Channel Information

Port Channel1
ProtocolStatic

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/18	None	None	down	None	None	<div>Edit</div>
eth1/0/19	None	None	down	None	None	<div>Edit</div>

Port Channel Neighbor Information

Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/18	None	None	None	None	None
eth1/0/19	None	None	None	None	None

Note:

LACP State:

bndl: Port is attached to an aggregator and bundled with other ports.
indep: Port is in an independent state(not bundled but able to switch data traffic).
hot-sby: Port is in a hot-standby state.
down: Port is down.

Back

Figure 5-61 Link Aggregation (Show Detail) Window

The fields that can be configured are described below:

Parameter	Description
Description	Enter the description for the port channel here. This string can be up to 64 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete Description** button to delete the description for the port channel.

Click the **Edit** button to re-configure the specific entry.

Click the **Back** button to return to the previous page.

L2 Protocol Tunnel

This window is used to display and configure the Layer 2 protocol tunnel settings.

To view the following window, click **L2 Features > L2 Protocol Tunnel**, as shown below:

Protocol	Drop Counter
GVRP	0
STP	0
01-00-0C-CC-CC-CC	0
01-00-0C-CC-CC-CD	0

Figure 5-62 L2 Protocol Tunnel (L2 Protocol Tunnel Global Setting) Window

The fields that can be configured are described below:

Parameter	Description
CoS for Encapsulated Packets	Select the CoS value for encapsulated packets here. This value is between 0 and 7. Select the Default option to use the default value.
Drop Threshold	Enter the drop threshold value here. This value must be between 100 and 20000. By default, this value is 0. The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use this option to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped. Select the Default option to use the default value.

Click the **Apply** button to accept the changes made.

After selecting the **L2 Protocol Tunnel Port Setting** tab option, at the top of the page, the following page will be available.

Unit	From Port	To Port	Action	Type	Tunneled Protocol	Protocol MAC	Threshold
1	eth1/0/1	eth1/0/1	Add	None	GVRP	01-00-0C-CC-CC-CC	

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
eth1/0/22	gvrp	-	-	0	0	0

Figure 5-63 L2 Protocol Tunnel (L2 Protocol Tunnel Port Setting) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
Type	Select the type option here. Options to choose from are None , Shutdown , and Drop .
Tunneled Protocol	Select the tunneled protocol option here. Options to choose from are GVRP , STP , Protocol MAC , and All .

Parameter	Description
Protocol MAC	After selecting the Protocol MAC option as the Tunneled Protocol , the following option will be available. Select the protocol MAC option here. Options to choose from are 01-00-0C-CC-CC-CC and 01-00-0C-CC-CC-CD .
Threshold	After selecting the Shutdown or Drop option in the Type field, the following parameter will be available. Enter the threshold value here. This value must be between 1 and 4096 .

Click the **Apply** button to accept the changes made.

Click the **Clear All** button to clear all the counter information.

Click the **Clear** button to clear all the counter information of the specific entry.

L2 Multicast Control

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under **IGMP Global Settings** at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as shown below:

Figure 5-64 IGMP Snooping Settings Window

The fields that can be configured in **Global Settings** are described below:

Parameter	Description
Global State	Select this option to globally enable or disable IGMP snooping.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable IGMP snooping on the VLAN.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IGMP Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Click the **Show Detail** button to see the detail information of the specific VLAN.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following window will appear.

The screenshot shows a web interface window titled "IGMP Snooping VLAN Parameters". Inside, there is a table of parameters for VID 1. The parameters and their values are as follows:

Parameter	Value
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 seconds
Querier State	Disabled
Query Version	v3
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Member Query Interval	1 seconds
Proxy Reporting	Disabled Source Address (0.0.0.0)
Rate Limit	0
Ignore Topology Change	Disabled

At the bottom right of the window, there is a button labeled "Modify".

Figure 5-65 IGMP Snooping Settings (Show Detail) Window

The window displays the detail information about IGMP snooping VLAN.

Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in IGMP Snooping Settings window, the following window will appear.

IGMP Snooping VLAN Settings

IGMP Snooping VLAN Settings

VID (1-4094)	<input style="width: 100%;" type="text" value="1"/>
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Minimum Version	<input style="width: 100%;" type="text" value="1"/> ▼
Fast Leave	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Report Suppression	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Suppression Time (1-300)	<input style="width: 100%;" type="text" value="10"/>
Querier State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Query Version	<input style="width: 100%;" type="text" value="3"/> ▼
Query Interval (1-31744)	<input style="width: 100%;" type="text" value="125"/> sec
Max Response Time (1-25)	<input style="width: 100%;" type="text" value="10"/> sec
Robustness Value (1-7)	<input style="width: 100%;" type="text" value="2"/>
Last Member Query Interval (1-25)	<input style="width: 100%;" type="text" value="1"/> sec
Proxy Reporting	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
	Source Address <input style="width: 100%;" type="text" value="."/> . <input style="width: 100%;" type="text" value="."/> . <input style="width: 100%;" type="text" value="."/> . <input style="width: 100%;" type="text" value="."/>
Rate Limit (1-1000)	<input style="width: 100%;" type="text" value=""/> <input checked="" type="checkbox"/> No Limit
Ignore Topology Change	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Figure 5-66 IGMP Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum IGMP host version that is allowed on the VLAN. Options to choose from are 1 , 2 , and 3 .
Fast Leave	Select this option to enable or disable the IGMP snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message.
Report Suppression	Select this option to enable or disable the report suppression. The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expires. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.
Suppression Time	Enter the interval of suppressing duplicate IGMP reports or leaves. The range is from 1 to 300.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the IGMP snooping querier. Options to choose from are 1 , 2 , and 3 .
Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically. The range is from 1 to 31744.
Max Response Time	Enter the maximum response time, in seconds, advertised in IGMP snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable used in IGMP snooping. The range is from 1 to 7.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.

Parameter	Description
Source Address	Enter the source IP of proxy reporting. This is available when Enabled is selected in Proxy Reporting .
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Tick the No Limit option to apply no rate limit on this profile.
Ignore Topology Change	Select to enable or disable the Ignore Topology Change feature here.

Click the **Apply** button to accept the changes made.

IGMP Snooping AAA Settings

This window is used to display and configure the IGMP snooping AAA settings.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping AAA Settings**, as shown below:

Figure 5-67 IGMP Snooping AAA Settings Window, accounting

The fields that can be configured in **IGMP Snooping AAA Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Authentication	Select to enable or disable authentication here. This is used to enable or disable the authentication function for IGMP join messages. When enabled and the client wants to join a group, the system will perform authentication first.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IGMP Snooping AAA Table** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here.
From Port - To Port	Select the range of ports that will be used for this display here.

Click the **Find** button to generate the display based on the selections made.

Click the **Show All** button to display all the available entries.

IGMP Snooping Groups Settings

This window is used to display and configure the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:

Figure 5-68 IGMP Snooping Groups Settings Window

The fields that can be configured in **IGMP Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Enter an IP multicast group address.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured in **IGMP Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.
Detail	Select this option to display the IGMP group detail information.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

IGMP Snooping Statistics Settings

This window is used to view and clear the IGMP snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings**, as shown below:

Figure 5-69 IGMP Snooping Statistics Settings Window

The fields that can be configured in **IGMP Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are All , VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Statistics drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when Port is selected in the Statistics drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Statistics drop-down list.

Click the **Clear** button to clear the IGMP snooping related statistics.

The fields that can be configured in **IGMP Snooping Statistics Table** are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Find Type drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when Port is selected in the Find Type drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Find Type drop-down list.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

These types of messages are transferred between devices using MLD snooping. These messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

- **Multicast Listener Query** - Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router: the General Query, which is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which is used to advertise a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
- **Multicast Listener Report, Version 1** - Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
- **Multicast Listener Done** - Similar to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.
- **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

MLD Snooping Settings

This window is used to display and configure the MLD snooping settings.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings**, as shown below:

MLD Snooping Settings

Global Settings

Global State ☐ Enabled ☒ Disabled Apply

VLAN Status Settings

VID (1-4094) ☐ Enabled ☒ Disabled Apply

MLD Snooping Table

VID (1-4094) Find Show All

Total Entries: 1

VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit

1/1 < << **1** >> > Go

Figure 5-70 MLD Snooping Settings Window

The fields that can be configured in **Global Settings** are described below:

Parameter	Description
Global State	Select this option to enable or disable the global MLD snooping state.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable MLD snooping on the VLAN.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **MLD Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Click the **Show Detail** button to see the detail information of the specific VLAN.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following window will appear.

The screenshot shows a window titled "MLD Snooping VLAN Parameters". Inside, there is a list of parameters and their current values:

MLD Snooping VLAN Parameters	
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 seconds
Proxy Reporting	Disabled Source Address (::)
Mrouter Port Learning	Enabled
Querier State	Disabled
Query Version	v2
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Listener Query Interval	1 seconds
Rate Limit	0
Ignore Topology Change	Disabled

At the bottom right of the window, there is a button labeled "Modify".

Figure 5-71 MLD Snooping Settings (Show Detail) Window

The window displays the detail information about MLD snooping VLAN.

Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in MLD Snooping Settings window, the following window will appear.

MLD Snooping VLAN Settings

MLD Snooping VLAN Settings

VID (1-4094)

Status ☒ Enabled ☐ Disabled

Minimum Version ▼

Fast Leave ☐ Enabled ☒ Disabled

Report Suppression ☐ Enabled ☒ Disabled

Suppression Time (1-300)

Proxy Reporting ☐ Enabled ☒ Disabled
Source Address

Mrouter Port Learning ☒ Enabled ☐ Disabled

Querier State ☐ Enabled ☒ Disabled

Query Version ▼

Query Interval (1-31744) sec

Max Response Time (1-25) sec

Robustness Value (1-7)

Last Listener Query Interval (1-25) sec

Rate Limit (1-1000) ☒ No Limit

Ignore Topology Change ☐ Enabled ☒ Disabled

Figure 5-72 MLD Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN. Options to choose from are 1 and 2 .
Fast Leave	Select this option to enable or disable the MLD snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the MLD leave message.
Report Suppression	Select this option to enable or disable the report suppression.
Suppression Time	Enter the interval of suppressing duplicate MLD reports or leaves. The range is from 1 to 300.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when Enabled is selected in Proxy Reporting .
Mrouter Port Learning	Select this option to enable or disable Mrouter port learning.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the MLD snooping querier. Options to choose from are 1 , and 2 .
Query Interval	Enter the interval at which the MLD snooping querier sends MLD general query messages periodically. The range is from 1 to 31744.
Max Response Time	Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable used in MLD snooping. The range is from 1 to 7.
Last Listener Query Interval	Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Tick the No Limit option to apply no rate limit on this profile.

Parameter	Description
Ignore Topology Change	Select to enable or disable the Ignore Topology Change feature here.

Click the **Apply** button to accept the changes made.

MLD Snooping Groups Settings

This window is used to display and configure the MLD snooping static group, and view MLD snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings**, as shown below:

Figure 5-73 MLD Snooping Groups Settings Window

The fields that can be configured in **MLD Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID of the multicast group here. The range is from 1 to 4094.
Group Address	Enter the IPv6 multicast group address here.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured in **MLD Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.
Detail	Select this option to display the MLD group detail information.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

MLD Snooping Mrouter Settings

This window is used to display and configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports on the VLAN interface on the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings**, as shown below:

Figure 5-74 MLD Snooping Mrouter Settings Window

The fields that can be configured in **MLD Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	<p>Select the port configuration. Options to choose from are Port, Forbidden Port, and Learn PIMv6.</p> <ul style="list-style-type: none"> Port - Select to have the configured ports as being connected to multicast-enabled routers. Forbidden Port - Select to have the configured ports as being not connected to multicast-enabled routers. Learn PIMv6 - Select to enable dynamic learning of multicast router port.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

The fields that can be configured in **MLD Snooping Mrouter Table** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MLD Snooping Statistics Settings

This window is used to view and clear the MLD snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings**, as shown below:

Figure 5-75 MLD Snooping Statistics Settings Window

The fields that can be configured in **MLD Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are All , VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Statistics drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when Port is selected in the Statistics drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Statistics drop-down list.

Click the **Clear** button to clear the MLD snooping related statistics.

The fields that can be configured in **MLD Snooping Statistics Table** are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Find Type drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when Port is selected in the Find Type drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Find Type drop-down list.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast VLAN

Multicast VLAN Settings

This window is used to display and configure the multicast VLAN settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Settings**, as shown below:

Multicast VLAN Settings

Multicast VLAN Global Settings

Multicast VLAN IPv4 State ☐ Enabled ☒ Disabled Forward Unmatched ☐ Enabled ☒ Disabled

Multicast VLAN IPv6 State ☐ Enabled ☒ Disabled Ignore VLAN ☐ Enabled ☒ Disabled Apply

VID (2-4094) VLAN Name Delete Add

Member Port Settings

VID (2-4094) Action Role Type Unit From Port To Port Apply

Replace Source IP Settings

VID (2-4094) Action Address Type IP Address From Apply

Multicast VLAN Table

VID (2-4094) Find Show All

Total Entries: 0

VID	VLAN Name	Untagged Receiver	Tagged Receiver	Untagged Source	Tagged Source	Replace Source IP
Total Entries: 0						

Figure 5-76 Multicast VLAN Settings Window

The fields that can be configured in **Multicast VLAN Global Settings** are described below:

Parameter	Description
Multicast VLAN IPv4 State	Select to enable or disable the IPv4 IGMP control packet process in multicast VLANs.
Forward Unmatched	Select the enable or disable the Forward Unmatched feature here. This specifies that if the received IGMP or MLD control packet is untagged, does not match any profile, and the associated default VLAN is a multicast VLAN, or is tagged with a multicast VLAN, but does not match the associated profile, then the packet will be forwarded or dropped based on this setting. By default, the packet will be dropped.
Multicast VLAN IPv6 State	Select to enable or disable the IPv6 MLD control packet process in multicast VLANs.
Ignore VLAN	Select the enable or disable the ignore VLAN feature here. This specifies the setting for tagged IGMP or MLD control packets. If enabled, then the packet's VLAN is ignored and taken to match the profile to find its multicast VLAN. When this option is enabled, the Switch will ignore the VLAN of the receiving IGMP or MLD control packet and try to find a match profile.
VID	Enter the VLAN ID of the multicast VLAN that will be created or deleted here. The range is 2 to 4094.
VLAN Name	Enter the VLAN name of the multicast VLAN that will be created or deleted here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

The fields that can be configured in **Member Port Settings** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
Role	Select the role here. Options to choose from are Receiver and Source . <ul style="list-style-type: none"> • 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 . <ul style="list-style-type: none"> • Tagged - Specifies that if a port is a tagged member, the packets sent from the port are tagged with the Multicast VLAN ID. • Untagged - Specifies that if the port is an untagged member, then the packets will be forwarded in the untagged form.
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Replace 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 . <ul style="list-style-type: none"> • IPv4 - Specifies to enter the source IPv4 address for IGMP control packet reporting up to routers. • IPv6 - Specifies to enter the source IPv6 address for MLD control packet reporting up to routers.
IP Address	Enter the IPv4/IPv6 address here.
From	Select the "from" option here. Options to choose from are Receiver , Source , and Both . <ul style="list-style-type: none"> • Receiver - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any multicast VLAN receiver port will be replaced. • Source - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any multicast VLAN source port will be replaced. • Both - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any port in the multicast VLAN will be replaced.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Multicast VLAN Table** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast VLAN Group Settings

This window is used to view and configure the multicast VLAN group settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Group Settings**, as shown below:

Multicast VLAN Group Settings

Group Profile Settings

Profile Name: 32 chars Apply

Profile Name: 32 chars Action: Add Address Type: IPv4 From IP Address: To IP Address: Apply

Access Group Settings

VID (2-4094): Profile Name: 32 chars Action: Add Apply

Group Profile Table

Profile Name: 32 chars Find Show All

Total Entries: 1 Delete All

Profile Name	Multicast Addresses
profile	Delete

1/1 |< < 1 > >| Go

Access Group Table

VID (2-4094): Find Show All

Total Entries: 1

VID	Multicast Group Profiles
2	

1/1 |< < 1 > >| Go

Figure 5-77 Multicast VLAN Group Settings Window

The fields that can be configured in **Group Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the group profile name for the multicast VLAN feature here. This name can be up to 32 characters long.
Action	Select the action that will be taken here. Options to choose from are Add and Delete . Multiple ranges can be added to a multicast VLAN profile. The IP address ranges, specified in a single profile, must be of the same address family.
Address Type	Select the address type here. Options to choose from are IPv4 and IPv6 .

Parameter	Description
	<ul style="list-style-type: none"> 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 1 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 1 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast Filtering

This window is used to display and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering**, as shown below:

Multicast Filtering

Multicast Filtering

VID List: 3 or 1-5 Multicast Filter Mode: Forward Unregistered Apply

Total Entries: 2

VLAN	Multicast Filter Mode
default	Forward Unregistered Groups
MVLAN	Forward Unregistered Groups

1/1 < < 1 > > Go

Figure 5-78 Multicast Filtering Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filter Mode	<p>Select the multicast filter mode here. Options to choose from are Forward Unregistered, Forward All, and Filter Unregistered.</p> <ul style="list-style-type: none"> When selecting the Forward Unregistered option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the Forward All option, all multicast packets will be flooded based on the VLAN domain. When selecting the Filter Unregistered option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

LLDP

LLDP Global Settings

This window is used to display and configure the global LLDP settings.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:

LLDP Global Settings

LLDP Global Settings

LLDP State ☒ Enabled ☐ Disabled

LLDP Forward State ☐ Enabled ☒ Disabled

LLDP Trap State ☐ Enabled ☒ Disabled

LLDP-MED Trap State ☐ Enabled ☒ Disabled Apply

LLDP-MED Configuration

Fast Start Repeat Count (1-10) times Apply

LLDP Configurations

Message TX Interval (5-32768) sec

Message TX Hold Multiplier (2-10) sec

Relnit Delay (1-10) sec

TX Delay (1-8192) sec Apply

LLDP System Information

Chassis ID Subtype	MAC Address
Chassis ID	20-00-14-64-11-12
System Name	Switch
System Description	L3 Stackable Managed Switch
System Capabilities Supported	Repeater, Bridge
System Capabilities Enabled	Repeater, Bridge

LLDP-MED System Information

Device Class	Network Connectivity Device
Hardware Revision	A1
Firmware Revision	1.00.001
Software Revision	1.01.011
Serial Number	DGS31300001
Manufacturer Name	D-Link
Model Name	DGS-3130-30TS
Asset ID	

Figure 5-79 LLDP Global Settings Window

The fields that can be configured in **LLDP Global Settings** are described below:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the LLDP State is disabled and LLDP Forward State is enabled, the received LLDPDU packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the LLDP-MED trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **LLDP-MED Settings** are described below:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **LLDP Configurations** are described below:

Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDU's transmission interval that used to calculate the TTL value of an LLDPDU. This value must be between 2 and 10.
Relnit Delay	Enter the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

Click the **Apply** button to accept the changes made.

LLDP Port Settings

This window is used to display and configure the LLDP port settings.

To view the following window, click **L2 Features > LLDP > LLDP Port Settings**, as shown below:

LLDP Port Settings

LLDP Port Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Notification: Disabled Subtype: Local Admin State: TX and RX IP Subtype: Default Action: Remove Address:

Note: The address should be the switch's address.

Unit 1 Settings

Port	Notification	Subtype	Admin State	IPv4/IPv6 Address
eth1/0/1	Disabled	Local	TX and RX	
eth1/0/2	Disabled	Local	TX and RX	
eth1/0/3	Disabled	Local	TX and RX	
eth1/0/4	Disabled	Local	TX and RX	
eth1/0/5	Disabled	Local	TX and RX	
eth1/0/6	Disabled	Local	TX and RX	
eth1/0/7	Disabled	Local	TX and RX	
eth1/0/8	Disabled	Local	TX and RX	

Figure 5-80 LLDP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select to enable or disable the notification feature here.
Subtype	Select the subtype of LLDP TLV(s). Options to choose from are MAC Address , and Local .
Admin State	<p>Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are TX, RX, TX and RX, and Disabled.</p> <ul style="list-style-type: none"> TX - The local LLDP agent can only transmit LLDP frames. RX - The local LLDP agent can only receive LLDP frames. TX and RX - The local LLDP agent can both transmit and receive LLDP frames. Disabled - The local LLDP agent can neither transmit nor receive LLDP frames. <p>The default value is TX and RX.</p>

Parameter	Description
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are Default , IPv4 and IPv6 .
Action	Select the action that will be taken here. Options to choose from are Remove and Add .
Address	Enter the IP address that will be sent.

Click the **Apply** button to accept the changes made.



NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

This window is used to view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP Management Address List**, as shown below:

LLDP Management Address List				
All <input type="button" value="v"/>	<input type="text" value="Find"/>			
Subtype	Address	IF Type	OID	Advertising Ports
IPv4	10.90.90.90(default)	Ifindex	1.3.6.1.4.1.171.10.1...	-
IPv4	10.90.90.90	Ifindex	1.3.6.1.4.1.171.10.1...	-

Figure 5-81 LLDP Management Address List Window

The fields that can be configured are described below:

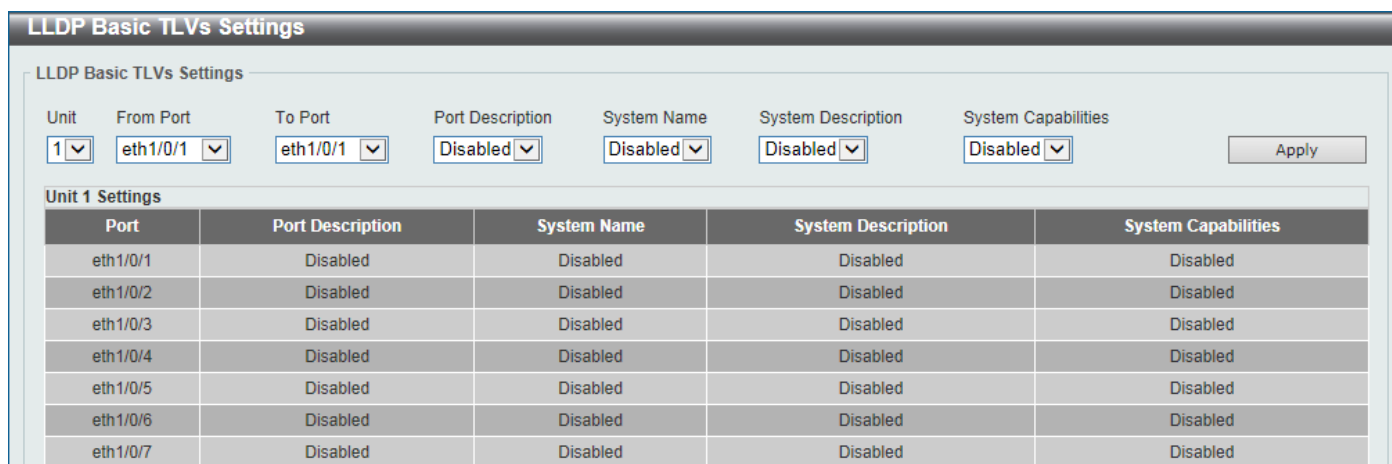
Parameter	Description
Subtype	Select the subtype. Options to choose from are All , IPv4 and IPv6 . After selecting the IPv4 option, enter the IPv4 address in the space provided. After selecting the IPv6 option, enter the IPv6 address in the space provided.

Click the **Find** button to locate a specific entry based on the selection made.

LLDP Basic TLVs Settings

The Type-Length-Value (TLV) field allows specific information to be sent within LLDP packets. This window is used to configure basic TLV settings. An active LLDP port on the Switch always includes mandatory data in its outbound advertisements. There are four optional data types that can be configured to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of TLVs: end of LLDPDU TLV, chassis ID TLV, port ID TLV, and TTL TLV. The mandatory data types cannot be disabled. There are also four data types which can be optionally selected. These include: Port Description, System Name, System Description and System Capability.

To view the following window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**, as shown below:



LLDP Basic TLVs Settings

LLDP Basic TLVs Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Port Description: Disabled System Name: Disabled System Description: Disabled System Capabilities: Disabled Apply

Unit 1 Settings

Port	Port Description	System Name	System Description	System Capabilities
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled

Figure 5-82 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

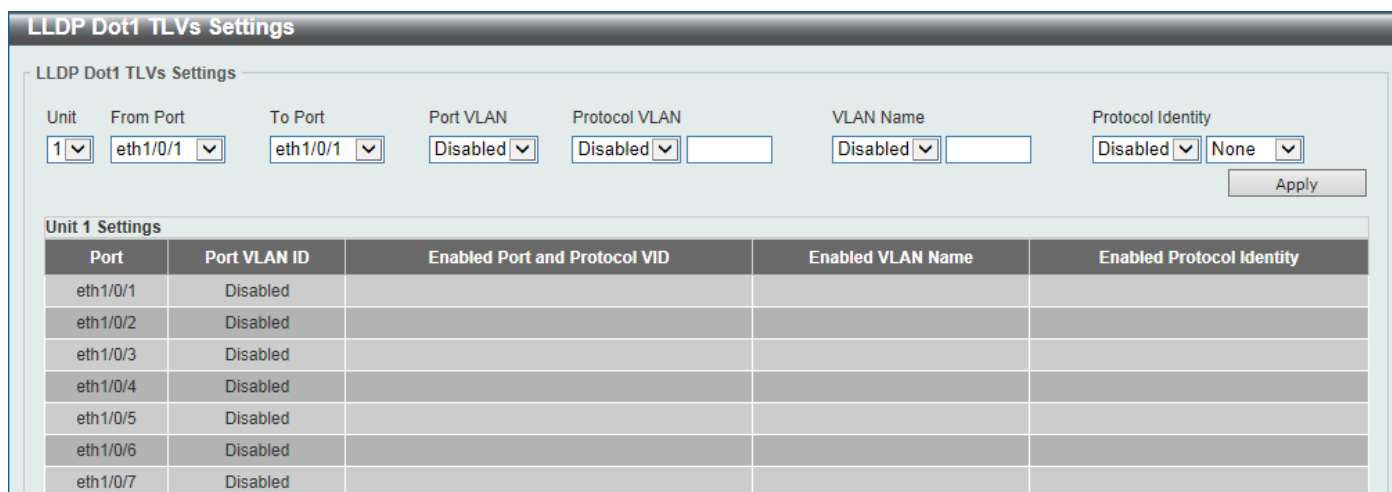
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Port Description	Select this option to enable or disable the Port Description option.
System Name	Select this option to enable or disable the System Name option.
System Description	Select this option to enable or disable the System Description option.
System Capabilities	Select this option to enable or disable the System Capabilities option.

Click the **Apply** button to accept the changes made.

LLDP Dot1 TLVs Settings

The LLDP Dot1 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.1 organizationally unique port VLAN ID TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**, as shown below:



LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Port VLAN: Disabled Protocol VLAN: Disabled VLAN Name: Disabled Protocol Identity: Disabled None Apply

Unit 1 Settings

Port	Port VLAN ID	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
eth1/0/1	Disabled			
eth1/0/2	Disabled			
eth1/0/3	Disabled			
eth1/0/4	Disabled			
eth1/0/5	Disabled			
eth1/0/6	Disabled			
eth1/0/7	Disabled			

Figure 5-83 LLDP Dot1 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Port VLAN	Select this option to enable or disable sending the port VLAN ID TLV. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port VLAN ID (PVID) that will be associated with untagged or priority tagged frames.
Protocol VLAN	Select this option to enable or disable sending the Port and Protocol VLAN ID (PPVID) TLV. Enter the VLAN ID in PPVID TLV.
VLAN Name	Select this option to enable or disable sending the VLAN name TLV. Enter the ID of the VLAN in the VLAN name TLV.
Protocol Identity	Select this option to enable or disable sending the Protocol Identity TLV and the protocol name. Options for protocol name to choose from are None , EAPOL , LACP , GVRP , STP , and All .

Click the **Apply** button to accept the changes made.

LLDP Dot3 TLVs Settings

The LLDP Dot3 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.3 organizationally unique TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**, as shown below:

LLDP Dot3 TLVs Settings

LLDP Dot3 TLVs Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 MAC/PHY Configuration/Status: Disabled Link Aggregation: Disabled Maximum Frame Size: Disabled Energy-Efficient Ethernet: Disabled Apply

Unit 1 Settings

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Energy-Efficient Ethernet
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled

Figure 5-84 LLDP Dot3 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
Link Aggregation	Select this option to enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an

Parameter	Description
	aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
Maximum Frame Size	Select this option to enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
Energy-Efficient Ethernet	Select this option to enable or disable the Energy Efficient Ethernet TLV to send. The Energy Efficient Ethernet TLV indicates the reduce energy consumption capability of a link when no packets are being sent.

Click the **Apply** button to accept the changes made.

LLDP-MED Port Settings

The LLDP-MED Port Settings page is used to enable or disable outbound LLDP advertisements for LLDP-MED TLVs.

To view the following window, click **L2 Features > LLDP > LLDP-MED Port Settings**, as shown below:

Unit	From Port	To Port	Notification	Capabilities	Inventory	Network Policy
1	eth1/0/1	eth1/0/1	Disabled	Disabled	Disabled	Disabled

Unit 1 Settings				
Port	Notification	Capabilities	Inventory	Network Policy
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled

Figure 5-85 LLDP-MED Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable transmitting the LLDP-MED notification TLV.
Capabilities	Select this option to enable or disable transmitting the LLDP-MED capabilities TLV.
Inventory	Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.
Network Policy	Select this option to enable or disable transmitting the LLDP-MED network policy TLV.

Click the **Apply** button to accept the changes made.

LLDP Statistics Information

This window is used to view the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch.

To view the following window, click **L2 Features > LLDP > LLDP Statistics Information**, as shown below:

Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
eth1/0/1	0	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0	0

Figure 5-86 LLDP Statistics Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used here.
Port	Select the port number that will be used here.

Click the **Clear Counter** button to clear the counter information for the statistics displayed.

Click the **Clear All** button to clear all the counter information displayed.

LLDP Local Port Information

This window is used to display the information currently available for populating outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Local Port Information**, as shown below:

Port	Port ID Subtype	Port ID	Port Description
------	-----------------	---------	------------------

Figure 5-87 LLDP Local Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be displayed.
Port	Select the port number that will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view detailed information of the specific port.

After clicking the **Show Detail** button, the following window will appear.



Figure 5-88 LLDP Local Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the [Show Detail](#) hyperlink. Click the **Back** button to return to the previous window.

After clicking the [Show Detail](#) hyperlink, a new section will appear at the bottom of the window.



Figure 5-89 LLDP Local Port Information (Show Detail) Window

Click the **Back** button to return to the previous window.

LLDP Neighbor Port Information

This window is used to display the LLDP information learned from neighboring switches. The Switch receives packets from a remote station but is able to store the information locally.

To view the following window, click **L2 Features > LLDP > LLDP Neighbor Port Information**, as shown below:

LLDP Neighbor Port Information

LLDP Neighbor Port Brief Table

Unit: 1 Port: eth1/0/1

Find Clear Clear All

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description
--------	--------------------	------------	-----------------	---------	------------------

Figure 5-90 LLDP Neighbor Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be displayed.
Port	Select the port number that will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear the specific port information.

Click the **Clear All** button to clear all the port information displayed.

6. Layer 3 Features

ARP

Gratuitous ARP

IPv6 Neighbor

Interface

UDP Helper

IPv4 Static/Default Route

IPv4 Route Table

IPv6 Static/Default Route

IPv6 Route Table

Route Preference

ECMP Settings

IPv6 General Prefix

RIP

RIPng

IP Route Filter

Policy Route

VRRP Settings

ARP

ARP Aging Time

This window is used to display and configure the ARP aging time settings.

To view the following window, click **L3 Features > ARP > ARP Aging Time**, as shown below:

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	After click the Edit button, enter the ARP aging timeout value here.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Static ARP

This window is used to display and configure the static ARP settings.

To view the following window, click **L3 Features > ARP > Static ARP**, as shown below:

Static ARP

Static ARP

IP Address: Hardware Address:

Interface Name	IP Address	Hardware Address	Aging Time	Type
----------------	------------	------------------	------------	------

Figure 6-2 Static ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Proxy ARP

This window is used to display and configure the Proxy ARP settings. The Proxy ARP feature will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP responder. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway. The host, usually a Layer 3 Switch, will respond to packets destined for another device.

To view the following window, click **L3 Features > ARP > Proxy ARP**, as shown below:

Proxy ARP

Proxy ARP

Total Entries: 1

Interface Name	Proxy ARP State	Local Proxy ARP State	
vlan1	Disabled	Disabled	<input type="button" value="Edit"/>

1/1 < < 1 > >

Figure 6-3 Proxy ARP Window

The fields that can be configured are described below:

Parameter	Description
Proxy ARP State	Select to enable or disable the Proxy ARP state here.
Local Proxy ARP State	Select to enable or disable the local Proxy ARP state here. This local Proxy ARP function allows the Switch to respond to the Proxy ARP, if the source IP and destination IP are in the same interface.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Table

This window is used to display and configure the ARP table settings.

To view the following window, click **L3 Features > ARP > ARP Table**, as shown below:

Figure 6-4 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. This value must be between 1 and 4094 .
IP Address	Select and enter the IP address to display here.
Mask	After the IP Address option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Type	Select the Type option here. Options to choose from are All and Dynamic .
Mgmt	Select this option to display the Management port information.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear All** button to clear all dynamic ARP cache.

Click the **Clear** button to clear the dynamic ARP cache associated with the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Gratuitous ARP

This window is used to display and configure the gratuitous ARP settings. A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.

Generally, a device uses the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

To view the following window, click **L3 Features > Gratuitous ARP**, as shown below:

Figure 6-5 Gratuitous ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Gratuitous ARP State	Select to enable or disable the learning of gratuitous ARP packets in the ARP cache table.
Gratuitous ARP Trap State	Select to enable or disable the gratuitous ARP feature trap state here.
IP Gratuitous ARP Dad-Reply State	Select to enable or disable the IP gratuitous ARP Dad-reply state.
Gratuitous ARP Learning State	Select to enable or disable the gratuitous ARP learning state. Normally, the system will only learn ARP entries from ARP reply packets or a normal ARP request packet that asks for the MAC address of the Switch IP address. This option used to enable or disable the learning of ARP entries based on received gratuitous ARP packets. The gratuitous ARP packet is sent by a source IP address and is identical to the IP that the packet is querying.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the field that can be configured for **Gratuitous ARP Send Interval** is described below:

Parameter	Description
Interval Time	Enter the gratuitous ARP sending interval time, in seconds, here.

Click the **Apply** button to accept the changes made.

IPv6 Neighbor

This window is used to display and configure the IPv6 neighbor settings.

To view the following window, click **L3 Features > IPv6 Neighbor**, as shown below:

Figure 6-6 IPv6 Neighbor Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information for the specific interface.

Click the **Clear All** button to clear all the dynamic IPv6 neighbor information in this table.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Interface

IPv4 Interface

This window is used to display and configure the IPv4 interface settings.

To view the following window, click **L3 Features > Interface > IPv4 Interface**, as shown below:

Figure 6-7 IPv4 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. This value must be between 1 and 4094.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will be available.

Figure 6-8 IPv4 Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.
IP MTU	Enter the MTU value here. The range is from 512 to 16383 bytes. By default, this value is 1500 bytes.
IP Directed Broadcast	Select to enable or disable the IP directed broadcast feature here. This parameter is used to enable or disable the conversion of IP directed broadcasts received by the interface to physical broadcasts when the destination network is directly connected to the Switch.
Description	Enter the description for this entry here. This string can be up to 64 characters long.
Get IP From	Select the get IP from option here. Options to choose from are Static and DHCP . <ul style="list-style-type: none"> When the Static option is selected, users can enter the IPv4 address of this interface manually in the fields provided. When the DHCP option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for this interface here.
Mask	Enter the IPv4 subnet mask for this interface here.
Secondary	Tick this option to use the IPv4 address and mask as the secondary interface configuration.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After selecting the **DHCP Client** tab, the following page will appear.

Figure 6-9 IPv4 Interface (Edit, DHCP Client) Window

The fields that can be configured are described below:

Parameter	Description
DHCP Client Client-ID	Enter the DHCP Client ID here. The range is from 1 to 4094. This parameter is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message.
Class ID String	Enter the class ID string here. This string can be up to 32 characters long. Select the Hex option to enter the Class ID string in the hexadecimal format. This string can be up to 64 characters long. This parameter is used to specify the vendor class identifier used as the value of Option 60 in the DHCP discover message.
Host Name	Enter the host name here. This string can be up to 64 characters long. This parameter is used to specify the value of the host name option to be sent with the DHCP discover message.
Lease	Enter and optionally select the DHCP client lease time here. In the text box the lease time, in days, can be entered. The range is from 0 to 10000 days. Hours and Minutes can also be selected optionally.

Click the **Apply** button to accept the changes made.

IPv6 Interface

This window is used to display and configure the IPv6 interface settings.

To view the following window, click **L3 Features > Interface > IPv6 Interface**, as shown below:

Figure 6-10 IPv6 Interface Window

The fields that can be configured in **IPv6 Interface** are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID that will be associated with the IPv6 entry.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view and configure more detailed settings for the IPv6 interface entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will be available.

Figure 6-11 IPv6 Interface (Detail, IPv6 Interface Settings) Window

The fields that can be configured are described below:

Parameter	Description
IPv6 MTU	Enter the IPv6 MTU value here. The range is from 1280 to 65534 bytes. By default, this value is 1500 bytes. This parameter is used to configure the MTU to be advertised in RA messages.
IPv6 State	Select to enable or disable the IPv6 interface global state here.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **IPv6 Address Autoconfig** are described below:

Parameter	Description
State	Select to enable or disable the automatic configuration of the IPv6 address using stateless auto-configuration here. Select the Default option to specify that if the default router is selected on this interface, a default route will be installed using that default router. This option can only be specified on one interface.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Static IPv6 Address Settings** are described below:

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here. Select the EUI-64 option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the Link Local option to configure a link-local address for the IPv6 interface.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **NS Interval Settings** are described below:

Parameter	Description
NS Interval	Enter the Neighbor Solicitation (NS) interval value here. The range is from 0 to 3600000 milliseconds, in multiples of 1000. If the specified time is 0, the router will use 1 second on the interface and advertise 0 (unspecified) in the Router Advertisement (RA) message.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **ND Settings** are described below:

Parameter	Description
Hop Limit	Enter the hop limit value here. The range is from 0 to 255. The IPv6 packet originated by the system will also use this value as the initial hop limit.
Reachable Time	Enter the Reachable Time here. The range is from 0 to 3600000 milliseconds. If the specified time is 0, the router will use 1200 seconds on the interface and advertise 1200 (unspecified) in the RA message. The Reachable Time is used by the IPv6 node in determining the reachability of the neighbor nodes.
Managed Config Flag	Turn the Managed Config Flag option On or Off here. When the neighbor host receives the RA which has flag turned on, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Turn the Other Config Flag option On or Off here. By setting the other configuration flag on, the router instructs the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than the IPv6 address.
RA Min Interval	Enter the minimum RA interval time value here. The range is from 3 to 1350 seconds. This value must be smaller than 0.75 times the maximum value.
RA Max Interval	Enter the maximum RA interval time value here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA instructs the received host the lifetime value for taking the router as the default router.
RA Suppress	Select to enable or disable the RA suppress feature here.

Click the **Apply** button to accept the changes made.

After selecting the **Interface IPv6 Address** tab option, at the top of the page, the following page will be available.

The screenshot shows the 'IPv6 Interface' configuration window. At the top, there are four tabs: 'IPv6 Interface Settings', 'Interface IPv6 Address' (which is selected), 'Neighbor Discover', and 'DHCPv6 Client'. Below the tabs, it says 'Total Entries: 0'. There is a table with two columns: 'Address Type' and 'IPv6 Address'. The table is currently empty.

Figure 6-12 IPv6 Interface (Detail, Interface IPv6 Address) Window

Click the **Delete** button to delete the specified entry.

After selecting the **Neighbor Discover** tab option, at the top of the page, the following page will be available.

Figure 6-13 IPv6 Interface (Detail, Neighbor Discover) Window

After selecting the **DHCPv6 Client** tab option, at the top of the page, the following page will be available.

Figure 6-14 IPv6 Interface (Detail, DHCPv6 Client) Window

Click the **Restart** button to restart the DHCPv6 client service.

The fields that can be configured for **DHCPv6 Client Settings** are described below:

Parameter	Description
Client State	Select to enable or disable the DHCPv6 client service here. Select the Rapid Commit option to proceed with two-message exchange for address delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **DHCPv6 Client PD Settings** are described below:

Parameter	Description
Client PD State	Select to enable or disable the DHCPv6 client process that requests a Prefix Delegation (PD) through a specified interface. Select the Rapid Commit option to proceed with two-message exchange for prefix delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.
General Prefix Name	Enter the IPv6 general prefix name here. This name can be up to 12 characters long.

Click the **Apply** button to accept the changes made.

Loopback Interface

This window is used to display and configure the loopback interface settings. A loopback interface is a software only interface which always stays in the up status.

To view the following window, click **L3 Features > Interface > Loopback Interface**, as shown below:

Figure 6-15 Loopback Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface Loopback	Enter the loopback interface ID here. The range is from 1 to 8.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify the specified entry.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

Figure 6-16 Loopback Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the loopback interface here.
Description	Enter the description for the loopback interface here. This string can be up to 64 characters long.
IP Address	Enter the IPv4 address associated with this loopback interface here.
Mask	Enter the IPv4 subnet mask associated with this loopback interface here.
IPv6 Address	Enter the IPv6 address associated with this loopback interface here.
Link Local	Select this option to specify that the IPv6 address entered is the link-local IPv6 address.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Null Interface

This window is used to display and configure the Null interface settings.

To view the following window, click **L3 Features > Interface > Null Interface**, as shown below:

Interface	State	Link Status	Description
null0	Enabled	Link Up	<button>Edit</button>

Figure 6-17 Null Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface Null	Enter the Null interface ID here. This value can only be 0.
Description	After clicking the Edit button, enter the description for the Null interface here. This string can be up to 64 characters long.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to modify the description for the Null interface.

UDP Helper

IP Forward Protocol

This window is used to display and configure the IP forward protocol settings. This feature is used to enable the forwarding of a specific UDP service type of packets.

To view the following window, click **L3 Features > UDP Helper > IP Forward Protocol**, as shown below:

UDP Port	Application	Delete
37	Time Service	<button>Delete</button>
42	IEN-116 Name Service	<button>Delete</button>
49	TACACS	<button>Delete</button>
53	DNS	<button>Delete</button>
69	TFTP	<button>Delete</button>
137	NetBIOS-NS	<button>Delete</button>
138	NetBIOS-DS	<button>Delete</button>

Figure 6-18 IP Forward Protocol Window

The fields that can be configured are described below:

Parameter	Description
IP Forward Protocol UDP Port	Enter the destination port of the UDP service to be forwarded here. The range is from 1 to 65535.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IP Helper Address

This window is used to add or remove a target address for the forwarding of UDP broadcast packets. This feature takes effect only when the received interface has an IP address assigned.

The system only forwards packets that satisfy the following restrictions:

- The destination MAC address must be a broadcast address.
- The destination IP address must be an all-one broadcast.
- The packets are IPv4 UDP packets.
- The IP TTL value must be greater than or equal to 2.

To view the following window, click **L3 Features > UDP Helper > IP Helper Address**, as shown below:

Figure 6-19 IP Helper Address Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
Helper Address	Enter the target IPv4 address for the forwarding of the UDP broadcast packet here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv4 Static/Default Route

This window is used to display and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 formatted addressing. Users can create up to 512 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route with a different next hop. This secondary next hop device route is considered as a backup static route when the primary static route is down. If the primary route is lost, the backup route will become active and begin forwarding traffic.

Entries into the Switch's forwarding table can be made using an IP address, subnet mask and gateway.

To view the following window, click **L3 Features > IPv4 Static/Default Route**, as shown below:

Figure 6-20 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address for this route here. Tick the Default Route option to use the default route as the IPv4 address.
Mask	Enter the IPv4 network mask for this route here.
IP Tunnel	Select the IP Tunnel option to use the IP tunnel feature and enter the tunnel ID in the space provided. The range of IDs is from 0 to 9999.
Gateway	Enter the gateway address for this route here.
Null Interface	Select to enable or disable the NULL interface here.
Backup State	Select the backup state option here. <ul style="list-style-type: none"> • Weight - Specifies a weight number greater than zero, but less than the maximum paths number. This number is used to replicate identical route paths (multiple copies) in the routing table, so the paths get more chance of being hit for traffic routing. If the weight number is not specified for the static route, the default for the path exists in the hashing table. Enter the weight value in the space provided. The range is from 1 to 64.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv4 Route Table

This window is used to display and configure the IPv4 route table settings.

To view the following window, click **L3 Features > IPv4 Route Table**, as shown below:

Figure 6-21 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
RIP	Select this option to display only RIP routes.
Connected	Select this option to display only connected routes.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Static/Default Route

This window is used to display and configure the IPv6 static or default routes.

To view the following window, click **L3 Features > IPv6 Static/Default Route**, as shown below:

Figure 6-22 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the Default Route option to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Distance	Enter the administrative distance of the static route here. This value must be between 1 and 254 . A lower value represents a better route. If not specified, the default administrative distance for a static route is 1 .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Route Table

This window is used to display and configure the IPv6 route table.

To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:

Figure 6-23 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address to display here.
IPv6 Address/Prefix Length	Select and enter the IPv6 address and prefix length to display here. Select the Longer Prefixes option to display the route and all of the more specific routes.
Interface Name	Select and enter the name of the interface to display here.
Connected	Select this option to display only connected routes.
RIPng	Select this option to display only RIPng routes.
Database	Select this option to display all the related entries in the routing database instead of just the best route.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

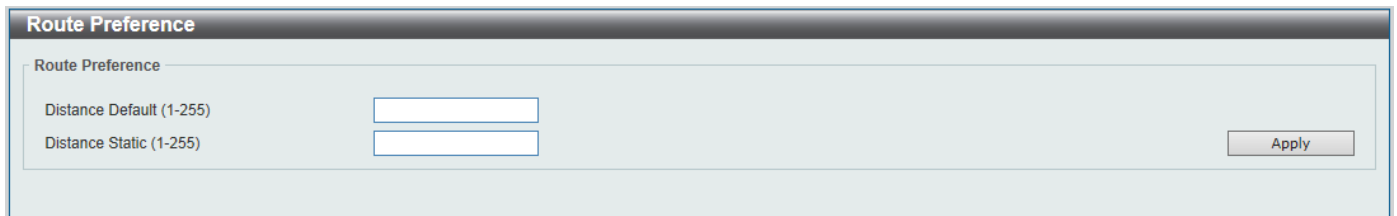
Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Route Preference

This window is used to display and configure the route preference settings. Use this window to configure the distance, which represents the route's trust rating. The route with a lower distance value is preferred over the route with a higher distance value. A route with the distance 255 will not be installed for routing of packets since it indicates that the route is not trusted.

To view the following window, click **L3 Features > Route Preference**, as shown below:



The screenshot shows the 'Route Preference' window. It has a title bar 'Route Preference' and a sub-header 'Route Preference'. Below the header, there are two input fields: 'Distance Default (1-255)' and 'Distance Static (1-255)'. An 'Apply' button is located on the right side of the window.

Figure 6-24 Route Preference Window

The fields that can be configured are described below:

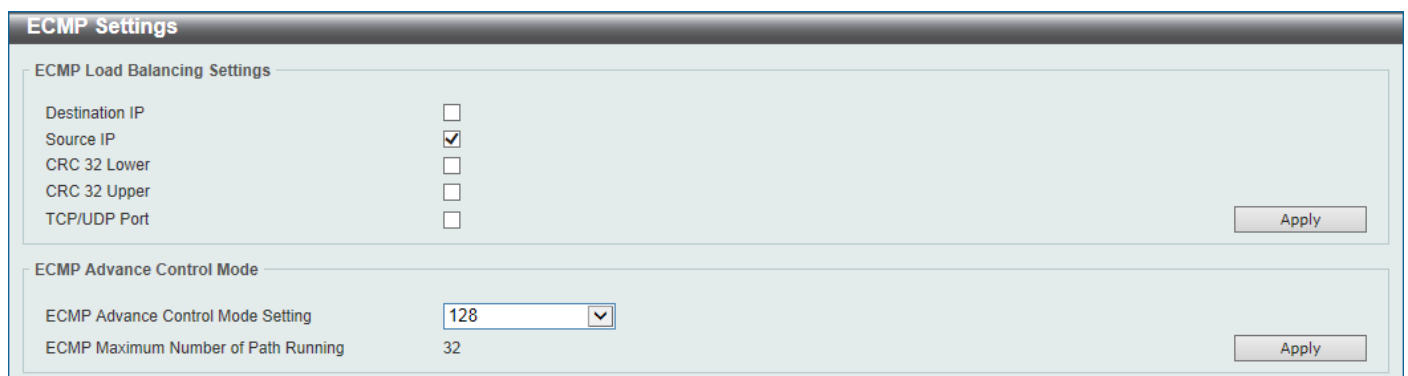
Parameter	Description
Distance Default	Enter the administrative distance of default routes here. The range is from 1 to 255. By default, this value is 1.
Distance Static	Enter the administrative distance of static default routes here. The range is from 1 to 255. By default, this value is 60.

Click the **Apply** button to accept the changes made.

ECMP Settings

This window is used to display and configure the Equal-Cost Multi-Path (ECMP) routing settings. This is used to configure the load balancing hash algorithm and used to determine the next hop entry for multiple paths destined for the same destination.

To view the following window, click **L3 Features > ECMP Settings**, as shown below:



The screenshot shows the 'ECMP Settings' window. It has a title bar 'ECMP Settings' and a sub-header 'ECMP Load Balancing Settings'. Below the header, there are five checkboxes: 'Destination IP', 'Source IP' (checked), 'CRC 32 Lower', 'CRC 32 Upper', and 'TCP/UDP Port'. An 'Apply' button is on the right. Below this section is the 'ECMP Advance Control Mode' section, which contains two fields: 'ECMP Advance Control Mode Setting' (a dropdown menu showing '128') and 'ECMP Maximum Number of Path Running' (a text field showing '32'). Another 'Apply' button is at the bottom right.

Figure 6-25 ECMP Settings Window

The fields that can be configured in **ECMP Load Balancing Settings** are described below:

Parameter	Description
Destination IP	Select this option to use the destination IP address as the ECMP hash key.
Source IP	Select this option to use the least significant bits of the source IP address as the ECMP hashing algorithm.
CRC 32 Lower	Select this option to use the lower bits of CRC-32 as the ECMP hashing algorithm.
CRC 32 Upper	Select this option to use the upper bits of CRC-32 as the ECMP hashing algorithm.
TCP/UDP Port	Select this option to use TCP/UDP port number as ECMP hash key.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **ECMP Advance Control Mode** are described below:

Parameter	Description
ECMP Advance Control Mode Setting	Select the ECMP advance control mode settings here. This specifies the number of ECMP or multipath routes and the number of next-hops of each ECMP or multipath route that will be changed according to the specified value. Options to choose from are 64 , 128 , 256 , and 512 .

Click the **Apply** button to accept the changes made.

IPv6 General Prefix

This window is used to display and configure the VLAN interface IPv6 general prefix settings.

To view the following window, click **L3 Features > IPv6 General Prefix**, as shown below:

Figure 6-26 IPv6 General Prefix Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
Prefix Name	Enter the IPv6 general prefix entry name here. This name can be up to 12 characters long.
IPv6 Address	Enter the IPv6 address and prefix length here. The prefix length of the IPv6 address is also the local subnet on the VLAN interface.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **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.

RIP

RIP Settings

This window is used to display and configure Routing Information Protocol (RIP) settings.

To view the following window, click **L3 Features > RIP > RIP Settings**, as shown below:

RIP Settings

RIP Global Settings

RIP State ☒ Enabled ☐ Disabled Apply

Redistribution Configuration

Redistribution Disabled Connected metric (0-16) route-map (16 chars) Apply

RIP Configuration

Update Time (1-65535) 30 sec ☐ Default

Invalid Time (1-65535) 180 sec ☐ Default

Flush Time (1-65535) 120 sec ☐ Default

Default Metric (1-16) 0 ☐ Default

Version v1 ☐ Default

Distance (1-255) 100 ☐ Default

Send Version v1

Receive Version any version

Next Update 28

Redistribution Disabled Apply

Routing Information Sources

Gateway	Last Update
---------	-------------

Figure 6-27 RIP Settings Window

The fields that can be configured in **RIP Global Settings** are described below:

Parameter	Description
RIP State	Select to globally enable or disable the Routing Information Protocol (RIP) feature here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Click the **Back** button to return to the previous window.

The fields that can be configured in **Redistribution Configuration** are described below:

Parameter	Description
Redistribution	<ul style="list-style-type: none"> First, select to enable or disable the RIP redistribution feature here. Second, select the routing protocol (domain) that will be redistributed into RIP. Options to choose from are Connected and Static. The Static option means redistribute IP static routes. The Connected option refers to routes that are established automatically through configuring an IP address on an interface. Third, enter the value to be used as the metric for the redistributed route here. The range is from 0 to 16. Fourth, enter the Route Map name that is used in the filtering of the routes to be redistributed to the current routing protocol. If not specified, all routes are redistributed.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RIP Configuration** are described below:

Parameter	Description
Update Time	Enter the update interval in seconds at which the update message is sent. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 30 seconds.
Invalid Time	Enter the invalid time value in seconds here. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 180 seconds.
Flush Time	Enter the flush time value in seconds here. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 120 seconds.
Default Metric	Enter the default metric value here. The range is from 1 to 16. The default metric is used in redistributing routes from other routing protocols. The routes being redistributed are learned by other protocols and may have an incompatible metric to RIP. The specifying of the metric allows the metric to be synced. Select the Default option to use the default metric value, which is 0.
Version	Select the global RIP version that will be used as the default version for all interfaces here. Options to choose from are v1 (RIPv1) and v2 (RIPv2). Select the Default option to specify that this feature should use the default configuration. By default, RIPv1 and RIPv2 packets are received, but only RIPv1 packets are sent.
Distance	Enter the Administrative Distance for RIP here. The range is from 1 to 255. A lower value represents a better route. Select the Default option to use the default Administrative Distance for RIP, which is 100.

Click the **Apply** button to accept the changes made.

RIP Distribute List

This window is used to display and configure the RIP distribution list settings.

To view the following window, click **L3 Features > RIP > RIP Distribute List**, as shown below:

Figure 6-28 RIP Distribute List Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access list name that will be used here. This name can be up to 32 characters long.
Interface Name	Enter the interface name that will be used here. This name can be up to 12 characters long.

Click the **Apply** button to accept the changes made.

Click the **Show Detail** button to view more detailed information about the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

RIP Interface Settings

This window is used to display and configure the RIP interface settings.

To view the following window, click **L3 Features > RIP > RIP Interface Settings**, as shown below:

Figure 6-29 RIP Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Network	Enter the IPv4 network address used by RIP here. Interfaces that have a subnet belonging to the network specified here will be activated for RIP.
Passive Interface	<p>Select to enable or disable the passive interface feature here. This feature is used to disable the sending and receiving of routing updates on an interface. However, RIP packets from other routers received on this interface will continue to be processed.</p> <p>Enter the name of the passive interface in the space provided. This name can be up to 12 characters long.</p> <p>Select the Default option to use this as the default for all interfaces.</p>

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an entry based on the information entered.

RIP Database

This window is used to display the Routing Information Protocol (RIP) routing database. Summary address entries will appear in the database only if relevant child routes exist and are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

To view the following window, click **L3 Features > RIP > RIP Database**, as shown below:

Figure 6-30 RIP Database Window

The fields that can be configured are described below:

Parameter	Description
Network Address	Enter the subnet prefix and the prefix length of the network(s) to be displayed here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

RIPng

RIPng Settings

This window is used to display and configure the Routing Information Protocol Next Generation (RIPng) settings, also known as IPv6 RIP.

To view the following window, click **L3 Features > RIPng > RIPng Settings**, as shown below:

Figure 6-31 RIPng Settings Window

The fields that can be configured in **RIPng Global Settings** are described below:

Parameter	Description
Global State	Select to globally enable or disable the RIPng feature here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RIPng Settings** are described below:

Parameter	Description
Default Metric	Enter the default metric value here. The range is from 1 to 16. This value is used to specify the default metric for routes redistributed from other routing protocols. If the routes being redistributed are learned from other protocols, then they have an incompatible metric with IPv6 RIP. Re-specifying of metric allows the metric to be synced. Select the Default option to use the default metric value, which is 1.
Distance	Enter the administrative distance for RIPng here. The range is from 1 to 254. The distance value represents the trust rating of the route. The route with a lower distance value is preferred over the route with the higher distance value.

Parameter	Description
	A route with a distance of 255 will not be installed for the routing of packets since it indicates that the route is not trusted. Select the Default option to use the default administrative distance for RIPng, which is 120.
Update Time	Enter the update interval value at which the update message is sent here. The range is from 5 to 65535 seconds. Select the Default option to use the default value here which is 30 seconds.
Invalid Time	Enter the invalidate timer value in seconds here. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 180 seconds.
Flush Time	Enter the flush timer value in seconds here. The range is from 1 to 65535 seconds. Select the Default option to use the default value here which is 120 seconds.
Poison Reverse	Select to enable or disable the Poison Reverse feature here. When Poison Reverse is enabled, the routes learned from an interface will be advertised out to the same interface with an unreachable metric.
Split Horizon	Select to enable or disable the Split Horizon feature here. When Split Horizon is enabled, the routes learned from an interface will be not advertised out to the same interface.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Redistribute Settings** are described below:

Parameter	Description
Protocol	Select the protocol whose routes are to be redistributed here. Options to choose from are Connected and Static . The Static option means to redistribute IPv6 static routes. The Connected option refers to routes that are established automatically by virtue of configuring IPv6 address on an interface.
Metric	Enter the value to be used as the metric for the redistributed routes here. The range is from 0 to 16. Select the Default option to use the default metric value.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an entry based on the information entered.

RIPng Interface Settings

This window is used to display and configure the RIPng interface settings.

To view the following window, click **L3 Features > RIPng > RIPng Interface Settings**, as shown below:

Figure 6-32 RIPng Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094. Select the All Interface option to use all available interfaces in this configuration.
State	Select to enable or disable the IPv6 RIP feature on the VLAN interface specified.
Metric Offset	Enter the value to be added to the metric of an IPv6 RIP route received on the configured interface here. The range is from 1 to 16. The metric refers to the hop count. By default, when receiving an IPv6 RIP route, a metric value of 1 is added to the route before it is inserted into the routing table. Use this option to influence the metric of routes received on different interfaces and influence the preference of the route. Select the Default option to use the default metric offset value, which is 1.
Passive Interface	Select to enable or disable the passive interface feature here. If this option is disabled, the router will not send RIPng packets out through the interface. However, RIPng packets from other routers received on the interface will continue to be processed.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

RIPng Database

This window is used to display the RIPng routing database.

To view the following window, click **L3 Features > RIPng > RIPng Database**, as shown below:

Figure 6-33 RIPng Database Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address that will be used for these results here.

Click the **Find** button to locate a specific entry based on the information entered.

IPMC

Control Packet CPU Filtering

This window is used to display and configure the IPMC control packet CPU filtering settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPMC > Control Packet CPU Filtering**, as shown below:

Control Packet CPU Filtering

Control Packet CPU Filtering Settings

Unit: 1, From Port: eth1/0/1, To Port: eth1/0/1, Packet Type: DVMRP, Action: Add, Apply

Control Packet CPU Filtering Table

Unit: 1, From Port: eth1/0/1, To Port: eth1/0/1, Find

Port	Filter Packet
eth1/0/11	DVMRP

Figure 6-34 Control Packet CPU Filtering Window

The fields that can be configured in **Control Packet CPU Filtering Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Packet Type	Select the packet type here. Options to choose from are: <ul style="list-style-type: none"> • DVMRP - Specifies that the CPU will discard DVMRP Layer 3 control packets sent to it. • PIM - Specifies that the CPU will discard PIM Layer 3 control packets sent to it. • IGMP Query - Specifies that the CPU will discard IGMP Query Layer 3 control packets sent to it. • OSPF - Specifies that the CPU will discard OSPF Layer 3 control packets sent to it. • RIP - Specifies that the CPU will discard RIP Layer 3 control packets sent to it. • VRRP - Specifies that the CPU will discard VRRP Layer 3 control packets sent to it.
Action	Select the action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> • Add - Specifies to add a new entry based on the information entered. • Delete - Specifies to delete an entry based on the information entered.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Control Packet CPU Filtering Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here.
From Port - To Port	Select the range of ports that will be used for this display here.

Click the **Find** button to find and display entries based on the selections made.

IP Route Filter

Route Map

This window is used to display and configure the route map settings.

To view the following window, click **L3 Features > IP Route Filter > Route Map**, as shown below:

Figure 6-35 Route Map Window

The fields that can be configured are described below:

Parameter	Description
Route Map Name	Enter the route map name here. This name can be up to 16 characters long.
Direction	Select the direction for this rule here. Options to choose from are Permit and Deny . <ul style="list-style-type: none"> Permit - Specifies that routes that match the rule entry are permitted. Deny - Specifies that routes that match the rule entry are denied.
Sequence ID	Enter the sequence ID for this rule here. The range is from 1 to 65535.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify the specified entry.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button in the **Match Clauses** column, the following page will appear.

Figure 6-36 Route Map (Match Clauses, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.

Parameter	Description
Interface Name	Select and enter the interface name that will be used here. This option is used to define a clause to match the route's outgoing interface.
IP Address ACL	Select and enter the standard or extended IP access list name here. This option is used to define a clause to match the route based on the standard or extended IP access list. This string can be up to 32 characters long.
IP Next Hop ACL	Select and enter the standard IP access list name here. This option is used to define a clause to match the route's next hop based on the standard IP access list. This string can be up to 32 characters long.
Route Source	Select and enter the standard or extended IP/IPv6 access list name here. This option is used to define a clause to match the route's source based on the standard or extended IP/IPv6 access list. This string can be up to 32 characters long.
Metric	Select and enter the metric value of the route here. The range is from 0 to 4294967294. This option is used to define a clause to match the route metric.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

After clicking the **Edit** button in the **Set Clauses** column, the following page will appear.

Figure 6-37 Route Map (Set Clauses, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select Add to add a new entry based in the information entered. Select Delete to delete an entry based in the information entered.
IP Default Next Hop	Enter the default next-hop IP addresses in the spaces provided that will be used to route the packet. This feature can be used to specify multiple default next hop routers. If default next hops are already configured, the default next hops configured later will be added to the default next hop list. When the first default next hop router specified is down, the next default next hop router specified is tried in turn to route the packet. Up to 8 default next-hop IP addresses can be entered.
IP Next Hop	Select the IP next hop type here. This feature is used to configure the next-hop router to route the packet that passes the match clauses of the configured route map sequence. Options to choose from are IP Address , Peer Address , and Recursive . <ul style="list-style-type: none"> IP Address - Specifies the IP addresses of the next-hops to route the packet. Enter the next-hop IP addresses in the spaces provided here. Up to 8 next-hop IP addresses can be entered.

Parameter	Description
	<ul style="list-style-type: none"> • Peer Address - Specifies the BGP peer address as the next-hop. • Recursive - Specifies the IP address of the recursive as the next-hop router. Enter the recursive next-hop IP address in the space provided here.
IP Precedence	Select the IP precedence option here. Options to choose from are Routine , Priority , Immediate , Flash , Flash Override , Critical , Internet , and Network . Use this feature to set the precedence value in the IP header. This option only takes effect when policy routing involves the IPv4 packet.
Metric	Select and enter the metric value here that will be used in the modification. The range is from 0 to 4294967294.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

Policy Route

This window is used to display and configure the policy route settings.

To view the following window, click **L3 Features > Policy Route**, as shown below:

The screenshot shows the 'Policy Route' window. At the top, it says 'Policy Route'. Below that, 'Total Entries: 1'. There is a table with two columns: 'Interface Name' and 'Route Map'. The first row shows 'vian1' under 'Interface Name' and an empty space under 'Route Map'. To the right of the table is an 'Edit' button. At the bottom right, there are navigation buttons: '1/1', '<', '<<', '1', '>>', '>', and a 'Go' button.

Figure 6-38 Policy Route Window

Click the **Edit** button to modify the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

The screenshot shows the 'Policy Route (Edit)' window. It has the same layout as Figure 6-38, but the 'Edit' button has been replaced by an 'Apply' button. The 'Route Map' column is now an empty text input field. The navigation buttons at the bottom right remain the same.

Figure 6-39 Policy Route (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Route Map	Enter the route map name here that will be used in this policy route entry.

Click the **Apply** button to accept the changes made.

VRRP Settings

This window is used to display and configure the Virtual Router Redundancy Protocol (VRRP) settings. All routers in the same VRRP group must be configured with the same virtual router ID and IP address.

A virtual router group is represented by a virtual router ID. The IP address of the virtual router is the default router configured on hosts. The virtual router's IP address can be a real address configured on the routers, or an unused IP address. If the virtual router address is a real IP address, the router that has this IP address is the IP address owner.

A master will be elected in a group of routers that supports the same virtual routers. Others are the backup routers. The master is responsible for forwarding the packets that are sent to the virtual router.

To view the following window, click **L3 Features > VRRP Settings**, as shown below:

Figure 6-40 VRRP Settings Window

The fields that can be configured in **VRRP Settings** are described below:

Parameter	Description
SNMP Server Traps VRRP New master	Select to enable or disable the SNMP server traps feature for the new VRRP master. If enabled, once the device has transitioned to the master state, a trap will be sent out.
SNMP Server Traps VRRP Auth Fail	Select to enable or disable the SNMP server traps feature for authentication failures. If enabled, if a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type, then a trap will be sent out.
Non-owner-ping Response	Select to enable or disable the non-owner ping response feature here. This feature is used to enable the virtual router in the master state to respond to ICMP echo requests for an IP address not owned but associated with this virtual router.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Virtual Router Settings** are described below:

Parameter	Description
VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
VRID	Enter the virtual router ID used here. This ID is used to identify the virtual router in the VRRP group. The range is from 1 to 255.

Parameter	Description
Virtual IP Address	Enter the IPv4 address for the created virtual router group here.
VRRP Authentication	Select to enable and then enter the plain text authentication password for VRRP authentication on the interface here. This string can be up to 8 characters long. The authentication is applied to all virtual routers on this interface. The devices in the same VRRP group must have the same authentication password.
Interface Name	Enter the interface name used here. This name can be up to 12 characters long.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify the specified entry.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

Figure 6-41 VRRP Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Advertisement Interval	Enter the advertisement interval value here. This is the time interval between successive VRRP advertisements by the master router. The range is from 1 to 255 seconds. By default, this value is 1 second.
Preemption	Select to enable or disable the preemption feature here. This feature is used to allow a router to take over the master role if it has a better priority than the current master.
Priority	Enter the priority value here. The range is from 1 to 254.
Critical IP Address	Enter the critical IPv4 address here. If the critical IP is configured on one virtual router, the virtual router cannot be activated when the critical IP address is unreachable. One VRRP group can only track one critical IP.
Shutdown	Select to enable or disable the shutdown feature here. This feature is used to disable a virtual router on an interface. Avoid the common mistake of shutting down the IP address owner router before shutting down other non-owner routers.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

7. Quality of Service (QoS)

Basic Settings
Advanced Settings
WRED

Basic Settings

Port Default CoS

This window is used to display and configure the port default CoS settings.

To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:

Port	Default CoS	Override
eth1/0/1	0	No
eth1/0/2	0	No
eth1/0/3	0	No
eth1/0/4	0	No
eth1/0/5	0	No
eth1/0/6	0	No

Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7. Select the Override option to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port. Select the None option to specify that the CoS of the packets will be the packet's CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.

Click the **Apply** button to accept the changes made.

Port Scheduler Method

This window is used to display and configure the port scheduler method settings. To view the following window, click **QoS > Basic Settings > Port Scheduler Method**, as shown below:

Port Scheduler Method

Port Scheduler Method

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Scheduler Method: WRR [Apply]

Unit 1 Settings

Port	Scheduler Method
eth1/0/1	WRR
eth1/0/2	WRR
eth1/0/3	WRR
eth1/0/4	WRR
eth1/0/5	WRR
eth1/0/6	WRR
eth1/0/7	WRR

Figure 7-2 Port Scheduler Method Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Scheduler Method	<p>Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (SP), Round-Robin (RR), Weighted Round-Robin (WRR), and Weighted Deficit Round-Robin (WDRR). By default, the output queue scheduling algorithm is WRR.</p> <ul style="list-style-type: none"> • Strict Priority (SP) specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest. • Round-Robin (RR) specifies that all queues use round-robin scheduling. It provides fair access to service a single packet at each queue before moving on to the next one. • Weighted Round-Robin (WRR) operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time. • Weighted Deficit Round-Robin (WDRR) operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration. <p>To set a CoS queue in the SP mode, any higher priority CoS queue must also be in the strict priority mode.</p>

Click the **Apply** button to accept the changes made.

Queue Settings

This window is used to display and configure the queue settings.

To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:

Port	Queue ID	WRR Weight	WDRR Quantum
eth1/0/1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1
eth1/0/2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1

Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Enter the queue ID value here. This value must be between 0 and 7.
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0 and 127.

Click the **Apply** button to accept the changes made.

CoS to Queue Mapping

This window is used to display and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:

CoS	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Apply

Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7.

Click the **Apply** button to accept the changes made.

Port Rate Limiting

This window is used to display and configure the port rate limiting settings.

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:

Port Rate Limiting					
Unit	From Port	To Port	Direction	Rate Limit	
1	eth1/0/1	eth1/0/1	Input	<input checked="" type="radio"/> Bandwidth (8-10000000) <input type="text"/> Kbps <input type="radio"/> Percent (1-100) <input type="text"/> % <input type="radio"/> None	Burst Size (0-128000) <input type="text"/> Kbyte Burst Size (0-128000) <input type="text"/> Kbyte Apply
Unit 1 Settings					
Port	Input		Output		
	Rate	Burst	Rate	Burst	
eth1/0/1	No Limit	No Limit	No Limit	No Limit	
eth1/0/2	No Limit	No Limit	No Limit	No Limit	
eth1/0/3	No Limit	No Limit	No Limit	No Limit	
eth1/0/4	No Limit	No Limit	No Limit	No Limit	
eth1/0/5	No Limit	No Limit	No Limit	No Limit	
eth1/0/6	No Limit	No Limit	No Limit	No Limit	

Figure 7-5 Port Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are Input and Output . When Input is selected, the rate limit for ingress packets is configured. When Output is selected, the rate limit for egress packets is configured.
Rate Limit	Select and enter the rate limit value here.

Parameter	Description
	<ul style="list-style-type: none"> When Bandwidth is selected, enter the input/output bandwidth value used in the space provided. This value must be between 8 and 10000000 kbps. Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes. When Percent is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes. Select the None option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

Click the **Apply** button to accept the changes made.

Queue Rate Limiting

This window is used to display and configure the queue rate limiting settings.

To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:

Queue Rate Limiting

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Queue ID: 0 Rate Limit: ☒ Min Bandwidth (8-10000000) Kbps Kbps % %

☐ Min Percent (1-100) % %

☐ None

Unit 1 Settings

Port	Queue0		Queue1		Queue2		Queue3		Queue4		Queue5		Queue6		Queue7	
	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate
eth1/0/1	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/2	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/3	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/4	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/5	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/6	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...

Figure 7-6 Queue Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Select the queue ID that will be configured here. Options to choose from are 0 to 7.
Rate Limit	Select and enter the queue rate limit settings here. <ul style="list-style-type: none"> When the Min Bandwidth option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 8 and 10000000 kbps. Also enter the maximum bandwidth (Max Bandwidth) rate limit in the space provided. This value must be between 8 and 10000000 kbps.

Parameter	Description
	<p>When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available.</p> <p>When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied.</p> <p>The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports.</p> <ul style="list-style-type: none"> When the Min Percent option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also enter the maximum percentage value (Max Percent) in the space provided. This value must be between 1 and 100 percent (%).

Click the **Apply** button to accept the changes made.

Advanced Settings

DSCP Mutation Map

This window is used to display and configure the Differentiated Services Code Point (DSCP) mutation map settings. When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments. The DSCP-CoS map and DSCP-color map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP.

To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:

DSCP Mutation Map

DSCP Mutation Map

Mutation Name: 32 chars Input DSCP List (0-63): 1,3,60-63 Output DSCP (0-63): **Apply**

Total Entries: 1

Mutation Name	Digit in tens	Digit in ones										
		0	1	2	3	4	5	6	7	8	9	
mutation	00	0	10	2	3	4	5	6	7	8	9	Delete
	10	10	11	12	13	14	15	16	17	18	19	
	20	20	21	22	23	24	25	26	27	28	29	
	30	30	31	32	33	34	35	36	37	38	39	
	40	40	41	42	43	44	45	46	47	48	49	
	50	50	51	52	53	54	55	56	57	58	59	
	60	60	61	62	63							

1/1 < < 1 > > Go

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63.
Output DSCP List	Enter the output DSCP list value here. This value must be between 0 and 63.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Port Trust State and Mutation Binding

This window is used to display and configure the port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:

Port Trust State and Mutation Binding

Port Trust State and Mutation Binding

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Trust State: CoS DSCP Mutation Map: 32 chars (selected) None (radio button) Apply

Unit 1 Settings

Port	Trust State	DSCP Mutation Map
eth1/0/1	Trust CoS	
eth1/0/2	Trust CoS	
eth1/0/3	Trust CoS	
eth1/0/4	Trust CoS	
eth1/0/5	Trust CoS	
eth1/0/6	Trust CoS	

Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Trust State	Select the port trust state option here. Options to choose from are CoS and DSCP .
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long. Select the None option to not allocate a DSCP mutation map to the port(s).

Click the **Apply** button to accept the changes made.

DSCP CoS Mapping

This window is used to display and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:

DSCP CoS Mapping

DSCP CoS Mapping

Unit: From Port: To Port: CoS: DSCP List (0-63):

Apply

Unit 1 Settings

Port	CoS	DSCP List
eth1/0/1	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
eth1/0/2	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63

Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
CoS	Select the CoS value to map to the DSCP list. Options to choose from are 0 to 7.
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63.

Click the **Apply** button to accept the changes made.

CoS Color Mapping

This window is used to display and configure the CoS color mapping settings.

To view the following window, click **QoS > Advanced Settings > CoS Color Mapping**, as shown below:

CoS Color Mapping

CoS Color Mapping

Unit: From Port: To Port: CoS List (0-7): Color:

Unit 1 Settings

Port	Color	CoS List
eth1/0/1	Green	0-7
	Yellow	
	Red	
eth1/0/2	Green	0-7
	Yellow	
	Red	
eth1/0/3	Green	0-7
	Yellow	
	Red	
eth1/0/4	Green	0-7
	Yellow	
	Red	

Figure 7-10 CoS Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
CoS List	Enter the CoS value that will be mapped to the color. This value must be between 0 and 7.
Color	Select the color option that will be mapped to the CoS value. Options to choose from are Green , Yellow , and Red .

Click the **Apply** button to accept the changes made.

DSCP Color Mapping

This window is used to display and configure the DSCP color mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP Color Mapping**, as shown below:

DSCP Color Mapping

DSCP Color Mapping

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 DSCP List (0-63): Color: Green Apply

Unit 1 Settings

Port	Color	DSCP List
eth1/0/1	Green	0-63
	Yellow	
	Red	
eth1/0/2	Green	0-63
	Yellow	
	Red	
eth1/0/3	Green	0-63
	Yellow	
	Red	
eth1/0/4	Green	0-63
	Yellow	
	Red	

Figure 7-11 DSCP Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
DSCP List	Enter the DSCP list value here that will be mapped to a color. This value must be between 0 and 63.
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are Green , Yellow , and Red .

Click the **Apply** button to accept the changes made.

Class Map

This window is used to display and configure the class map settings.

To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:

Class Map

Class Map Name: 32 chars Multiple Match Criteria: Match Any Apply

Total Entries: 2

Class Map Name	Multiple Match Criteria	Match	Delete
class	Match Any	Match	Delete
class-default	Match Any	Match	Delete

1/1 < < 1 > > Go

Figure 7-12 Class Map Window

The fields that can be configured are described below:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are Match All and Match Any .

Click the **Apply** button to accept the changes made.

Click the **Match** button to configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Match** button, the following page will be available.

Figure 7-13 Class Map (Match) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7. Tick the Inner option to match the inner most CoS of QinQ packets on a Layer 2 class of service (CoS) marking.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are ARP, BGP, DHCP, DNS, EGP, FTP, IPv4, IPv6, NetBIOS, NFS, NTP, OSPF, PPPOE, RIP, RTSP, SSH, Telnet, and TFTP .
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. Tick the Inner option to match the inner-most VLAN ID in an 802.1Q double tagged frame.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Aggregate Policer

This window is used to display and configure the aggregate policer settings.

To view the following window, click **QoS > Advanced Settings > Aggregate Policer**, as shown below:

Figure 7-14 Aggregate Policer (Single Rate Setting) Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here.
Average Rate	Enter the average rate value here. This value must be between 0 and 10000000 kbps.
Normal Burst Size	Enter the normal burst size value here. This value must be between 0 and 16384 Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. This value must be between 0 and 16384 Kbytes.
Confirm Action	<p>Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <ul style="list-style-type: none"> When selecting the Drop option, the packet will be dropped. When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. When selecting the Transmit option, packets will be transmitted unaltered. When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.
Exceed Action	<p>Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <ul style="list-style-type: none"> When selecting the Drop option, the packet will be dropped. When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. When selecting the Transmit option, packets will be transmitted unaltered.

Parameter	Description
	<ul style="list-style-type: none"> When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.
Violate Action	<p>Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for single rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are None, Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <ul style="list-style-type: none"> When selecting the None option, no action will be taken. When selecting the Drop option, the packet will be dropped. When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. When selecting the Transmit option, packets will be transmitted unaltered. When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.
Color Aware	<p>Select the color aware option here. Options to choose from are Enabled and Disabled. When color aware is disabled, the policer works in the color blind mode. When color aware is enabled, the policer works in the color aware mode.</p>

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After selecting the **Two Rate Settings** tab option, at the top of the page, the following page will be available.

Aggregate Policier

Single Rate Settings | **Two Rate Settings**

Aggregate Policier Name *

CIR * (0-10000000) Kbps

PIR * (0-10000000) Kbps

Conform Action

Violate Action

* Mandatory Field

Confirm Burst (0-16384) Kbyte

Peak Burst (0-16384) Kbyte

Exceed Action

Color Aware

Total Entries: 1

Name	CIR	Confirm Burst	PIR	Peak Burst	Conform Action	Exceed Action	Violate Action	Color Aware	
name	10000	1234	10000	1234	Transmit	Drop	Drop	Disabled	<input type="button" value="Delete"/>

1/1

Figure 7-15 Aggregate Policier (Two Rate Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policier Name	Enter the aggregate policer name here.

Parameter	Description
CIR	Enter the Committed Information Rate (CIR) value here. This value must be between 0 and 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. This value must be between 0 and 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.
PIR	Enter the Peak Information Rate (PIR) value here. This value must be between 0 and 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. This value must be between 0 and 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.
Confirm Action	<p>Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to Transmit. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <ul style="list-style-type: none"> • When selecting the Drop option, the packet will be dropped. • When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the Transmit option, packets will be transmitted unaltered. • When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.
Exceed Action	<p>Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is Drop. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <ul style="list-style-type: none"> • When selecting the Drop option, the packet will be dropped. • When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the Transmit option, packets will be transmitted unaltered. • When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.
Violate Action	<p>Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for single rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are Drop, Set-DSCP-Transmit, Set-1P-Transmit, Transmit, and Set-DSCP-1P.</p> <ul style="list-style-type: none"> • When selecting the Drop option, the packet will be dropped. • When selecting the Set-DSCP-Transmit option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.

Parameter	Description
	<ul style="list-style-type: none"> When selecting the Set-1P-Transmit option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. When selecting the Transmit option, packets will be transmitted unaltered. When selecting the Set-DSCP-1P option, enter the IP DSCP and 1P transmit values in the spaces provided.
Color Aware	Select the color aware option here. Options to choose from are Disabled and Enabled . When color aware is disabled, the policer works in the color blind mode. When color aware is enabled, the policer works in the color aware mode.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Policy Map

This window is used to display and configure the policy map settings.

To view the following window, click **QoS > Advanced Settings > Policy Map**, as shown below:

Figure 7-16 Policy Map Window

The fields that can be configured for **Create/Delete Policy Map** are described below:

Parameter	Description
Policy Map Name	Enter the policy map name here that will be created or deleted. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Set Action** button to configure the set action settings for the specified entry.

Click the **Policer** button to configure the policer settings for the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Set Action** button, the following page will appear.

Figure 7-17 Policy Map (Set Action) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to specify that no action will be taken.
Specify	Select this option to specify that action will be taken based on the configurations made.
New Precedence	Select the new precedence value for the packet here. The range is from 0 to 7. Select the IPv4 only option to specify that IPv4 precedence will be marked only. If not selected, then both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of the traffic class of the IPv6 header. Setting the precedence will not affect the CoS queue selection.
New DSCP	Select the new DSCP value for the packet here. The range is from 0 to 63. Select the IPv4 only option to specify that the IPv4 DSCP will be marked only. If not selected, then both the IPv4 and IPv6 DSCP will be marked. Setting the DSCP will not affect the CoS queue selection.
New CoS	Select the new CoS value to the packet here. The range is from 0 to 7. Setting the CoS will not affect the CoS queue selection.
New Cos Queue	Select the new CoS queue value to the packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

After clicking the **Policer** button, the following page will appear.

Figure 7-18 Policy Map (Policer) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.
Average Rate	Enter the average rate value here. The range is from 0 to 10000000 Kbps.
Normal Burst Size	Enter the normal burst size value here. The range is from 0 to 16384 Kbps.
Maximum Burst Size	Enter the maximum burst size value here. The range is from 0 to 16384 Kbps.
Conform Action	<p>Select the conform action that will be taken here. This action will be taken on green color packets. Option to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the conform action is to drop the packet. • Set-DSCP-Transmit - Specifies that the conform action is to modify the DSCP value and then to transmit the packet with the new DSCP value. Enter the new DSCP value in the space provided. • Set-1P-Transmit - Specifies that the conform action is to modify the 802.1p value and then to transmit the packet with the new 802.1p value. Enter the new 802.1p value in the space provided. • Transmit - Specifies that the conform action is to transmit the packet unmodified. • Set-DSCP-1P - Specifies that the conform action is to modify the DSCP and 802.1p values and then to transmit the packet with the new DSCP and 802.1p values. Enter the new DSCP and 802.1p values in the spaces provided.
Exceed Action	<p>Select the exceed action that will be taken here. This action will be taken on yellow color packets that exceed the rate limit. Option to choose from are:</p> <ul style="list-style-type: none"> • Drop - Specifies that the exceed action is to drop the packet. • Set-DSCP-Transmit - Specifies that the exceed action is to modify the DSCP value and then to transmit the packet with the new DSCP value. Enter the new DSCP value in the space provided. • Set-1P-Transmit - Specifies that the exceed action is to modify the 802.1p value and then to transmit the packet with the new 802.1p value. Enter the new 802.1p value in the space provided.

Parameter	Description
	<ul style="list-style-type: none"> • Transmit - Specifies that the exceed action is to transmit the packet unmodified. • Set-DSCP-1P - Specifies that the exceed action is to modify the DSCP and 802.1p values and then to transmit the packet with the new DSCP and 802.1p values. Enter the new DSCP and 802.1p values in the spaces provided.
Violate Action	<p>Select the violate action that will be taken here. This action will be taken on red color packets. Option to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies that no violate action will be taken. • Drop - Specifies that the violate action is to drop the packet. • Set-DSCP-Transmit - Specifies that the violate action is to modify the DSCP value and then to transmit the packet with the new DSCP value. Enter the new DSCP value in the space provided. • Set-1P-Transmit - Specifies that the violate action is to modify the 802.1p value and then to transmit the packet with the new 802.1p value. Enter the new 802.1p value in the space provided. • Transmit - Specifies that the violate action is to transmit the packet unmodified. • Set-DSCP-1P - Specifies that the violate action is to modify the DSCP and 802.1p values and then to transmit the packet with the new DSCP and 802.1p values. Enter the new DSCP and 802.1p values in the spaces provided.
Color Aware	Select to enable or disable the color aware feature here. When disabled, the policer works in the color blind mode. When enabled, the policer works in the color aware mode.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

Policy Binding

This window is used to display and configure the policy binding settings.

To view the following window, click **QoS > Advanced Settings > Policy Binding**, as shown below:

Policy Binding

Policy Binding Setting

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Direction: Input Policy Map Name: 32 chars ☐ None

Unit 1 Settings

Port	Direction	Policy Map Name
eth1/0/1		
eth1/0/2		
eth1/0/3		
eth1/0/4		
eth1/0/5		
eth1/0/6		

Figure 7-19 Policy Binding Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are Input and Output . Input specified ingress traffic and output specifies egress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the None option to not tie a policy map to this entry.

Click the **Apply** button to accept the changes made.

WRED

Weighted Random Early Detection (WRED) is another implementation for QoS that will help the overall throughput for your QoS queues. Based on the egress queue of the QoS function set on the Switch, this method will analyze these packets and their QoS queue to determine if there will be an overflow of packets entering the QoS queues and consequentially, minimize the packet flow into these queues by dropping random packets. WRED employs two methods of avoiding congestion within the QoS queue.

1. Every QoS queue has a minimum and a maximum level for acceptance of packets. Once the maximum threshold has been reached for this queue, the Switch will begin discarding all ingress packets, this minimizing the allotted bandwidth for QoS. When below the minimum threshold, the Switch will accept all ingress packets.
2. When the ingress packets are somewhere between the maximum and minimum queue, the Switch will use a slope probability function to determine a random method of dropping packets based on the maximum drop rate which specifies the drop probability when the queues reach maximum threshold. If queues are closer to the maximum threshold, the Switch will increase the discarding of random packets to even out the flow to the queues and avoid overflows to higher priority queues.

WRED Profile

This window is used to display and configure the Weighted Random Early Detection (WRED) profile settings.

To view the following window, click **QoS > WRED > WRED Profile**, as shown below:

WRED Profile

WRED Profile

Profile (1-128)

Packet Colour

Min Threshold (0-100)

Max Threshold (0-100)

Max Drop Rate (0-14)

Green

20

80

0

Apply

Profile (1-128)

Find

Total Entries: 128

WRED Profile	Packet Type	Min Threshold	Max Threshold	Max Drop Rate	
1	GREEN	20	80	0	Reset Configuration
	YELLOW	20	80	0	
	RED	20	80	0	
2	GREEN	20	80	0	Reset Configuration
	YELLOW	20	80	0	
	RED	20	80	0	
3	GREEN	20	80	0	Reset Configuration
	YELLOW	20	80	0	
	RED	20	80	0	

Figure 7-20 WRED Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Packet Colour	Select the packet color here. Options to choose from are Green , Yellow , and Red . <ul style="list-style-type: none"> • Green - Specifies the WRED drop parameters for green packets to be set. • Yellow - Specifies the WRED drop parameters for yellow packets to be set. • Red - Specifies the WRED drop parameters for red packets to be set.
Min Threshold	Enter the minimum threshold value here that will be used to start WRED dropping. The range is from 0 to 100.
Max Threshold	Enter the maximum threshold value here over which WRED will drop all packets destined for this queue. The range is from 0 to 100.
Max Drop Rate	Enter the maximum drop-rate value here. The range is from 0 to 14. This feature specifies the drop probability when the average queue size reaches the maximum threshold. When this value is zero, then the packet will not be dropped or remarked for ECN.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Reset Configuration** button to reset the configuration on the specified entry.

WRED Queue

This window is used to display and configure the WRED queue settings. WRED drops packets, based on the average queue size exceeding a specific threshold, to indicate congestion. Explicit Congestion Notification (ECN) is an extension to WRED in that ECN marks packets instead of dropping them when the average queue size exceeds a specific threshold value. When configuring the WRED ECN feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

To view the following window, click **QoS > WRED > WRED Queue**, as shown below:

Unit	From Port	To Port	CoS	WRED State	Profile (1-128)	Weight (0-15)
1	eth1/0/1	eth1/0/1	0	Disabled		9

Unit 1 Settings				
Port	CoS	WRED State	Exp-weight-constant	Profile
eth1/0/1	0	Disabled	9	1
	1	Disabled	9	1
	2	Disabled	9	1
	3	Disabled	9	1
	4	Disabled	9	1
	5	Disabled	9	1
	6	Disabled	9	1
	7	Disabled	9	1

Figure 7-21 WRED Queue Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.
CoS	Select the CoS value here. The range is from 0 to 7.

Parameter	Description
WRED State	Select to enable or disable the WRED feature state on the specified port(s) here.
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Weight	Enter the exponential weight value here. The range is from 0 to 15. This feature is used to configure the WRED exponential weight factor for the average queue size calculation for the queue.

Click the **Apply** button to accept the changes made.

8. Access Control List (ACL)

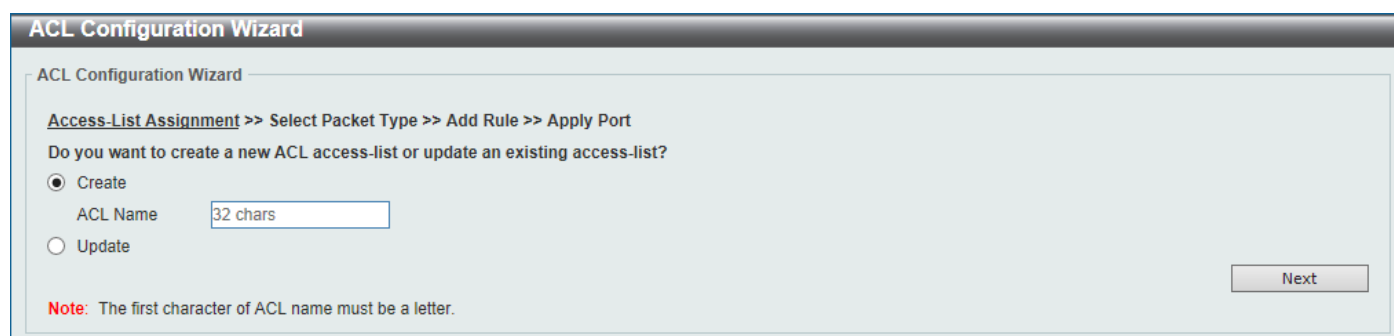
[ACL Configuration Wizard](#)
[ACL Access List](#)
[ACL Interface Access Group](#)
[ACL VLAN Access Map](#)
[ACL VLAN Filter](#)
[CPU ACL](#)

ACL Configuration Wizard

This window is used to guide the user to create a new ACL access list or configure an existing ACL access list.

Step 1 - Create/Update

To view the following window, click **ACL > ACL Configuration Wizard**, as shown below:



ACL Configuration Wizard

ACL Configuration Wizard

[Access-List Assignment](#) >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

☒ Create

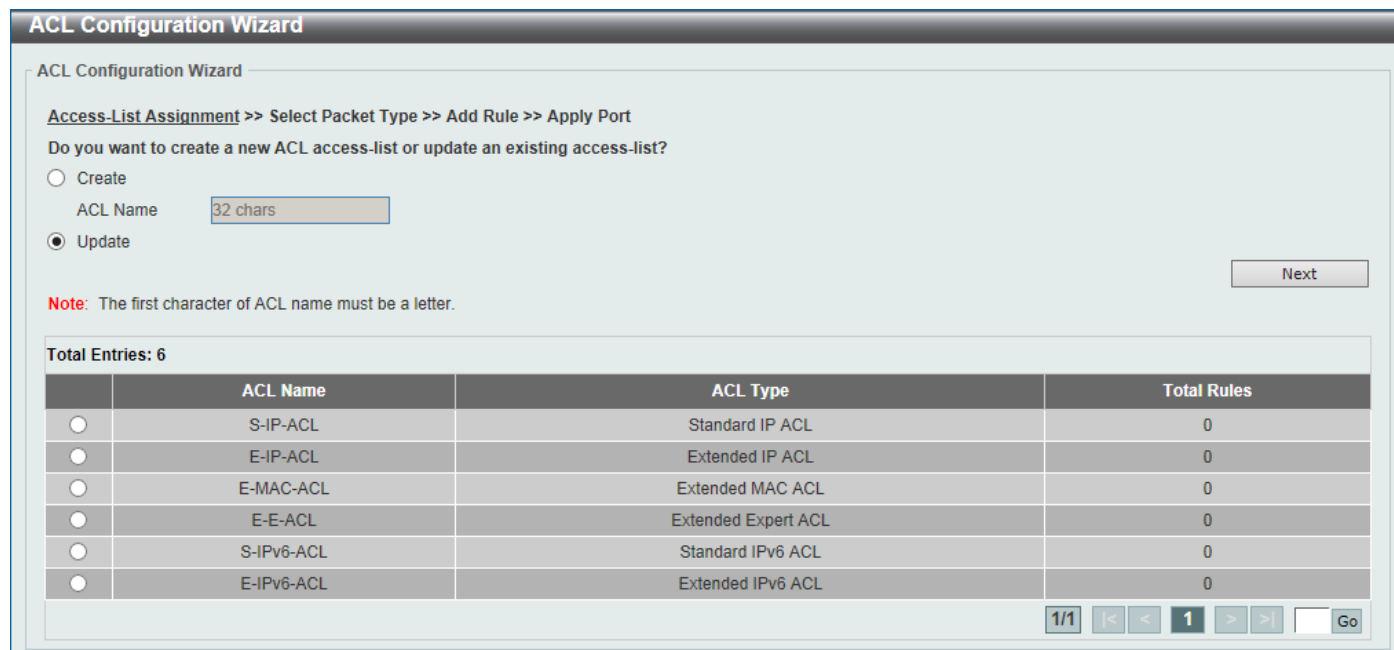
ACL Name

☐ Update

Note: The first character of ACL name must be a letter.

Next

Figure 8-1 ACL Configuration Wizard (Create) Window



ACL Configuration Wizard

ACL Configuration Wizard

[Access-List Assignment](#) >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

☐ Create

ACL Name

☒ Update

Note: The first character of ACL name must be a letter.

Next

Total Entries: 6

	ACL Name	ACL Type	Total Rules
<input type="radio"/>	S-IP-ACL	Standard IP ACL	0
<input type="radio"/>	E-IP-ACL	Extended IP ACL	0
<input type="radio"/>	E-MAC-ACL	Extended MAC ACL	0
<input type="radio"/>	E-E-ACL	Extended Expert ACL	0
<input type="radio"/>	S-IPv6-ACL	Standard IPv6 ACL	0
<input type="radio"/>	E-IPv6-ACL	Extended IPv6 ACL	0

1/1 |< < 1 > >| Go

Figure 8-2 ACL Configuration Wizard (Update) Window

The fields that can be configured are described below:

Parameter	Description
Create	Select this option to create a new ACL access list using the configuration wizard.
ACL Name	Enter the new ACL name here. This name can be up to 32 characters long.
Update	Select this option to update an existing ACL access list. Select the existing ACL in the table to process with the update.

Click the **Next** button to continue to the next step.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Step 2 - Select Packet Type

After clicking the **Next** button, the following window will appear.

Figure 8-3 ACL Configuration Wizard (Create, Packet Type) Window

The fields that can be configured are described below:

Parameter	Description
MAC	Select to create/update a MAC ACL.
IPv4	Select to create/update an IPv4 ACL.
IPv6	Select to create/update an IPv6 ACL.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Step 3 - Add Rule

MAC

After clicking the **MAC** radio button and the **Next** button, the following window will appear.

Figure 8-4 ACL Configuration Wizard (Create, Packet Type, MAC) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Source	<p>Select and enter the source MAC address information here. Options to choose from are Any, Host, and MAC.</p> <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	<p>Select and enter the destination MAC address information here. Options to choose from are Any, Host, and MAC.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decnet-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x600 and 0xFFFF. When any Ethernet type profile is selected in the Specify

Parameter	Description
	Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7 .
Inner CoS	After selecting the CoS value, select the inner CoS value that will be used here. The range is from 0 to 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit , Deny and Deny CPU .

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

IPv4

After clicking the **IPv4** radio button and the **Next** button, the following window will appear.

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> **Add Rule** >> Apply Port

Please assign a sequence number to create a new rule.

☒ Sequence No. (1-65535) ☐ Auto Assign

Protocol Type (0-255) ☐ Fragments

Assign rule criteria

IPv4 Address

Source: ☒ Any ☐ Host ☐ IP ☐ Wildcard

Destination: ☒ Any ☐ Host ☐ IP ☐ Wildcard

Port

Source Port: (0-65535) (0-65535)

Destination Port: (0-65535) (0-65535)

IPv4 DSCP

☒ IP Precedence Value (0-7)

☐ ToS Value (0-15)

☐ DSCP (0-63) Value (0-63)

TCP Flag

TCP Flag ☐ ack ☐ fin ☐ psh ☐ rst ☐ syn ☐ urg

Time Range

Action ☒ Permit ☐ Deny

Figure 8-5 ACL Configuration Wizard (Create, Packet Type, IPv4) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Protocol Type	<p>Select the protocol type option here. Options to choose from are TCP, UDP, ICMP, EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID, and None.</p> <ul style="list-style-type: none"> Value - The protocol ID can also manually be entered here. The range is from 0 to 255. Fragments - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	<p>Select and enter the source information here. Options to choose from are Any, Host, and IP.</p> <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	<p>Select and enter the destination information here. Options to choose from are Any, Host, and IP.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	<p>Select and enter the source port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>

Parameter	Description
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type ICMP .
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
IP Precedence	Select the IP precedence value used here. Options to choose from are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), and network (7). <ul style="list-style-type: none">• Value - The IP precedence value can also manually be entered here. The range is from 0 to 7.
ToS	Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8). <ul style="list-style-type: none">• Value - The ToS value can also manually be entered here. The range is from 0 to 15.
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none">• Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available in the protocol type TCP .
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit , Deny and Deny CPU .

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

IPv6

After clicking the **IPv6** radio button and the **Next** button, the following window will appear.

ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> **Add Rule** >> Apply Port

Please assign a sequence number to create a new rule.

☒ Sequence No. (1-65535) ☐ Auto Assign

Protocol Type (0-255) ☐ Fragments

Assign rule criteria

IPv6 Address

☒ Any ☐ Host ☐ IPv6

Source Destination Prefix Length

Port

Source Port (0-65535) (0-65535)

Destination Port (0-65535) (0-65535)

IPv6 DSCP

☒ DSCP (0-63)

☐ Traffic Class (0-255)

TCP Flag

TCP Flag ☐ ack ☐ fin ☐ psh ☐ rst ☐ syn ☐ urg

Flow Label

Flow Label (0-1048575)

Time Range

Action

☒ Permit ☐ Deny

Figure 8-6 ACL Configuration Wizard (Create, Packet Type, IPv6) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50) , PCP (108) , SCTP (132) , and None . <ul style="list-style-type: none"> Value - The protocol ID can also manually be entered here. The range is from 0 to 255. Fragments - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	<p>Select and enter the source information here. Options to choose from are Any, Host, and IPv6.</p> <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	<p>Select and enter the destination information here. Options to choose from are Any, Host, and IPv6.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	<p>Select and enter the source port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available in the protocol type ICMP.</p>

Parameter	Description
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available in the protocol type TCP .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit , Deny and Deny CPU .

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Step 4 - Apply Port

After clicking the **Next** button, the following window will appear.

Figure 8-7 ACL Configuration Wizard (Create, Port) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are In and Out .

Click the **Back** button to return to the previous step.

Click the **Apply** button to accept the changes made and return to the main ACL Wizard window.

ACL Access List

This window is used to display and configure the ACLs, ACL rules and settings.

To view the following window, click **ACL > ACL Access List**, as shown below:

The screenshot shows the 'ACL Access List' window. At the top, there are search filters: 'ACL Type' (set to 'All'), 'ID (1-14999)' (empty), and 'ACL Name' (set to '32 chars'). A 'Find' button is on the right. Below the filters, it says 'Total Entries: 6' and has an 'Add ACL' button. The main table lists 6 ACL entries:

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	S-IP-ACL	Standard IP ACL	10	10	Enabled		Edit Delete
2000	E-IP-ACL	Extended IP ACL	10	10	Disabled		Edit Delete
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		Edit Delete
8000	E-E-ACL	Extended Expert ACL	10	10	Disabled		Edit Delete
11000	S-IPv6-ACL	Standard IPv6 ACL	10	10	Disabled		Edit Delete
13000	E-IPv6-ACL	Extended IPv6 ACL	10	10	Disabled		Edit Delete

Below the table is a pagination bar showing '1/1' and navigation buttons. Below that, the 'S-IP-ACL (ID: 1) Rule' section is expanded, showing a table of rules:

Sequence No.	Action	Rule	Time Range	Counter	
10	Permit	any any		(Ing: 0 packets Egr: 0...)	Delete

There is also a 'Clear All Counter' button, a 'Clear Counter' button, and an 'Add Rule' button. A second pagination bar is at the bottom of the rule section.

Figure 8-8 ACL Access List Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type to find here. Options to choose from are All , IP ACL , IPv6 ACL , MAC ACL , and Expert ACL .
ID	Select and enter the access list ID here. The range is from 1 to 14999.
ACL Name	Select and enter the access list name here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add ACL** button to create a new ACL.

Click the **Edit** button to re-configure the specific ACL.

Click the **Delete** button, next to the ACL, to remove the specific ACL.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Clear All Counter** button to clear all the counter information displayed.

Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the **Add Rule** button to create an ACL rule for the ACL selected.

Click the **Delete** button, next to the ACL rule, to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

The screenshot shows the 'ACL Access List' window. At the top, there's a header 'ACL Access List'. Below it, a sub-header 'ACL Access List' is followed by configuration options: 'ACL Type' set to 'All', a radio button for 'ID (1-14999)' with an empty text box, and a radio button for 'ACL Name' with a text box containing '32 chars'. A 'Find' button is on the right. Below this, 'Total Entries: 2' is shown next to an 'Add ACL' button. A table lists two entries: ID 1 (ACL1, Standard IP ACL, Start Sequence No. 10, Step 10) and ID 4 (ACL4, Standard IP ACL, Start Sequence No. 10, Step 10). Each entry has 'Apply' and 'Delete' buttons. At the bottom, there's a '1/1' indicator and a 'Go' button. Below the table, there's a section for 'ACL1 (ID: 1) Rule' with an 'Add Rule' button and a table with columns: 'Sequence No.', 'Action', 'Rule', and 'Time Range'.

Figure 8-9 ACL Access List (Edit) Window

After clicking the **Edit** button, the fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number step here. The step range is from 1 to 32. This specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.

Click the **Apply** button to accept the changes made.

After clicking the **Add ACL** button, the following page will appear.

The screenshot shows the 'Add ACL Access List' window. It has a header 'Add ACL Access List'. Below it, a sub-header 'Add ACL Access List' is followed by configuration options: 'ACL Type' set to 'Standard IP ACL', 'ID (1-1999)' with an empty text box, and 'ACL Name' with a text box containing '32 chars'. An 'Apply' button is on the right. At the bottom, a red note states: 'Note: The first character of ACL name must be a letter.'

Figure 8-10 ACL Access List (Add ACL) Window

After clicking the **Add ACL** button, the fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , Extended MAC ACL , and Extended Expert ACL .
ID	Enter the ID for the ACL here. <ul style="list-style-type: none"> For a Standard IP ACL, the range from 1 to 1999. For an Extended IP ACL, the range from 2000 to 3999. For a Standard IPv6 ACL, the range from 11000 to 12999. For an Extended IPv6 ACL, the range from 13000 to 14999. For an Extended MAC ACL, the range from 6000 to 7999. For an Extended Expert ACL, the range from 8000 to 9999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Standard IP ACL

After selecting a Standard IP ACL and clicking the **Add Rule** button, the following page will appear.

Figure 8-11 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit , Deny , and Deny CPU .
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended IP ACL

After selecting an Extended IP ACL and clicking the **Add Rule** button, the following page will appear.

The screenshot shows the 'Add ACL Rule' window with the following configuration:

- ID:** 2000
- ACL Name:** ACL2000
- ACL Type:** Extended IP ACL
- Sequence No. (1-65535):** (If it isn't specified, the system automatically assigns.)
- Action:** ☒ Permit ☐ Deny
- Protocol Type:** TCP (0-255) ☐ Fragments
- Match IP Address:**
 - Source:** ☒ Any ☐ Host ☐ IP ☐ Wildcard
 - Destination:** ☒ Any ☐ Host ☐ IP ☐ Wildcard
- Match Port:**
 - Source Port:** Please Select (0-65535)
 - Destination Port:** Please Select (0-65535)
- TCP Flag:** ☐ ack ☐ fin ☐ psh ☐ rst ☐ syn ☐ urg
- IP Precedence:**
 - ☒ ToS: Please Select (0-15)
 - ☐ DSCP (0-63): Please Select (0-63)
- Time Range:** 32 chars
- Buttons:** Back, Apply

Figure 8-12 Extended IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit , Deny , and Deny CPU .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP (88) , ESP (50) , GRE (47) , IGMP (2) , OSPF (89) , PIM (103) , VRRP (112) , IP-in-IP (94) , PCP (108) , Protocol ID , and None . <ul style="list-style-type: none"> Value - The protocol ID can also manually be entered here. The range is from 0 to 255. Fragments - Select this option to include packet fragment filtering.
Source	Select and enter the source IP information here. Options to choose from are Any , Host , and IP . <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit

Parameter	Description
	corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	<p>Select and enter the destination IP information here. Options to choose from are Any, Host, and IP.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	<p>Select and enter the source port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available in the protocol type ICMP.</p>
ICMP Message Type	<p>When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available in the protocol type ICMP.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p>

Parameter	Description
	This parameter is only available in the protocol type ICMP .
TCP Flag	<p>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.</p> <p>This parameter is only available in the protocol type TCP.</p>
IP Precedence	<p>Select the IP precedence value used here. Options to choose from are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), and network (7).</p> <ul style="list-style-type: none"> Value - The IP precedence value can also manually be entered here. The range is from 0 to 7.
ToS	<p>Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8).</p> <ul style="list-style-type: none"> Value - The ToS value can also manually be entered here. The range is from 0 to 15.
DSCP	<p>Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46).</p> <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Standard IPv6 ACL

After selecting a Standard IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

Add ACL Rule

Add ACL Rule

ID: 11000

ACL Name: ACL11000

ACL Type: Standard IPv6 ACL

Sequence No. (1-65535): (If it isn't specified, the system automatically assigns.)

Action: ☒ Permit ☐ Deny

Match IPv6 Address:

Source: ☒ Any ☐ Host ☐ IPv6

Destination: ☒ Any ☐ Host ☐ IPv6

Prefix Length:

Time Range: 32 chars

Figure 8-13 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	<p>Select and enter the source IPv6 information here. Options to choose from are Any, Host, IPv6, and Prefix Length.</p> <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	<p>Select and enter the destination IPv6 information here. Options to choose from are Any, Host, IPv6, and Prefix Length.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended IPv6 ACL

After selecting an Extended IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

Add ACL Rule

Add ACL Rule

ID: 13000
 ACL Name: ACL13000
 ACL Type: Extended IPv6 ACL
 Sequence No. (1-65535): (If it isn't specified, the system automatically assigns.)
 Action: ☒ Permit ☐ Deny
 Protocol Type: (0-255) ☐ Fragments

Match IPv6 Address

Source: ☒ Any ☐ Host ☐ IPv6
 Destination: ☒ Any ☐ Host ☐ IPv6
 Prefix Length:

Match Port

Source Port: (0-65535)
 Destination Port: (0-65535)

TCP Flag

☐ ack ☐ fin ☐ psh ☐ rst ☐ syn ☐ urg

☒ DSCP (0-63) Value (0-63)

☐ Traffic Class (0-255)

Flow Label (0-1048575)

Time Range

Figure 8-14 Extended IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit , Deny , and Deny CPU .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50) , PCP (108) , SCTP (132) , and None . <ul style="list-style-type: none"> Value - The protocol ID can also manually be entered here. The range is from 0 to 255. Fragments - Select this option to include packet fragment filtering.
Source	Select and enter the source IPv6 information here. Options to choose from are Any , Host , and IPv6 . <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination IPv6 information here. Options to choose from are Any , Host , and IPv6 .

Parameter	Description
	<ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	<p>Select and enter the source port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are =, >, <, ≠, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the ≠ option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
TCP Flag	<p>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.</p> <p>This parameter is only available in the protocol type TCP.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available in the protocol type ICMP.</p>
ICMP Message Type	<p>When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available in the protocol type ICMP.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available in the protocol type ICMP.</p>

Parameter	Description
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended MAC ACL

After selecting an Extended MAC ACL and clicking the **Add Rule** button, the following page will appear.

Figure 8-15 Extended MAC ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source MAC address information here. Options to choose from are Any , Host , MAC , and Wildcard . <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule.

Parameter	Description
	<ul style="list-style-type: none"> When the Host option is selected, enter the source host MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	<p>Select and enter the destination MAC address information here. Options to choose from are Any, Host, MAC, and Wildcard.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host MAC address here. When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decnet-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x600 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7 .
Inner CoS	After selecting the CoS value, select the inner CoS value that will be used here. The range is from 0 to 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

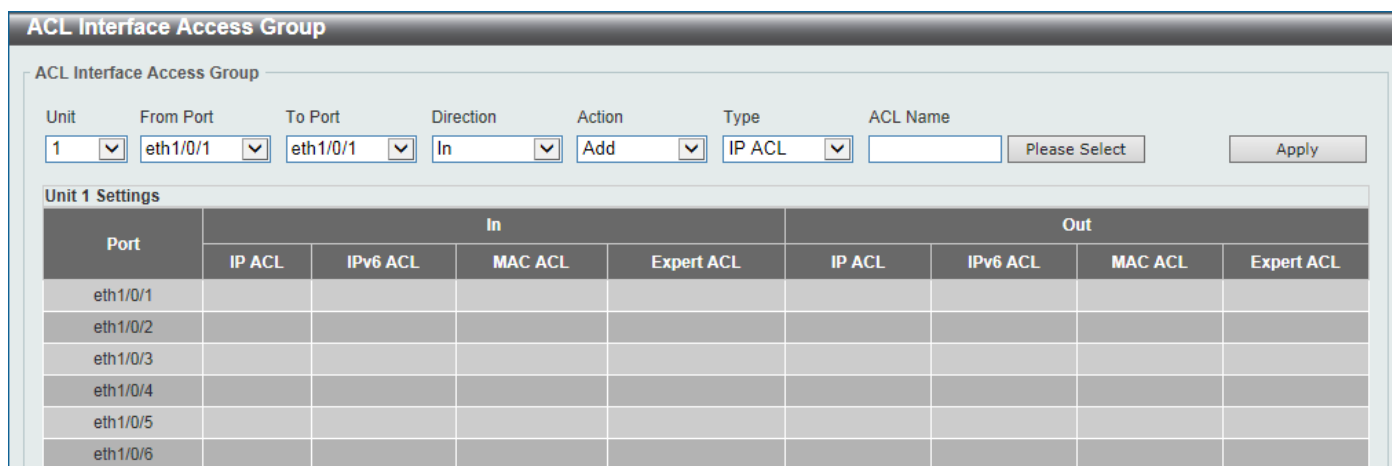
Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

ACL Interface Access Group

This window is used to display and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:



The screenshot shows the 'ACL Interface Access Group' window. At the top, there are dropdown menus for 'Unit' (set to 1), 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Direction' (In), 'Action' (Add), and 'Type' (IP ACL). There is an 'ACL Name' field and a 'Please Select' button. An 'Apply' button is on the right. Below this is a section titled 'Unit 1 Settings' containing a table with columns for 'Port', 'IP ACL', 'IPv6 ACL', 'MAC ACL', and 'Expert ACL' for both 'In' and 'Out' directions. The 'Port' column lists eth1/0/1 through eth1/0/6.

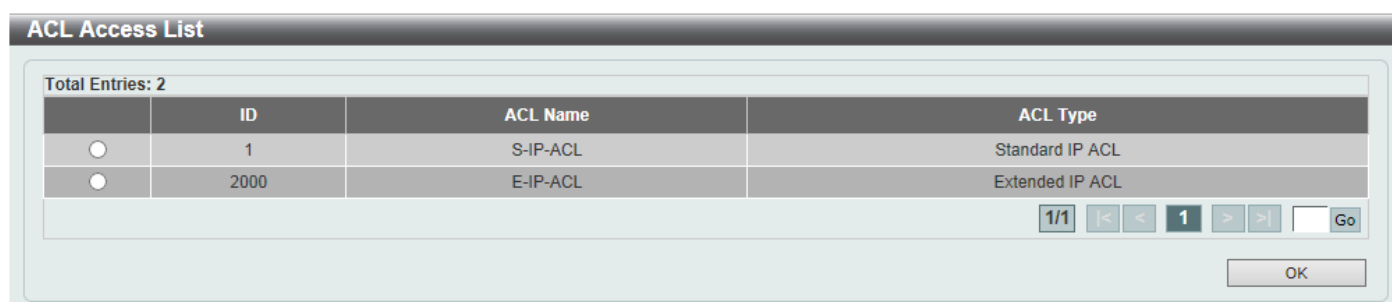
Figure 8-16 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction here. Options to choose from are In and Out .
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the ACL type here. Options to choose from are IP ACL , IPv6 ACL , and MAC ACL .
ACL Name	Enter the ACL name here. This name can be up to 32 characters long. Click the Please Select button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

After clicking the **Please Select** button, the following window will appear:



The screenshot shows the 'ACL Access List' window. It displays 'Total Entries: 2'. Below is a table with columns 'ID', 'ACL Name', and 'ACL Type'. The first entry has ID 1, ACL Name S-IP-ACL, and ACL Type Standard IP ACL. The second entry has ID 2000, ACL Name E-IP-ACL, and ACL Type Extended IP ACL. At the bottom right, there is a pagination control showing '1/1' and a 'Go' button. An 'OK' button is at the bottom right of the window.

Figure 8-17 ACL Interface Access Group (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

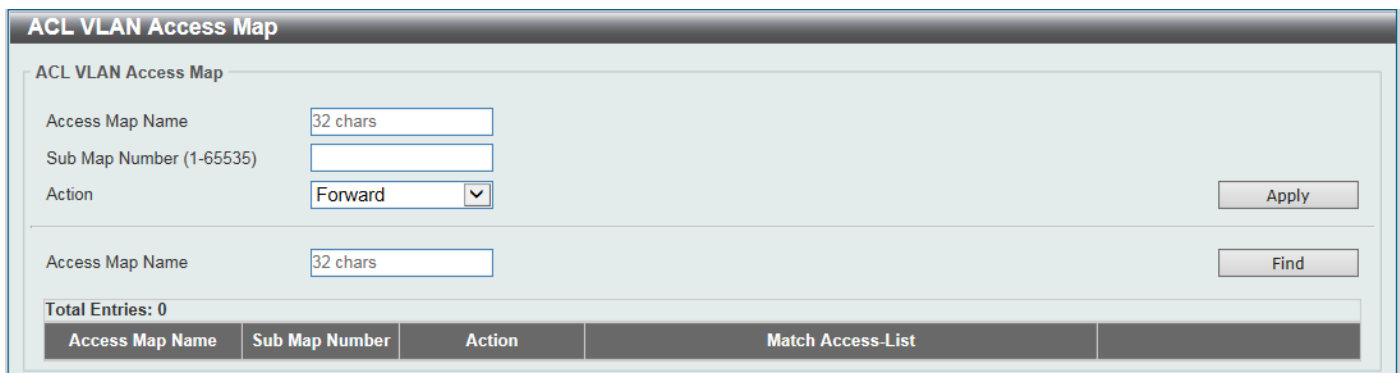
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

ACL VLAN Access Map

This window is used to display and configure the ACL VLAN access map settings.

To view the following window, click **ACL > ACL VLAN Access Map**, as shown below:



The screenshot shows the 'ACL VLAN Access Map' window. It has a title bar 'ACL VLAN Access Map'. Below it is a section 'ACL VLAN Access Map' containing three input fields: 'Access Map Name' (with a '32 chars' hint), 'Sub Map Number (1-65535)', and 'Action' (a dropdown menu currently showing 'Forward'). To the right of these fields is an 'Apply' button. Below this section is another 'Access Map Name' field (also with a '32 chars' hint) and a 'Find' button. At the bottom, it says 'Total Entries: 0' and displays a table with the following headers: 'Access Map Name', 'Sub Map Number', 'Action', and 'Match Access-List'.

Figure 8-18 ACL VLAN Access Map Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long.
Sub Map Number	Enter the sub-map number here. This value must be between 1 and 65535.
Action	Select the action that will be taken here. Options to choose from are Forward , Drop , and Redirect . When the Redirect option is selected, select the redirected interface from the drop-down list.

Click the **Apply** button to accept the changes made.

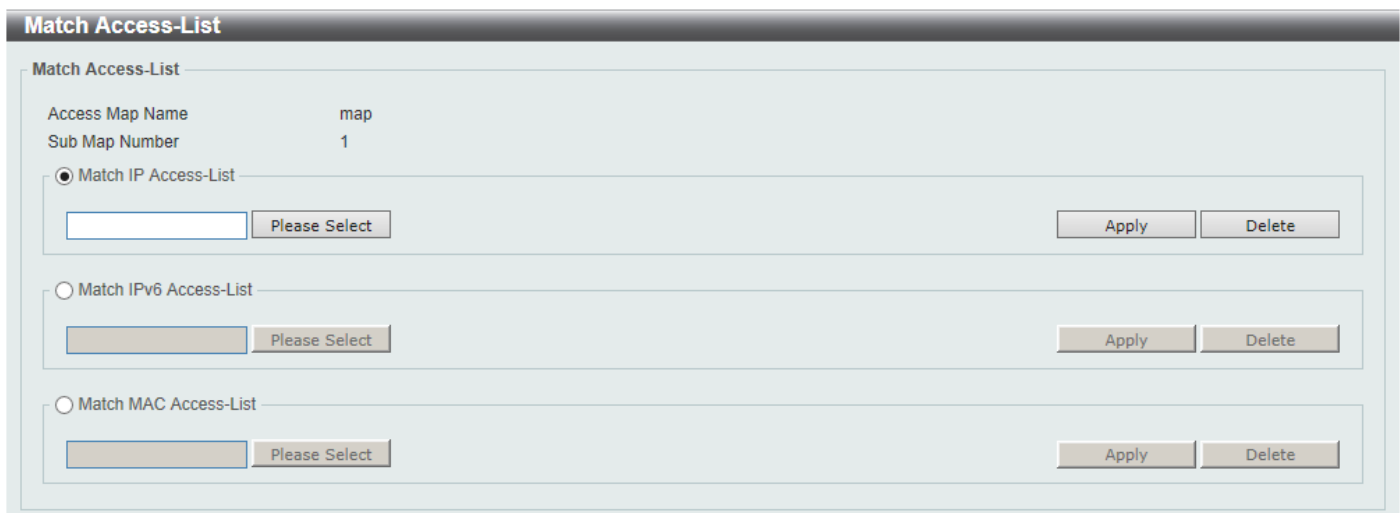
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Binding** button to match an access list to the ACL VLAN access map.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Binding** button, the following window will appear:



The screenshot shows the 'Match Access-List' window. It has a title bar 'Match Access-List'. Below it is a section 'Match Access-List' containing two input fields: 'Access Map Name' (with value 'map') and 'Sub Map Number' (with value '1'). Below these fields are three radio button options: 'Match IP Access-List' (selected), 'Match IPv6 Access-List', and 'Match MAC Access-List'. Each option has a corresponding 'Please Select' button. To the right of each option are 'Apply' and 'Delete' buttons.

Figure 8-19 ACL VLAN Access Map (Binding) Window

The fields that can be configured are described below:

Parameter	Description
Match IP Access-List	Here the IP access list that will be matched will be displayed.
Match IPv6 Access-List	Here the IPv6 access list that will be matched will be displayed.
Match MAC Access-List	Here the MAC access list that will be matched will be displayed.

Click the **Please Select** button navigate to a list of access lists that can be selected to be used in this configuration.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

After clicking the **Please Select** button, the following window will appear:

ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
<input type="radio"/>	1	S-IP-ACL	Standard IP ACL
<input type="radio"/>	2000	E-IP-ACL	Extended IP ACL

1/1 |< < 1 > >| Go

OK

Figure 8-20 ACL VLAN Access Map (Binding, Selection) Window

Select the radio button next to the entry to use that access list in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

ACL VLAN Filter

This window is used to display and configure the ACL VLAN filter settings.

To view the following window, click **ACL > ACL VLAN Filter**, as shown below:

ACL VLAN Filter

ACL VLAN Filter

Access Map Name: 32 chars

Action: Add

VID List: 1,3-5 ☐ All VLANs

Apply

Total Entries: 1

Access Map Name	VID List
map	1

Delete

1/1 |< < 1 > >| Go

Figure 8-21 ACL VLAN Filter Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
VID List	Enter the VLAN ID list that will be used here. Select the All VLANs option to apply this configuration to all the VLANs configured on this Switch.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

CPU ACL

This window is used to display and configure the CPU ACL settings.
To view the following window, click **ACL > CPU ACL**, as shown below:

CPU ACL

CPU ACL

Filter Map Name

32 chars

Apply

Find

Total Entries: 0

Filter Map Name	Match Access-list			Match Ingress Interface
	IP ACL	IPv6 ACL	MAC ACL	

Figure 8-22 CPU ACL Window

The fields that can be configured are described below:

Parameter	Description
Filter Map Name	Enter the CPU ACL filter map name here. This name can be up to 32 characters long.

- Click the **Apply** button to accept the changes made.
- Click the **Find** button to locate a specific entry based on the information entered.
- Click the **Binding** button to configure the binding settings for the specified entry.
- Click the **Delete** button to delete the specified entry.
- Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Binding** button, the following page will appear.

Match Access-List

CPU ACL Configure

Filter Map Name

FMN

Match IP Access List

Sequence No. (1-65535)

ACL Name

Please Select

Apply

Delete

Match IPv6 Access List

Sequence No. (1-65535)

ACL Name

Please Select

Apply

Delete

Match MAC Access List

Sequence No. (1-65535)

ACL Name

Please Select

Apply

Delete

Match Ingress Interface

Unit

1

From Port

eth1/0/1

To Port

eth1/0/1

Apply

Delete

Figure 8-23 CPU ACL (Binding) Window

The fields that can be configured in **Match IP Access List** are described below:

241

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the standard or extended IP access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the Please Select button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match IPv6 Access List** are described below:

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the standard or extended IPv6 access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the Please Select button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match MAC Access List** are described below:

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the extended MAC access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the Please Select button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match Ingress Interface** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

After clicking the **Please Select** button, the following window will appear:

	ID	ACL Name	ACL Type
<input type="radio"/>	1	S-IP-ACL	Standard IP ACL
<input type="radio"/>	2000	E-IP-ACL	Extended IP ACL

1/1 |< < 1 > >| Go

OK

Figure 8-24 CPU ACL (Binding, Please Select) Window

The fields that can be configured are described below:

Parameter	Description
ACL List	Select the radio button next to the access list entry to use that access list in the configuration.

Select the ACL and click the **OK** button to accept the selection made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9. Security

Port Security

802.1X

AAA

RADIUS

TACACS

IMPB

DHCP Server Screening

ARP Spoofing Prevention

BPDU Attack Protection

MAC Authentication

Web-based Access Control

Network Access Authentication

Safeguard Engine

Trusted Host

Traffic Segmentation Settings

Storm Control

DoS Attack Prevention Settings

SSH

SSL

SFTP Server Settings

Port Security

Port Security Global Settings

This window is used to display and configure the global port security settings. Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view the following window, click **Security > Port Security > Port Security Global Settings**, as shown below:

Port Security Global Settings

Port Security Trap Settings

Trap State
☐ Enabled
☒ Disabled

Apply

Port Security Trap Rate Settings

Trap Rate (0-1000)

Apply

Port Security System Settings

System Maximum Address (1-12288)
☒ No Limit

Apply

Port Security VLAN Settings

VID List
VLAN Max Learning Address (1-12288)
☒ No Limit

Apply

Find VLAN

VID (1-4094)

Find

VID	Max Learning Address	Current No.
1	No Limit	0

Figure 9-1 Port Security Global Settings Window

The fields that can be configured in **Port Security Trap Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable port security traps on the Switch.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Port Security Trap Rate Settings** are described below:

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 31 indicates an SNMP trap to be generated for every security violation.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Port Security System Settings** are described below:

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit. The valid range is from 1 to 12288. Tick the No Limit checkbox to allow the maximum number of secure MAC address.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Port Security VLAN Settings** are described below:

Parameter	Description
VID List	Enter the VLAN ID(s) here.
VLAN Max Learning Address	Enter the maximum number of allowed MAC addresses that can be learned on the specified VLAN(s) here. The range is from 1 to 12288. Tick the No Limit checkbox to allow the maximum number of secure MAC address.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Find VLAN** are described below:

Parameter	Description
VID	Enter the VLAN ID that will be located here.

Click the **Find** button to locate a specific entry based on the information entered.

Port Security Port Settings

This window is used to display and configure the port security port settings.

To view the following window, click **Security > Port Security > Port Security Port Settings**, as shown below:

Port Security Port Settings

Port Security Port Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 State: Disabled Maximum (0-12288): 32 Violation Action: Protect Security Mode: Delete-on-Timeout Aging Time (0-1440): Aging Type: Absolute

Apply

Unit 1 Settings

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
eth1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/4	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/7	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/8	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute

Figure 9-2 Port Security Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 0 and 12288. By default, this value is 32.
Violation Action	<p>Select the violation action that will be taken here. Options to choose from are Protect, Restrict, and Shutdown.</p> <ul style="list-style-type: none"> Selecting Protect specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. Selecting Restrict specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. Selecting Shutdown specifies to shut down the port if there is a security violation and record the system log.
Security Mode	<p>Select the security mode option here. Options to choose from are Permanent and Delete-on-Timeout.</p> <ul style="list-style-type: none"> Selecting Permanent specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries. Selecting Delete-on-Timeout specifies that under this mode, all learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.
Aging Type	<p>Select the aging type here. Options to choose from are Absolute and Inactivity.</p> <ul style="list-style-type: none"> Selecting Absolute specifies that all the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type.

Parameter	Description
	<ul style="list-style-type: none"> Selecting Inactivity specifies that the secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Click the **Apply** button to accept the changes made.

Port Security Address Entries

This window is used to view, clear and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:

Figure 9-3 Port Security Address Entries Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the appropriate port range used for the configuration here.
MAC Address	Enter the MAC address here. Select the Permanent option to specify that all learned MAC addresses will not be purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID here. This value must be between 1 and 4094.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove a new entry based on the information entered.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

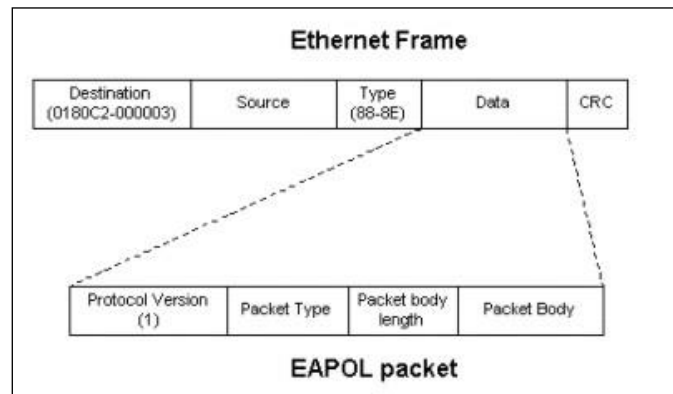


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

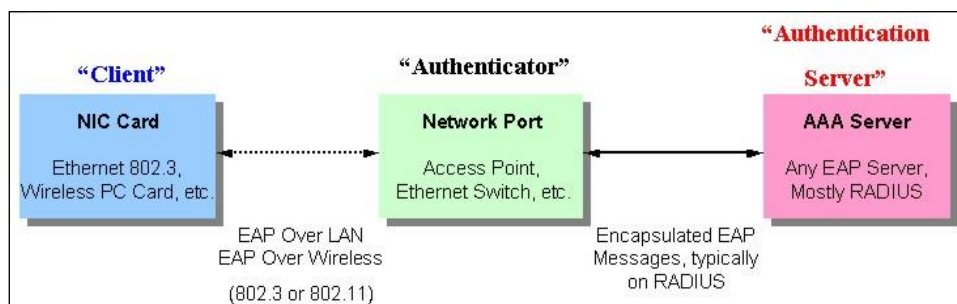


Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or Switches services.

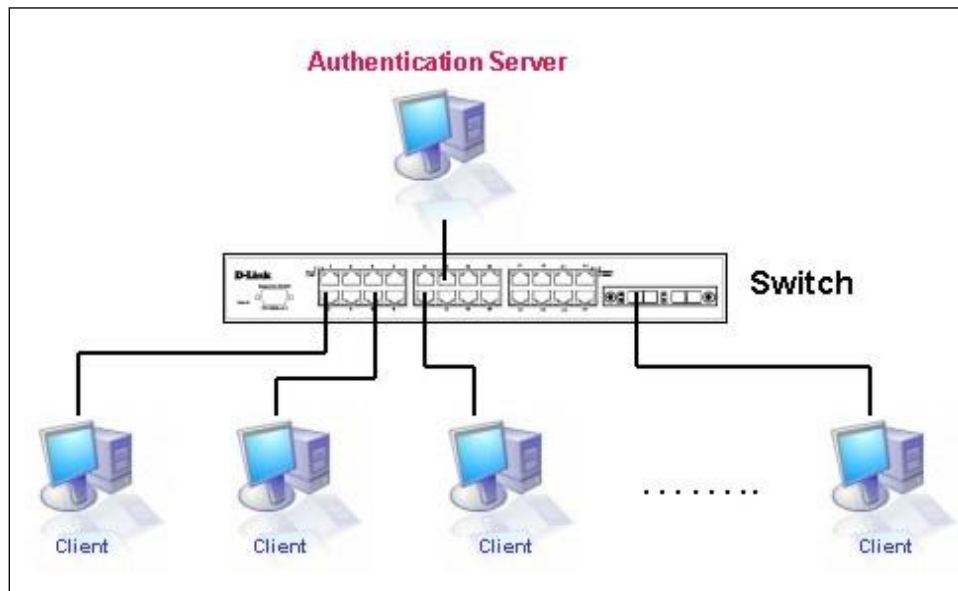


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

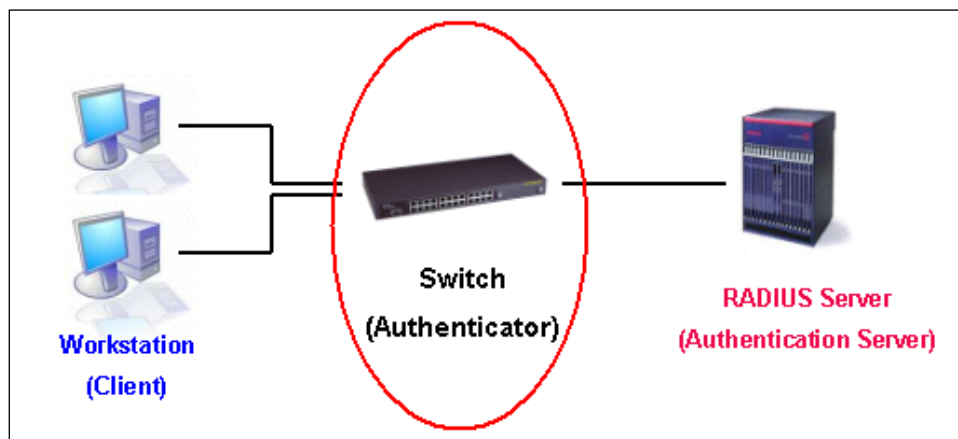


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X State must be Enabled. (**Security > 802.1X > 802.1X Global Settings**)
- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or Switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows 7 and later, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

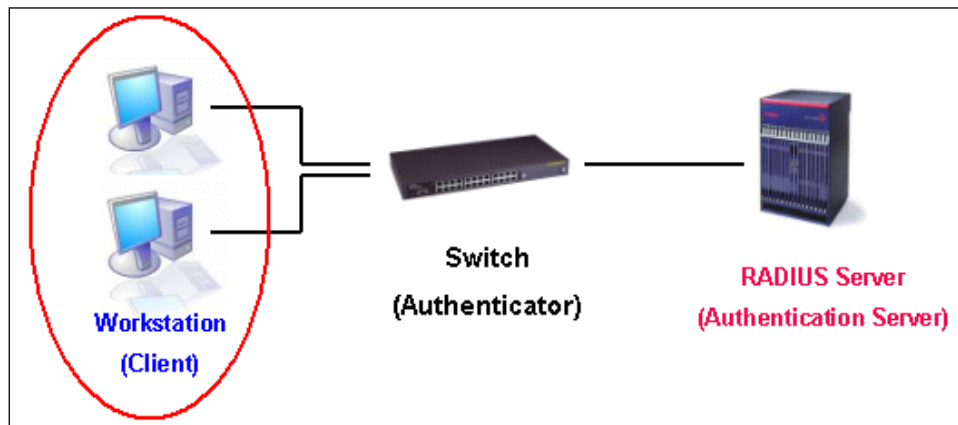


Figure 9-8 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

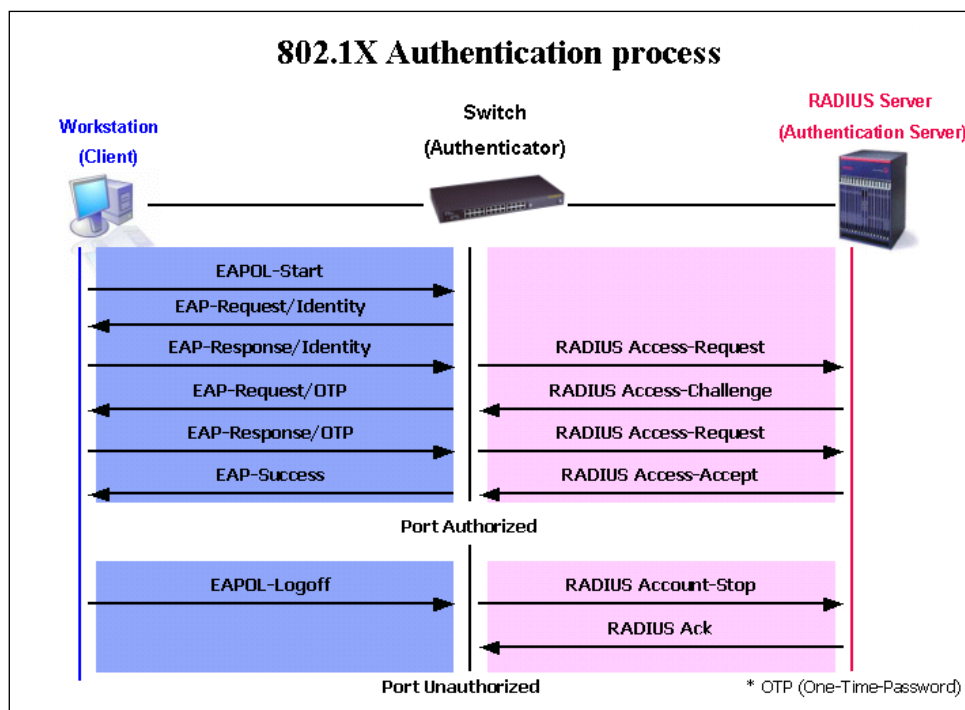


Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **Port-based Access Control** - This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
- **Host-based Access Control** - Using this method, the Switch will automatically learn up to a maximum of 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

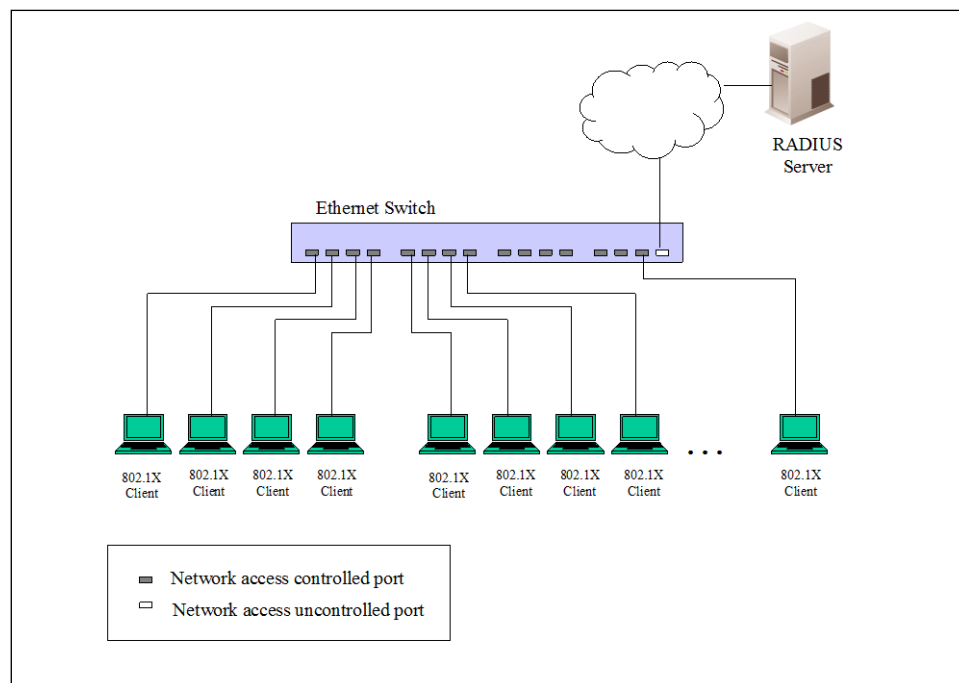


Figure 9-10 Example of Typical Port-based Configuration

Host-based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

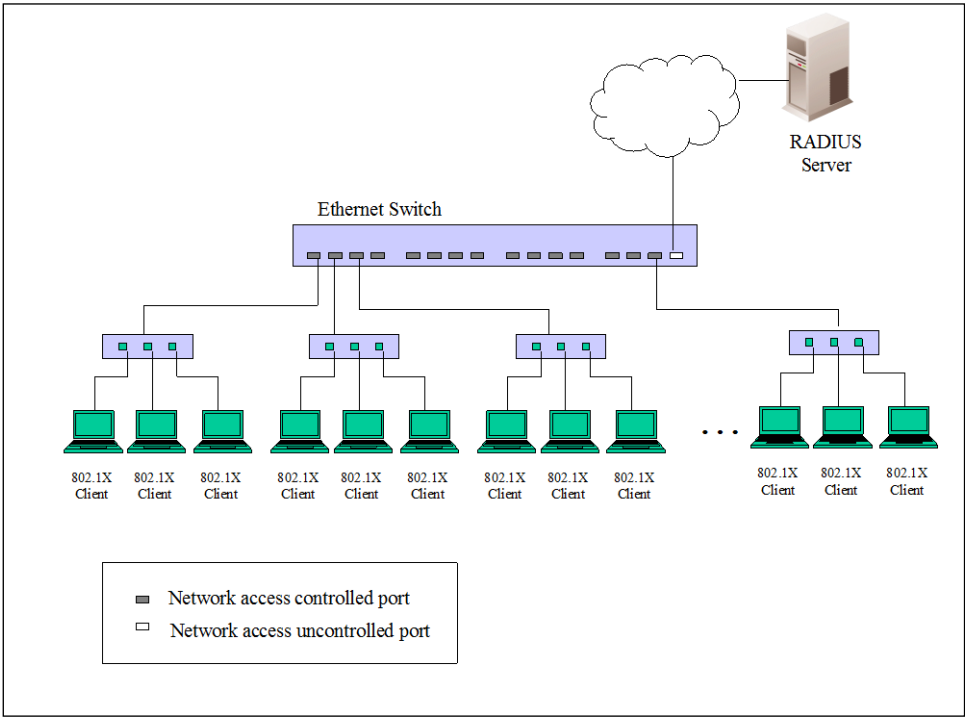


Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to display and configure the global 802.1X settings.
To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:

802.1X Global Settings

802.1X Global Settings

802.1X State

Disabled

802.1X Trap State

Disabled

Apply

Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

Parameter	Description
802.1X State	Select to enable or disable the global 802.1X state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

Click the **Apply** button to accept the changes made.

802.1X Port Settings

This window is used to display and configure the 802.1X port settings.
To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:

802.1X Port Settings

Unit: 1, From Port: eth1/0/1, To Port: eth1/0/1, Direction: Both, Port Control: Auto, Forward PDU: Disabled, MaxReq (1-10): 2 times, PAE Authenticator: Disabled, ServerTimeout (1-65535): 30 sec, SuppTimeout (1-65535): 30 sec, TX Period (1-65535): 30 sec. [Apply]

Unit 1 Settings

Port	Direction	Port Control	Forward PDU	MaxReq	PAE Authenticator	ServerTimeout	SuppTimeout	TX Period
eth1/0/1	Both	Auto	Disabled	2	None	30	30	30
eth1/0/2	Both	Auto	Disabled	2	None	30	30	30
eth1/0/3	Both	Auto	Disabled	2	None	30	30	30
eth1/0/4	Both	Auto	Disabled	2	None	30	30	30
eth1/0/5	Both	Auto	Disabled	2	None	30	30	30
eth1/0/6	Both	Auto	Disabled	2	None	30	30	30

Figure 9-13 802.1X Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are Both and In . This option configures the direction of the traffic on a controlled port as unidirectional (In) or bidirectional (Both).
Port Control	Select the port control option here. Options to choose from are ForceAuthorized , Auto , and ForceUnauthorized . If the port control is set to force-authorized, then the port is not controlled in both directions. If the port control is set to automatic, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to force-unauthorized, then the access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. This value must be between 1 and 10. By default, this option is 2. This option configures the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
SuppTimeout	Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
TX Period	Enter the transmission period value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

Click the **Apply** button to accept the changes made.

Authentication Sessions Information

This window is used to display and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Sessions Information**, as shown below:



The screenshot shows the 'Authentication Sessions Information' window. At the top, there are three dropdown menus: 'Unit' (set to 1), 'From Port' (set to eth1/0/1), and 'To Port' (set to eth1/0/1). To the right of these are two buttons: 'Init by Port' and 'ReAuth by Port'. Below these is a section titled 'Total Entries: 1'. It contains a table with two columns: 'Port' and 'MAC Address'. The table has one row with 'eth1/0/1' and '10-BF-48-D6-E2-E2'. To the right of the table are two buttons: 'Init by MAC' and 'ReAuth by MAC'. At the bottom right, there is a pagination control showing '1/1' and a 'Go' button.

Figure 9-14 Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Init by Port** button to initiate the session information based on the port selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the port selections made.

Click the **Init by MAC** button to initiate the session information based on the MAC address.

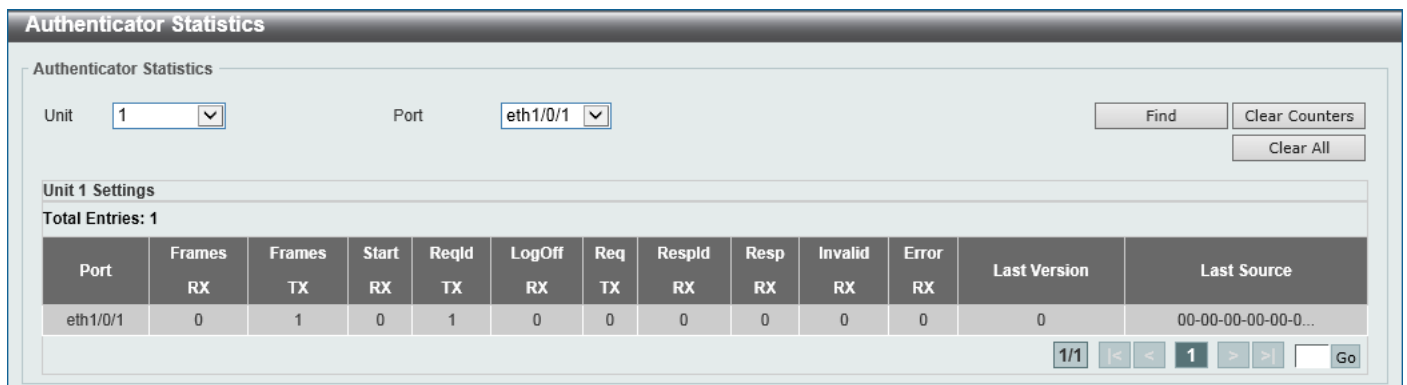
Click the **ReAuth by MAC** button to re-authenticate the session information based on the MAC address.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:



The screenshot shows the 'Authenticator Statistics' window. At the top, there are two dropdown menus: 'Unit' (set to 1) and 'Port' (set to eth1/0/1). To the right of these are three buttons: 'Find', 'Clear Counters', and 'Clear All'. Below these is a section titled 'Unit 1 Settings'. It contains a table with 13 columns: 'Port', 'Frames RX', 'Frames TX', 'Start RX', 'ReqId TX', 'LogOff RX', 'Req TX', 'RespId RX', 'Resp RX', 'Invalid RX', 'Error RX', 'Last Version', and 'Last Source'. The table has one row with 'eth1/0/1' and various statistics. At the bottom right, there is a pagination control showing '1/1' and a 'Go' button.

Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Session Statistics

This window is used to view and clear the authenticator session statistics.

To view the following window, click **Security > 802.1X > Authenticator Session Statistics**, as shown below:

Authenticator Session Statistics

Authenticator Session Statistics

Unit: 1 Port: eth1/0/1

Find Clear Counters Clear All

Unit 1 Settings

Total Entries: 0

Port	Octets RX	Octets TX	Frames RX	Frames TX	ID	AuthenticMethod	Time	TerminateCause	User Name
------	-----------	-----------	-----------	-----------	----	-----------------	------	----------------	-----------

Figure 9-16 Authenticator Session Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

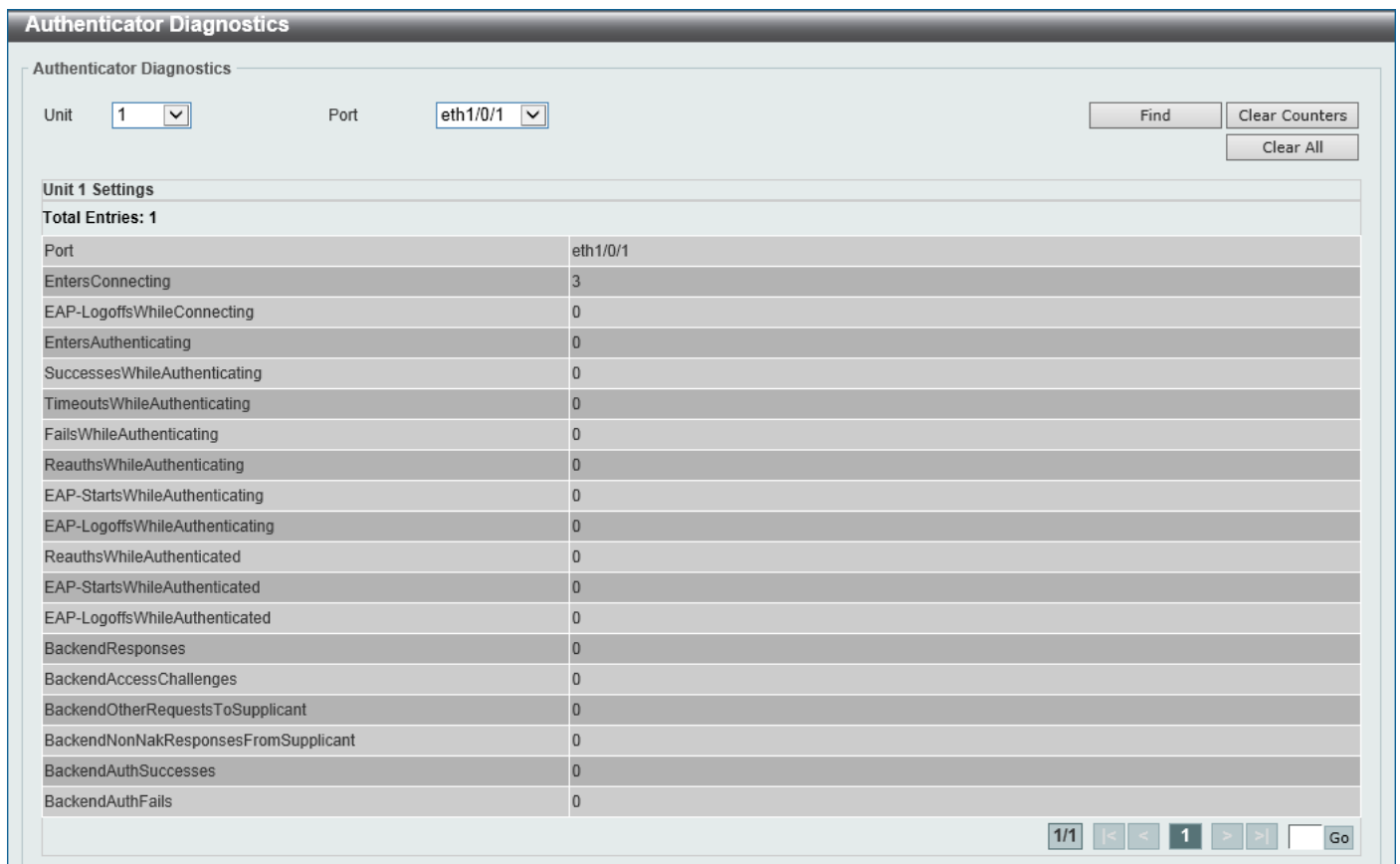
Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Authenticator Diagnostics

This window is used to view and clear the authenticator diagnostics information.

To view the following window, click **Security > 802.1X > Authenticator Diagnostics**, as shown below:



The Authenticator Diagnostics window displays a table of authentication statistics for a specific unit and port. At the top, there are dropdown menus for 'Unit' (set to 1) and 'Port' (set to eth1/0/1). To the right are buttons for 'Find', 'Clear Counters', and 'Clear All'. Below the filters, the 'Unit 1 Settings' section shows a table with 20 rows of statistics. The first row, 'Port', is highlighted and shows 'eth1/0/1'. The other rows show various counters, most of which are 0, except for 'EntersConnecting' which is 3. At the bottom right, there is a pagination control showing '1/1' and navigation buttons.

Unit 1 Settings	
Total Entries: 1	
Port	eth1/0/1
EntersConnecting	3
EAP-LogoffsWhileConnecting	0
EntersAuthenticating	0
SuccessesWhileAuthenticating	0
TimeoutsWhileAuthenticating	0
FailsWhileAuthenticating	0
ReauthsWhileAuthenticating	0
EAP-StartsWhileAuthenticating	0
EAP-LogoffsWhileAuthenticating	0
ReauthsWhileAuthenticated	0
EAP-StartsWhileAuthenticated	0
EAP-LogoffsWhileAuthenticated	0
BackendResponses	0
BackendAccessChallenges	0
BackendOtherRequestsToSupplicant	0
BackendNonNakResponsesFromSupplicant	0
BackendAuthSuccesses	0
BackendAuthFails	0

Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

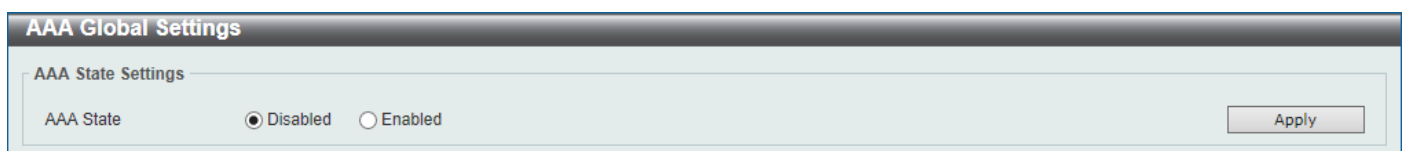
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

AAA

AAA Global Settings

This window is used to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

To view the following window, click **Security > AAA > AAA Global Settings**, as shown below:



The AAA Global Settings window shows the 'AAA State Settings' section. It contains a label 'AAA State' followed by two radio buttons: 'Disabled' (which is selected) and 'Enabled'. An 'Apply' button is located on the right side of the window.

Figure 9-18 AAA Global Settings Window

The fields that can be configured are described below:

Parameter	Description
AAA State	Select to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

Click the **Apply** button to accept the changes made.

Application Authentication Settings

This window is used to display and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:

Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit

Figure 9-19 Application Authentication Settings Window

Click the **Edit** button to re-configure the specific entry.

Application	Login Method List	
Console	default	Apply
Telnet	default	Edit
SSH	default	Edit

Figure 9-20 Application Authentication Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the Edit button for the specific entry, enter the login method list name used here.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Application Accounting Settings

This window is used to display and configure the application accounting settings.

To view the following window, click **Security > AAA > Application Accounting Settings**, as shown below:

Figure 9-21 Application Accounting Settings Window

Click the **Edit** button to re-configure the specific entry.

Figure 9-22 Application Accounting Settings (Edit) Window

The fields that can be configured in **Application Accounting Exec Method list** are described below:

Parameter	Description
Exec Method List	After clicking the Edit button for the specific entry, enter the EXEC method list name used here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Application Accounting Commands Method List** are described below:

Parameter	Description
Application	Select the application used here. Options to choose from are Console , Telnet , and SSH .
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
Commands Method List	Enter the commands method list name used here.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authentication Settings

This window is used to display and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:

Figure 9-23 Authentication Settings Window

The fields that can be configured in **AAA Authentication 802.1X** are described below:

Parameter	Description
Status	Select to enable or disable the AAA 802.1X authentication state here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> • 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	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> • none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. • local - Specifies to use the local database for authentication.

Parameter	Description
	<ul style="list-style-type: none"> • group - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • radius - Specifies to use the servers defined by the RADIUS server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication WEB-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA Web authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: <ul style="list-style-type: none"> • none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. • local - Specifies to use the local database for authentication. • group - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • radius - Specifies to use the servers defined by the RADIUS server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication IGMP-Auth Default Group RADIUS** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication IGMP authentication default group RADIUS feature here.

Click the **Apply** button to accept the changes made.

After clicking the **AAA Authentication Exec** tab, the following page will appear.

Authentication Settings

AAA Authentication Network | **AAA Authentication Exec**

AAA Authentication Enable

Status:

Method 1: Method 2:

Method 3: Method 4:

AAA Authentication Login

List Name:

Method 1: Method 2:

Method 3: Method 4:

Total Entries: 1

Name	Method 1	Method 2	Method 3	Method 4
list	radius	tacacs+	local	

Figure 9-24 Authentication Settings (AAA Authentication EXEC) Window

The fields that can be configured in **AAA Authentication Enable** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> • none - Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by previous method authentication. • enable - Specifies to use the local enable password for authentication. • group - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • radius - Specifies to use the servers defined by the RADIUS server host command. • tacacs+ - Specifies to use the servers defined by the TACACS+ server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication Login** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> • none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method's authentication. • local - Specifies to use the local database for authentication. • group - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • radius - Specifies to use the servers defined by the RADIUS server host command. • tacacs+ - Specifies to use the servers defined by the TACACS+ server host command.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Accounting Settings

This window is used to display and configure the AAA accounting settings.

To view the following window, click **Security > AAA > Accounting Settings**, as shown below:

Figure 9-25 Accounting Settings Window

The fields that can be configured in **AAA Accounting Network** are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ . The none option is only available for Method 1 .

Click the **Apply** button to accept the changes made.

After clicking the **AAA Accounting System** tab, the following page will appear.

Figure 9-26 Accounting Settings (AAA Accounting System) Window

The fields that can be configured in **AAA Accounting System** are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ . The none option is only available for Method 1 .

Click the **Apply** button to accept the changes made.

After clicking the **AAA Accounting Exec** tab, the following page will appear.

Name	Method 1	Method 2	Method 3	Method 4
list	radius	tacacs+		

Figure 9-27 Accounting Settings (AAA Accounting Exec) Window

The fields that can be configured in **AAA Accounting Exec** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA accounting EXEC option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ . The none option is only available for Method 1 .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

After clicking the **AAA Accounting Commands** tab, the following page will appear.

Figure 9-28 Accounting Settings (AAA Accounting Commands) Window

The fields that can be configured are described below:

Parameter	Description
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
List Name	Enter the method list name that will be used with the AAA accounting commands option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , and tacacs+ . The none option is only available for Method 1 .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

RADIUS

RADIUS Global Settings

This window is used to display and configure the global RADIUS settings.

To view the following window, click **Security > RADIUS > RADIUS Global Settings**, as shown below:

Figure 9-29 RADIUS Global Settings Window

The fields that can be configured in **RADIUS Global Settings** are described below:

Parameter	Description
DeadTime	<p>Enter the dead time value here. This value must be between 1 and 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries.</p> <p>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.</p>

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RADIUS Global IPv4 Source Interface** are described below:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the IPv4 RADIUS source interface here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RADIUS Global IPv6 Source Interface** are described below:

Parameter	Description
IPv6 RADIUS Source Interface Name	Enter the name of the IPv6 RADIUS source interface here.

Click the **Apply** button to accept the changes made.

RADIUS Server Settings

This window is used to display and configure the RADIUS server settings.

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:

RADIUS Server Settings

RADIUS Server Settings

☒ IP Address ☐ IPv6 Address

Authentication Port (0-65535): 1812 Accounting Port (0-65535): 1813

Retransmit (0-20): 2 times Timeout (1-255): 5 sec

Key Type: Plain Text Key: 32 chars

Apply

Total Entries: 1

IPv4/IPv6 Address	Authentication Port	Accounting Port	Timeout	Retransmit	Key	
10.90.90.91	1812	1813	5	2	*****	Delete

Figure 9-30 RADIUS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server IPv4 address here.
IPv6 Address	Enter the RADIUS server IPv6 address here.

Parameter	Description
Authentication Port	Enter the authentication port number used here. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. This value must be between 0 and 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 3. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:

RADIUS Group Server Settings

RADIUS Group Server Settings

Group Server Name: 32 chars

☒ IP Address

☐ IPv6 Address: 2013::1

Add

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
group	10.1.1.1	-	-	-	-	-	-	-	Show Detail
radius	10.90.90.9...	-	-	-	-	-	-	-	Delete

Figure 9-31 RADIUS Group Server Settings Window

The fields that can be configured are described below:

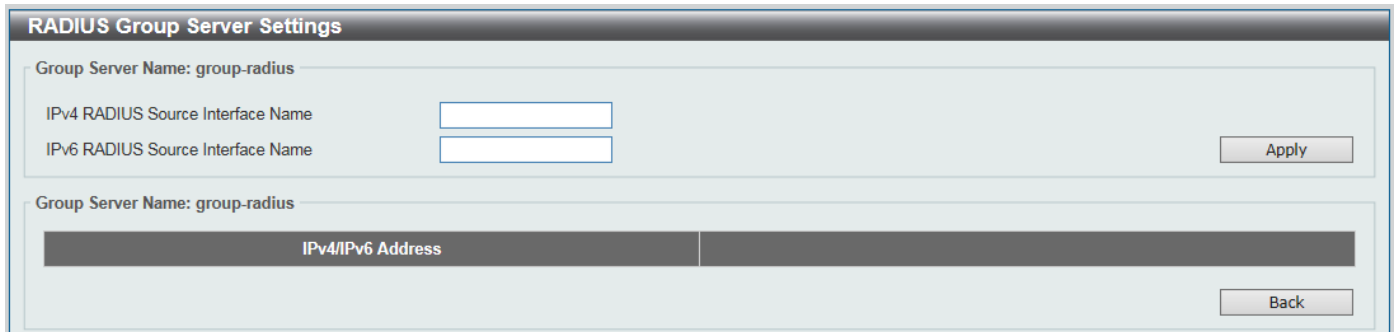
Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IP Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure more detailed settings for the RADIUS group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.



RADIUS Group Server Settings

Group Server Name: group-radius

IPv4 RADIUS Source Interface Name

IPv6 RADIUS Source Interface Name

Apply

Group Server Name: group-radius

IPv4/IPv6 Address

Back

Figure 9-32 RADIUS Group Server Settings (Detail) Window

The fields that can be configured are described below:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the source IPv4 RADIUS interface here.
IPv6 RADIUS Source Interface Name	Enter the name of the source IPv6 RADIUS interface here.

Click the **Apply** button to accept the changes made.

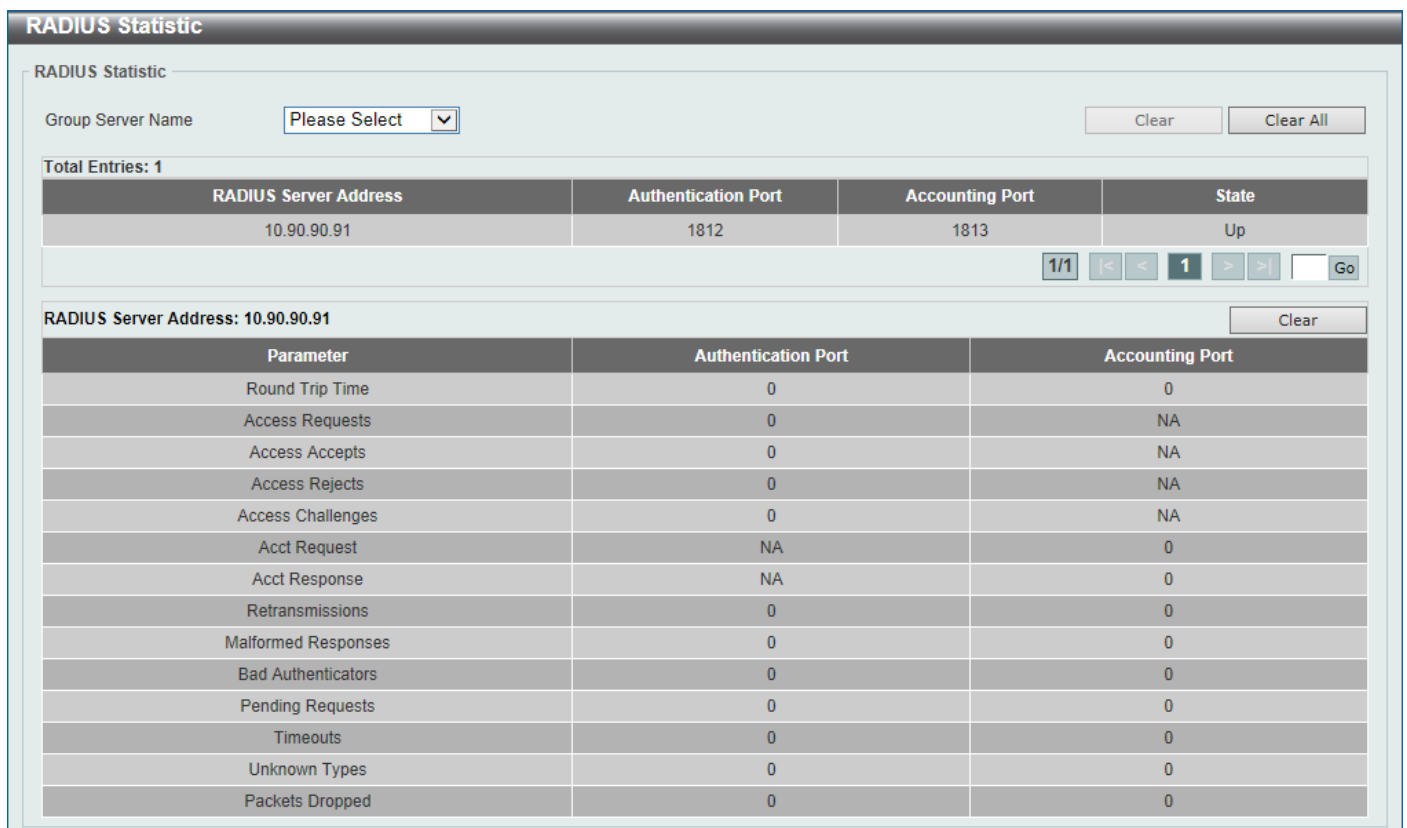
Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:



RADIUS Statistic

RADIUS Statistic

Group Server Name **Clear** **Clear All**

Total Entries: 1

RADIUS Server Address	Authentication Port	Accounting Port	State
10.90.90.91	1812	1813	Up

1/1 |< < 1 > >| Go

RADIUS Server Address: 10.90.90.91 **Clear**

Parameter	Authentication Port	Accounting Port
Round Trip Time	0	0
Access Requests	0	NA
Access Accepts	0	NA
Access Rejects	0	NA
Access Challenges	0	NA
Acct Request	NA	0
Acct Response	NA	0
Retransmissions	0	0
Malformed Responses	0	0
Bad Authenticators	0	0
Pending Requests	0	0
Timeouts	0	0
Unknown Types	0	0
Packets Dropped	0	0

Figure 9-33 RADIUS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

TACACS



NOTE: In this section, settings associated with the TACACS+ feature will be configured, even though the word “TACACS” is used in the Web UI.

TACACS Global Settings

This window is used to display and configure the global TACACS+ server settings.

To view the following window, click **Security > TACACS > TACACS Global Settings**, as shown below:

Figure 9-34 TACACS Global Settings Window

The fields that can be configured in **TACACS Global IPv4 Source Interface** are described below:

Parameter	Description
IPv4 TACACS Source Interface Name	Enter the name of the IPv4 TACACS+ source interface here.

Click the **Apply** button to accept the changes made.

TACACS Server Settings

This window is used to display and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS > TACACS Server Settings**, as shown below:

Figure 9-35 TACACS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server IPv4 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

TACACS Group Server Settings

This window is used to display and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS > TACACS Group Server Settings**, as shown below:

Figure 9-36 TACACS Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 TACACS Server IP	Enter the group server IPv4 address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure more detailed settings for the TACACS+ group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.

Figure 9-37 TACACS Group Server Settings (Show Detail) Window

The fields that can be configured are described below:

Parameter	Description
IPv4 TACACS Source Interface Name	Enter the name of the source IPv4 TACACS+ interface here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

TACACS Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click **Security > TACACS > TACACS Statistic**, as shown below:

Figure 9-38 TACACS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the information based on the group selected.

Click the **Clear All** button to clear all the information in this table.

Click the second **Clear** button to clear all the information for the specific entry.

IMPB

The IP network layer uses a four-byte address. The Ethernet link-layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port Binding (IMPB) is to restrict the access to a Switch to a number of authorized users. Authorized clients can access a Switch's port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the Switch will automatically learn the IP/MAC pairs by snooping DHCP packets and

saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

This window is used to display and configure the global DHCP snooping settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:

Figure 9-39 DHCP Snooping Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Snooping	Select to enable or disable the global DHCP snooping status.
Information Option Allow Untrusted	Select to enable or disable the option to globally allow DHCP packets with the relay Option 82 on the untrusted interface.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address.
Station Move Deny	Select to enable or disable the DHCP snooping station move state. When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

Click the **Apply** button to accept the changes made.

DHCP Snooping Port Settings

This window is used to display and configure the DHCP snooping port settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings**, as shown below:

Port	Trusted	Rate Limit	Entry Limit
eth1/0/1	No	No Limit	No Limit
eth1/0/2	No	No Limit	No Limit
eth1/0/3	No	No Limit	No Limit
eth1/0/4	No	No Limit	No Limit
eth1/0/5	No	No Limit	No Limit
eth1/0/6	No	No Limit	No Limit
eth1/0/7	No	No Limit	No Limit
eth1/0/8	No	No Limit	No Limit

Figure 9-40 DHCP Snooping Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. 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.

DHCP Snooping VLAN Settings

This window is used to display and configure the DHCP snooping VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:

Figure 9-41 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Parameter	Description
State	Select to enable or disable the DHCP snooping VLAN setting here.

Click the **Apply** button to accept the changes made.

DHCP Snooping Database

This window is used to display and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:

Figure 9-42 DHCP Snooping Database Window

The fields that can be configured in **DHCP Snooping Database** are described below:

Parameter	Description
Write Delay	Enter the write delay time value here. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds.

Click the **Reset** button to reset the information entered.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be stored to here. Locations to choose from are TFTP , FTP , and Flash . An example URL is given.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Load DHCP Snooping Database** are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be loaded from here. Locations to choose from are TFTP , FTP , and Flash . An example URL is given.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear all the counter information.

DHCP Snooping Binding Entry

This window is used to display and configure the DHCP snooping binding entries.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry**, as shown below:

Figure 9-43 DHCP Snooping Binding Entry Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID of the DHCP snooping binding entry here. This value must be between 1 and 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Dynamic ARP Inspection

ARP Access List

This window is used to display and configure the dynamic ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:

The screenshot shows the 'ARP Access List' configuration window. At the top, there's a title bar 'ARP Access List'. Below it, a section 'ARP Access List' contains a text input field for 'ARP Access List Name' with a '32 chars' limit and an 'Add' button. Below this, a table shows 'Total Entries: 1'. The table has two columns: 'ARP Access List Name' and an empty column. The first row contains the entry 'ARP'. To the right of the table are 'Edit' and 'Delete' buttons.

Figure 9-44 ARP Access List Window

The fields that can be configured are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

Click the **Add** button to add a new entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Edit** button, the following window will appear.

The screenshot shows the 'ARP Access List (Edit)' window. It has a title bar 'ARP Access List'. Below it, there are configuration fields: 'Action' (dropdown with 'Permit'), 'IP' (dropdown with 'Any'), 'MAC' (dropdown with 'Any'), 'Sender IP' (text input), 'Sender IP Mask' (text input), 'Sender MAC' (text input), and 'Sender MAC Mask' (text input). There are 'Back' and 'Apply' buttons. Below these fields, it says 'ARP Access List Name: ARP'. At the bottom, a table shows 'Total Entries: 1'. The table has columns: 'Action', 'IP Type', 'Sender IP', 'Sender IP Mask', 'MAC Type', 'Sender MAC', 'Sender MAC Mask', and an empty column. The first row contains the entry 'Permit', 'Any', '-', '-', 'Any', '-', '-'. To the right of the table is a 'Delete' button.

Figure 9-45 ARP Access List (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Permit and Deny .
IP	Select the type of sender IP address that will be used here. Options to choose from are Any , Host , and IP with Mask .
Sender IP	After selecting the Host or IP with Mask options as the type of IP , enter the sender IP address used here.
Sender IP Mask	After selecting the IP with Mask option as the type of IP , enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are Any , Host , and MAC with Mask .
Sender MAC	After selecting the Host or MAC with Mask options as the type of MAC , enter the sender MAC address used here.
Sender MAC Mask	After selecting the MAC with Mask option as the type of MAC , enter the sender MAC mask used here.

Click the **Back** button to return to the previous page.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Inspection Settings

This window is used to display and configure the ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings**, as shown below:

Figure 9-46 ARP Inspection Settings Window

The fields that can be configured in **ARP Inspection Validation** are described below:

Parameter	Description
Src-MAC	Select to enable or disable the source MAC option here. This option specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
Dst-MAC	Select to enable or disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
IP	Select to enable or disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting Yes or No .

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Port Settings

This window is used to display and configure the ARP inspection port settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:

Port	Trust State	Rate Limit (pps)	Burst Interval
eth1/0/1	Untrusted	15	1
eth1/0/2	Untrusted	15	1
eth1/0/3	Untrusted	15	1
eth1/0/4	Untrusted	15	1
eth1/0/5	Untrusted	15	1
eth1/0/6	Untrusted	15	1
eth1/0/7	Untrusted	15	1
eth1/0/8	Untrusted	15	1

Figure 9-47 ARP Inspection Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 150 packets per seconds.
Burst Interval	Enter the burst interval value here. This value must be between 1 and 15. Tick the None option to disable the option.
Trust State	Select to enable or disable the trust state here.

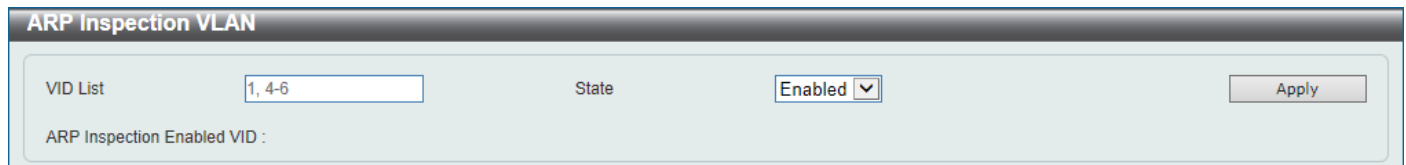
Click the **Apply** button to accept the changes made.

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

This window is used to display and configure the ARP inspection VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:



The screenshot shows the 'ARP Inspection VLAN' configuration window. It has a title bar 'ARP Inspection VLAN'. Inside, there is a 'VID List' input field containing '1, 4-6', a 'State' dropdown menu set to 'Enabled', and an 'Apply' button. Below these fields, it says 'ARP Inspection Enabled VID :'. The background is light blue.

Figure 9-48 ARP Inspection VLAN Window

The fields that can be configured are described below:

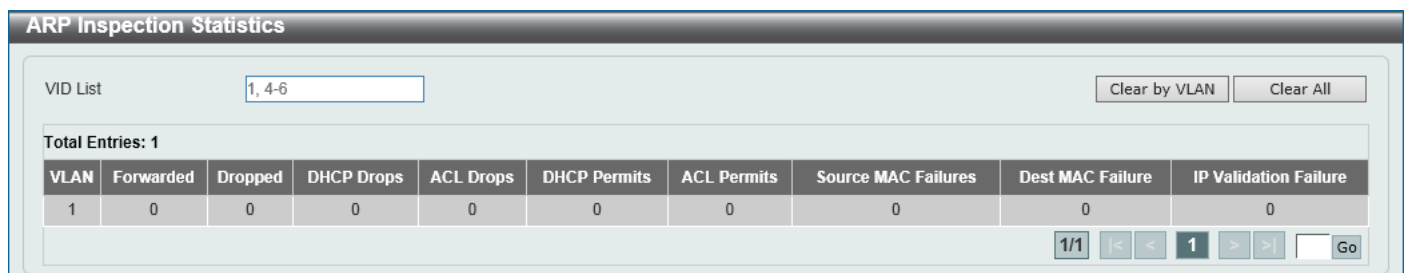
Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the ARP inspection option's state for the specified VLAN here.

Click the **Apply** button to accept the changes made.

ARP Inspection Statistics

This window is used to view and clear the ARP inspection statistics information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics**, as shown below:



The screenshot shows the 'ARP Inspection Statistics' window. It has a title bar 'ARP Inspection Statistics'. Inside, there is a 'VID List' input field containing '1, 4-6', and two buttons: 'Clear by VLAN' and 'Clear All'. Below these, it says 'Total Entries: 1'. There is a table with 10 columns: VLAN, Forwarded, Dropped, DHCP Drops, ACL Drops, DHCP Permits, ACL Permits, Source MAC Failures, Dest MAC Failure, and IP Validation Failure. The first row shows values for VLAN 1. At the bottom right, there is a pagination control showing '1/1' and a 'Go' button.

VLAN	Forwarded	Dropped	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Source MAC Failures	Dest MAC Failure	IP Validation Failure
1	0	0	0	0	0	0	0	0	0

Figure 9-49 ARP Inspection Statistics Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Click the **Clear by VLAN** button to clear the information based on the VLAN ID(s) entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Log

This window is used to view, configure and clear the ARP inspection log information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log**, as shown below:



The ARP Inspection Log window has a title bar 'ARP Inspection Log'. Below it, there's a section 'ARP Inspection Log' containing a 'Log Buffer (1-1024)' field with the value '32' and two buttons: 'Apply' and 'Clear Log'. Below this, it says 'Total Entries: 0'. At the bottom, there's a table with five columns: 'Port', 'VLAN', 'Sender IP', 'Sender MAC', and 'Occurrence'.

Port	VLAN	Sender IP	Sender MAC	Occurrence
------	------	-----------	------------	------------

Figure 9-50 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
Log Buffer	Enter the log buffer value used here. This value must be between 1 and 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

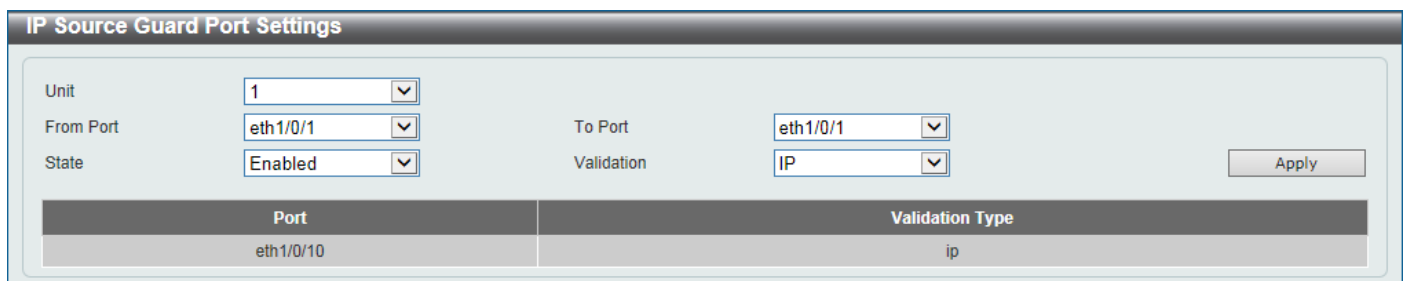
Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to display and configure the IP source guard port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:



The IP Source Guard Port Settings window has a title bar 'IP Source Guard Port Settings'. It contains several configuration fields: 'Unit' (dropdown with '1'), 'From Port' (dropdown with 'eth1/0/1'), 'To Port' (dropdown with 'eth1/0/1'), 'State' (dropdown with 'Enabled'), and 'Validation' (dropdown with 'IP'). There is an 'Apply' button. Below these fields is a table with two columns: 'Port' and 'Validation Type'.

Port	Validation Type
eth1/0/10	ip

Figure 9-51 IP Source Guard Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IP source guard's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are IP and IP-MAC . Selecting IP means that the IP address of the received packets will be checked. Selecting IP-MAC means that the IP address and the MAC address of the received packets will be checked.

Click the **Apply** button to accept the changes made.

IP Source Guard Binding

This window is used to display and configure the IP source guard binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:

Figure 9-52 IP Source Guard Binding Window

The fields that can be configured in **IP Source Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
IP Address	Enter the IP address of the binding entry here.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IP Source Binding Entry** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
From Port - To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	<p>Select the type of binding entry to find here. Options to choose from are All, DHCP Snooping, and Static.</p> <ul style="list-style-type: none"> Selecting All specifies that all the DHCP binding entries will be displayed. Selecting DHCP Snooping specifies to display the IP-source guard binding entry learned by DHCP binding snooping. Selecting Static specifies to display the IP-source guard binding entry that is manually configured.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IP Source Guard HW Entry

This window is used to view the IP source guard hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:

Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
eth1/0/10	ip	Active	10.90.90.233	-	1

Figure 9-53 IP Source Guard HW Entry Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
From Port - To Port	Select the appropriate port range used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Advanced Settings

IP-MAC-Port Binding Settings

This window is used to display and configure the IP-MAC-Port binding settings.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings**, as shown below:

Port	Mode
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled

Figure 9-54 IP-MAC-Port Binding Settings Window

The fields that can be configured in **IP-MAC-Port Binding Trap Settings** are described below:

Parameter	Description
Trap State	Select the enable or disable the IP-MAC-Port binding option's trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IP-MAC-Port Binding Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are Disabled , Strict , and Loose . When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

Click the **Apply** button to accept the changes made.

IP-MAC-Port Binding Blocked Entry

This window is used to view and clear the IP-MAC-Port binding blocked entry table.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry**, as shown below:

Figure 9-55 IP-MAC-Port Binding Blocked Entry Window

The fields that can be configured are described below:

Parameter	Description
Clear by Port	Select this option to clear the entry table based on the port(s) selected.
Unit	Select the Switch unit that will be clear here.
From Port - To Port	Select the appropriate port range that will be cleared here.
Clear by MAC	Select this option to clear the entry table based on the MAC address entered. Enter the MAC address that will be cleared in the space provided.
Clear All	Select this option to clear all entries that contain MAC addresses.

Click the **Apply** button to accept the changes made.

IPv6

IPv6 Snooping

This window is used to display and configure the IPv6 snooping settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Snooping**, as shown below:

Figure 9-56 IPv6 Snooping Window

The fields that can be configured in **Station Move Setting** are described below:

Parameter	Description
Station Move	Select the station move options here. Options to choose from are Permit and Deny .

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IPv6 Snooping Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 511. Tick the No Limit option to disable this option.
Protocol	<p>Select the protocol state here. Options to choose from are Enabled and Disabled.</p> <ul style="list-style-type: none"> Select DHCP to specify that addresses should be snooped in DHCPv6 packets. Select NDP to specify that addresses should be snooped in NDP packets. Select DHCP-PD to specify that the IPv6 prefix should be snooped in DHCPv6-PD packets. <p>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</p>

Parameter	Description
	NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not. DHCP-PD snooping performs DHCPv6 snooping of Prefix Delegation (PD) to setup bindings between the Delegating Router (assigned with an IPv6 prefix) and the corresponding Requesting Router. The bindings can be used to validate the source prefix in the packets.
VID List	Enter the VLAN ID list used here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 ND Inspection

This window is used to display and configure the IPv6 ND inspection settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 ND Inspection**, as shown below:

Figure 9-57 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.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 RA Guard

This window is used to display and configure the IPv6 Router Advertisement (RA) guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 RA Guard**, as shown below:

Figure 9-58 IPv6 RA Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Host and Router . By default, the device's role is Host , which will block all the RA packets. If the device's role is Router , RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the Please Select button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:

Figure 9-59 IPv6 RA Guard (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

IPv6 DHCP Guard

This window is used to display and configure the IPv6 DHCP guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:

Policy Name	Device Role	Match IPv6 Access List	Target Port
policy	Client	S-IPv6-ACL	eth1/0/14

Figure 9-60 IPv6 DHCP Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Client and Server . By default, the device's role is set as Client , which will block all the DHCPv6 packets from the DHCPv6 Server. If the device's role is set as Server , DHCPv6 Server packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the Please Select button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
Unit	Select the Switch unit that will be used for this configuration here.
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:

ID	ACL Name	ACL Type
11000	S-IPv6-ACL	Standard IPv6 ACL
13000	E-IPv6-ACL	Extended IPv6 ACL

Figure 9-61 IPv6 DHCP Guard (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

IPv6 Source Guard

IPv6 Source Guard Settings

This window is used to display and configure the IPv6 source guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:

Policy Name	Global Auto-Configure Address	Link Local Traffic	Validate Address	Validate Prefix	Target Port		
Policy	Permit	Deny	Enabled	Disabled		Edit	Delete

Figure 9-62 IPv6 Source Guard Settings Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to permit or 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.
Link Local Traffic	Select to permit or deny hardware permitted data traffic sent by the link-local address.
Validate Address	Select to enable or disable the validate address feature here. This is used to enable the IPv6 source guard to perform the validate address feature.
Validate Prefix	Select to enable or disable the validate prefix feature here. This is used to enable the IPv6 source guard to perform the IPv6 prefix-guard operation.
Target Port	Tick this option to specify the target port.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 Neighbor Binding

This window is used to display and configure the IPv6 neighbor binding settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding**, as shown below:

Figure 9-63 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.
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IPv6 Neighbor Binding Entry** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this search here.
From Port - To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCP Server Screening

This function allows users to not only to restrict all DHCP server packets but also to receive any specified DHCP server packet by any specified DHCP client. It is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

When the DHCP Server Screening function is enabled on a port, all DHCP server packets received on this ports will be redirected to the CPU for a software-based check. Legal DHCP server packets will be forwarded out and illegal DHCP server packets will be dropped.

When DHCP Server Screening function is enabled all DHCP Server packets will be filtered from a specific port.

DHCP Server Screening Global Settings

This window is used to display and configure the global DHCP server screening settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Global Settings**, as shown below:

Figure 9-64 DHCP Server Screening Global Settings Window

The fields that can be configured in **Trap Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DHCP server screening trap here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.
Client MAC	Enter the MAC address used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Delete Profile** button to remove the specified profile.

The fields that can be configured in **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. This value must be between 10 and 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

Click the **Clear Log** button to clear the log.

DHCP Server Screening Port Settings

This window is used to display and configure the DHCP server screening port settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:

Unit	From Port	To Port	State	Server IP	Profile Name	
1	eth1/0/1	eth1/0/1	Disabled		32 chars	Apply

Port	State	Server IP	Profile Name	
eth1/0/1	Disabled	-	-	Delete
eth1/0/2	Disabled	-	-	Delete
eth1/0/3	Disabled	-	-	Delete
eth1/0/4	Disabled	-	-	Delete
eth1/0/5	Disabled	-	-	Delete
eth1/0/6	Disabled	-	-	Delete
eth1/0/7	Disabled	-	-	Delete
eth1/0/8	Disabled	-	-	Delete

Figure 9-65 DHCP Server Screening Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the DHCP server screening function on the port(s) specified.
Server IP	Enter the DHCP server IP address here.
Profile Name	Enter the DHCP server screening profile that will be used for the port(s) specified here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Spoofing Prevention

This window is used to display and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

To view the following window, click **Security > ARP Spoofing Prevention**, as shown below:

ARP Spoofing Prevention

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Gateway IP: .

Gateway MAC: 00-11-22-33-44-aa

Apply

Total Entries: 1

Gateway IP	Gateway MAC	Port	
10.90.90.1	00-11-22-33-44-55	eth1/0/16	Delete

Figure 9-66 ARP Spoofing Prevention Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway IP address used here.
Gateway MAC	Enter the gateway MAC address used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

BPDU Attack Protection

This window is used to display and configure the BPDU attack protection settings. In generally, there are two states in the BPDU attack protection function. One is normal state, and another is under attack state. The under attack state has three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet and it will take action based on the configuration.

BPDU protection has a higher priority than the (Forward BPDU) FBPDU setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

To view the following window, click **Security > BPDU Attack Protection**, as shown below:

BPDUs Attack Protection

BPDUs Attack Protection Global Settings

BPDUs Attack Protection State ☐ Enabled ☒ Disabled

BPDUs Attack Protection Trap State ☐ Enabled ☒ Disabled

Apply

BPDUs Attack Protection Port Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 State: Disabled Mode: Shutdown

Apply

Unit 1 Settings

Port	State	Mode	Status
eth1/0/1	Disabled	Shutdown	Normal
eth1/0/2	Disabled	Shutdown	Normal
eth1/0/3	Disabled	Shutdown	Normal
eth1/0/4	Disabled	Shutdown	Normal
eth1/0/5	Disabled	Shutdown	Normal
eth1/0/6	Disabled	Shutdown	Normal

Figure 9-67 BPDUs Attack Protection Window

The fields that can be configured in **BPDUs Attack Protection Global Settings** are described below:

Parameter	Description
BPDUs Attack Protection State	Select to enable or disable the global BPDUs attack protection state here.
BPDUs Attack Protection Trap State	Select to enable or disable the BPDUs attack protection trap state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **BPDUs Attack Protection Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the BPDUs attack protection state on the port(s) specified.
Mode	<p>Select the BPDUs attack protection mode that will be applied to the port(s) specified. Options to choose from are Drop, Block and Shutdown.</p> <ul style="list-style-type: none"> Drop - Drop all received BPDUs packets when the port enters under attack state. Block - Drop all packets (include BPDUs and normal packets) when the port enters under attack state. Shutdown - Shut down the port when the port enters under attack state.

Click the **Apply** button to accept the changes made.

MAC Authentication

This window is used to display and configure the MAC authentication settings. MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

To view the following window, click **Security > MAC Authentication**, as shown below:

MAC Authentication

MAC Authentication Global Settings

MAC Authentication State ☐ Enabled ☒ Disabled

MAC Authentication Trap State ☐ Enabled ☒ Disabled Apply

MAC Authentication User Name and Password Settings

User Name ☒ Default Password ☐ Encrypt ☒ Default Apply

MAC Authentication Port Settings

Unit From Port To Port State Apply

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled

Figure 9-68 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
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

Click the **Apply** button to accept the changes made.

Web-based Access Control

Web-based Access Control (WAC) is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages (e.g., <http://www.dlink.com>) through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is unauthenticated, the Switch will launch a pop-up user name and password window to query users. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

D-Link's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration. If the virtual IP is not configured, then access cannot start Web authentication.

The Switch's implementation of WAC features a user-defined port number that allows the configuration of the TCP port for either the HTTP or HTTPS protocols. This TCP port for HTTP or HTTPS is used to identify the HTTP or HTTPS packets that will be trapped to the CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80 and the default port number for HTTPS is 443. If no protocol is specified, the default protocol is HTTP.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:

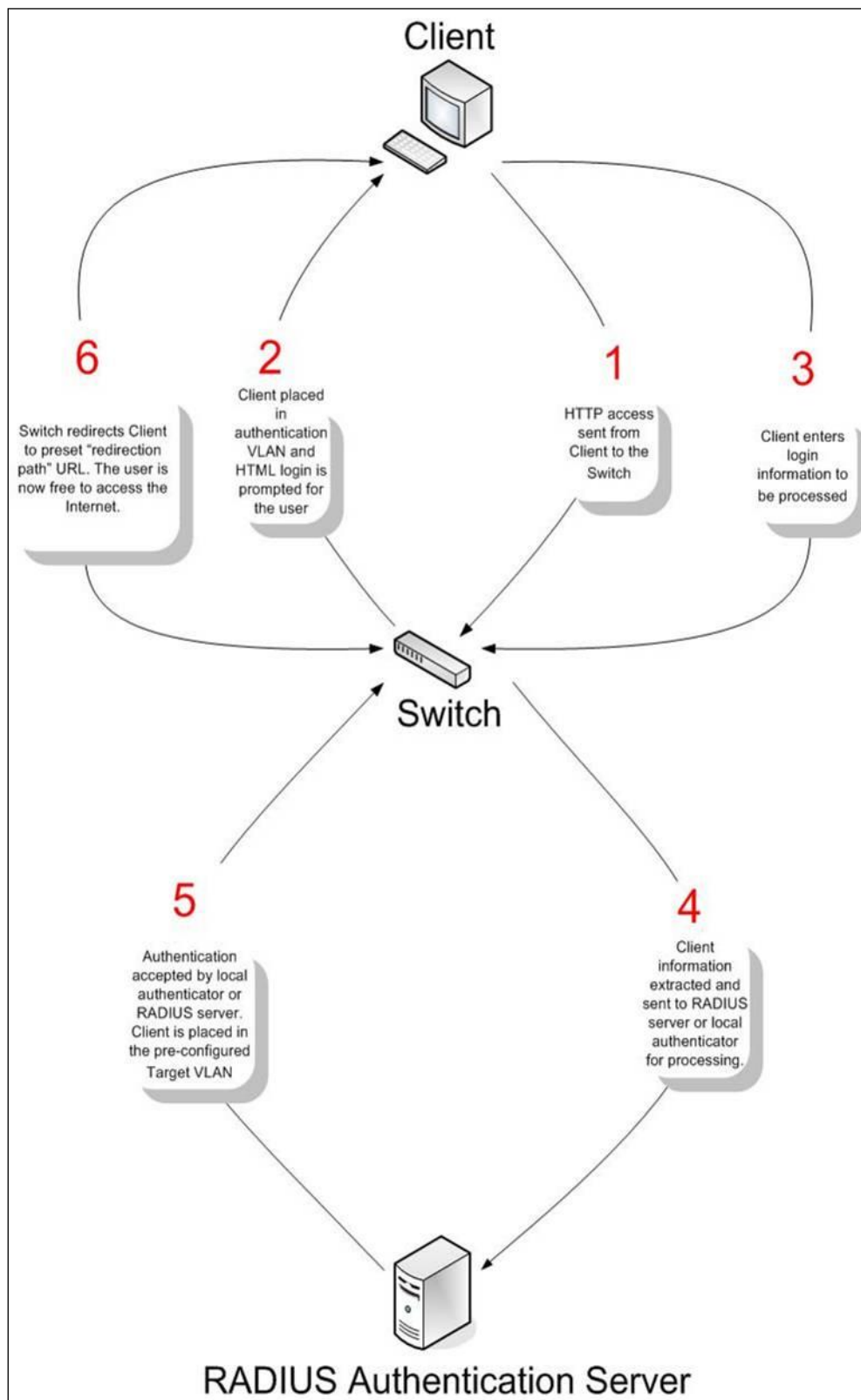


Figure 9-69 RADIUS Authentication Server

Conditions and Limitations

- If the client is utilizing DHCP to attain an IP address, the authenticating VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.
- Certain functions exist on the Switch that will filter HTTP packets, such as the ACL function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
- If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

Web Authentication

This window is used to display and configure the Web authentication settings.

To view the following window, click **Security > Web-based Access Control > Web Authentication**, as shown below:

Figure 9-70 Web Authentication Window

The fields that can be configured are described below:

Parameter	Description
Web Authentication State	Select to enable or disable the global Web authentication state.
Trap State	Select to enable or disable the Web authentication trap state.
Virtual IPv4	Enter the virtual IPv4 address used here. The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. So it's not allowed to configure virtual IP in the same subnet as the Switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly. The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command. If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication.
Virtual IPv6	Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.
Virtual URL	Enter the virtual URL used here. This URL can be up to 128 characters long.
Redirection Path	Enter the redirection path here. This path can be up to 128 characters long.

Click the **Apply** button to accept the changes made.



NOTE: The WAC virtual IP address should be configured before enabling WAC because WAC will not function correctly if the virtual IP is not configured.

WAC Port Settings

This window is used to display and configure the WAC port settings.

To view the following window, click **Security > Web-based Access Control > WAC Port Settings**, as shown below:

WAC Port Settings

WAC Port Settings

Unit: From Port: To Port: State:

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled

Figure 9-71 WAC Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the WAC feature on the port(s) specified.

Click the **Apply** button to accept the changes made.

WAC Customize Page

This window is used to display and configure the WAC customized login page.

To view the following window, click **Security > Web-based Access Control > WAC Customize Page**, as shown below:

WAC Customize Page

Note: Name should be less than 128 characters.

Current Status: **Un-Authenticated**

Authentication Login

User Name:

Password:

Logout From The Network

Notification

Figure 9-72 WAC Customize Page Window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login Window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout Window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There a 5 lines available for additional information.

Click the **Set to Default** button to replace the information with the default information.

Click the **Apply** button to accept the changes made.

Network Access Authentication

Guest VLAN

This window is used to display and configure the network access authentication guest VLAN settings.

To view the following window, click **Security > Network Access Authentication > Guest VLAN**, as shown below:

Figure 9-73 Guest VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Network Access Authentication Global Settings

This window is used to display and configure the global Network Access Authentication settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:

Network Access Authentication Global Settings

Network Access Authentication MAC Format Settings

Case: Uppercase
 Delimiter: Dot
 Delimiter Number: 2
 Apply

General Settings

Max Users (1-1000): 1000
 Authorization State: Enabled
 Apply

User Information

User Name: 32 chars
 Password Type: Plain Text
 VID (1-4094):
 Password: 32 chars
 Apply

Total Entries: 0

User Name	Password	Password Type	VID	

Figure 9-74 Network Access Authentication Global Settings Window

The fields that can be configured in **Network Access Authentication MAC Format Settings** are described below:

Parameter	Description
Case	Select the case format that will be used for the network access authentication MAC address here. Options to choose from are Lowercase and Uppercase .
Delimiter	Select the delimiter that will be used for the network access authentication MAC address here. Options to choose from are Hyphen , Colon , Dot , and None .
Delimiter Number	Select the delimiter number option here. Options to choose from are 1 , 2 , and 5 .

Click the **Apply** button to accept the changes made.

The fields that can be configured in **General Settings** are described below:

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. This value must be between 1 and 1000. By default, this option is 1000.
Authorization State	Select to enable or disable the authorized state here. The option is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example VLAN, 802.1p default priority, bandwidth, and ACL) assigned by the RADIUS server will be accepted if the authorization status is enabled. Bandwidth and ACL are assigned on a per-port basis. If in the multi-authenticated mode, VLAN and 802.1p are assigned on a per-host basis. Otherwise, Bandwidth and ACL are assigned on a per-port basis.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **User Information** are described below:

Parameter	Description
User Name	Enter the user name used here. This name can be up to 32 characters long.
VID	Enter the VLAN ID used here.

Parameter	Description
Password Type	Select the password type option here. Options to choose from are Plain Text and Encrypted .
Password	Enter the password used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Network Access Authentication Port Settings

This window is used to display and configure the network access authentication port settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Port Settings**, as shown below:

Port	Host Mode	VID List	CompAuth Mode	Max Users	Periodic	ReAuth	Inactivity Timer	Restart
eth1/0/1	Multi Auth		Any	1000	Disabled	3600	Disabled	60
eth1/0/2	Multi Auth		Any	1000	Disabled	3600	Disabled	60
eth1/0/3	Multi Auth		Any	1000	Disabled	3600	Disabled	60
eth1/0/4	Multi Auth		Any	1000	Disabled	3600	Disabled	60
eth1/0/5	Multi Auth		Any	1000	Disabled	3600	Disabled	60
eth1/0/6	Multi Auth		Any	1000	Disabled	3600	Disabled	60
eth1/0/7	Multi Auth		Any	1000	Disabled	3600	Disabled	60

Figure 9-75 Network Access Authentication Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are Multi Host and Multi Auth . If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. If the port is operated in the multi-authenticated mode, then each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.
VID List Action	Select the VID list action here. Options to choose from are None , Add , and Delete .
VID List	After selecting the Multi Auth option as the Host Mode , the following parameter is available. Enter the VLAN ID used here. This is useful when different VLANs on the Switch have different authentication requirements. After

Parameter	Description
	the client is authenticated, the client will not be re-authenticated when received from other VLANs. This option is useful for trunk ports to do per-VLAN authentication control. When a port's authentication mode is changed to multi-host, the previous authentication VLAN(s) on this port will be cleared.
CompAuth Mode	<p>Select the compound authentication mode option here. Options to choose from are Any and MAC-WAC.</p> <ul style="list-style-type: none"> Selecting Any specifies that if any of the authentication method (802.1X, MAC-based Access Control or WAC) to passes, then pass. Selecting MAC-WAC specifies to verify MAC-based authentication first. If the client passes, WAC will be verified next. Both authentication methods need to be passed.
Max Users	Enter the maximum users value used here. This value must be between 1 and 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol.
ReAuth Timer	Enter the re-authentication timer value here. This value must be between 1 and 65535 seconds. By default, this value is 3600 seconds.
Inactivity State	Select to enable or disable the inactivity state here. Select the Time option to enable this feature.
Inactivity Timer	When the Inactivity State is enabled, enter the inactivity timer value here. This value must be between 120 and 65535 seconds. This parameter only affects the WAC authentication protocol.
Restart	Enter the restart time value used here. This value must be between 1 and 65535 seconds.

Click the **Apply** button to accept the changes made.

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:

Figure 9-76 Network Access Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate Switch unit and port used for the query here.
MAC Address	Enter the MAC address used here.
Protocol	Select the protocol option used here. Options to choose from are MAC , WAC , and DOT1X .

Click the **Clear by Port** button to 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 by Protocol** button to clear the information based on the protocol selected.

Click the **Clear All** button to clear all the information in this table.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to locate and display all the entries.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the Switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Packets that are destined to the CPU can be classified into three groups. These groups, otherwise known as sub-interfaces, are logical interfaces that the CPU will use to identify certain types of traffic. The three groups are **Protocol**, **Manage**, and **Route**. Generally, the **Protocol** group should receive the highest priority when the Switch's CPU processes received packets and the **Route** group should receive the lowest priority as the Switch's CPU usually does get involved in the processing of routing packets. In the **Protocol** group, packets are protocol control packets identified by the router. In the **Manage** group, packets are destined to any router or system network management interface by means of interactive access protocols, like Telnet and SSH. In the **Route** group, packets are identified as traversing routing packets that is generally processed by the router CPU.

In the following table a list of supported protocols are displayed with their respective sub-interfaces (groups):

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol
BGP	Protocol	Border Gateway Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
DVMRP	Protocol	Distance Vector Multicast Routing Protocol
GVRP	Protocol	GARP VLAN Registration Protocol
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)

Protocol Name	Sub-interface (Group)	Description
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol
NTP	Protocol	Network Time Protocol
OSPF	Protocol	Open Shortest Path First
PIM	Protocol	Protocol Independent Multicast
PPPoE	Protocol	Point-to-point protocol over Ethernet
RIP	Protocol	Routing Information Protocol
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
VRRP	Protocol	Virtual Router Redundancy Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's sub-interfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.



NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to display and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:

Figure 9-77 Safeguard Engine Settings Window

The fields that can be configured in **Safeguard Engine Settings** are described below:

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.

Parameter	Description
Trap State	Select to enable or disable the safeguard engine trap state here.

The fields that can be configured in **CPU Utilization Settings** are described below:

Parameter	Description
Rising Threshold	Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

Click the **Apply** button to accept the changes made.

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:

Figure 9-78 CPU Protect Counters Window

The fields that can be configured are described below:

Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , Route , and All . This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

CPU Protect Sub-Interface

This window is used to display and configure the CPU protection sub-interface settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Sub-Interface**, as shown below:

Unit	Total	Drop
1	23	0

Figure 9-79 CPU Protect Sub-Interface Window

The fields that can be configured in **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , and Route .
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the No Limit option to disable the rate limit.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Sub-Interface Information** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , and Route .

Click the **Find** button to locate a specific entry based on the information entered.

CPU Protect Type

This window is used to display and configure the CPU protection type settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Type**, as shown below:

Unit	Total	Drop
1	0	0

Figure 9-80 CPU Protect Type Window

The fields that can be configured in **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here.

Parameter	Description
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the No Limit option to disable the rate limit.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Protect Type Information** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here.

Click the **Find** button to locate a specific entry based on the information entered.

Trusted Host

This window is used to display and configure the trusted host settings.

To view the following window, click **Security > Trusted Host**, as shown below:

Figure 9-81 Trusted Host Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access class' name here. This name can be up to 32 characters long.
Type	Select the trusted host type here. Options to choose from are Telnet , SSH , Ping , HTTP , and HTTPS .

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

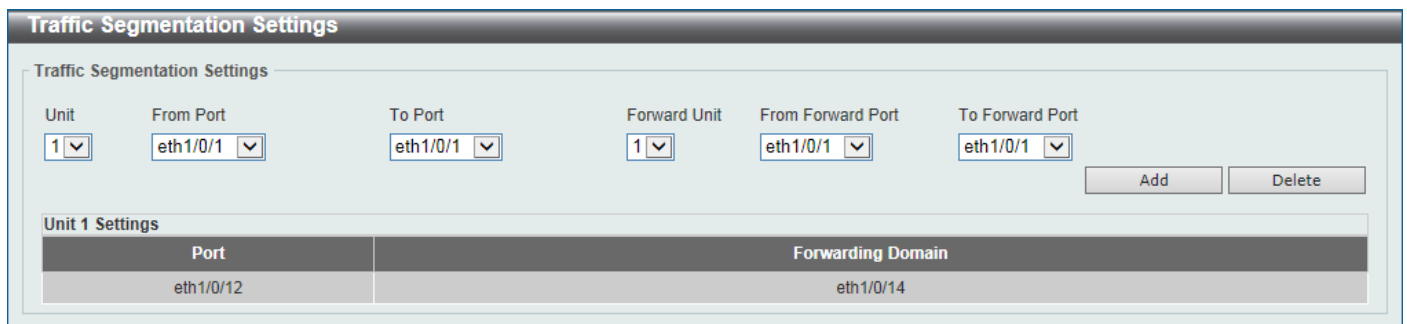
Traffic Segmentation Settings

This window is used to display and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

To view the following window, click **Security > Traffic Segmentation Settings**, as shown below:



Port	Forwarding Domain
eth1/0/12	eth1/0/14

Figure 9-82 Traffic Segmentation Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the receiving Switch unit that will be used for this configuration here.
From Port - To Port	Select the receiving port range used for the configuration here.
Forward Unit	Select the forward Switch unit that will be used for this configuration here.
From Forward Port ~ To Forward Port	Select the forward port range used for the configuration here.

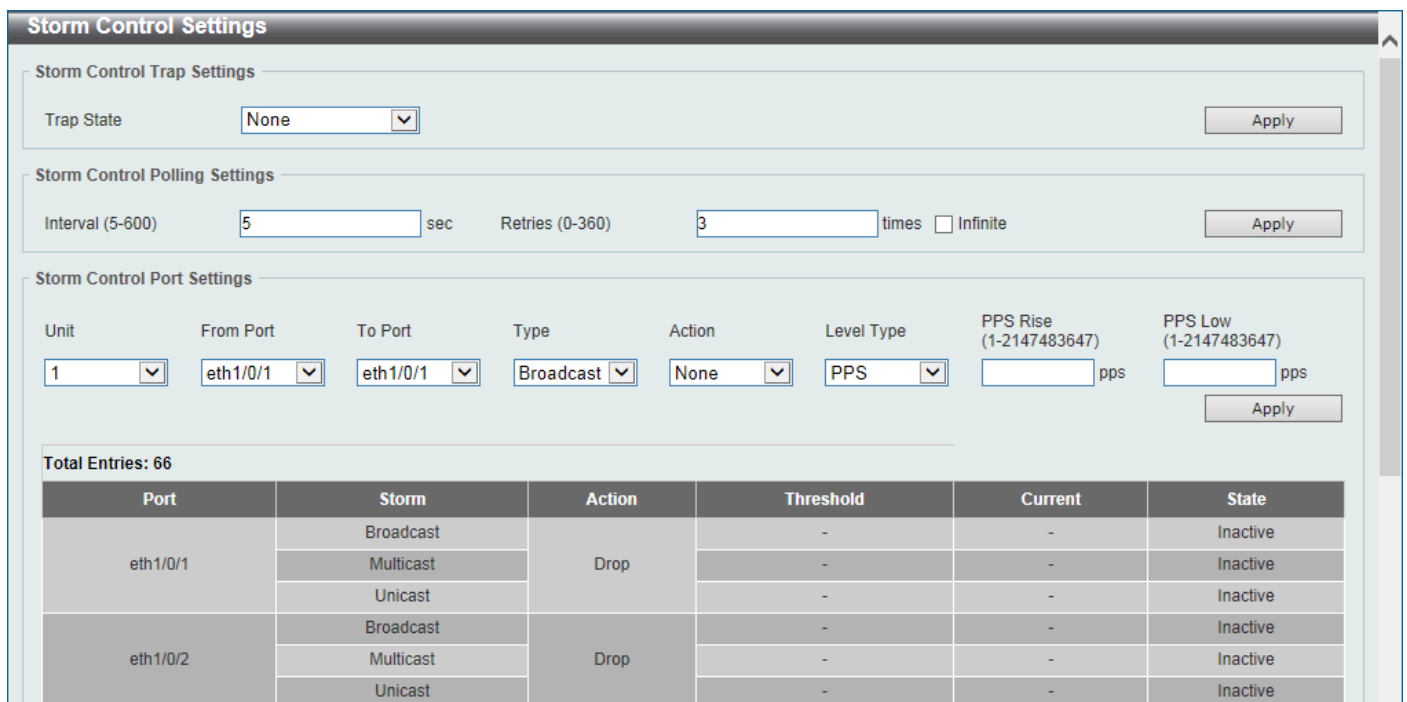
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Storm Control

This window is used to display and configure the storm control settings.

To view the following window, click **Security > Storm Control**, as shown below:



Port	Storm	Action	Threshold	Current	State
eth1/0/1	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
eth1/0/2	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive

Figure 9-83 Storm Control Window

The fields that can be configured in **Storm Control Trap Settings** are described below:

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are None , Storm Occur , Storm Clear , and Both . When None is selected, no traps will be sent. When Storm Occur is selected, a trap notification will be sent when a storm event is detected. When Storm Clear is selected, a trap notification will be sent when a storm event is cleared.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.
Retries	Enter the retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the Infinite option to disable this feature.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are Broadcast , Multicast , and Unicast . When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Action	Select the action that will be taken here. Options to choose from are None , Shutdown , and Drop . Selecting None specifies not to filter the storm packets. Selecting Shutdown specifies to shut down the port when the value specified for rise threshold is reached. Selecting Drop specifies to discards packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are PPS , Kbps , and Level .
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 1 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 1 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

Click the **Apply** button to accept the changes made.

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.

The screenshot shows the 'Storm Control Port Settings' window. It contains several dropdown menus and input fields. The 'Unit' dropdown is set to '1'. The 'From Port' dropdown is set to 'eth1/0/1' and the 'To Port' dropdown is also set to 'eth1/0/1'. The 'Type' dropdown is set to 'Broadcast'. The 'Action' dropdown is set to 'None'. The 'Level Type' dropdown is set to 'Kbps'. To the right of 'Level Type', there are two input fields: 'KBPS Rise (1-2147483647)' and 'KBPS Low (1-2147483647)', both followed by 'Kbps' text. An 'Apply' button is located at the bottom right of the form.

Figure 9-84 Storm Control (Level Type - Kbps) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 1 and 2147483647 Kbps.
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 1 and 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

Click the **Apply** button to accept the changes made.

After selecting the **Level** option as the **Level Type**, the following parameters are available.

The screenshot shows the 'Storm Control Port Settings' window. It contains several dropdown menus and input fields: 'Unit' (set to 1), 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Type' (Broadcast), 'Action' (None), 'Level Type' (Level), 'Level Rise (1-100)' (empty), and 'Level Low (1-100)' (empty). An 'Apply' button is located at the bottom right.

Figure 9-85 Storm Control (Level Type - Level) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 1% and 100%.
Level Low	Enter the low level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 1% and 100%. If the low level is not specified, the default value is 80% of the specified risen level.

Click the **Apply** button to accept the changes made.

DoS Attack Prevention Settings

This window is used to display and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types which can be detected by most Switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack:** This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets which contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets which contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size which is 65535 bytes). The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte

ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.

- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

DoS Type	State	Action
Land Attack	Disabled	Drop
Blat Attack	Disabled	Drop
TCP Null	Disabled	Drop
TCP Xmas	Disabled	Drop
TCP SYN-FIN	Disabled	Drop
TCP SYN SrcPort Less 1024	Disabled	Drop
Ping of Death Attack	Disabled	Drop
TCP Tiny Fragment Attack	Disabled	Drop

Figure 9-86 DoS Attack Prevention Settings Window

The fields that can be configured in **SNMP Server Enable Traps DoS Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DoS attack prevention trap state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **DoS Attack Prevention Settings** are described below:

Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
State	Select to enable or disable the global DoS attack prevention state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is Drop .

Click the **Apply** button to accept the changes made.

SSH

Secure Shell (SSH) is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and

will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

This window is used to display and configure the global SSH settings.

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

Figure 9-87 SSH Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IP SSH Server State	Select to enable or disable the global SSH server state.
IP SSH Service Port	Enter the SSH service port number used here. This value must be between 1 and 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

Click the **Apply** button to accept the changes made.

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:

The Host Key Management window contains two sections. The top section, titled 'Host Key Management', has two dropdown menus: 'Crypto Key Type' set to 'RSA' and 'Key Modulus' set to '768' with a 'bit' label. To the right are 'Generate' and 'Delete' buttons. The bottom section, titled 'Host Key', shows the 'Crypto Key Type' dropdown set to 'RSA'. Below this are labels for 'Key pair was generated at', 'Key Size', and 'Key Data', which are currently empty.

Figure 9-88 Host Key Window

The fields that can be configured in **Host Key Management** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.
Key Modulus	Select the key modulus value here. Options to choose from are 360 , 512 , 768 , 1024 , and 2048 bit.

Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured in **Host Key** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.

After clicking the **Generate** button, the following window will appear:

The Host Key Management window shows the 'Result' field with the text 'Generating...'.

Figure 9-89 Host Key (Generating) Window

After the key was successfully generated, the following window will appear.

The Host Key Management window shows the 'Result' field with the text 'Success.'.

Figure 9-90 Host Key (Generating, Success) Window

SSH Server Connection

This window is used to view the SSH server connections table.

To view the following window, click **Security > SSH > SSH Server Connection**, as shown below:

SSH Server Connection				
SSH Table				
Total Entries: 1				
SID	Version	Cipher	User ID	Client IP Address
0	V2	aes256-cbc/hmac-sha1...	user	10.90.90.14

Figure 9-91 SSH Server Connection Window

SSH User Settings

This window is used to display and configure the SSH user settings.

To view the following window, click **Security > SSH > SSH User Settings**, as shown below:

SSH User Settings				
SSH User Settings				
User Name	<input type="text" value="32 chars"/>	Authentication Method	<input type="text" value="Password"/>	
Key File	<input type="text" value="779 chars"/>	Host Name	<input type="text" value="255 chars"/>	
<input checked="" type="radio"/> IPv4 Address	<input type="text" value=""/>	<input type="radio"/> IPv6 Address	<input type="text" value="2013::1"/>	<input type="button" value="Apply"/>
Total Entries: 1				
User Name	Authentication Method	Key File	Host Name	Host IP
user	Password			
				1/1 < < 1 > > <input type="text" value=""/> Go

Figure 9-92 SSH User Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the SSH user's username used here. This name can be up to 32 characters long.
Authentication Method	Select the authentication methods used here. Options to choose from are Password , Public Key , and Host-based .
Key File	After selecting the Public Key or Host-based option as the Authentication Method , enter the public key here.
Host Name	After selecting the Host-based option as the Authentication Method , enter the host name here.
IPv4 Address	After selecting the Host-based option as the Authentication Method , select and enter the IPv4 address here.
IPv6 Address	After selecting the Host-based option as the Authentication Method , select and enter the IPv6 address here.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the Cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
 - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
 - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports TLS 1.0 and TLS 1.1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch supports TLS 1.0 and TLS 1.1. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

This window is used to display and configure the global SSL settings.

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:

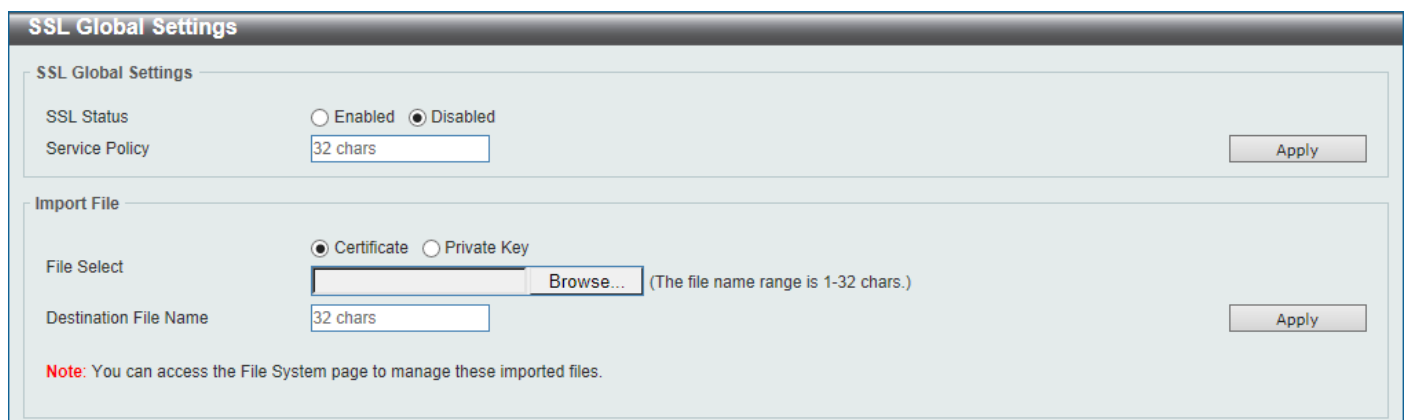


Figure 9-93 SSL Global Settings Window

The fields that can be configured in **SSL Global Settings** are described below:

Parameter	Description
SSL Status	Select to enable or disable the global SSL status here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Import File** are described below:

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are Certificate and Private Key . After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the Browse button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Crypto PKI Trustpoint

This window is used to display and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:

Figure 9-94 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server path here.
Type	<p>Select the type of certificate that will be imported here. Options to choose from are Both, CA, and Local.</p> <ul style="list-style-type: none"> Selecting Both specifies to import the CA certificate, local certificate and key pairs. Selecting CA specifies to import the CA certificate only.

Parameter	Description
	<ul style="list-style-type: none"> Selecting Local specifies to import local certificate and key pairs only.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SSL Service Policy

This window is used to display and configure the SSL service policy settings.

To view the following window, click **Security > SSL > SSL Service Policy**, as shown below:

SSL Service Policy

Policy Name: 32 chars [Apply] [Find]

Policy Name: 32 chars

Session Cache Timeout (60-86400): 600 sec

Secure Trustpoint: 32 chars

Cipher Suites:

- ☐ DHE_DSS_WITH_3DES_EDE_CBC_SHA
- ☐ RSA_WITH_3DES_EDE_CBC_SHA
- ☐ RSA_WITH_RC4_128_SHA
- ☐ RSA_EXPORT_WITH_RC4_40_MD5
- ☐ RSA_WITH_RC4_128_MD5

[Apply]

Total Entries: 1

Policy Name	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint
policy	DHE_DSS_WITH_3DES_ED...	600	

[Edit] [Delete]

Figure 9-95 SSL Service Policy Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the SSL service policy name here. This name can be up to 32 characters long.
Session Cache Timeout	Enter the session cache timeout value used here. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust point name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

SFTP Server Settings

This window is used to display and configure the Secure File Transfer Protocol (SFTP) server settings. SFTP is a remotely secure file transfer protocol over a reliable data stream. Because SFTP itself does not provide authentication and security, the SFTP server runs as a sub-system of the SSH server.



NOTE: Only IPv4 SFTP servers are supported.

To view the following window, click **Security > SFTP Server Settings**, as shown below:

SFTP Server Settings

SFTP Server Settings

SFTP Server ☐ Enabled ☒ Disabled

Idle Timeout (30-600) sec

Protocol Version

Apply

Figure 9-96 SFTP Server Settings Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server	Select to globally enable or disable the SFTP server feature here.
Idle Timeout	Enter the idle timeout value here. If the SFTP server detects no operation after the duration of the idle timer for a specific SFTP session, the Switch will close this SFTP session. The range is from 30 to 600 seconds. By default, this value is 120 seconds.

Click the **Apply** button to accept the changes made.

10. OAM

Cable Diagnostics
Ethernet OAM
DDM

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

The screenshot shows the 'Cable Diagnostics' window. At the top, there are three dropdown menus: 'Unit' (set to 1), 'From Port' (set to eth1/0/1), and 'To Port' (set to eth1/0/1). To the right of these is a 'Test' button. Below these is a 'Unit 1 Settings' section with a 'Clear All' button. The main part of the window is a table with the following columns: Port, Type, Link Status, Test Result, Cable Length (M), and an action column. The table contains data for ports eth1/0/1 through eth1/0/6. Port eth1/0/1 is 'Link Up' and shows four test results: 'Pair 1 Open at 0M', 'Pair 2 Ok at 5M', 'Pair 3 Ok at 6M', and 'Pair 4 Open at 0M'. The other ports are 'Link Down'. Each row has a 'Clear' button in the action column.

Port	Type	Link Status	Test Result	Cable Length (M)	
eth1/0/1	10GBASE-T	Link Up	Pair 1 Open at 0M	-	Clear
			Pair 2 Ok at 5M		
			Pair 3 Ok at 6M		
			Pair 4 Open at 0M		
eth1/0/2	10GBASE-T	Link Down	-	-	Clear
eth1/0/3	10GBASE-T	Link Down	-	-	Clear
eth1/0/4	10GBASE-T	Link Down	-	-	Clear
eth1/0/5	10GBASE-T	Link Up	-	-	Clear
eth1/0/6	10GBASE-T	Link Down	-	-	Clear

Figure 10-1 Cable Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Test** button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.



NOTE: Cable diagnostic function limitations. Cable length detection is only supported on GE ports.



NOTE: The maximum cable diagnosis length is 120 meters.



NOTE: The deviation of cable length detection is about 5 meters for GE ports.

Fault messages:

- **Open** - This pair is left open.
- **Short** - Two lines of this pair is shorted.
- **CrossTalk** - Lines of this pair is short with lines in other pairs.
- **Unknown** - The diagnosis does not obtain the cable status, please try again.
- **NA** - No cable was found, maybe it's because cable is out of diagnosis specification or the quality is too bad.

Ethernet OAM

Ethernet OAM Settings

This window is used to display and configure the Ethernet Operations, Administration, and Maintenance (OAM) settings.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Settings**, as shown below:

Ethernet 1/0/1	
Local Client	
Admin State	Disable
Mode	Active
Max OAMPDU size	1518 Bytes
Remote loopback	Supproted
Unidirectional	No supported
Link monitoring	Supproted
Variable request	No supported

Figure 10-2 Ethernet OAM Settings Window

The fields that can be configured in **Ethernet OAM Settings** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.
State	Select to enable or disable the Ethernet OAM feature on the specified port(s) here. After enabling this function on the interface, the interface will start OAM discovery. If the OAM mode of this interface is active, it initiates the discovery. Otherwise, it reacts to the discovery received from the peer.
Mode	Select the Ethernet OAM mode here. Options to choose from are Active and Passive . The following two actions are allowed by ports in the active mode, but

Parameter	Description
	disallowed by ports in the passive mode. (1) Initiate OAM discovery. (2) Start or stop remote loopback.
Received Remote Loopback	<p>Select to configure the behavior of the received remote loopback requirement from the peer on the specified port(s) here. Options to choose from are Ignore and Process.</p> <ul style="list-style-type: none"> • Ignore - Specifies not to react to remote loopback requirements from a peer. • Process - Specifies to react to remote loopback requirements from a peer. <p>The feature is used to configure the client to process or to ignore the received Ethernet OAM remote loopback feature. In the remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback feature will prevent the port from entering the remote loopback mode.</p>
Remote Loopback	<p>Select the remote loopback action here. Options to choose from are Start and Stop.</p> <ul style="list-style-type: none"> • Start - Specifies to request the peer to change to the remote loopback mode. • Stop - Specifies to request the peer to change to the normal operation mode. <p>If the remote peer is configured to ignore the remote loopback request, then the remote peer will not enter or exit the remote loopback mode upon receiving the request. To start the remote peer to enter the remote loopback mode, administrators must ensure that the local client is in the active mode and the OAM connection is established. If the local client is already in the remote loopback mode, then this feature cannot be applied.</p>

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Ethernet OAM Table** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Ethernet OAM Configuration Settings

This window is used to display and configure the Ethernet OAM configuration settings.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Configuration Settings**, as shown below:

Ethernet OAM Configuration Settings

Ethernet OAM Configuration Settings

Unit:
From Port:
To Port:
Dying Gasp:
Critical Event:

Link Monitor:
Notify State:
Threshold (0-4294967295):
Window (10-600):
Deciseconds

Ethernet OAM Configuration Table

Unit:
From Port:
To Port:

Ethernet1/0/1	
Ethernet oam state	Disabled
Mode	Active
Dying gasp	Enabled
Critical event	Enabled
Remote loopback OAMPDU	Not Processed
Error symbol period event	
Notify state	Enabled
Threshold	1 Error Symbol
Window	10 deciseconds
Error frame event	
Notify state	Enabled
Threshold	1 Error Frame
Window	10 deciseconds
Error frame period event	
Notify state	Enabled
Threshold	1 Error Frame
Window	14881000 Frames
Error frame seconds event	
Notify state	Enabled
Threshold	1 Error Seconds
Window	600 deciseconds
Ethernet1/0/2	
Ethernet oam state	Disabled

Figure 10-3 Ethernet OAM Configuration Settings Window

The fields that can be configured in **Ethernet OAM Configuration Settings** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.
Dying Gasp	Select to enable or disable the dying gasp feature here. This feature is used to configure the capability of the dying gasp event. If the capability for the dying gasp event is disabled, the port will never send out OAM PDUs with the dying gasp event bit set when an unrecoverable local failure condition has occurred.
Critical Event	Select to enable or disable the critical event feature here. This feature is used to configure the capability of the critical event. If the capability for a critical event is disabled, the port will never send out OAM PDUs with critical event bit set when an unspecified critical event has occurred.
Link Monitor	Select the link monitor feature here. Options to choose from are Error Symbol , Error Frame , Error Frame Seconds , and Error Frame Period . <ul style="list-style-type: none"> • Error Symbol - This feature is used to enable notifying the Ethernet OAM error symbol event and configure the monitor threshold and window on the specified port. • Error Frame - This feature is used to enable notifying the Ethernet OAM error frame event and configure the monitor threshold and window on the specified port.

Parameter	Description
	<ul style="list-style-type: none"> • Error Frame Seconds - This feature is used to enable notifying the Ethernet OAM error frame second event and configure the monitor threshold and window on the specified port. • Error Frame Period - This feature is used to enable notifying the Ethernet OAM error frame period event and configure the monitor threshold and window on the specified port.
Notify State	Select to enable or disable the notify state here.
Threshold	<p>Enter the threshold value here.</p> <ul style="list-style-type: none"> • When Error Symbol is selected as the link monitor, enter the number of symbol errors here. If symbol errors occur in the specified window and it exceeds the threshold value, then the event is generated. The range is from 0 to 4294967295. • When Error Frame is selected as the link monitor, enter the number of frame errors here. If the error frames occur in the specified window and exceeds the threshold value, then an error frame event is triggered. The range is from 0 to 4294967295. • When Error Frame Seconds is selected as the link monitor, enter the number of error frames in seconds here. If the number of the error frames occurred in the specified window and exceeds the threshold value, then the frame event is triggered. The range is from 1 to 900 seconds. • When Error Frame Period is selected as the link monitor, enter the number of frame errors that must occur for this event to be triggered here. The range is from 0 to 4294967295.
Window	<p>Enter the window value here.</p> <ul style="list-style-type: none"> • When Error Symbol is selected as the link monitor, enter the amount of time over which the threshold is defined here. If threshold symbol errors occur within the period, an event notification OAM PDU should be generated with an error symbol period event TLV, indicating that the threshold has been crossed in this window. The range is from 10 to 600 deciseconds. • When Error Frame is selected as the link monitor, enter the amount of time over which the threshold is defined here. If the threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame event TLV, indicating that the threshold has been crossed in this window. The range is from 10 to 600 deciseconds. • When Error Frame Seconds is selected as the link monitor, enter the amount of time over which the threshold is defined here. If threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame seconds summary event TLV indicating that the threshold has been crossed in this window. The range is from 100 to 9000 deciseconds. • When Error Frame Period is selected as the link monitor, enter the number of frames over which the threshold is defined here. If threshold frame errors occur within the period, an event notification OAM PDU should be generated with an error frame period event TLV indicating that the threshold has been crossed in this window. The lower bound is the number of minimum frame-size frames that can be received in 100ms on the underlying physical layer. The upper bound is the number of minimum frame-size frames that can be received in one minute on the underlying physical layer. The range is from 148810 to 892860000.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Ethernet OAM Configuration Table** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Ethernet OAM Event Log Table

This window is used to view and clear the Ethernet OAM event log table.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Event Log Table**, as shown below:

Ethernet1/0/1 Records Statistics					
Local Faults	Link Fault	0	Remote Faults	Link Fault	0
	Dying Gasp	0		Dying Gasp	0
	Critical Event	0		Critical Event	0
Local event Logs	Errored Symbol	0	Remote event Logs	Errored Symbol	0
	Errored Frame	0		Errored Frame	0
	Errored Frame Period	0		Errored Frame Period	0
	Errored Frame Second	0		Errored Frame Second	0

Total Entries: 0

Ethernet1/0/1 Event Log Table							
Index	Location	Type	Time Stamp	Value	Window	Threshold	Accumulated Errors

Figure 10-4 Ethernet OAM Event Log Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
Port	Select the Switch port that will be used here.
Action	<p>Select the Find option to find and display the log entries associated with the specified port.</p> <p>Select the Clear option to clear the log entries associated with the specified port.</p>

Click the **Find** button to find and display the log entries associated with the specified port.

Ethernet OAM Statistics Table

This window is used to view and clear the Ethernet OAM statistics table.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Statistics Table**, as shown below:

Unit	From Port	To Port	Action	Find	Show All
1	eth1/0/1	eth1/0/1	Find		
Ethernet1/0/1					
Information OAMPDU TX	0	Information OAMPDU RX	0		
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0		
Duplicate event notification OAMPDU TX	0	Duplicate event notification OAMPDU RX	0		
Loopback control OAMPDU TX	0	Loopback control OAMPDU RX	0		
Variable request OAMPDU TX	0	Variable request OAMPDU RX	0		
Variable response OAMPDU TX	0	Variable response OAMPDU RX	0		
Organization specific OAMPDU TX	0	Organization specific OAMPDU RX	0		
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0		
Frame lost due to OAM	0				
Ethernet1/0/2					
Information OAMPDU TX	0	Information OAMPDU RX	0		
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0		

Figure 10-5 Ethernet OAM Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.
Action	Select the Find option to find and display the statistics information associated with the specified port. Select the Clear option to clear the statistics information associated with the specified port(s).

Click the **Find** button to find and display the statistics information associated with the specified port(s).

Click the **Show All** button to display all the statistics information.

DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP/SFP+ modules inserting to the Switch and to configure alarm settings, warning settings, temperature threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to view and configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:

DDM Settings

DDM Global Settings

Transceiver Monitoring Traps Alarm ☒ Disabled ☐ Enabled

Transceiver Monitoring Traps Warning ☒ Disabled ☐ Enabled Apply

DDM Shutdown Settings

Unit: From Port: To Port: State: Shutdown: Apply

Unit 1 Settings

Port	State	Shutdown
eth1/0/21	Disabled	None
eth1/0/22	Disabled	None
eth1/0/23	Disabled	None
eth1/0/24	Disabled	None
eth1/0/25	Disabled	None
eth1/0/26	Disabled	None

Figure 10-6 DDM Settings Window

The fields that can be configured in **DDM Global Settings** are described below:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select to enable or disable the transceiver monitoring traps alarm feature here.
Transceiver Monitoring Traps Warning	Select to enable or disable the transceiver monitoring traps warning feature here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **DDM Shutdown Settings** are described below:

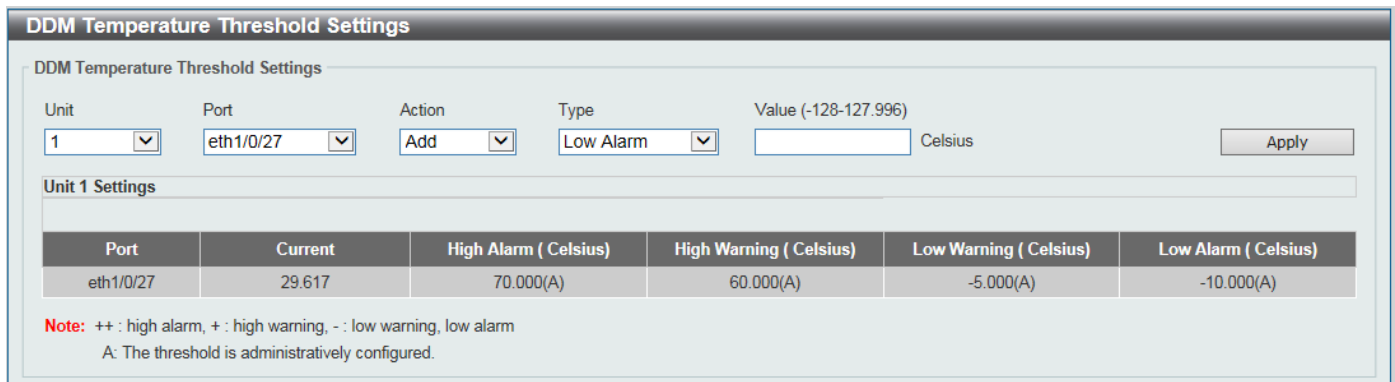
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the Alarm or Warning threshold. <ul style="list-style-type: none"> Alarm - Shutdown the port when the configured alarm threshold range is exceeded. Warning - Shutdown the port when the configured warning threshold range is exceeded. None - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

Click the **Apply** button to accept the changes made.

DDM Temperature Threshold Settings

This window is used to display and configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:



DDM Temperature Threshold Settings

DDM Temperature Threshold Settings

Unit: 1 Port: eth1/0/27 Action: Add Type: Low Alarm Value (-128-127.996): Celsius Apply

Unit 1 Settings

Port	Current	High Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)	Low Alarm (Celsius)
eth1/0/27	29.617	70.000(A)	60.000(A)	-5.000(A)	-10.000(A)

Note: ++ : high alarm, + : high warning, - : low warning, low alarm
A: The threshold is administratively configured.

Figure 10-7 DDM Temperature Threshold Settings Window

The fields that can be configured are described below:

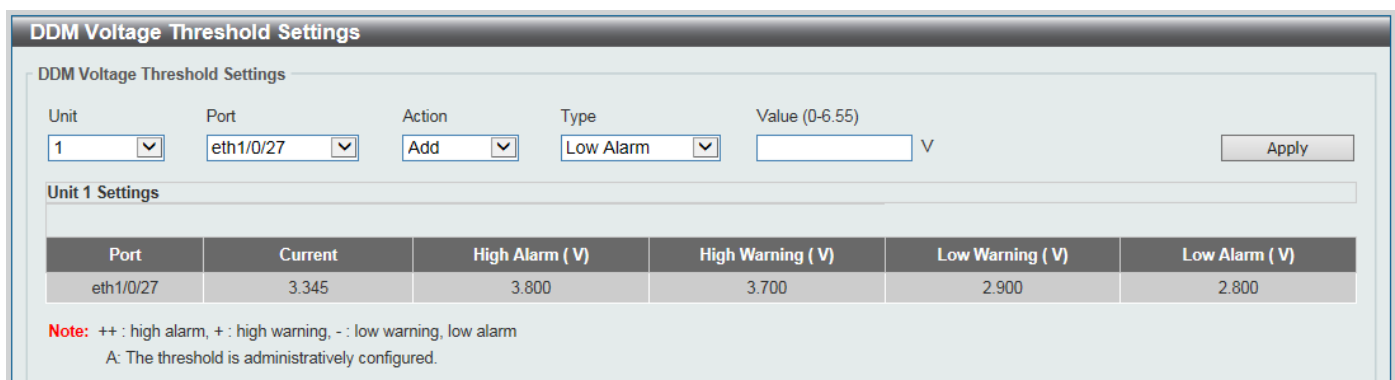
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of temperature threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. This value must be between -128 and 127.996 °C.

Click the **Apply** button to accept the changes made.

DDM Voltage Threshold Settings

This window is used to display and configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Voltage Threshold Settings**, as shown below:



DDM Voltage Threshold Settings

DDM Voltage Threshold Settings

Unit: 1 Port: eth1/0/27 Action: Add Type: Low Alarm Value (0-6.55): V Apply

Unit 1 Settings

Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
eth1/0/27	3.345	3.800	3.700	2.900	2.800

Note: ++ : high alarm, + : high warning, - : low warning, low alarm
A: The threshold is administratively configured.

Figure 10-8 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of voltage threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .

Parameter	Description
Value	Enter the threshold value. This value must be between 0 and 6.55 Volt.

Click the **Apply** button to accept the changes made.

DDM Bias Current Threshold Settings

This window is used to display and configure the threshold of the bias current for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Bias Current Threshold Settings**, as shown below:

DDM Bias Current Threshold Settings

DDM Bias Current Threshold Settings

Unit: 1 Port: eth1/0/27 Action: Add Type: Low Alarm Value (0-131): mA Apply

Unit 1 Settings

Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
eth1/0/27	6.254	20.000	18.000	1.000	0.500

Note: ++ : high alarm, + : high warning, - : low warning, low alarm
A: The threshold is administratively configured.

Figure 10-9 DDM Bias Current Threshold Settings Window

The fields that can be configured are described below:

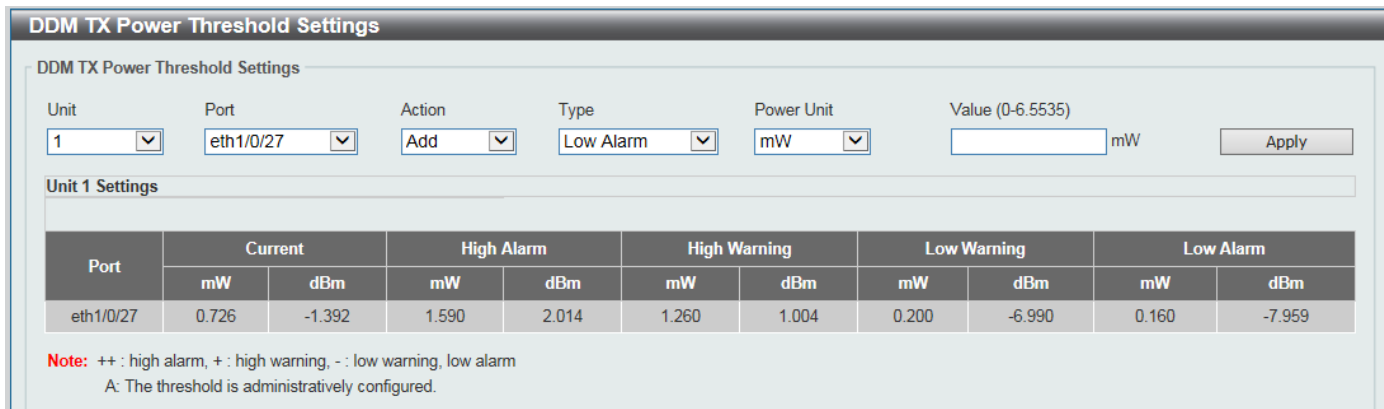
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of bias current threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. This value must be between 0 and 131 mA.

Click the **Apply** button to accept the changes made.

DDM TX Power Threshold Settings

This window is used to display and configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:



DDM TX Power Threshold Settings

DDM TX Power Threshold Settings

Unit: Port: Action: Type: Power Unit: Value (0-6.5535): mW

Unit 1 Settings

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
eth1/0/27	0.726	-1.392	1.590	2.014	1.260	1.004	0.200	-6.990	0.160	-7.959

Note: ++ : high alarm, + : high warning, - : low warning, low alarm
A: The threshold is administratively configured.

Figure 10-10 DDM TX Power Threshold Settings Window

The fields that can be configured are described below:

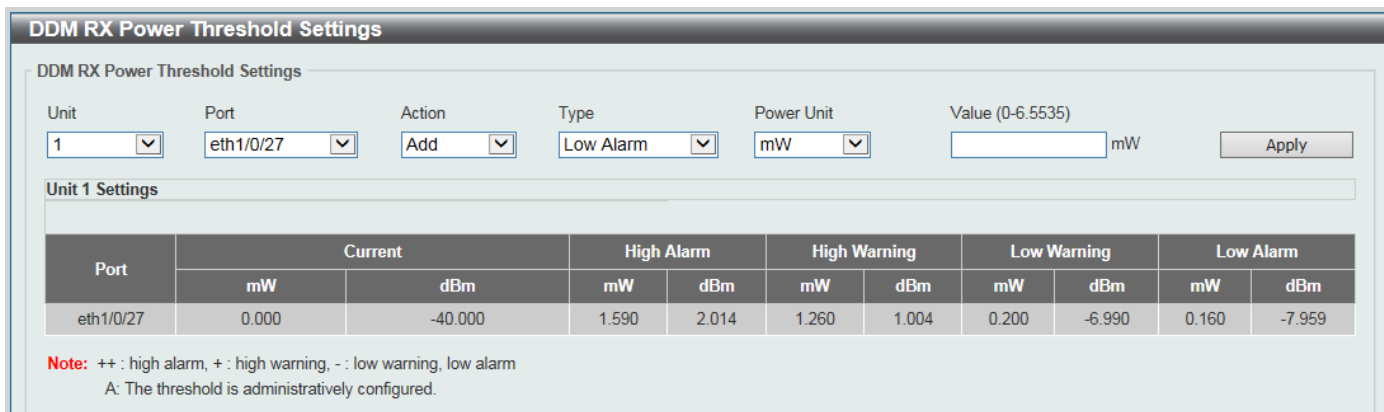
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of TX power threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value either in mW or dBm here. <ul style="list-style-type: none"> When selecting mW in the Power Unit drop-down list, this value must be between 0 and 6.5535. When selecting dBm in the Power Unit drop-down list, this value must be between -40 and 8.1647.

Click the **Apply** button to accept the changes made.

DDM RX Power Threshold Settings

This window is used to display and configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:



DDM RX Power Threshold Settings

DDM RX Power Threshold Settings

Unit: Port: Action: Type: Power Unit: Value (0-6.5535): mW

Unit 1 Settings

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
eth1/0/27	0.000	-40.000	1.590	2.014	1.260	1.004	0.200	-6.990	0.160	-7.959

Note: ++ : high alarm, + : high warning, - : low warning, low alarm
A: The threshold is administratively configured.

Figure 10-11 DDM RX Power Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of RX power threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value either in mW or dBm here. <ul style="list-style-type: none"> When selecting mW in the Power Unit drop-down list, this value must be between 0 and 6.5535. When selecting dBm in the Power Unit drop-down list, this value must be between -40 and 8.1647.

Click the **Apply** button to accept the changes made.

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:

DDM Status Table							
DDM Status Table							
Total Entries: 1							
Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
				mW	dBm	mW	dBm
eth1/0/27	34.550	3.345	6.254	0.723	-1.409	0.000	-40.000
Note: ++ : high alarm, + : high warning, - : low warning, low alarm							

Figure 10-12 DDM Status Table Window

11. Monitoring

[Utilization](#)
[Statistics](#)
[Mirror Settings](#)
[sFlow](#)
[Device Environment](#)

Utilization

Port Utilization

This window is used to view the port utilization table.

To view the following window, click **Monitoring > Utilization > Port Utilization**, as shown below:

The screenshot shows the 'Port Utilization' window. At the top, there's a title bar 'Port Utilization'. Below it, a subtitle 'Port Utilization' is present. The main area contains a form with three dropdown menus: 'Unit' (set to 1), 'From Port' (set to eth1/0/1), and 'To Port' (set to eth1/0/1). To the right of these are 'Find' and 'Refresh' buttons. Below the form is a table with four columns: 'Port', 'TX (packets/sec)', 'RX (packets/sec)', and 'Utilization'. The table contains six rows of data for ports eth1/0/1 through eth1/0/6.

Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	1	1	1
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth1/0/4	0	0	0
eth1/0/5	0	0	1
eth1/0/6	0	0	0

Figure 11-1 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used here.
From Port - To Port	Select the range of ports that will be used here.

Click the **Find** button to display entries in the table based on the information entered/selected.

Click the **Refresh** button to refresh the information displayed in the table.

Statistics

Port

This window is used to view the port statistics information.

To view the following window, click **Monitoring > Statistics > Port**, as shown below:

Port

Port

Unit

1

From Port

eth1/0/1

To Port

eth1/0/1

Find

Refresh

Port	RX				TX				
	Rate		Total		Rate		Total		
	bits/sec	packets/sec	bytes	packets	bits/sec	packets/sec	bytes	packets	
eth1/0/1	0	0	190169	2319	0	0	1122976	11029	Show Detail
eth1/0/2	0	0	0	0	0	0	0	0	Show Detail
eth1/0/3	0	0	2986503	23855	0	0	4205950	9374	Show Detail
eth1/0/4	0	0	0	0	0	0	0	0	Show Detail
eth1/0/5	0	0	0	0	0	0	0	0	Show Detail
eth1/0/6	0	0	0	0	0	0	0	0	Show Detail
eth1/0/7	0	0	0	0	0	0	0	0	Show Detail
eth1/0/8	0	0	0	0	0	0	0	0	Show Detail

Figure 11-2 Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used in this display here.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Detail** button to view more detailed statistics information on the specified port.

After clicking the **Show Detail** button, the following window will appear:

Port Detail	
Port Detail	
<div>Back Refresh</div>	
eth1/0/1	
RX rate	0 bits/sec
TX rate	0 bits/sec
RX rate	0 packets/sec
TX rate	0 packets/sec
RX bytes	190169
TX bytes	1122976
RX packets	2319
TX packets	11029
RX multicast	207
RX broadcast	4607
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	257
RX MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0
TX late collision	0
TX collision	0

Figure 11-3 Port (Show Detail) Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Interface Counters

This window is used to view the interface counter information.

To view the following window, click **Monitoring > Statistics > Interface Counters**, as shown below:

Interface Counters

Interface Counters

Type

Unit

From Port

To Port

Port

1

eth1/0/1

eth1/0/1

Find

Refresh

Unit 1 Settings

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
eth1/0/1	190169	1151	207	961	1122976	755	4607	5667	Show Errors
eth1/0/2	0	0	0	0	0	0	0	0	Show Errors
eth1/0/3	3032288	10927	5991	7263	4278175	9217	127	175	Show Errors
eth1/0/4	0	0	0	0	0	0	0	0	Show Errors
eth1/0/5	0	0	0	0	0	0	0	0	Show Errors
eth1/0/6	0	0	0	0	0	0	0	0	Show Errors
eth1/0/7	0	0	0	0	0	0	0	0	Show Errors
eth1/0/8	0	0	0	0	0	0	0	0	Show Errors

Figure 11-4 Interface Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here. Option supports Port .
Unit	Select the Switch unit that will be used in this display here.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Errors** button to view more detailed error information on the specified port.

After clicking the **Show Errors** button, the following window will appear:

Counters Errors	
Counters Errors	
<div>Back</div> <div>Refresh</div>	
eth1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Undersize	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Multi-Col	0
Late-Col	0
Excess-Col	0
Carri-Sen	0
Runts	0
Giants	0
Symbol-Err	0
SQETest-Err	0
DeferredTx	0
IntMacTx	0
IntMacRx	0

Figure 11-5 Interface Counters (Show Errors) Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Counters

This window is used to view and clear counter information.

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:

Port	linkChange	
eth1/0/1	2	Show Detail
eth1/0/2	0	Show Detail
eth1/0/3	1	Show Detail
eth1/0/4	0	Show Detail
eth1/0/5	0	Show Detail
eth1/0/6	0	Show Detail
eth1/0/7	0	Show Detail
eth1/0/8	0	Show Detail

Figure 11-6 Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here. Options supports Port .
Unit	Select the Switch unit that will be used in this display here.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the counter information displayed in the table.

Click the **Clear** button clear the counter information displayed in the table based on the information selected.

Click the **Clear All** button clear all the counter information displayed in the table.

Click the **Show Detail** button to view more detailed counter information on the specified port.

After clicking the **Show Detail** button, the following window will appear:

Port Counters Detail	
Port Counters Detail	
<div>Back Refresh</div>	
eth1/0/1 Counters	
rxHCTotalPkts	2319
txHCTotalPkts	11029
rxHCUnicastPkts	1151
txHCUnicastPkts	755
rxHCMulticastPkts	207
txHCMulticastPkts	4607
rxHCBroadcastPkts	961
txHCBroadcastPkts	5667
txHCOctets	190169
txHCOctets	1122976
rxHCPkt64Octets	1065
rxHCPkt65to127Octets	1153
rxHCPkt128to255Octets	84
rxHCPkt256to511Octets	13
rxHCPkt512to1023Octets	2
rxHCPkt1024to1518Octets	2
rxHCPkt1519to1522Octets	0
rxHCPkt1519to2047Octets	0
rxHCPkt2048to4095Octets	0
rxHCPkt4096to9216Octets	0
txHCPkt64Octets	3075
txHCPkt65to127Octets	7050
txHCPkt128to255Octets	214
txHCPkt256to511Octets	611
txHCPkt512to1023Octets	45

Figure 11-7 Counters (Show Detail) Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Mirror Settings

This window is used to display and configure the mirror feature's settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:

Mirror Settings

RSPAN VLAN Settings

VID List (1-4094)

Mirror Settings

Session Number

Destination ☐

Source ☐

☐ CPU RX

Mirror Session Table

Session Number	Session Type
1	Local Session

Figure 11-8 Mirror Settings Window

The fields that can be configured for **RSPAN VLAN Settings** are described below:

Parameter	Description
VID List	Enter the VLAN list ID(s) that will be associated with this configuration here.

Click the **Add** button to add the VLAN(s) to the configuration.

Click the **Delete** button to delete the VLAN(s) from the configuration.

The fields that can be configured for **Mirror Settings** are described below:

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	<p>Tick the checkbox, next to the Destination option, to configure the destination for this port mirror entry.</p> <p>In the first drop-down menu select the destination type option. Options to choose from are Port, Remote VLAN, and Replace.</p> <ul style="list-style-type: none"> • Port - After selecting this option, select the Switch Unit ID and destination Port number from the drop-down menus. • Remote VLAN - After selecting this option, select the Switch Unit ID and destination Port number from the drop-down menus and enter the VID in the space provided. The VID must be between 2 and 4094. • Replace - After selecting this option, enter the ACL Access List name and VID (VLAN ID) in the spaces provided.
Source	<p>Tick the checkbox, next to the Source option, to configure the source for this port mirror entry.</p> <p>In the first drop-down menu select the source type option. Options to choose from are Port, ACL, VLAN, and Remote VLAN.</p> <ul style="list-style-type: none"> • Port - After selecting this option, select the Switch Unit ID, From Port and To Port numbers from the drop-down menus. Lastly select the Frame Type option from the last drop-down menu. Options to choose from are Both, RX, TX, and TX Forwarding. When selecting Both, traffic in both

Parameter	Description
	<p>the incoming and outgoing directions will be mirrored. When selecting RX, traffic in only the incoming direction will be mirrored. When selecting TX, traffic in only the outgoing direction will be mirrored. Select the CPU RX option to also monitor CPU RX traffic.</p> <ul style="list-style-type: none"> • ACL - After selecting this option, enter the ACL Name in the space provided. • VLAN - After selecting this option, enter the VID List in the space provided and select the Frame Type from the drop-down menu. • Remote VLAN - After selecting this option, enter the VID in the space provided. The VID must be between 2 and 4094.

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

The fields that can be configured for **Mirror Session Table** are described below:

Parameter	Description
Mirror Session Type	<p>Select the mirror session type of information that will be displayed from the drop-down menu. Options to choose from are All Session, Session Number, Remote Session, and Local Session.</p> <p>After selecting the Session Number option, select the session number from the second drop-down menu. This number is from 1 to 4.</p>

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information about the mirror session.

After clicking the **Show Detail** button, the following window will appear:

The screenshot shows a window titled "Mirror Session Detail". Inside, there is a table with the following data:

Session Number	1
Session Type	Local Session
Both Port	eth1/0/10
RX Port	
TX Port	
CPU RX	
RX VLAN	
Flow Based Source	
Destination Port	Ethernet1/0/9

At the bottom right of the window is a "Back" button.

Figure 11-9 Mirror Settings (Show Detail) Window

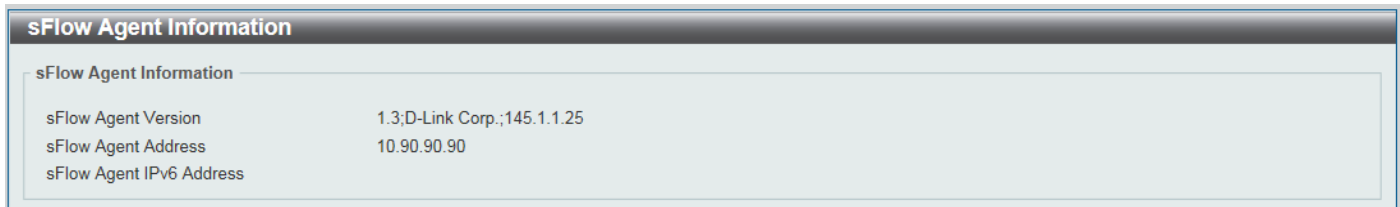
Click the **Back** button to return to the previous page.

sFlow

sFlow Agent Information

This window is used to view the sFlow agent information.

To view the following window, click **Monitoring > sFlow > sFlow Agent Information**, as shown below:



sFlow Agent Information

sFlow Agent Information

sFlow Agent Version: 1.3;D-Link Corp.;145.1.1.25

sFlow Agent Address: 10.90.90.90

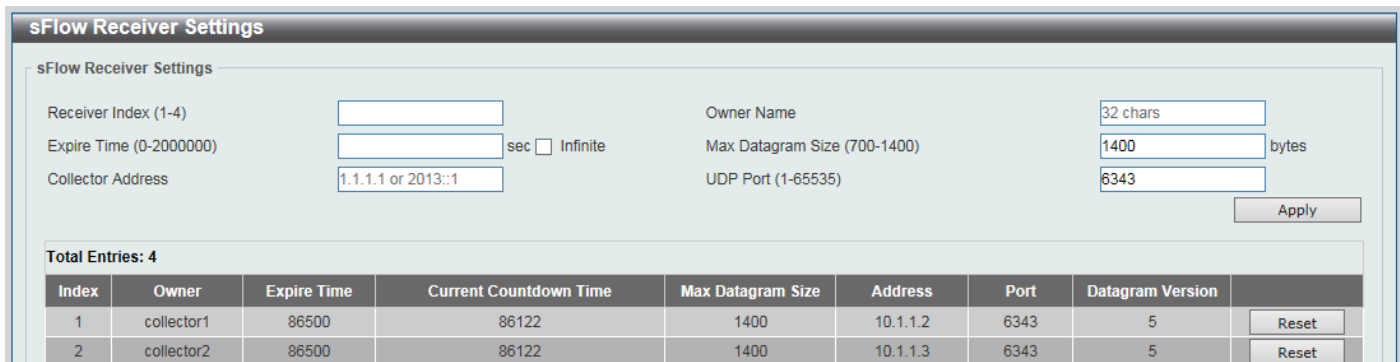
sFlow Agent IPv6 Address:

Figure 11-10 sFlow Agent Information Window

sFlow Receiver Settings

This window is used to display and configure receivers for the sFlow agents. Receivers cannot be added to or removed from the sFlow agent.

To view the following window, click **Monitoring > sFlow > sFlow Receiver Settings**, as shown below:



sFlow Receiver Settings

sFlow Receiver Settings

Receiver Index (1-4): Owner Name: (32 chars)

Expire Time (0-2000000): sec ☐ Infinite Max Datagram Size (700-1400): (1400) bytes

Collector Address: (1.1.1.1 or 2013::1) UDP Port (1-65535): (6343)

Total Entries: 4

Index	Owner	Expire Time	Current Countdown Time	Max Datagram Size	Address	Port	Datagram Version	
1	collector1	86500	86122	1400	10.1.1.2	6343	5	<input type="button" value="Reset"/>
2	collector2	86500	86122	1400	10.1.1.3	6343	5	<input type="button" value="Reset"/>

Figure 11-11 sFlow Receiver Settings Window

The fields that can be configured are described below:

Parameter	Description
Receiver Index	Enter the index number of the receiver here. This number must be between 1 and 4.
Owner Name	Enter the owner name of the receiver here. This name can be up to 32 characters long.
Expire Time	Enter the expiration time for the entry here. The parameters of the entry will reset when the timer expired. The range is from 0 to 2000000 seconds. Selecting Infinite specifies that the entry will not expire.
Max Datagram Size	Enter the maximum number of data bytes of a single sFlow datagram here. The range is from 700 to 1400 bytes. By default, this value is 1400 bytes.
Collector Address	Enter the remote sFlow collector's IPv4 or IPv6 address here.
UDP Port	Enter the remote sFlow collector's UDP port number here. This number must be between 1 and 65535. By default, this value is 6343.

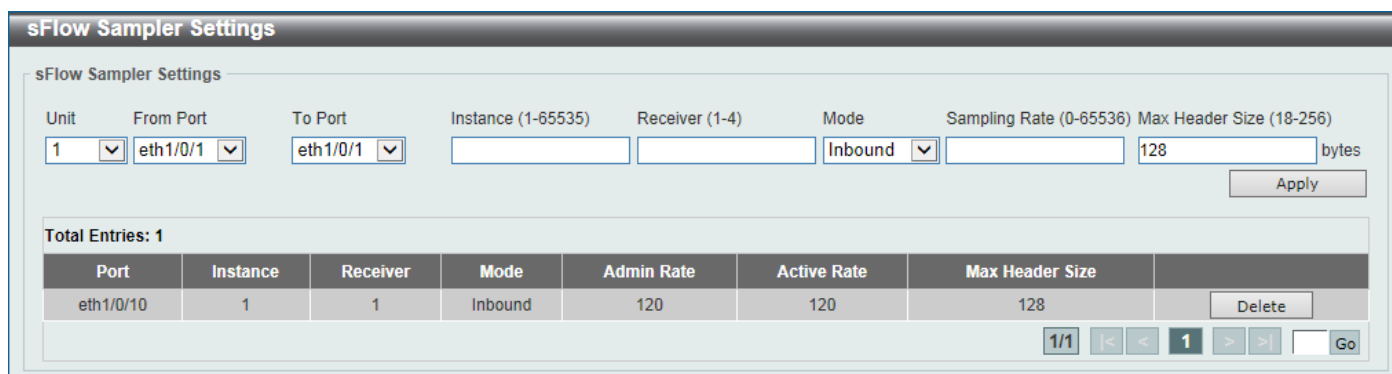
Click the **Apply** button to accept the changes made.

Click the **Reset** button to reset the specified entry's settings to the default settings.

sFlow Sampler Settings

This window is used to display and configure the sFlow sampler settings.

To view the following window, click **Monitoring > sFlow > sFlow Sampler Settings**, as shown below:



The screenshot shows the 'sFlow Sampler Settings' window. At the top, there are input fields for 'Unit' (set to 1), 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Instance (1-65535)' (empty), 'Receiver (1-4)' (empty), 'Mode' (Inbound), 'Sampling Rate (0-65536)' (empty), and 'Max Header Size (18-256)' (128 bytes). An 'Apply' button is on the right. Below this is a table titled 'Total Entries: 1' with columns: Port, Instance, Receiver, Mode, Admin Rate, Active Rate, Max Header Size, and a 'Delete' button. The table contains one entry: Port eth1/0/10, Instance 1, Receiver 1, Mode Inbound, Admin Rate 120, Active Rate 120, Max Header Size 128. At the bottom, there is a pagination bar showing '1/1' and a 'Go' button.

Figure 11-12 sFlow Sampler Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver index for this sampler. If not specified, the value is 0. This value must be between 1 and 4.
Mode	Select the mode here. Options to choose from are Inbound and Outbound . <ul style="list-style-type: none"> Selecting Inbound specifies to sample ingress packets. This is the default direction of a sampler. Selecting Outbound specifies to sample egress packets.
Sampling Rate	Enter packet sampling rate here. This value must be between 0 and 65536. Entering 0 will disable this function. If not specified, the default value is 0.
Max Header Size	Enter the maximum number of bytes that should be copied from sampled packets. This value must be between 18 and 256 bytes. By default, this value is 128 bytes.

Click the **Apply** button to accept the changes made.

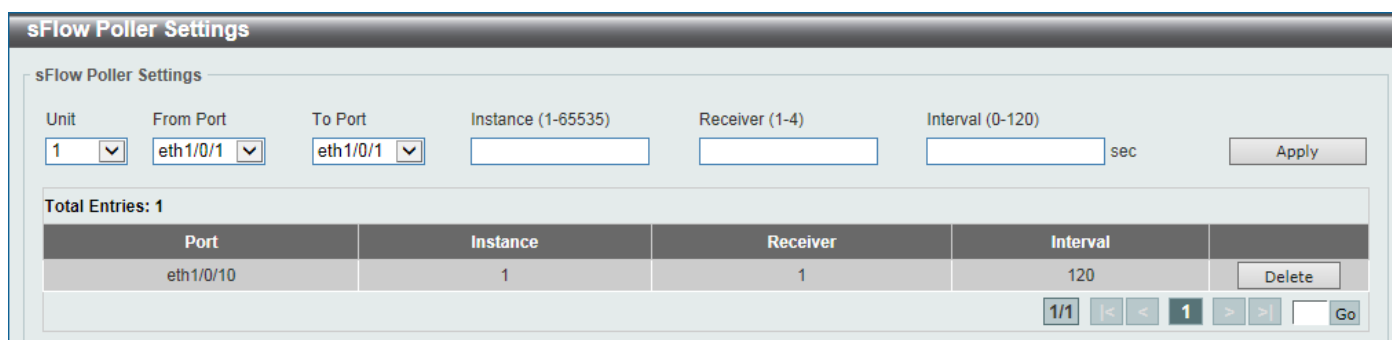
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

sFlow Poller Settings

This window is used to display and configure the sFlow poller settings.

To view the following window, click **Monitoring > sFlow > sFlow Poller Settings**, as shown below:



The screenshot shows the 'sFlow Poller Settings' window. At the top, there are input fields for 'Unit' (set to 1), 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Instance (1-65535)' (empty), 'Receiver (1-4)' (empty), and 'Interval (0-120)' (empty) with a 'sec' label. An 'Apply' button is on the right. Below this is a table titled 'Total Entries: 1' with columns: Port, Instance, Receiver, Interval, and a 'Delete' button. The table contains one entry: Port eth1/0/10, Instance 1, Receiver 1, Interval 120. At the bottom, there is a pagination bar showing '1/1' and a 'Go' button.

Figure 11-13 sFlow Poller Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver index value for this poller here. This value must be between 1 and 4.
Interval	Enter the maximum number of seconds between successive polling samples. This value must be between 0 and 120 seconds. Entering 0 will disable this feature. By default this value is 0.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Device Environment

The device environment feature displays the Switch internal temperature status.

To view the following window, click **Monitoring > Device Environment**, as shown below:

Device Environment

Detail Temperature Status

Unit	Temperature Descr/ID	Current/Threshold Range
1	Central Temperature /1	37C/0~45C
1	Central Temperature /2	33C/0~45C

Status code: * temperature is out of threshold range

Detail Fan Status

Items	Status
Fan 1	(OK)

Detail Power Status

Unit	Power Module	Power Status
1	Power 1	In-operation
	Power 2	Empty

Figure 11-14 Device Environment Window

12. Green

Power Saving EEE

Power Saving

This window is used to display and configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:

Figure 12-1 Power Saving Global Settings Window

The fields that can be configured in **Power Saving Global Settings** are described below:

Parameter	Description
Link Detection Power Saving	Select this option to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Length Detection Power Saving	Select this option to enable or disable the cable length detection power saving feature. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power.
Scheduled Port-shutdown Power Saving	Select this option to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Dim-LED Power Saving	Select this option to enable or disable applying the power saving by scheduled dimming LEDs.
Administrative Dim-LED	Select this option to enable or disable the port LED function.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Time Range Settings** are described below:

Parameter	Description
Type	DIM-LED is selected as the power saving type.
Time Range	Enter the name of the time range to associate with the power saving type.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.



NOTE: The **hibernation** feature can only be configured when physical stacking is disabled on this Switch.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Time Range	Enter the name of the time range to associate with the ports.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:

Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of this feature here.

Click the **Apply** button to accept the changes made.

13. Save and Tools

[Save Configuration](#)
[Firmware Upgrade & Backup](#)
[Configuration Restore & Backup](#)
[Log Backup](#)
[Ping](#)
[Trace Route](#)
[Reset](#)
[Reboot System](#)

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

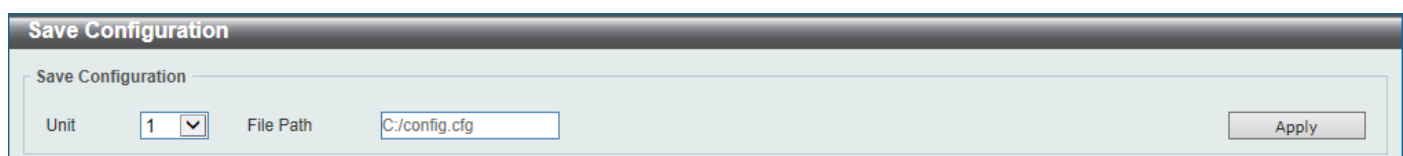


Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

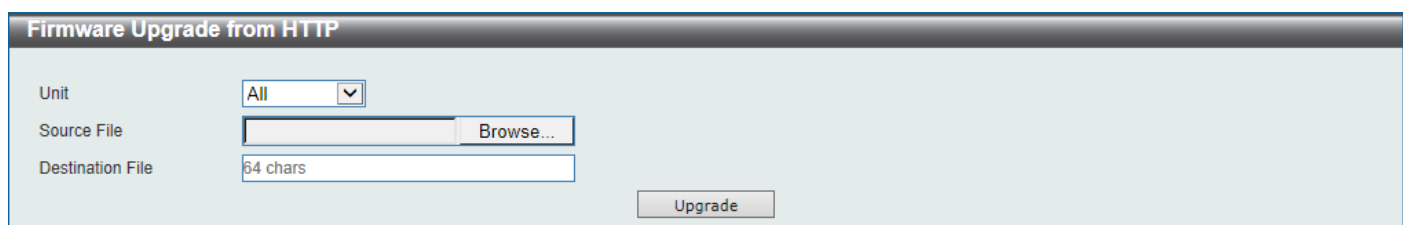


Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.

Parameter	Description
Source File	In this field the source firmware file's filename and path will be displayed after selection. To navigate to the location of the firmware file located on the local PC, either double click in the text box or click the Browse button.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP**, as shown below:

Figure 13-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Figure 13-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

Figure 13-5 Firmware Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
VRF Name	Enter the name of the VRF instance here. This name can be up to 12 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the TFTP server here. This field can be up to 64 characters long.

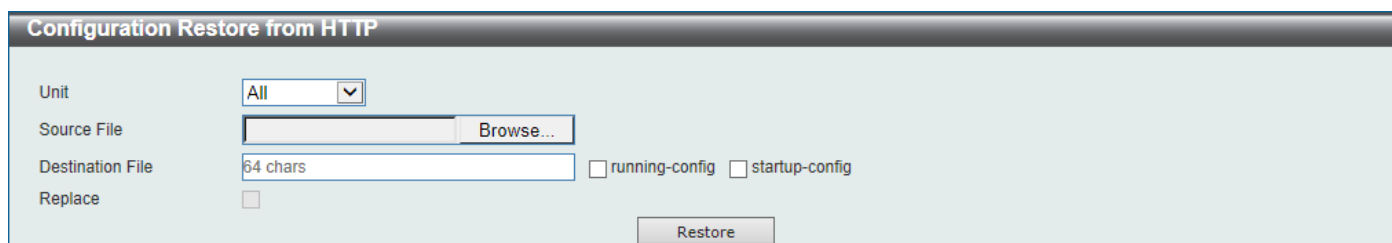
Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:



The screenshot shows the 'Configuration Restore from HTTP' window. It includes a 'Unit' dropdown menu set to 'All'. Below it is a 'Source File' field with a 'Browse...' button. The 'Destination File' field is labeled '64 chars'. To the right of this field are two checkboxes: 'running-config' and 'startup-config'. At the bottom left is a 'Replace' checkbox, and at the bottom right is a 'Restore' button.

Figure 13-6 Configuration Restore from HTTP Window

The fields that can be configured are described below:

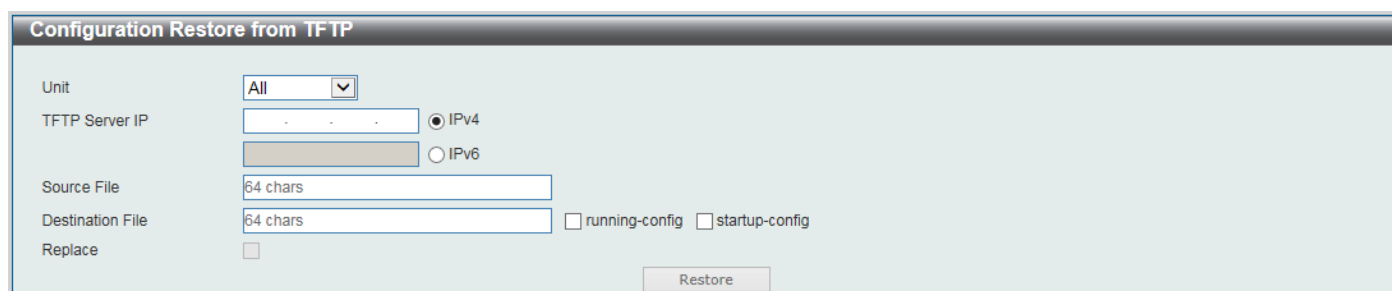
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	In this field the source configuration file's filename and path will be displayed after selection. To navigate to the location of the configuration file located on the local PC, either double click in the text box or click the Browse button.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:



The screenshot shows the 'Configuration Restore from TFTP' window. It includes a 'Unit' dropdown menu set to 'All'. Below it is a 'TFTP Server IP' field with two radio buttons: 'IPv4' (selected) and 'IPv6'. The 'Source File' field is labeled '64 chars'. The 'Destination File' field is labeled '64 chars'. To the right of this field are two checkboxes: 'running-config' and 'startup-config'. At the bottom left is a 'Replace' checkbox, and at the bottom right is a 'Restore' button.

Figure 13-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the running-config option to restore and overwrite the running configuration file on

Parameter	Description
	the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 13-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

Figure 13-9 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

Figure 13-10 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	<p>Select the log type that will be backed up to the local PC using HTTP.</p> <ul style="list-style-type: none"> When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

Figure 13-11 Log Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Destination File	Enter the destination path and location where the log file should be stored on the TFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the TFTP server. <ul style="list-style-type: none"> When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view the following window, click **Tools > Ping**, as shown below:

Figure 13-12 Ping Window

The fields that can be configured in **Ping Access Class** are described below:

Parameter	Description
ACL Name	Enter the name of the ACL that will be used here. This name can be up to 32 characters long. Click the Please Select button to select an existing ACL from the list.
Action	Select the action to be taken here. Options to choose from are Add and Clear .

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Length	Enter the length value here. This specifies the number of data bytes to send. The default value is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. It does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420 bytes.
ToS	Enter the ToS value here. This is used to configure the QoS on ICMP datagrams. The range is from 0 to 255.
Stop Time	Enter the stop time value here. This specifies to stop the ping after the amount of times entered here. If this value is configured as 0, then the ping can only be stopped by clicking the Stop button manually. The range is from 0 to 99.
Source IPv4 Address	Enter the source IPv4 address. If the current Switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the **Start** button to initiate the Ping Test for each individual section.

The fields that can be configured in **IPv6 Ping** are described below:

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Length	Enter the length value here. This specifies the number of data bytes to send. The default value is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. It does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420 bytes.
Stop Time	Enter the stop time value here. This specifies to stop the ping after the amount of times entered here. If this value is configured as 0, then the ping can only be stopped by clicking the Stop button manually. The range is from 0 to 99.

Parameter	Description
Source IPv6 Address	Enter the source IPv6 address. If the current Switch has more than one IPv6 address, you can enter one of them to this field. When entered, this IPv6 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the **Start** button to initiate the Ping Test for each individual section.

After clicking the **Please Select** button, the following window will appear:

ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
<input type="radio"/>	1	S-IP-ACL	Standard IP ACL
<input type="radio"/>	11000	S-IPv6-ACL	Standard IPv6 ACL

1/1 |< < 1 > >| Go

OK

Figure 13-13 Ping (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

IPv4 Ping Result

```
[1] Reply from 10.90.90.90, time<10ms
[2] Reply from 10.90.90.90, time<10ms
[3] Reply from 10.90.90.90, time<10ms
[4] Reply from 10.90.90.90, time<10ms
Ping Statistics for 10.90.90.90
Packets: Sent = 4, Received = 4, Lost = 0
```

Stop Back

Figure 13-14 Ping (Start) Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Trace Route

The trace route page allows the user to trace a route between the Switch and a given host on the network.

To view the following window, click **Tools > Trace Route**, as shown below:

The screenshot shows the 'Trace Route' window with two sections: 'IPv4 Trace Route' and 'IPv6 Trace Route'. Each section has a 'Start' button.

IPv4 Trace Route Configuration:

- ☒ IPv4 Address: []
- ☐ Domain Name: [255 chars]
- Initial TTL (1-255): [1]
- Max TTL (1-255): [30]
- Port (1-65535): [33434]
- Timeout (1-65535): [5] sec
- Length (1-1420): [40] bytes
- ToS (0-255): [0]
- Source IPv4 Address: []
- Probe Number (1-1000): [1]
- [Start]

IPv6 Trace Route Configuration:

- ☒ IPv6 Address: [2233::1]
- ☐ Domain Name: [255 chars]
- Initial TTL (1-255): [1]
- Max TTL (1-255): [30]
- Port (1-65535): [33434]
- Timeout (1-65535): [5] sec
- Length (1-1420): [40] bytes
- Source IPv6 Address: [2233::2]
- Probe Number (1-1000): [1]
- [Start]

Figure 13-15 Trace Route Window

The fields that can be configured in **IPv4 Trace Route** are described below:

Parameter	Description
IPv4 Address	Select and enter the IPv4 address of the destination here.
Domain Name	Select and enter the domain name of the destination here.
Initial TTL	Enter the initial Time-To-Live (TTL) value here. The range is from 1 to 255.
Max TTL	Enter the Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 255 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Length	Enter the length value here. This specifies the number of bytes of the outgoing datagram. The range is from 1 to 1420 bytes.
ToS	Enter the ToS value here. This specifies the ToS to be set in the IP header of the outgoing datagram. The range is from 0 to 255.
Source IPv4 Address	Enter the source IPv4 address here. The specified IPv4 address must one of the IPv4 addresses configured for the Switch.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

The fields that can be configured in **IPv6 Trace Route** are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address of the destination here.
Domain Name	Select and enter the domain name of the destination here.
Initial TTL	Enter the initial Time-To-Live (TTL) value here. The range is from 1 to 255.
Max TTL	Enter the Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 255 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Length	Enter the length value here. This specifies the number of bytes of the outgoing datagram. The range is from 1 to 1420 bytes.
Source IPv6 Address	Enter the source IPv6 address here. The specified IPv6 address must one of the IPv6 addresses configured for the Switch.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

After clicking the **Start** button in **IPv4 Trace Route** section, the following **IPv4 Trace Route Result** section will appear:

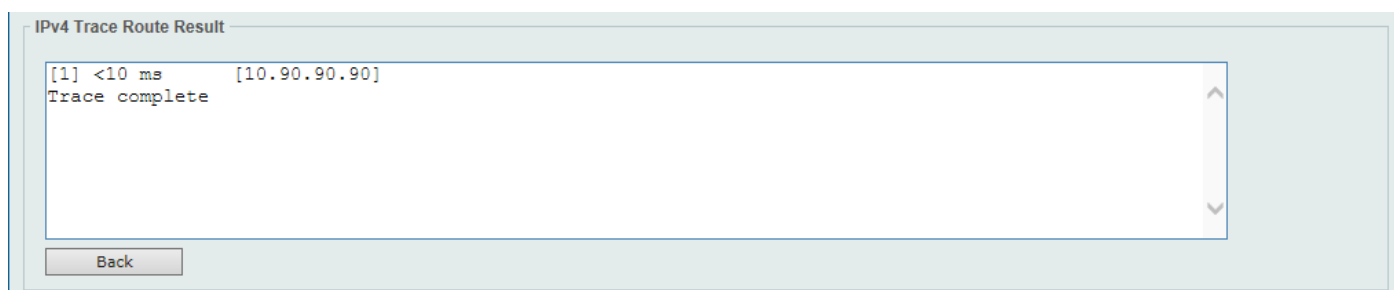


Figure 13-16 Trace Route (Start) Window

Click the **Back** button to stop the trace route and return to the IPv4 Trace Route section.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

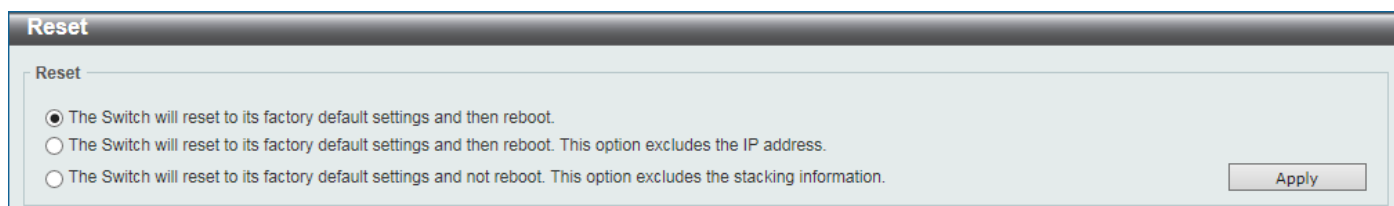


Figure 13-17 Reset Window

Select one of the following options:

- The Switch will reset to its factory default settings and then reboot.
- The Switch will reset to its factory default settings and then reboot. This option excludes the IP address.

- The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information.

Click the **Apply** button to initiate the reset.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:

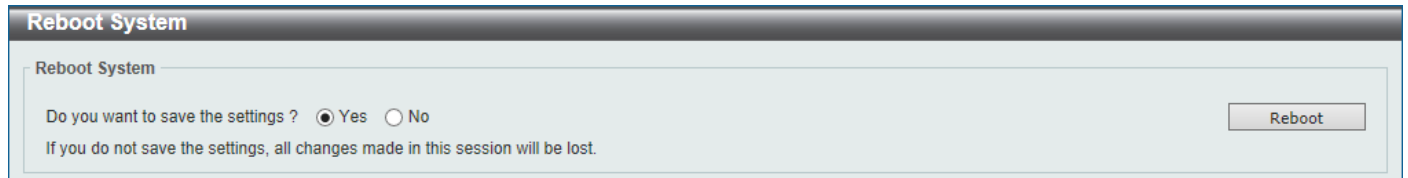


Figure 13-18 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

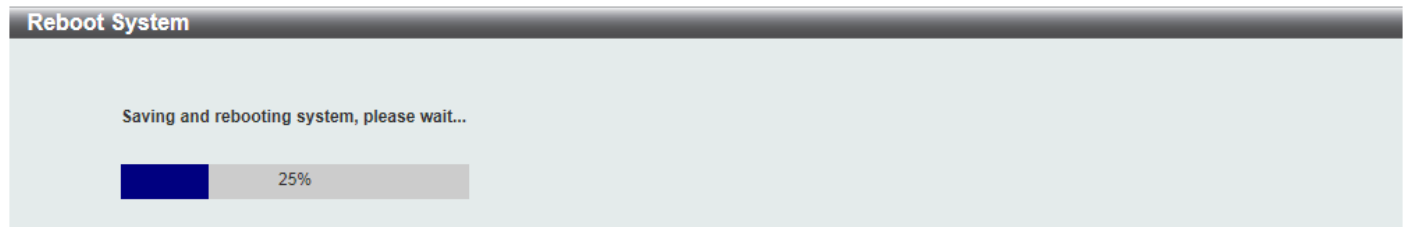


Figure 13-19 Reboot System (Rebooting) Window

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DGS-3130-30TS Switch.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords will be forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the **Password Recovery** feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on this Switch to easily recover passwords. Complete these steps to reset the password:

- For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the Switch.
- Power on the Switch. After the **UART init** is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (**Shift+6**) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled.

```

Boot Procedure                                     v1.00.006
-----
Power On Self Test ..... 100 %

MAC Address   : F0-7D-68-36-30-00
H/W Version   : A1

Please Wait, Loading 1.00.008 Runtime Image ..... 100 %
UART init ..... 100 %

```

```

Password Recovery Mode
Switch(reset-config)#

```

In the "Password Recovery Mode" only the following commands can be used.

Command	Description
<code>no enable password</code>	This command is used to delete all account level passwords.
<code>no login password</code>	This command is used to clear the local login methods.
<code>no username</code>	This command is used to delete all local user accounts.
<code>password-recovery</code>	This command is used to initiate the password recovery procedure.
<code>reload</code>	This command is used to save and reboot the Switch.
<code>reload clear running-config</code>	This command is used to reset the running configuration to the factory default settings and then reboot the Switch.
<code>show running-config</code>	This command is used to display the current running configuration.
<code>show username</code>	This command is used to display local user account information.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

802.1X

Log Description	Severity
<p>Event description: 802.1X Authentication failure.</p> <p>Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <p>reason: The reason for the failed authentication.</p> <p>username: The user that is being authenticated.</p> <p>interface-id: The interface name.</p> <p>macaddr: The MAC address of the authenticated device.</p>	Critical
<p>Event description: 802.1X Authentication successful.</p> <p>Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <p>username: The user that is being authenticated.</p> <p>interface-id: The interface name.</p> <p>macaddr: The MAC address of the authenticated device.</p>	Informational

AAA

Log Description	Severity
<p>Event description: AAA global state is enabled or disabled.</p> <p>Log Message: AAA is <status>.</p> <p>Parameters description:</p> <p>status: The status indicates the AAA enabled or disabled.</p>	Informational
<p>Event description: Successful login.</p> <p>Log Message: Successful login through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event description: Login failed.</p> <p>Log Message: Login failed through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p>	Warning

Log Description	Severity
<p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	
<p>Event description: Login failed due to AAA server timeout or improper configuration.</p> <p>Log Message: Login failed through <exec-type> from <client-ip> due to AAA server <server-ip> timeout (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: Enable privilege successfully.</p> <p>Log Message: Successful enable privilege through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event description: Enable privilege failure.</p> <p>Log Message: Enable privilege failed through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: the remote server does not respond to the enable password authentication request.</p> <p>Log Message: Enable privilege failed through <exec-type> from <client-ip> due to AAA server <server-ip> timeout (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: RADIUS assigned a valid VLAN ID attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>vid: The assign VLAN ID that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event description: RADIUS assigned a valid bandwidth attributes.</p>	Informational

Log Description	Severity
<p>Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface -id> (Username: <username>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>direction: It indicates the direction for bandwidth control, e.g.: ingress or egress.</p> <p>threshold: The assign threshold of bandwidth that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	
<p>Event description: RADIUS assigned a valid priority attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port <interface -id> (Username: <username>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>priority: The assign priority that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event description: RADIUS assigned ACL script but fails to apply to the system due to insufficient resource.</p> <p>Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port <interface -id> (<acl-script>)</p> <p>Parameters description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>username: It indicates the username for authentication.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>acl-script: The assign ACL script that authorized by from RADIUS server.</p>	Warning

ARP

Log Description	Severity
<p>Event description: Gratuitous ARP detected duplicate IP.</p> <p>Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>).</p> <p>Parameters description:</p> <p>ipaddr: The IP address which is duplicated with our device.</p> <p>macaddr: The MAC address of the device that has duplicated IP address as our device.</p> <p>unitID: 1.Interger value;2.Represent the id of the device in the stacking system.</p> <p>portNum: 1.Interger value;2.Represent the logic port number of the device.</p> <p>ipif_name: The name of the interface of the Switch which has the conflict IP address.</p>	Warning

Auto-save

Log Description	Severity
<p>Event description: Record the event when the configure information of DDP is saved automatically.</p> <p>Log Message:CONFIG-6-DDPSAVECONFIG: [Unit <unitID>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <p>Unit: Box ID</p>	Informational

Log Description	Severity
username: Represent current login user. ipaddr: Represent client IP address	

BPDU Protection

Log Description	Severity
Event description: Record the event when the BPDU attack happened. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Parameters description: interface-id: Interface on which detected STP BPDU attack. mode: BPDU Protection mode of the interface. Mode can be drop, block, or shutdown	Informational
Event description: Record the event when the STP BPDU attack recovered. Log Message: <interface-id> recover from BPDU under protection state. Parameters description: interface-id: Interface on which detected STP BPDU attack.	Informational

Configuration/Firmware

Log Description	Severity
Event description: Firmware upgraded successfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event description: Firmware upgraded unsuccessfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event description: Firmware uploaded successfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)	Informational

Log Description	Severity
<p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	
<p>Event description: Firmware uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
<p>Event description: Configuration downloaded successfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
<p>Event description: Configuration downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr : Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
<p>Event description: Configuration uploaded successfully.</p> <p>Log Message: [Unit <unitID>] Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p>	Informational

Log Description	Severity
username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	
Event description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>] Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event description: Unknown type files downloaded unsuccessfully. Log Message: [Unit <unitID>] Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning

DAD

Log Description	Severity
Event description: When DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages. Parameters description: ipv6address : IPv6 address in Neighbor Solicitation Messages interface-id : port interface ID	Warning
Event description: When DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages. Parameters description: ipv6address : IPv6 address in Neighbor Advertisement Messages interface-id : port interface ID	Warning

DDM

Log Description	Severity
<p>Event description: when the any of SFP parameters exceeds from the warning threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded.</p> <p>Parameters description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type. It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p> <p>high-low: High or low threshold.</p>	Warning
<p>Event description: when the any of SFP parameters exceeds from the alarm threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded.</p> <p>Parameters description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type. It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p> <p>high-low: High or low threshold.</p>	Critical
<p>Event description: when the any of SFP parameters recovers from the warning threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> back to normal.</p> <p>Parameters description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type. It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p>	Warning

DHCPv6 Client

Log Description	Severity
<p>Event description: DHCPv6 client interface administrator state changed.</p> <p>Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled].</p> <p>Parameters description:</p> <p><ipif-name>: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: DHCPv6 client obtains an IPv6 address from a DHCPv6 server.</p> <p>Log Message: DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name>.</p> <p>Parameters description:</p> <p>ipv6address: IPv6 address obtained from a DHCPv6 server.</p>	Informational

Log Description	Severity
ipif-name: Name of the DHCPv6 client interface.	
<p>Event description: The IPv6 address obtained from a DHCPv6 server starts renewing.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing.</p> <p>Parameters description:</p> <p>ipv6address: IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The IPv6 address obtained from a DHCPv6 server renews success.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success.</p> <p>Parameters description:</p> <p>ipv6address: IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The IPv6 address obtained from a DHCPv6 server starts rebinding</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding.</p> <p>Parameters description:</p> <p>ipv6address: IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The IPv6 address obtained from a DHCPv6 server rebinds success</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success.</p> <p>Parameters description:</p> <p>ipv6address: IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The IPv6 address from a DHCPv6 server was deleted.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted.</p> <p>Parameters description:</p> <p>ipv6address: IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: DHCPv6 client PD interface administrator state changed.</p> <p>Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled disabled></p> <p>Parameters description:</p> <p>intf-name: Name of the DHCPv6 client PD interface.</p>	Informational
<p>Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router.</p> <p>Log Message: DHCPv6 client PD obtains an IPv6 prefix <ipv6networkaddr> on interface <intf-name></p> <p>Parameters description:</p> <p>ipv6networkaddr: IPv6 prefix obtained from a delegation router.</p> <p>intf-name: Name of the DHCPv6 client PD interface.</p>	Informational
<p>Event description: The IPv6 prefix obtained from a delegation router starts renewing.</p> <p>Log Message: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> starts renewing.</p> <p>Parameters description:</p> <p>ipv6networkaddr: IPv6 prefix obtained from a delegation router.</p> <p>intf-name: Name of the DHCPv6 client PD interface.</p>	Informational
<p>Event description: The IPv6 prefix obtained from a delegation router renews success.</p> <p>Log Message: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> renews success.</p>	Informational

Log Description	Severity
Parameters description: ipv6anetworkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	
Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> starts rebinding. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> rebinds success. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix from a delegation router was deleted. Log Message: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> was deleted. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational

DHCPv6 Relay

Log Description	Severity
Event description: DHCPv6 relay on a specify interface's administrator state changed Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] Parameters description: <ipif-name>: Name of the DHCPv6 relay agent interface.	Informational

DHCPv6 Server

Log Description	Severity
Event description: The address of the DHCPv6 Server pool is used up Log Message: The address of the DHCPv6 Server pool <pool-name> is used up. Parameters description: <pool-name>: Name of the DHCPv6 Server pool.	Informational
Event description: The number of allocated IPv6 addresses is equal to 4096 Log Message: The number of allocated IPv6 addresses of the DHCPv6 Server pool is equal to 4096.	Informational

DoS Prevention

Log Description	Severity
Event description: Detect DOS attack. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>).	Notice

Log Description	Severity
Parameters description: dos-type: DOS attack type ip-address: IP address. interface-id: Interface name	

Dynamic ARP Inspection

Log Description	Severity
Event description: Detect illegal ARP packet Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Parameters description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response. ipaddr: IP address macaddr: MAC address. vlanid: VLAN ID interface-id: Interface name	Warning
Event description: Detect legal ARP packet. Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Parameters description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response. ipaddr: IP address macaddr: MAC address. vlanid: VLAN ID interface-id: Interface name	Informational

ERPS

Log Description	Severity
Event description: manual Switch is issued. Log Message: "Manual Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: signal fail is detected. Log Message: "Signal fail detected on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: Signal fail cleared. Log Message: "Signal fail cleared on node(MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: Force Switch is issued.	Warning

Log Description	Severity
Log Message: "Force Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	
Event description: Clear command is issued. Log Message: "Clear command is issued on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: "RPL owner conflicted." Log Message: "RPL owner conflicted on the node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning

Ethernet OAM

Log Description	Severity
Event description: Dying gasp event(remote) Log Message: OAM dying gasp event received (Port<interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Dying gasp event(local) Log Message: Device encountered an OAM dying gasp event.	Warning
Event description: Critical event(remote) Log Message: OAM critical event received (Port<interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Critical event(local) Log Message: Device encountered an OAM critical event (Port<interface-id>, <condition>) Parameters description: interface-id: The interface name. condition: Display string for the condition of generating critical link event. e.g. OAM disable, Port shutdown, Port link down, Packet overload.	Warning
Event description: Errored Symbol Period Event(remote) Log Message: Errored symbol period event received (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Errored Frame Event Log Message: Errored frame event received(Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Errored Frame Period Event Log Message: Errored frame period event received(Port <interface-id>)	Warning

Log Description	Severity
Parameters description: interface-id: The interface name.	
Event description: Errored Frame Seconds Summary Event Log Message: Errored frame seconds summary event received (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Remote loopback start Log Message: OAM Remote loopback started (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Remote loopback stop Log Message: OAM Remote loopback stopped (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning

Interface

Log Description	Severity
Event description: Port link up. Log Message: Port <portNum> link up, <link state> Parameters description: portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex	Informational
Event description: Port link down. Log Message: Port <portNum> link down Parameters description: portNum: 1.Interger value; 2.Represent the logic port number of the device.	Informational

IP Directed Broadcast

Log Description	Severity
Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Parameters description: IP: the Broadcast IP destination address.	Informational
Event description: IP Directed-broadcast rate exceed 100 packets per second Log Message: IP Directed Broadcast rate is high.	Informational

IPSG

Log Description	Severity
Event description: When there is no hardware rule resource to set DHCP Snooping entry into IPSG table, the syslog will be record. Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>)	Warning

Log Description	Severity
Parameters description: ipaddr: IP address macaddr: MAC address. vlanid: VLAN ID interface-id: Interface name	

LACP

Log Description	Severity
Event description: Link Aggregation Group link up. Log Message: Link Aggregation Group <group_id> link up. Parameters description: group_id: The group id of the link up aggregation group.	Informational
Event description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group_id> link down. Parameters description: group_id: The group id of the link down aggregation group.	Informational
Event description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id>. Parameters description: Ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
Event description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id>. Parameters description: Ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

LBD

Log Description	Severity
Event Description: Loop back is detected under port-based mode. Log Message: IfInfo LBD loop occurred. Parameters Description: IfInfo: The interface info.	Critical
Event Description: Port recovered from LBD blocked state under port-based mode. Log Message: IfInfo LBD loop recovered. Parameters Description: IfInfo: The interface info.	Critical
Event Description: Loop back is detected under VLAN-based mode. Log Message: IfInfo VID <vlanID> LBD loop occurred. Parameters Description: IfInfo: The interface info. vlanID: The VLAN ID number.	Critical

Log Description	Severity
<p>Event Description: Port recovered from LBD blocked state under VLAN-based mode.</p> <p>Log Message:</p> <p>IfInfo VID <vlanID> LBD loop recovered.</p> <p>Parameters Description:</p> <p>IfInfo: The interface info.</p> <p>vlanID: The VLAN ID number.</p>	Critical
<p>Event Description: The number of VLANs that loop back has occurred hit the specified number.</p> <p>Log Message:</p> <p>Loop VLAN numbers overflow.</p> <p>Parameters Description:</p> <p>None</p>	Critical

LLDP-MED

Log Description	Severity
<p>Event description: LLDP-MED topology change detected</p> <p>Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID.</p> <p>portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID.</p> <p>deviceClass: LLDP-MED device type.</p>	Notice
<p>Event description: Conflict LLDP-MED device type detected</p> <p>Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number.</p> <p>chassisType: chassis ID subtype.</p>	Notice

Log Description	Severity
<p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID. portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID. deviceClass: LLDP-MED device type.</p>	
<p>Event description: Incompatible LLDP-MED TLV set detected</p> <p>Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters description:</p> <p>portNum: The port number. chassisType: chassis ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: chassis ID. portType: port ID subtype.</p> <p>Value list:</p> <ol style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) <p>portID: port ID. deviceClass: LLDP-MED device type.</p>	Notice

Login/Logout

Log Description	Severity
Event description: Login through console successfully. Log Message: [Unit <unitID>,] Successful login through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through console unsuccessfully. Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Warning
Event description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>)	Critical

Log Description	Severity
Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	
Event description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

MAC

Log Description	Severity
Event description: the host has passed MAC authentication Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host has aged out. Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Critical
Event description: the authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state.	Warning
Event description: the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: MAC-based Access Control recovers from stop learning state.	Warning
Event description: the authorized user number on an interface has reached the maximum user limit. Log Message: <interface-id> enters MAC-based Access Control stop learning state Parameters description: interface-id: the interface on which the host is authenticated.	Warning

Log Description	Severity
<p>Event description: the authorized user number on an interface is below the maximum user limit in a time interval.</p> <p>Log Message: <interface-id> recovers from MAC-based Access Control stop learning state.</p> <p>Parameters description:</p> <p>interface-id: the interface on which the host is authenticated.</p>	Warning

MSTP Debug Enhancement

Log Description	Severity
<p>Event description: Topology changed.</p> <p>Log Message: Topology changed [([Instance:<InstanceID>] , <portNum> ,MAC: <macaddr>)]</p> <p>Parameters description:</p> <p>InstanceID: Instance ID.</p> <p>portNum: Port ID</p> <p>macaddr: MAC address</p>	Notice
<p>Event description: Spanning Tree new Root Bridge</p> <p>Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>],MAC: <macaddr>, Priority :<value>)</p> <p>Parameters description:</p> <p>InstanceID: Instance ID.</p> <p>macaddr: Mac address</p> <p>value: priority value</p>	Informational
<p>Event description: Spanning Tree Protocol is enabled</p> <p>Log Message: Spanning Tree Protocol is enabled</p>	Informational
<p>Event description: Spanning Tree Protocol is disabled</p> <p>Log Message: Spanning Tree Protocol is disabled</p>	Informational
<p>Event description: New root port</p> <p>Log Message: New root port selected [([Instance:<InstanceID>] , <portNum>)]</p> <p>Parameters description:</p> <p>InstanceID: Instance ID.</p> <p>portNum: Port ID</p>	Notice
<p>Event description: Spanning Tree port status changed</p> <p>Log Message: Spanning Tree port status change [([Instance:<InstanceID>] , <portNum>)] <old_status> -> <new_status></p> <p>Parameters description:</p> <p>InstanceID: Instance ID.</p> <p>portNum: Port ID</p> <p>old_status: Old status</p> <p>new_status: New status</p>	Notice
<p>Event description: Spanning Tree port role changed.</p> <p>Log Message: Spanning Tree port role change. [([Instance:<InstanceID>] , <[portNum>)] <old_role> -> <new_role></p> <p>Parameters description:</p> <p>InstanceID: Instance ID.</p> <p>portNum: Port ID/</p> <p>old_role: Old role</p> <p>new_status: New role</p>	Informational

Log Description	Severity
Event description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance:<InstanceID>) Parameters description: InstanceID: Instance ID.	Informational
Event description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance:<InstanceID>) Parameters description: InstanceID: Instance ID.	Informational
Event description: Spanning Tree Version changed. Log Message: Spanning Tree version change.(New version:<new_version>) Parameters description: new_version: New STP version.	Informational
Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>). Parameters description: name : New name. revision_level: New revision level.	Informational
Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid: VLAN list	Informational
Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid: VLAN list	Informational
Event description: Spanning Tree port role change to alternate port due to the guard root. Log Message: Spanning Tree port role change (Instance : <InstanceID>, <portNum>) to alternate port due to the guard root. Parameters description: InstanceID: Instance ID. portNum: Port ID	Informational
Event description: Spanning Tree loop guard blocking. Log Message: Spanning Tree loop guard blocking(Instance : <InstanceID>, <portNum>) Parameters description: InstanceID: Instance ID. portNum: Port ID	Informational

Peripheral

Log Description	Severity
Event description: Fan Recovered. Log Message: Unit <unit-id>, <fan-descr> back to normal	Critical

Log Description	Severity
Parameters description: Unit <id>: The unit ID. <fan-descr>: For example, right fan, left fan etc.	
Event description: Fan Fail Log Message: Unit <unit-id> <fan-descr> failed. Parameters description: Unit <id>: The unit ID. <fan-descr>: For example, right fan, left fan etc.	Critical
Event description: Temperature sensor enters alarm state. Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> Parameters description: unitID: The unit ID. thermal-sensor-descr: Description of the sensor. degree: The current temperature of the sensor.	Warning
Event description: Temperature recovers to normal. Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal Parameters description: unitID: The unit ID. thermal-sensor-descr: Description of the sensor. degree: The current temperature of the sensor.	Informational
Event description: Power failed. Log Message: Unit <unit-id> <power-descr> failed Parameters description: Unit <id>: The unit ID. power-descr: Describe the power.	Critical
Event description: Power is recovered. Log Message: Unit <unit-id> <power-descr> back to normal Parameters description: Unit <id>: The unit ID. power-descr: Describe the power.	Critical
Event description: External Alarm state to change. Log Message: Unit <unit-id> External Alarm Channel <channelID> :<alarmMsg> Parameters description: Unit <id>: The unit ID. channelID: The channel ID. alarmMsg: The alarm Msg.	Critical

Port

Log Description	Severity
Event description: port linkup Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
Event description: port linkdown Log Message: Port <port> link down	Informational

Log Description	Severity
Parameters description: port: Represents the logical port number.	

Port Security

Log Description	Severity
Event description: Address full on a port Log Message: MAC address <mac-address> causes port security violation on <interface-id>. Parameters description: macaddr: The violation MAC address. interface-id: The interface name.	Warning
Event description: Address full on system Log Message: Limit on system entry number has been exceeded.	Warning

Reboot Schedule

Log Description	Severity
Event description: Tips is about will to reboot Switch within the specified time. Log Message: Display "Reboot scheduled in 5 minutes" when the countdown equals 5 minutes. Display "Reboot scheduled in 1 minute" when the countdown equals 1 minute.	Critical

Safeguard

Log Description	Severity
Event description: When the CPU utilization is over the rising threshold, the Switch enters exhausted mode, and the syslog will be recorded. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Parameters description: unit-id: Unit ID.	Warning
Event description: When the CPU utilization is lower than the falling threshold, the Switch enters normal mode, and the syslog will be recorded. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Parameters description: unit-id: Unit ID.	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event description: SSH server is disabled. Log Message: SSH server is disabled	Informational

SSL

Log Description	Severity
Event description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
Event description: Web (SSL) session timed out. Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Logout through Web (SSL). Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Stacking

Log Description	Severity
Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master (Unit <unitID>, MAC:<macaddr>). Parameters description:	Critical

Log Description	Severity
Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain. unitID: Box ID. Macaddr: MAC address.	
Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Slave changed to master Log Message: Slave changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). Parameters description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical
Event description: Stacking port link up. Log Message: Stacking port <portID> link up. Parameters description: portID: port ID.	Critical
Event description: Stacking port link down. Log Message: Stacking port <portID> link down. Parameters description: portID: port ID.	Critical
Event description: SIO interface link up. Log Message: SIO interface Unit <unitID> SIO<SIOID> link up. Parameters description: unitID: Box ID. SIOD: SIO ID.	Critical
Event description: SIO interface link down. Log Message: SIO interface Unit <unitID> SIO<SIOID> link down. Parameters description: unitID: Box ID. SIOD: SIO ID.	Critical

Storm Control

Log Description	Severity
Event description: Storm occurrence. Log Message: <Broadcast Multicast Unicast> storm is occurring on <interface-id>. Parameters description: Broadcast: Storm is resulted by broadcast packets (DA = FF:FF:FF:FF:FF:FF). Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast.	Warning

Log Description	Severity
Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets interface-id: The interface ID on which a storm is occurring.	
Event description: Storm cleared. Log Message: <Broadcast Multicast Unicast> storm is cleared on <interface-id>. Parameters description: Broadcast: Broadcast storm is cleared. Multicast: Multicast storm is cleared. Unicast: Unicast storm (including both known and unknown unicast packets) is cleared. interface-id: The interface ID on which a storm is cleared.	Informational
Event description: Port shut down due to a packet storm Log Message: <interface-id> is currently shut down due to the <Broadcast Multicast Unicast> storm. Parameters description: interface-id: The interface ID on which is error-disabled by storm. Broadcast: The interface is disabled by broadcast storm. Multicast: The interface is disabled by multicast storm. Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).	Warning

Telnet

Log Description	Severity
Event description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning
Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>). Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational

Traffic Control

Log Description	Severity
Event description: Broadcast storm occurrence. Log Message: <interface-id> Broadcast storm is occurring. Parameters description: interface-id: The interface name.	Warning
Event description: Broadcast storm cleared. Log Message: <interface-id> Broadcast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Multicast storm occurrence. Log Message: <interface-id> Multicast storm is occurring. Parameters description: interface-id: The interface name.	Warning
Event description: Multicast Storm cleared. Log Message: <interface-id>Multicast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Unicast storm occurrence. Log Message: <interface-id> Unicast storm is occurring. Parameters description: interface-id: The interface name.	Warning
Event description: Unicast Storm cleared. Log Message: <interface-id> Unicast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Port shut down due to a packet storm Log Message: <interface-id> is currently shut down due to a packet storm. Parameters description: interface-id: The interface name.	Warning

VRRP Debug Enhancement

Log Description	Severity
Event description: One virtual router state becomes Master. Log Message: VR <vr-id> at interface <intf-name> Switch to Master Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
Event description: One virtual router state becomes Backup. Log Message: VR <vr-id> at interface <intf-name> Switch to Backup Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
Event description: One virtual router state becomes Init. Log Message: VR <vr-id> at interface <intf-name> Switch to Init Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational

Log Description	Severity
<p>Event description: Authentication type mismatch of one received VRRP advertisement message.</p> <p>Log Message: Authentication type mismatch on VR <vr-id> at interface <intf-name></p> <p>Parameters description:</p> <p>vr-id: VRRP virtual router ID.</p> <p>intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: Authentication checking fail of one received VRRP advertisement message.</p> <p>Log Message: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type></p> <p>Parameters description:</p> <p>vr-id: VRRP virtual router ID.</p> <p>intf-name: Interface name on which virtual router is based.</p> <p>Auth-type: VRRP interface authentication type.</p>	Warning
<p>Event description: Checksum error of one received VRRP advertisement message.</p> <p>Log Message: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name></p> <p>Parameters description:</p> <p>vr-id: VRRP virtual router ID.</p> <p>intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: Virtual router ID mismatch of one received VRRP advertisement message.</p> <p>Log Message: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name></p> <p>Parameters description:</p> <p>vr-id: VRRP virtual router ID.</p> <p>intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: Advertisement interval mismatch of one received VRRP advertisement message.</p> <p>Log Message: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name></p> <p>Parameters description:</p> <p>vr-id: VRRP virtual router ID.</p> <p>intf-name: Interface name on which virtual router is based.</p>	Warning
<p>Event description: A virtual MAC address is added into Switch L2 table</p> <p>Log Message: Added a virtual MAC <vrrp-mac-addr> into L2 table</p> <p>Parameters description:</p> <p>vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: A virtual MAC address is deleted from Switch L2 table.</p> <p>Log Message: Deleted a virtual MAC <vrrp-mac-addr> from L2 table</p> <p>Parameters description:</p> <p>vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: A virtual MAC address is adding into Switch L3 table.</p> <p>Log Message: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table</p> <p>Parameters description:</p> <p>vrrp-ip-addr: VRRP virtual IP address</p> <p>vrrp-mac-addr: VRRP virtual MAC address</p>	Notice
<p>Event description: A virtual MAC address is deleting from Switch L3 table.</p> <p>Log Message: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table</p> <p>Parameters description:</p>	Notice

Log Description	Severity
vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	
Event description: Failed when adding a virtual MAC into Switch chip L2 table. Log Message: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behavior.	Error
Event description: Failed when deleting a virtual MAC from Switch chip L2 table. Log Message: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behavior.	Error
Event description: Failed when adding a virtual MAC into Switch L3 table. The L3 table is full. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Error
Event description: Failed when adding a virtual MAC into Switch L3 table. The port where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-port: port number of VRRP virtual MAC.	Error
Event description: Failed when adding a virtual MAC into Switch L3 table. The interface where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-intf: interface id on which VRRP virtual MAC address is based.	Error
Event description: Failed when adding a virtual MAC into Switch L3 table. The box where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-box: stacking box number of VRRP virtual MAC.	Error
Event description: Failed when adding a virtual MAC into Switch chip's L3 table. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Error

Log Description	Severity
vrrp-errcode: Err code of VRRP protocol behavior.	
Event description: Failed when deleting a virtual MAC from Switch chip's L3 table. Log Message: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error

WAC

Log Description	Severity
Event description: When a client host fails to authenticate. Log Message: WAC unauthenticated user (User Name: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>) Parameters description: string: User name ipaddr: IP address ipv6address: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
Event description: This log will be triggered when the number of authorized users reaches the maximum user limit on the whole device. Log Message: WAC enters stop learning state.	Warning
Event description: This log will be triggered when the number of authorized users is below the maximum user limit on whole device in a time interval (The interval is project dependent). Log Message: WAC recovered from stop learning state.	Warning
Event description: When a client host authenticated successful. Log Message: WAC authenticated user (Username: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>) Parameters description: string: User name ipaddr: IP address ipv6address: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Informational

Web

Log Description	Severity
Event description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational

Log Description	Severity
Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

802.1X

Trap Name	Description	OID
dDot1xExtLoggedSuccess	The trap is sent when a host has successfully logged in (passed 802.1X authentication). Binding objects: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.30.0.1
dDot1xExtLoggedFail	The trap is sent when a host failed to pass 802.1X authentication (login failed). Binding objects: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.14.30.0.2

802.3ah OAM

Trap Name	Description	OID
dot3OamThresholdEvent	This notification is sent when a local or remote threshold crossing event is detected. Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogWindowHi (6) dot3OamEventLogWindowLo (7) dot3OamEventLogThresholdHi (8) dot3OamEventLogThresholdLo (9) dot3OamEventLogValue (10) dot3OamEventLogRunningTotal (11) dot3OamEventLogEventTotal	1.3.6.1. 2.1.158. 0.1
dot3OamNonThresholdEvent	This notification is sent when a local or remote non-threshold crossing event is detected. Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogEventTotal	1.3.6.1. 2.1.158. 0.2

Authentication Fail

Trap Name	Description	OID
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

BPDU Protection

Trap Name	Description	OID
dBpduProtectionAttackOccur	This trap is sent when the BPDU attack happened on an interface. Binding objects: (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.17.1.14.47.0.1
dBpduProtectionAttackRecover	This trap is sent when the BPDU attack recovered on an interface. Binding objects: (1) ifIndex	1.3.6.1.4.1.17.1.14.47.0.2

DDM

Trap Name	Description	OID
dDdmAlarmTrap	A notification is generated when an abnormal alarm situation occurs or recovers from an abnormal alarm situation to normal status. Only when the current value > low warning or current value < high warning will send recover trap. Binding objects: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17.1.14.72.0.1
dDdmWarningTrap	A notification is generated when an abnormal warning situation occurs or recovers from an abnormal warning situation to normal status. Binding objects: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17.1.14.72.0.2

DHCP Server Screen Prevention

Trap Name	Description	OID
dDhcpFilterAttackDetected	When DHCP Server Screen is enabled, if the Switch received the forge DHCP Server packet, the Switch will trap the event if any attacking packet is received. Binding objects: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.17 1.14.133.0.1

DoS Prevention

Trap Name	Description	OID
dDosPreveAttackDetectedPacket	The trap is sent when detect DOS attack. Binding objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2

ERPS

Trap Name	Description	OID
dErpsFailedetectedNotif	A dErpsFailureNotification is sent when dErpsNotificationEnabled is 'true' and a signal failure is detected.	1.3.6.1.4.1.17 1.14.78.0.1
dErpsFailureClearedNotif	A dErpsFailureClearedNotif is sent when dErpsNotificationEnabled is 'true' and a signal failure is cleared.	1.3.6.1.4.1.17 1.14.78.0.2
dErpsRPLOwnerConflictNotif	A dErpsOwnerConflictNotif is sent when dErpsNotificationEnabled is 'true' and RPL owner conflict is detected	1.3.6.1.4.1.17 1.14.78.0.3

ErrDisable

Trap Name	Description	OID
dErrDisNotifyPortDisabledAssert	The trap is sent when a port enters into error disabled state. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.1
dErrDisNotifyPortDisabledClear	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.2

External Alarm

Trap Name	Description	OID
dExternalAlarmStatusChg	<p>The commander Switch will send this notification when External alarm state is changed.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) dExternalAlarmUnitID (2) dExternalAlarmChannel (3) dExternalAlarmStatus 	1.3.6.1.4.1.17 1.14.32.0.1

Gratuitous ARP

Trap Name	Description	OID
agentGratuitousARPTrap	<p>The trap is sent when IP address conflicted.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName 	1.3.6.1.4.1.17 1.14.75.0.1

IP-MAC-Port Binding

Trap Name	Description	OID
dImpbViolationTrap	<p>The address violation notification is generated when IP-MAC-Port Binding address violation is detected.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan 	1.3.6.1.4.1.17 1.14.22.0.1

LACP

Trap Name	Description	OID
linkUp	<p>A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ifIndex, (2) if AdminStatus (3) ifOperStatu 	1.3.6.1.6.3.1.1 .5.4
linkDown	<p>A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.</p> <p>Binding objects:</p>	1.3.6.1.6.3.1.1 .5.3

Trap Name	Description	OID
	(1) ifIndex, (2) if AdminStatus (3) ifOperStatus	

LBD

Trap Name	Description	OID
swPortLoopOccurred	The trap is sent when a port loop occurs. Binding objects: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.1
swPortLoopRestart	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.2
swVlanLoopOccurred	The trap is sent when a port loop occurs under LBD VLAN-based mode. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.3
swVlanLoopRestart	The trap is sent when a port loop restarts under LBD VLAN-based mode after the interval time. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.4

LLDP-MED

Trap Name	Description	OID
IldpRemTablesChange	A IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. Binding objects: (1) IldpStatsRemTablesInserts (2) IldpStatsRemTablesDeletes (3) IldpStatsRemTablesDrops (4) IldpStatsRemTablesAgeouts	1.0.8802.1.1.2 .0.0.1
IldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding objects: (1) IldpRemChassisIdSubtype (2) IldpRemChassisId (3) IldpXMedRemDeviceClass	1.0.8808.1.1.2 .1.5.4795.0.1

MAC-based Access Control

Trap Name	Description	OID
dMacAuthLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.1
dMacAuthLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.2
dMacAuthLoggedAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.3

MAC Notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicates the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1
dL2FdbMacNotificationWithVID	This trap indicates the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.17 1.14.3.0.2

MSTP

Trap Name	Description	OID
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17. 0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional	1.3.6.1.2.1.17. 0.2

Peripheral

Trap Name	Description	OID
dEntityExtFanStatusChg	The commander Switch will send this notification when a fan fails (dEntityExtEnvFanStatus is 'fault') or recovers (dEntityExtEnvFanStatus is 'ok'). Binding objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.17 1.14.5.0.1
dEntityExtThermalStatusChg	The commander Switch will send this notification when a thermal alarms (dEntityExtEnvTempStatus is 'abnormal') or recover (dEntityExtEnvTempStatus is 'ok'). Binding objects: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.17 1.14.5.0.2
dEntityExtPowerStatusChg	The commander Switch will send this notification when a power module fails, recovers or is removed. Binding objects: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.17 1.14.5.0.3

Port Security

Trap Name	Description	OID
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex, (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.14.8.0.1

Port

Trap Name	Description	OID
linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1 .5.4
linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1 .5.3

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Trap Name	Description	OID
dSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhaust. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0.1
dSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0.2

SIM

Trap Name	Description	OID
swSingleIPMSColdStart	The commander Switch will send this notification when its member generates a cold start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.11
swSingleIPMSWarmStart	The commander Switch will send this notification when its member generates a warm start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.12
swSingleIPMSLinkDown	The commander Switch will send this notification when its member generates a link down notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.13

Trap Name	Description	OID
	(3) ifIndex	
swSingleIPMSLinkUp	The commander Switch will send this notification when its member generates a link up notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.14
swSingleIPMSAuthFail	The commander Switch will send this notification when its member generates an authentication failure notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.15
swSingleIPMSNewRoot	The commander Switch will send this notification when its member generates a new root notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.16
swSingleIPMSTopologyChange	The commander Switch will send this notification when its member generates a topology change notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.17

Stacking

Trap Name	Description	OID
dStackInsertNotification	Unit Hot Insert notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.1
dStackRemoveNotification	Unit Hot Remove notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.2
dStackFailureNotification	Unit Failure notification. Binding objects: (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.3
dStackTPChangeNotification	The stacking topology change notification. Binding objects: (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.4
dStackRoleChangeNotification	The stacking unit role change notification. Binding objects: (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.5

Start

Trap Name	Description	OID
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2

Storm Control

Trap Name	Description	OID
dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17.1.14.25.0.1
dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17.1.14.25.0.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.17.1.14.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.17.1.14.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.17.1.14.14.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.17.1.14.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.17.1.14.14.0.5

Upload/Download

Trap Name	Description	OID
agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding objects: (1) swMultiImageVersion	1.3.6.1.4.1.17.1.12.1.7.2.0.7
agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded Binding objects: (1) unitID	1.3.6.1.4.1.17.1.12.1.7.2.0.9

Trap Name	Description	OID
	(2) agentCfgOperate (3) agentLoginUserName	

VRRP

Trap Name	Description	OID
vrrpTrapNewMaster	The newMaster trap indicates that the sending agent has transitioned to 'Master' state. Binding objects: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68.0.1
vrrpTrapAuthFailure	A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional. Binding objects: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68.0.2

WAC

Trap Name	Description	OID
swWACLoggedSuccess	The trap is sent when a WAC client pass the authentication. Binding objects: (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.171.14.154.0.1
swWACLoggedFail	The trap is sent when a WAC client failed to pass the authentication. Binding objects: (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.171.14.154.0.2

Appendix D - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the Switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of "0", the effective bandwidth will be set "no_limited", and if the bandwidth is configured less than "0" or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0 to 7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |   Length   |    Tag    | String...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name.



NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC based Access Control, or WAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

To assign the **ACL** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for an ACL.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	Used to assign the ACL script. The format is based on Access Control List (ACL) Commands .	ACL Script For example: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), and the 802.1X or MAC-based Access Control WAC is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject. For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

Appendix E - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the Switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link Switch.

RADIUS Authentication Attributes:

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

RADIUS Accounting Attributes:

Number	IETF Attribute
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address