

Web UI Reference Guide

Product Model: DXS-1210 Series

10 Gigabit Ethernet Smart Managed Switch

Release 1.00

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

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

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

© 2020 D-Link Corporation. All rights reserved.

FCC Compliance Statement

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

D-Link Corporate
17595 Mt. Hermann Street
Fountain Valley, CA 92708
(800) 326-1688

CE Mark Warning

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

VCCI Warning

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

BSMI Notice

此為甲類資訊技術設備,於居住環境中使用時,可能會造成射頻擾動,在此種情況下,使用者會被要求採取某些適當的對策。

Safety Compliance

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

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

Table of Contents

1.	Introduction	1
	Audience	1
	Other Documentation	1
	Typographical Conventions	1
	Notes and Cautions	1
2.	Web User Interface (Web UI)	2
	Connecting to the Web UI.....	2
	Logging into the Web UI	2
	Smart Wizard	3
	Step 1 - Web Mode.....	3
	Step 2 - System IP Information.....	4
	Step 3 - User Accounts Settings	5
	Step 4 - SNMP Settings.....	6
	Web Interface Navigation	7
3.	System	9
	Device Information	9
	System Information Settings.....	9
	Peripheral Settings	10
	Port Configuration.....	11
	Port Settings	11
	Port Status	13
	Port Auto Negotiation	13
	Error Disable Settings.....	14
	Jumbo Frame	15
	Interface Description.....	15
	System Log	16
	System Log Settings.....	16
	System Log Discriminator Settings	17
	System Log Server Settings	18
	System Log.....	19
	System Attack Log.....	20
	Time and SNTP	20
	Clock Settings.....	20
	Time Zone Settings	21
	SNTP Settings	22
	Time Range	23
4.	Management	25
	User Accounts Settings	25
	SNMP.....	26
	SNMP Global Settings.....	27
	SNMP Linkchange Trap Settings	28
	SNMP View Table Settings	29
	SNMP Community Table Settings.....	29
	SNMP Group Table Settings	31
	SNMP Engine ID Local Settings.....	32
	SNMP User Table Settings.....	32
	SNMP Host Table Settings.....	34
	RMON	35
	RMON Global Settings	35

RMON Statistics Settings	35
RMON History Settings	36
RMON Alarm Settings	37
RMON Event Settings	38
Telnet/Web.....	39
Session Timeout	39
DHCP.....	40
Service DHCP	40
DHCP Class Settings	41
DHCP Relay	42
DHCPv6 Relay	47
DHCP Auto Configuration.....	52
DHCP Auto Image Settings	52
DNS	53
DNS Global Settings.....	54
DNS Name Server Settings.....	54
DNS Host Settings.....	55
File System	55
D-Link Discovery Protocol	58
DDP Settings	58
DDP Neighbors.....	59
5. Layer 2 Features	60
FDB.....	60
Static FDB.....	60
MAC Address Table Settings	61
MAC Address Table	62
MAC Notification.....	63
VLAN.....	64
VLAN Configuration Wizard.....	64
802.1Q VLAN	67
VLAN Interface	68
Asymmetric VLAN	71
L2VLAN Interface Description	72
Auto Surveillance VLAN	73
Voice VLAN	77
STP	80
STP Global Settings	82
STP Port Settings	84
MST Configuration Identification	85
STP Instance	86
MSTP Port Information	87
Loopback Detection	87
Link Aggregation	89
L2 Multicast Control	91
IGMP Snooping	91
MLD Snooping.....	97
Multicast Filtering Mode.....	103
LLDP	104
LLDP Global Settings	104
LLDP Port Settings	105
LLDP Management Address List.....	106
LLDP Basic TLVs Settings	107

LLDP Dot1 TLVs Settings.....	108
LLDP Dot3 TLVs Settings.....	109
LLDP-MED Port Settings.....	110
LLDP Statistics Information	111
LLDP Local Port Information	112
LLDP Neighbor Port Information	113
6. Layer 3 Features	115
ARP.....	115
ARP Aging Time.....	115
Static ARP	116
ARP Table	116
Gratuitous ARP.....	117
IPv6 Neighbor	118
Interface.....	119
IPv4 Interface	119
IPv6 Interface	121
IPv4 Static/Default Route.....	124
IPv4 Route Table.....	125
IPv6 Static/Default Route.....	126
IPv6 Route Table.....	127
IP Multicast Routing Protocol.....	128
IPMC.....	128
IPv6MC.....	128
7. Quality of Service (QoS).....	130
Basic Settings	130
Port Default CoS.....	130
Port Scheduler Method.....	131
Queue Settings.....	132
CoS to Queue Mapping.....	133
Port Rate Limiting	133
Queue Rate Limiting.....	134
Advanced Settings.....	135
DSCP Mutation Map.....	135
Port Trust State and Mutation Binding	136
DSCP CoS Mapping.....	137
Class Map.....	137
Policy Map	139
Policy Binding.....	141
8. Access Control List (ACL)	142
ACL Configuration Wizard	142
Step 1 - Create/Update.....	142
Step 2 - Select Packet Type	143
Step 3 - Add Rule	144
Step 4 - Apply Port	151
ACL Access List.....	152
Standard IP ACL.....	154
Extended IP ACL	155
Standard IPv6 ACL.....	157
Extended IPv6 ACL	159
Extended MAC ACL	161
ACL Interface Access Group	163

9.	Security	164
	Port Security	164
	Port Security Global Settings.....	164
	Port Security Port Settings	165
	Port Security Address Entries.....	166
	802.1X.....	167
	802.1X Global Settings.....	171
	802.1X Port Settings.....	172
	Authentication Sessions Information	173
	Authenticator Statistics	173
	Authenticator Session Statistics	174
	Authenticator Diagnostics.....	175
	AAA.....	176
	AAA Global Settings	176
	Authentication Settings.....	176
	RADIUS	177
	RADIUS Global Settings.....	177
	RADIUS Server Settings	177
	RADIUS Group Server Settings	178
	RADIUS Statistic	179
	IMPB	180
	IPv4.....	180
	IPv6.....	193
	DHCP Server Screening.....	199
	DHCP Server Screening Global Settings	199
	DHCP Server Screening Port Settings.....	200
	ARP Spoofing Prevention	201
	Network Access Authentication	202
	Guest VLAN.....	202
	Network Access Authentication Global Settings	202
	Network Access Authentication Port Settings	203
	Network Access Authentication Sessions Information	204
	Safeguard Engine	205
	Safeguard Engine Settings.....	206
	CPU Protect Counters.....	207
	CPU Protect Sub-Interface	207
	CPU Protect Type.....	208
	Trusted Host	209
	Traffic Segmentation Settings.....	209
	Storm Control Settings.....	210
	DoS Attack Prevention Settings	212
	SSH.....	213
	SSH Global Settings.....	214
	Host Key	215
	SSH Server Connection	216
	SSH User Settings.....	216
	SSL	217
	SSL Global Settings	218
	Crypto PKI Trustpoint	218
	SSL Service Policy	220
	Network Protocol Port Protect Settings	221
10.	OAM	222

Cable Diagnostics.....	222
11. Monitoring	224
Utilization	224
Port Utilization	224
Statistics.....	225
Port	225
Interface Counters	226
Counters	228
Mirror Settings	229
Device Environment.....	231
12. Green.....	232
Power Saving.....	232
EEE.....	233
13. Toolbar	235
Save.....	235
Save Configuration	235
Tools	235
Firmware Upgrade & Backup	235
Configuration Restore & Backup	237
Certificate & Key Restore & Backup.....	240
Log Backup.....	242
Ping.....	243
Language Management.....	244
Reset	245
Reboot System	245
Wizard.....	246
Online Help	246
D-Link Support Site	246
User Guide	246
Surveillance Mode	246
Logout.....	247
14. Surveillance Mode	248
Surveillance Overview	248
Surveillance Topology	248
Device Information.....	250
Port Information	251
Group Details.....	252
IP-Camera Information	253
NVR Information	254
Management.....	255
File System	255
Time.....	256
Clock Settings.....	256
SNTP Settings	257
Surveillance Settings	258
Surveillance Log	259
Health Diagnostic.....	260
Toolbar.....	261
Wizard.....	261
Tools.....	261
Save.....	265

Help	265
Online Help	266
Standard Mode	266
Appendix A - System Log Entries	267
Appendix B - Trap Entries	283
Appendix C - RADIUS Attributes Assignment	289
Appendix D - IETF RADIUS Attributes Support	290

1. Introduction

Audience

The *Web UI Reference Guide* is intended for network administrators and other IT networking professionals responsible for managing the Switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the switches in the DXS-1210 Series, which will be generally be referred to simply as the 'Switch' within this manual. This manual is written in a way that assumes readers already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks (LANs).

Other Documentation

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

- *DXS-1210 Series Hardware Installation Guide*
- *DXS-1210 Series CLI Reference Guide*

Typographical 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 . Used to represent filenames, program names, and commands. For example, use the copy command.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example, Click Enter.
Menu Name > Menu Option	Indicates the menu structure. Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.
Blue Courier Font	Used to represent an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes and Cautions



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



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

2. Web User Interface (Web UI)

Connecting to the Web UI
Logging into the Web UI
Web Interface Navigation

The Web UI provides access to most of the software features available on the Switch. These features can be enabled, configured, disabled, or monitored using any standard web browser, like Microsoft's Internet Explorer, Mozilla Firefox, Google Chrome, or Safari. The MGMT port offers an Out-Of-Band (OOB) connection to the Web UI and the LAN ports offers an in-band connection to the Web UI using HTTP or HTTPS (SSL).

Connecting to the Web UI

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



Figure 2-1 IP address in Internet Explorer



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

Logging into the Web UI

In the authentication window, enter the **User Name** and **Password** and click the **Login** button to access the Web UI.

A screenshot of the Web UI login window. The title is "Connect to 10.90.90.90". There is a key icon. The "User Name" field contains "admin". The "Password" field is masked with dots. The "Language" dropdown menu is set to "English". There are "Login" and "Reset" buttons at the bottom.

Figure 2-2 Web UI Login Window



NOTE: For security reasons, it is highly recommended to configure a personal username and password for this Switch.



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

Smart Wizard

After successfully connecting to the Web UI for the first time, the **Smart Wizard** embedded Web utility will be launched. This wizard will guide the user through basic configuration steps that is essential for first time connection to the Switch.

Step 1 - Web Mode

The Switch supports two Web Modes:

- **Standard Mode:** Used to configure, manage, and monitor most of the software features on the Switch.
- **Surveillance Mode:** Used to configure, manage, and monitor surveillance features supported by the Switch.



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

Welcome to Smart Wizard

The wizard will guide you to do basic configurations on 4 steps for the Web Mode, IP Information, User Account and SNMP. If you are not changing the settings, click on "Exit" to go back to the main page.

Step 1 of 4: Choose the web interface mode.

Web Mode

Standard Mode Surveillance Mode

Ignore the wizard next time

Figure 2-3 Web Mode

The fields that can be configured are described below:

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

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

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

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

Step 2 - System IP Information

In this step, we can configure System IP Information.



NOTE: The Switch will probe for surveillance devices every 30 seconds. If a surveillance device is not in the same subnet as the switch, it will not be discovered automatically. Place the Switch management IP in the same subnet as the surveillance devices for ONVIF cameras to be added to the Surveillance Mode Web UI automatically.

Welcome to Smart Wizard

Step 2 of 4: The wizard will help to complete settings for System IP address, Netmask, and Gateway.

System IP Information

Static DHCP

IP Address: 10 - 90 - 90 - 90

Netmask: 8 (255.0.0.0) ▼

Gateway: 0 - 0 - 0 - 0

Ignore the wizard next time Exit Back Next

Figure 2-4 System IP Information Window

The fields that can be configured are described below:

Parameter	Description
Static	Select this option to manually assign and configure the IPv4 address settings for the Switch. After selecting this option, the following parameters can be configured: <ul style="list-style-type: none"> • IP Address - Enter the IPv4 address of the Switch here. • Netmask - Select the IPv4 subnet mask here. • Gateway - Enter the IPv4 address of the default gateway here.
DHCP	Select this option to obtain IPv4 address settings automatically from a DHCP server for the Switch.

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

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

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

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

Step 3 - User Accounts Settings

In this step, we can configure the user account settings.

The screenshot shows a web interface titled "Welcome to Smart Wizard" with a sub-header "Step 3 of 4: Configure User Account for management." The main content area is titled "User Accounts Settings" and contains three configuration fields: "User Name" with a dropdown menu set to "admin", "Password Type" with a dropdown menu set to "None", and "Password" with an empty text input field. At the bottom of the form, there is a checkbox labeled "Ignore the wizard next time" which is currently unchecked, and three buttons: "Exit", "Back", and "Next".

Figure 2-5 User Account Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user name here. This is normally an administrator-level account.
Password Type	Select the password type here. Options to choose from are: <ul style="list-style-type: none"> • None - Specifies that no password will be configured for this user account. • Plain Text - Specifies that the password for this user account will be in the plain text form.
Password	Enter the password for the user account here.

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

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

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

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

Step 4 - SNMP Settings

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

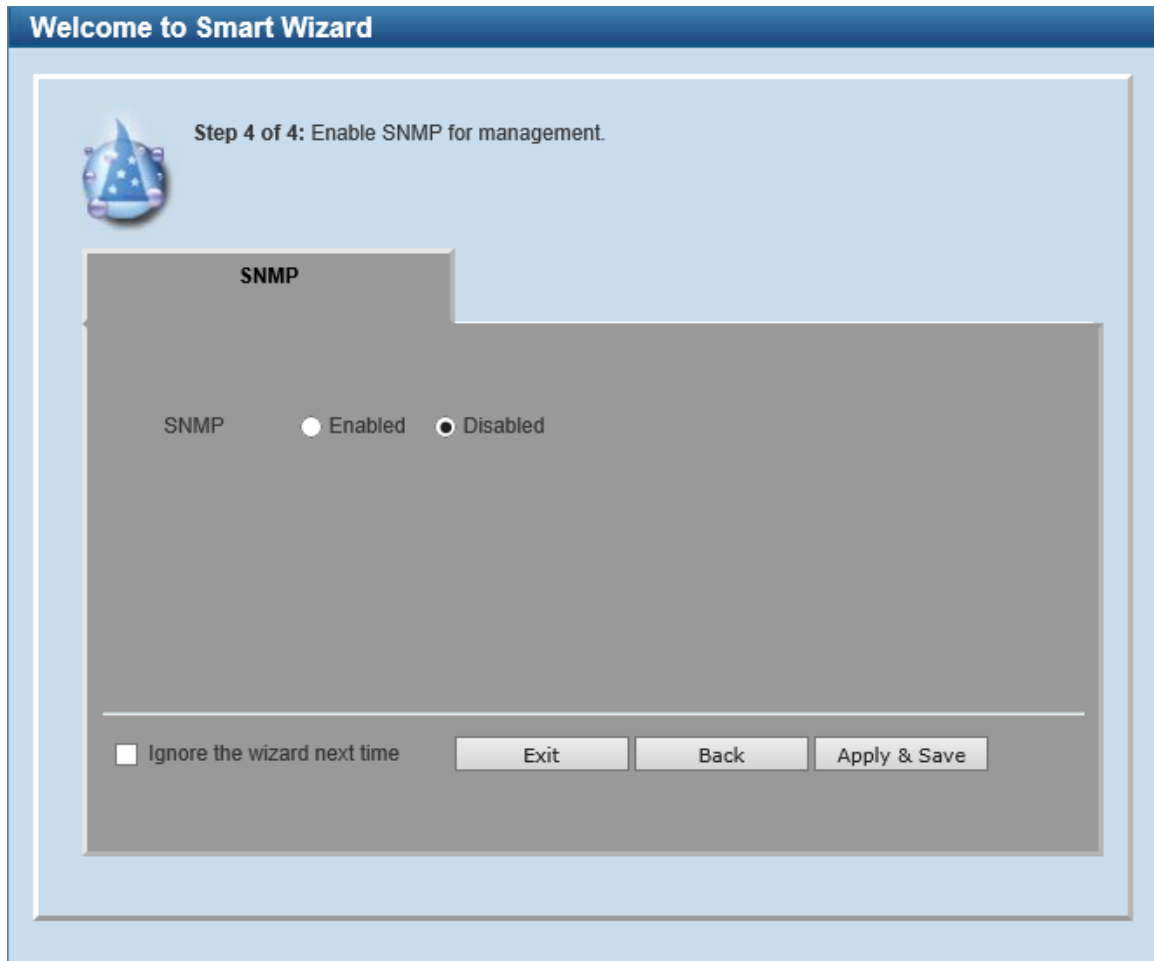


Figure 2-6 SNMP Window

The fields that can be configured are described below:

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

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

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

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

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

Web Interface Navigation

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



Figure 2-7 Web User Interface Areas (Standard Mode)

In the following table, the areas in the Web UI are described:

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



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

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

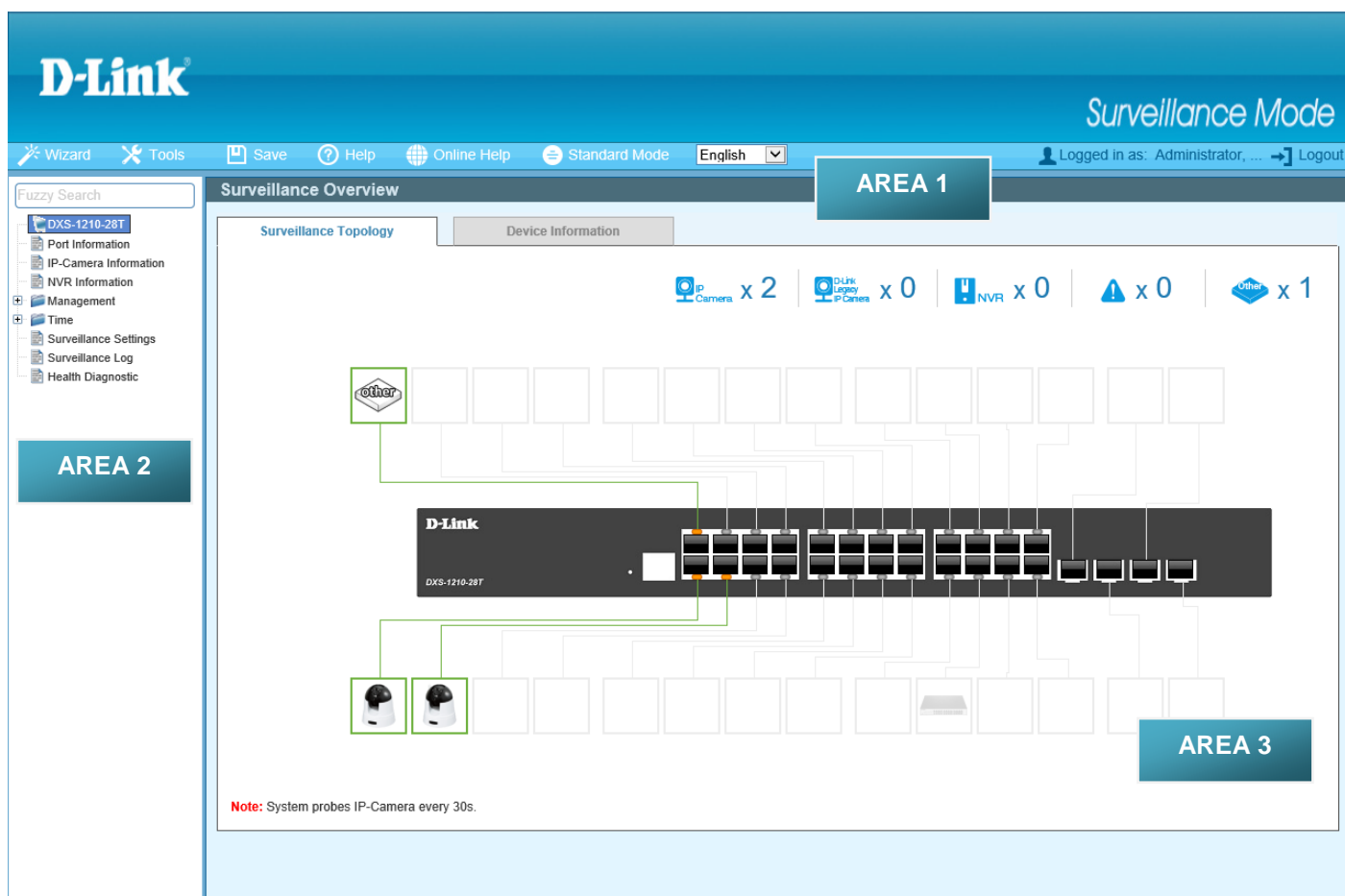


Figure 2-8 Web User Interface Areas (Surveillance Mode)

In the following table, the areas in the Web UI are described:

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

3. System

[Device Information](#)
[System Information Settings](#)
[Peripheral Settings](#)
[Port Configuration](#)
[Interface Description](#)
[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 **DXS-1210-28T** link.

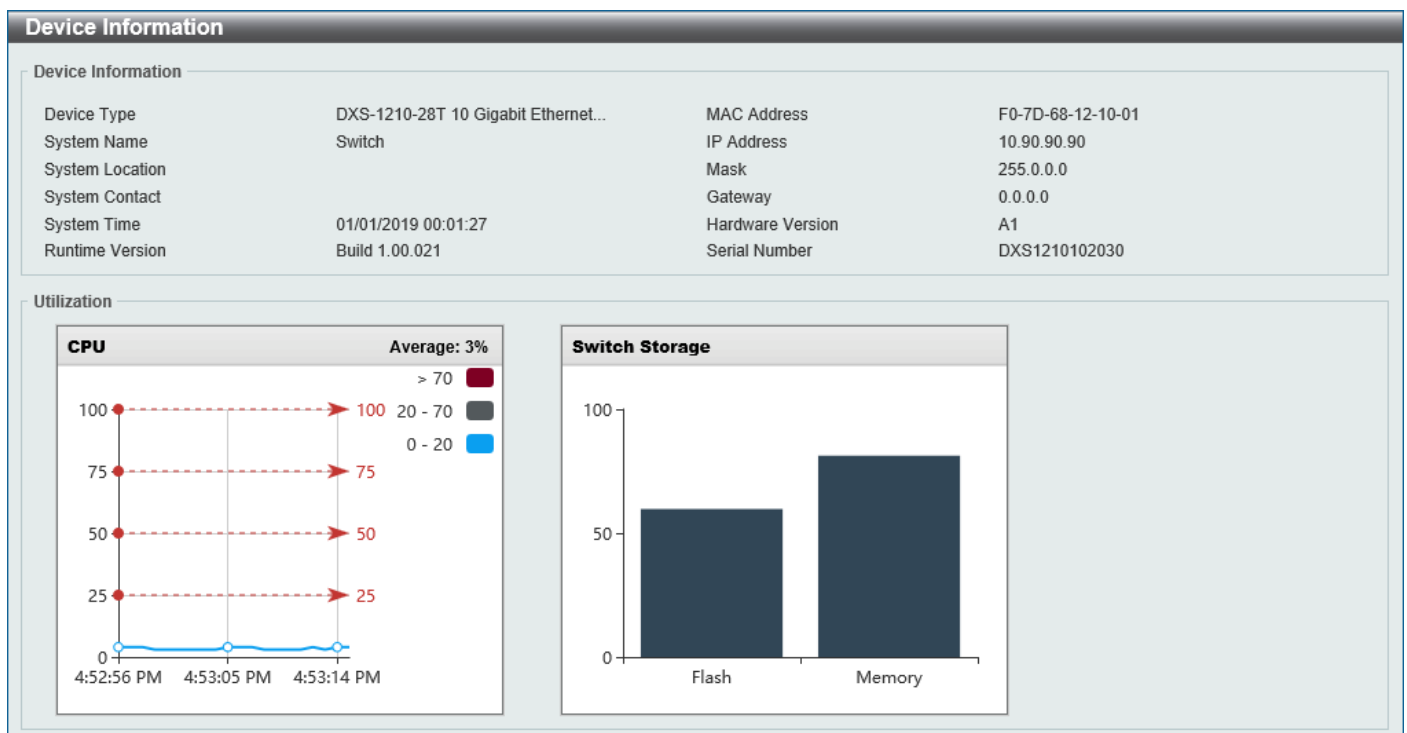


Figure 3-1 Device Information Window

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:

The screenshot displays the 'System Information Settings' window. It contains three input fields for configuration:

- System Name:
- System Location:
- System Contact:

An 'Apply' button is located at the bottom right of the form.

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.

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
High Threshold	Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. By default, this value is 79. Select the Default option to use the default value.
Low Threshold	Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. By default, this value is 11. Select the Default option to use the default value.

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

Port Configuration

Port Settings

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

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

Port Settings

Port Settings

From Port: eth1/0/1 To Port: eth1/0/1 State: Enabled MDIX: Auto Flow Control: Off

Duplex: Auto Speed: Auto Capability Advertised: 100M 1000M 10G Description: 64 chars **Apply**

Note: Port 25-28 speed must be consistent, both set to 10G or 25G.

Port	Link Status	State	MDIX	Flow Control		Duplex	Speed	Description
				Send	Receive			
eth1/0/1	Up	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/2	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/3	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/4	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/5	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/6	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/7	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/8	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
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 (DXS-1210-28T) Window

Port Settings

Port Settings

From Port: eth1/0/1 To Port: eth1/0/1 State: Enabled MDIX: Auto Flow Control: Off

Duplex: Auto Speed: Auto Capability Advertised: 100M 1000M 10G Description: 64 chars **Apply**

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	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/3	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/4	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/5	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/6	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/7	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/8	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
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 3-5 Port Settings (DXS-1210-28S) Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the physical port state here.

Parameter	Description
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are: <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 crossover cable. • Cross - Select this option for crossover cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another Switch through a straight cable.
Flow Control	Select to turn flow control On or Off here. Ports configured for full-duplex use 802.3x flow control and Auto ports use an automatic selection of the two.
Duplex	Select the duplex mode used here. Options to choose from are Auto and Full .
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to connect at the specified speed only. Options to choose from are: <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. • 100M - Specifies to force the port speed to 100 Mbps. This option is only available for 100 Mbps copper connections. • 1000M - Specifies to force the port speed to 1 Gbps. • 10G - Specifies to force the port speed to 10 Gbps. • 25G - Specifies to force the port speed to 25 Gbps. <p>Note: On the DXS-1210-28T, ports 25 to 28 must operate at the same speed.</p>
Capability Advertised	When the Speed is set to Auto , these capabilities are advertised during auto-negotiation.
Description	Select the checkbox and enter the description for the corresponding port here. This can be up to 64 characters long.

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

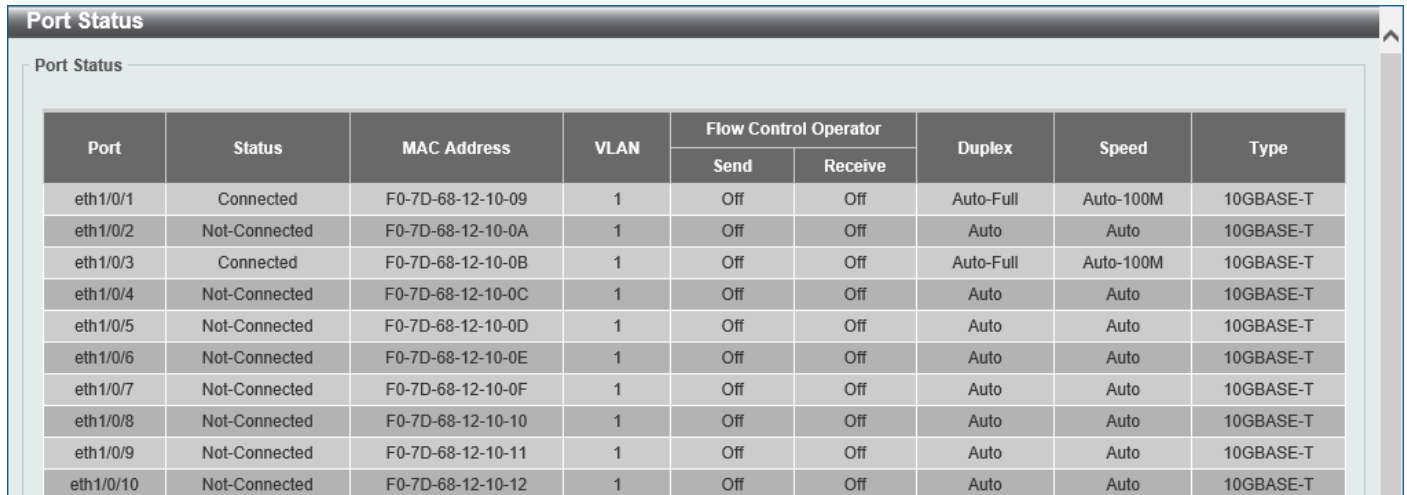


NOTE: The FEC function is not supported on the 25 Gbps SFP28 ports. If the 25 Gbps SFP28 connection between this switch and another non-DXS-1210 series switch is not working, the FEC function needs to be disabled on the remote switch.

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:



The screenshot shows the 'Port Status' window with a table listing 10 ports (eth1/0/1 to eth1/0/10). The table columns are Port, Status, MAC Address, VLAN, Flow Control Operator (Send, Receive), Duplex, Speed, and Type. Ports eth1/0/1, eth1/0/3, and eth1/0/4 are connected, while the others are not.

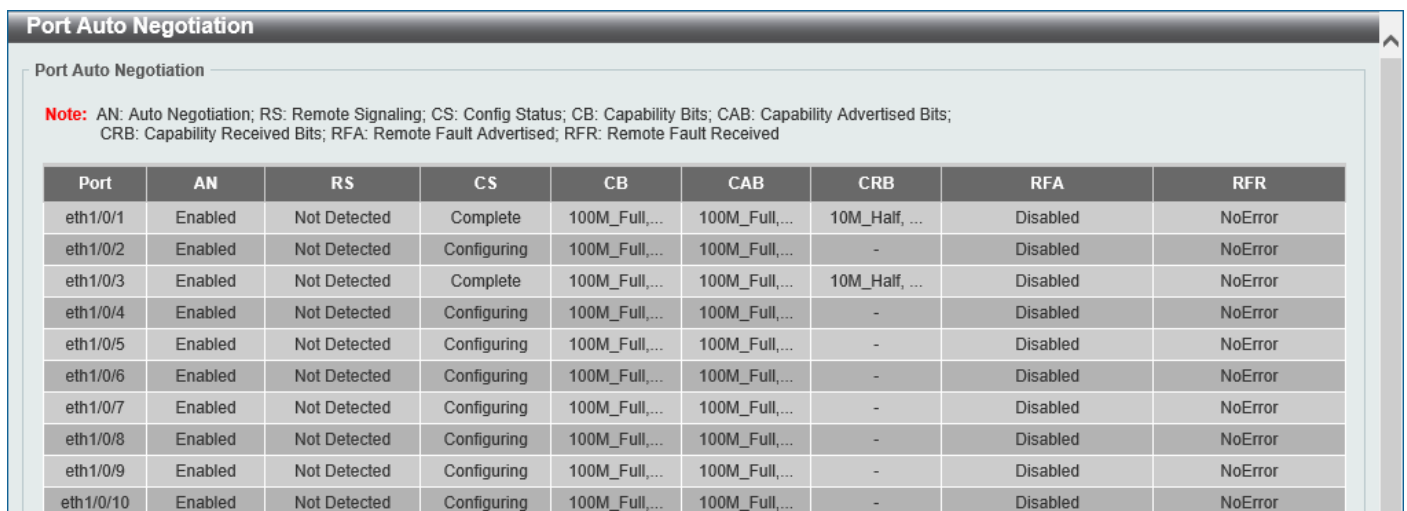
Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	F0-7D-68-12-10-09	1	Off	Off	Auto-Full	Auto-100M	10GBASE-T
eth1/0/2	Not-Connected	F0-7D-68-12-10-0A	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/3	Connected	F0-7D-68-12-10-0B	1	Off	Off	Auto-Full	Auto-100M	10GBASE-T
eth1/0/4	Not-Connected	F0-7D-68-12-10-0C	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/5	Not-Connected	F0-7D-68-12-10-0D	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/6	Not-Connected	F0-7D-68-12-10-0E	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/7	Not-Connected	F0-7D-68-12-10-0F	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/8	Not-Connected	F0-7D-68-12-10-10	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/9	Not-Connected	F0-7D-68-12-10-11	1	Off	Off	Auto	Auto	10GBASE-T
eth1/0/10	Not-Connected	F0-7D-68-12-10-12	1	Off	Off	Auto	Auto	10GBASE-T

Figure 3-6 Port Status Window

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:



The screenshot shows the 'Port Auto Negotiation' window. It includes a note defining abbreviations: 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. Below the note is a table with 9 columns: Port, AN, RS, CS, CB, CAB, CRB, RFA, and RFR. The table lists 10 ports (eth1/0/1 to eth1/0/10) with their respective auto-negotiation settings.

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

Figure 3-7 Port Auto Negotiation Window

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:

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. By default, this value is 0 and 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 , Dynamic ARP Inspection , DHCP Snooping , and Loopback Detect .
State	Select to enable or disable the error disabled recovery feature here.
Interval	Enter the interval time for the error-disabled state here. The range is from 5 to 86400 seconds. By default, this value is 300 seconds.

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

Jumbo Frame

This window is used to display and configure the jumbo frame size and settings.

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

Jumbo Frame

Jumbo Frame

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

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

Figure 3-9 Jumbo Frame Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the port range for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. The range is from 64 and 12288 bytes. By default, this value is 1536 bytes.

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

Interface Description

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

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

Interface Description

Interface Description

Total Entries: 30

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

1/3 |< < 1 2 3 > >| Go

Figure 3-10 Interface Description Window

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

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:

The screenshot shows the 'System Log Settings' window with the following configuration:

- Log State:** Enabled (dropdown), Apply button.
- Buffer Log Settings:**
 - Buffer Log State: Enabled (dropdown)
 - Severity: 4(Warnings) (dropdown)
 - Discriminator Name: 15 chars (text input)
 - Write Delay (0-65535): 300 (text input) sec Infinite
 - Apply button.
- Console Log Settings:**
 - Console Log State: Disabled (dropdown)
 - Severity: 4(Warnings) (dropdown)
 - Discriminator Name: 15 chars (text input)
 - Apply button.

Figure 3-11 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 **Buffer Log Settings** are described below:

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

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

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

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

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

System Log Discriminator Settings

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

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

System Log Discriminator Settings

Discriminator Log Settings

Discriminator Name: 15 chars

Action: Drops

Severity: Drops

Apply

Total Entries: 1

Name	Action	Facility List	Severity	Severity List	
Name	Drops	SSH	Drops	1	Delete

Figure 3-12 System Log Discriminator Settings Window

The fields that can be configured for **Discriminator Log Settings** 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

Total Entries: 1

Server IP	Severity	Facility	Discriminator Name	UDP Port
10.90.90.1	Warnings	23	Name	514

Figure 3-13 System Log Server Settings Window

The fields that can be configured are described below:

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

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

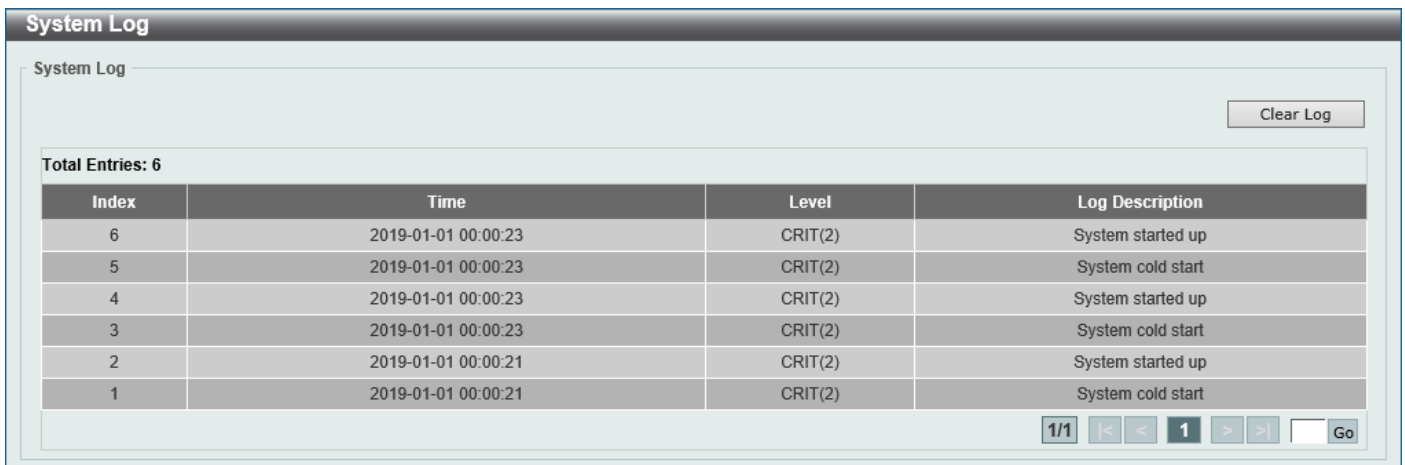
Click the **Apply** button to accept the changes made.

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

System Log

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

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



The screenshot shows the 'System Log' window with a 'Clear Log' button in the top right. Below the button, it indicates 'Total Entries: 6'. A table displays the log entries with columns for Index, Time, Level, and Log Description. At the bottom right, there are navigation controls including a page indicator '1/1', left and right arrows, a page number '1', and a 'Go' button.

Index	Time	Level	Log Description
6	2019-01-01 00:00:23	CRIT(2)	System started up
5	2019-01-01 00:00:23	CRIT(2)	System cold start
4	2019-01-01 00:00:23	CRIT(2)	System started up
3	2019-01-01 00:00:23	CRIT(2)	System cold start
2	2019-01-01 00:00:21	CRIT(2)	System started up
1	2019-01-01 00:00:21	CRIT(2)	System cold start

Figure 3-14 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:

Index	Time	Level	Log Description
Total Entries: 0			

Figure 3-15 System Attack Log Window

Time and SNTP

Clock Settings

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

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

Figure 3-16 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:

Figure 3-17 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: <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 weekday of the specified month. • Date Setting - Select to configure the summer time that should start and end on the specified date of the specified month.
Time Zone	Select to specify 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 range of this offset is 30, 60, 90, and 120. By default, this value is 60.

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

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

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

SNTP Settings

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

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

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

Figure 3-18 SNTP Settings Window

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

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

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

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

Parameter	Description
IPv4 Address	Select and enter the IPv4 address of the SNTP server here.
IPv6 Address	Select and enter the IPv6 address of the SNTP server here.

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 3-19 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

User Accounts Settings

SNMP

RMON

Telnet/Web

Session Timeout

DHCP

DHCP Auto Configuration

DHCP Auto Image Settings

DNS

File System

D-Link Discovery Protocol

User Accounts Settings

On this page, user accounts can be created and updated. Active user account sessions can also be viewed on this page. There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**.

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

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

Figure 4-1 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.
Password Type	Select the password type for this user account here. Options to choose from are None and Plain Text .
Password	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.

ID	Type	User Name	Login Time	IP Address
0	console	admin	51M38S	
19	* web	admin	5M6S	10.90.90.10

Figure 4-2 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.

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 4-3 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. The range is from 1 to 65535. By default, this value is 161.

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.

Parameter	Description
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.
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
eth1/0/8	Enabled	Enabled
eth1/0/9	Enabled	Enabled
eth1/0/10	Enabled	Enabled

Figure 4-4 SNMP Linkchange Trap Settings Window

The fields that can be configured are described below:

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

Total Entries: 8

View Name	Subtree OID	View Type	
restricted	1.3.6.1.2.1.1	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.2.1.11	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.6.3.10.2.1	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.6.3.11.2.1	Included	<input type="button" value="Delete"/>
restricted	1.3.6.1.6.3.15.1.1	Included	<input type="button" value="Delete"/>
CommunityView	1	Included	<input type="button" value="Delete"/>
CommunityView	1.3.6.1.6.3	Excluded	<input type="button" value="Delete"/>
CommunityView	1.3.6.1.6.3.1	Included	<input type="button" value="Delete"/>

Figure 4-5 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: <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:

SNMP Community Table Settings

SNMP Community Settings

Key Type: Plain Text

Community Name: 32 chars

View Name: 32 chars

Access Right: Read Only

IP Access-List Name: 32 chars

Add

Total Entries: 2

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

Figure 4-6 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Key Type	Specifies that the key type for the SNMP community is Plain Text .
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: <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:

The screenshot shows the 'SNMP Group Table Settings' window. The 'SNMP Group Settings' section includes the following fields:

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

There is an 'Add' button and a note '* Mandatory Field'. Below the settings is a table with 5 entries:

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

Figure 4-7 SNMP Group Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the SNMP group name here. This name can be up to 32 characters long. Spaces are not allowed.
Read View Name	Enter the read view name that users of the group can access.
User-based Security Model	Select the security model here. Options to choose from are: <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	When selecting SNMPv3 in the User-based Security Model drop-down list, this option is available. <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 manager will be encrypted.
Notify View Name	Enter the notify view name that users of the group can access. The notify view describes the object that can be reported its status via trap packets to the group user.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the group.

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

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

SNMP Engine ID Local Settings

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

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

Figure 4-8 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:

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

Figure 4-9 SNMP User Table Settings Window

The fields that can be configured are described below:

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

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

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

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

SNMP Host Table Settings

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

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

SNMP Host Table Settings

SNMP Host Settings

Host IPv4 Address

Host IPv6 Address

User-based Security Model: SNMPv1

Security Level: NoAuthNoPriv

UDP Port (1-65535): 162

Community String / SNMPv3 User Name: 32 chars

Add

Total Entries: 1

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

Delete

Figure 4-10 SNMP Host Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	Select the security model here. Options to choose from are: <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	When selecting SNMPv3 in the User-based Security Model drop-down list, this option is available. <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 manager will be encrypted.
UDP Port	Enter the UDP port number. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols. By default, this value is 162.
Community String / SNMPv3 User Name	Enter the community string or SNMPv3 user name to be sent with the notification packet.

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

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

RMON

RMON Global Settings

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

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

Figure 4-11 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 4-12 RMON Statistics Settings Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the physical port number here.
Index	Enter the RMON table index. The value is from 1 to 65535.
Owner	Enter the owner string. The string can be up to 127 characters.

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

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

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

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

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

RMON Statistics Table																		
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	eth1/0/10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4-13 RMON Statistics Settings (Show Detail) Window

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

RMON History Settings

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

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

RMON History Settings						
RMON History Settings						
Port *	Index (1-65535) *	Bucket Number (1-65535)	Interval (1-3600)	sec	Owner	
eth1/0/1	<input type="text"/>	50	1800		127 chars	<input type="button" value="Add"/>
Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	
1	eth1/0/10	50	50	1800	Owner	<input type="button" value="Delete"/> <input type="button" value="Show Detail"/>
<input type="text" value="1/1"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value="Go"/>						

Figure 4-14 RMON History Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

RMON History Table													
RMON History Table													
Index	Sample	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Utilization	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event
<input type="button" value="Back"/>													

Figure 4-15 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) *	<input type="text"/>	Interval (1-2147483647) *	<input type="text"/>	sec							
Variable *	<input type="text" value="N.N.N..N"/>	Type	Absolute		<input type="button" value="v"/>						
Rising Threshold (0-2147483647) *	<input type="text"/>	Falling Threshold (0-2147483647) *	<input type="text"/>								
Rising Event Number (1-65535)	<input type="text"/>	Falling Event Number (1-65535)	<input type="text"/>								
Owner	<input type="text" value="1-127 chars"/>										
<input type="button" value="Add"/>											
Total Entries: 0											
Index	Interval (sec)	Variable	Type	Last Value	Rising Threshold	Falling Threshold	Rising Event No.	Falling Event No.	Startup Alarm	Owner	

Figure 4-16 RMON Alarm Settings Window

The fields that can be configured are described below:

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

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

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

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

RMON Event Settings

This window is used to display and configure event entries.

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

RMON Event Settings

RMON Event Settings

Index (1-65535) *

Description 1-127 chars

Type None

Community 1-127 chars

Owner 1-127 chars

Add

Total Entries: 1

Index	Description	Community	Event Trigger	Owner	Last Trigger Time
1	event				0d:0h:0m:0s

Delete View Logs

1/1 < < 1 > > Go

Figure 4-17 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
-----------	----------	-----------------

Back

Figure 4-18 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 4-19 Telnet/Web Window

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

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

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

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

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

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

Session Timeout

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

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

Figure 4-20 Session Timeout Window

The fields that can be configured are described below:

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

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

DHCP

Service DHCP

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

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

Figure 4-21 Service DHCP Window

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

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

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

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

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

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

DHCP Class Settings

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

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

Figure 4-22 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 4-23 DHCP Class Settings (Edit) Window

The fields that can be configured are described below:

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

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

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

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

DHCP Relay

DHCP Relay Pool Settings

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

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

Figure 4-24 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

Figure 4-25 DHCP Relay Pool Source Settings Window

The fields that can be configured are described below:

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

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

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

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

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

Figure 4-26 DHCP Relay Pool Destination Settings Window

The fields that can be configured are described below:

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

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

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

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

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

Figure 4-27 DHCP Relay Pool Class Settings Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

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

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

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

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

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

DHCP Relay Pool Class Edit Settings

DHCP Relay Pool Class Edit Settings

Pool Name Pool
Class Name Class
Relay Target

Apply

Total Entries: 1

Target Address
10.90.90.150

Delete Back

Figure 4-28 DHCP Relay Pool Class Edit Settings Window

The fields that can be configured are described below:

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

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

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

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

DHCP Relay Information Settings

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

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

DHCP Relay Information Settings

DHCP Relay Information Global

Information Trust All Information Check
Information Policy Information Option

Apply

DHCP Relay Information

Total Entries: 1

Interface	Trusted	Check Relay	Policy Action	Option Insert
vian1	Disabled	Not Configured	Not Configured	Not Configured

Edit

1/1 < < 1 > > Go

Figure 4-29 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. By default, this is disabled.
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. By default, this is disabled.
Information Policy	Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are:

Parameter	Description
	<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. <p>By default, this is Replace.</p>
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets. By default, this is disabled.

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 4-30 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	<p>Select the DHCP information remote ID sub-option. Options to choose from are:</p> <ul style="list-style-type: none"> • Default - Select to use the Switch's system MAC address as the remote ID. • User Define - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box. • Vendor2 - Select to use vendor 2 as the remote ID. • Vendor3 - Select to use vendor 3 as the remote ID. <p>By default, this is Default.</p>

Parameter	Description
Information Format Circuit ID	<p>Select the DHCP information circuit ID sub-option. Options to choose from are:</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. • Vendor2 - Select to use vendor 2 as the circuit ID. • Vendor3 - Select to use vendor 3 as the circuit ID. • Vendor4 - Select to use vendor 4 as the circuit ID. • Vendor5 - Select to use vendor 5 as the circuit ID. • Vendor6 - Select to use vendor 6 as the circuit ID. <p>By default, this is Default.</p>

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
From Port - To Port	Select the range of ports that will be used for this configuration here.
Format	Specifies that the user-defined Vendor 3 string 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 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 4-31 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.

DHCPv6 Relay

DHCPv6 Relay Global Settings

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

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

Figure 4-32 DHCPv6 Relay Global Settings Window

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

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are Default , CID with User Define , User Define , and Expert UDF .
Standalone Unit Format	After selecting the Expert UDF option, select the standalone unit format here. Options to choose from are 0 and 1 .
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for the remote ID. Options to choose from are: <ul style="list-style-type: none"> None - Specifies to keep the UDF empty for the remote ID. ASCII - Select to enter the ASCII string with a maximum of 128 characters in the text box. HEX - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are: <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.
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 Information Option MAC Format** are described below:

Parameter	Description
Case	Select the case that will be used here. Options to choose from are:

Parameter	Description
	<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, AABCCDDEEFF.
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, AABCC.DDEEFF. • 2 - Specifies to use two delimiters. For example, AAB.CCDD.EEFF • 5 - Specifies to use multiple delimiters. For example, AA.BB.CC.DD.EE.FF

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

DHCPv6 Relay Interface Settings

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

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

DHCPv6 Relay Interface Settings

DHCPv6 Relay Interface Settings

Interface VLAN (1-4094)

Destination IPv6 Address

Output Interface VLAN (1-4094) Apply

Interface VLAN (1-4094) Find

Total Entries: 1

Interface	Destination IPv6 Address	Output Interface	
vlan2	2020::100	vlan2	Delete

1/1 < < **1** > > Go

Figure 4-33 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.

Parameter	Description
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 4-34 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 Expert UDF format type string for DHCPv6 Option 37 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. By default, this option is used. ○ 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

Parameter	Description
	<p>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. ➤ 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 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:

Port	Remote ID Format Type Expert UDF
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	
eth1/0/9	
eth1/0/10	

Figure 4-35 DHCPv6 Relay Format Type Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Type	Select the type here. The only option available is: <ul style="list-style-type: none"> Remote ID - Specifies to configure the Expert UDF format type string for DHCPv6 Option 37.
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 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 4-36 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 4-37 DHCP Auto Configuration Window

The fields that can be configured are described below:

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

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

DHCP Auto Image Settings

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

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

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

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

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

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

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

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

Figure 4-38 DHCP Auto Image Settings Window

The fields that can be configured are described below:

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

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

DNS

The Domain Name System (DNS) is used to map human-readable domain names to the IP addresses used by computers to communicate. A DNS server performs name-to-address translation, and may need to contact several name servers to translate a domain to an address. The address of the machine that supplies domain name service is

often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Global Settings

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

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

Figure 4-39 DNS Global Settings Window

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

Parameter	Description
IP Domain Lookup	Select to enable or disable the IP domain lookup state here.
IP Name Server Timeout	Enter the maximum time to wait for a response from a specified name server. The range is from 1 to 60 seconds.

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 4-40 DNS Name Server Settings Window

The fields that can be configured are described below:

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

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

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

DNS Host Settings

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

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

Figure 4-41 DNS Host Settings Window

The fields that can be configured are described below:

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

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

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

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

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

File System

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

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

Figure 4-42 File System Window

The fields that can be configured are described below:

Parameter	Description
Path	Enter the path string.

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

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

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

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

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

Index	Attr	Size (byte)	Update Time	Name	Delete
1	-rw	15774240	Feb 06 2085 12:10:42	Image1	Delete
2	-rw	15065632	Feb 06 2085 06:32:29	Image2	Delete
3	-rw	1502	Feb 26 2086 09:36:29	Config1	Delete
4	d--	0	Feb 26 2086 09:36:29	system	Delete

Figure 4-43 File System (Drive) Window

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.

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

Figure 4-44 File System (Copy) Window

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

Parameter	Description
Source	Select the source file to copy here. Options to choose from are: <ul style="list-style-type: none"> startup-config - Specifies to copy the start-up configuration to the destination. Image 1 - Specifies to copy firmware image 1 to the destination. Image 2 - Specifies to copy firmware image 2 to the destination.

Parameter	Description
	<ul style="list-style-type: none"> • Configuration 1 - Specifies to copy configuration 1 to the destination. • Configuration 2 - Specifies to copy configuration 2 to the destination.
Destination	Select the destination for the copy here. Options to choose from are: <ul style="list-style-type: none"> • running-config - Specifies to copy the source file to the running configuration. • startup-config - Specifies to copy the source file to the start-up configuration. • Image 1 - Specifies to copy the source file to firmware image 1. • Image 2 - Specifies to copy the source file to firmware image 2. • Configuration 1 - Specifies to copy the source file to configuration 1. • Configuration 2 - Specifies to copy the source file to configuration 2.
Replace	Select this option to replace the destination file with the source file.

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

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

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

Figure 4-45 File System (Boot File) Window

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

Parameter	Description
Boot Image	Select the boot image here. Options to choose from are: <ul style="list-style-type: none"> • Image 1 - Specifies to use firmware image 1 as the boot image. • Image 2 - Specifies to use firmware image 2 as the boot image.
Boot Configuration	Select the boot configuration here. Options to choose from are: <ul style="list-style-type: none"> • Configuration 1 - Specifies to use configuration 1 as the boot configuration. • Configuration 2 - Specifies to use configuration 2 as the boot configuration.

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

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

D-Link Discovery Protocol

DDP Settings

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

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

DDP Global Settings	
DDP Version	5
D-Link Discovery Protocol State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Report Timer	Never sec
Apply	
DDP Port Settings	
From Port	eth1/0/1
To Port	eth1/0/1
State	Disabled
Apply	
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 4-46 DDP Settings Window

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

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

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

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

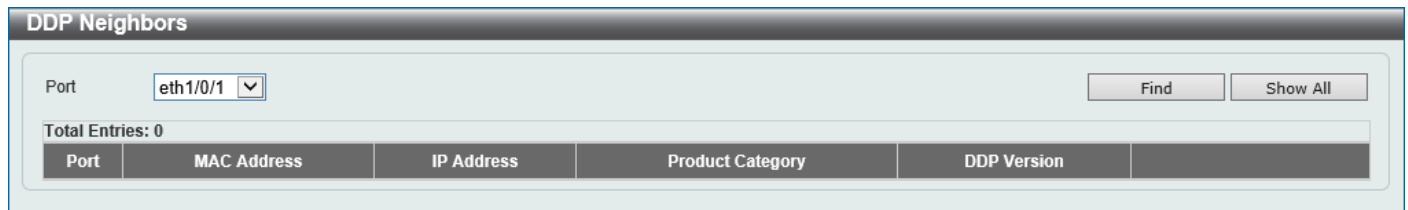
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DDP feature on the specified port(s) here.

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

DDP Neighbors

This window is used to display the DDP neighbors.

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



The screenshot shows the 'DDP Neighbors' window. At the top, there is a 'Port' dropdown menu with 'eth1/0/1' selected. To the right of the dropdown are two buttons: 'Find' and 'Show All'. Below the dropdown and buttons, it says 'Total Entries: 0'. Underneath is a table with the following columns: 'Port', 'MAC Address', 'IP Address', 'Product Category', and 'DDP Version'. The table is currently empty.

Figure 4-47 DDP Neighbors Window

The fields that can be configured are described below:

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

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

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

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

5. Layer 2 Features

FDB
VLAN
STP
Loopback Detection
Link Aggregation
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:

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 .
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.

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 5-2 MAC Address Table Settings (Global Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table aging time here. The range is from 10 to 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

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

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

Figure 5-3 MAC Address Table Settings (MAC Address Port Learning Settings) Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
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.

MAC Address Table

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

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

MAC Address Table

MAC Address Table

Port:

VID (1-4094):

MAC Address:

Clear Dynamic by Port

Clear Dynamic by VLAN

Clear Dynamic by MAC

Total Entries: 13

VID	MAC Address	Type	Port
1	00-00-5E-00-01-E8	Dynamic	eth1/0/3
1	00-23-7D-BC-2E-18	Dynamic	eth1/0/1
1	00-32-00-18-DC-01	Dynamic	eth1/0/3
1	00-40-66-91-36-11	Dynamic	eth1/0/3
1	00-40-66-C2-AA-0A	Dynamic	eth1/0/3
1	00-FF-47-77-70-B8	Dynamic	eth1/0/3
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/3
1	C4-65-16-11-17-80	Dynamic	eth1/0/3
1	D8-50-E6-C3-FB-05	Dynamic	eth1/0/3
1	D8-EB-97-D1-84-70	Dynamic	eth1/0/3

1/2 |< < 1 2 > >|

Figure 5-4 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select 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 5-5 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch
Interval	Enter the time value between notifications. The range is from 1 to 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. The range is from 0 to 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
Trap Type	Select the trap type here. Options to choose from are: <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.
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.

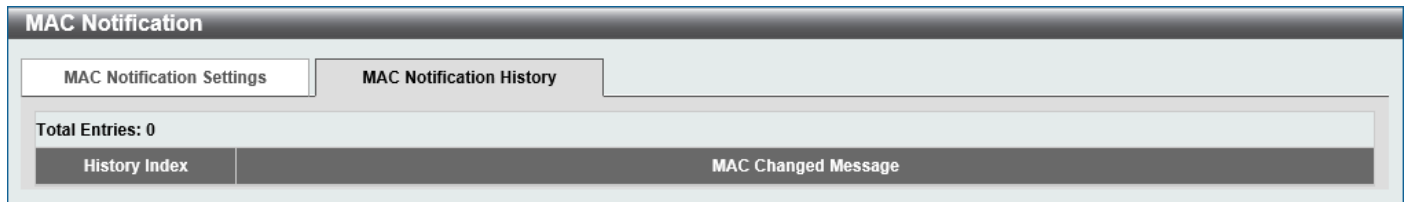


Figure 5-6 MAC Notification (MAC Notification History) Window

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

VLAN

VLAN Configuration Wizard

This window is used to start the VLAN configuration wizard.

Create/Configure VLAN

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

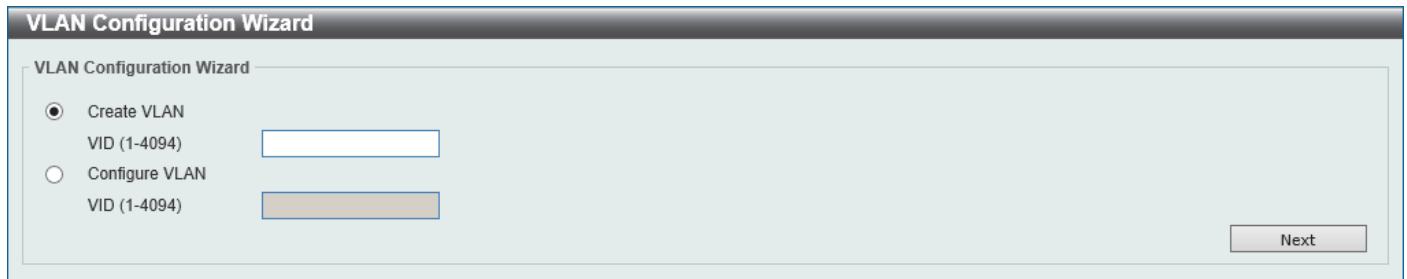


Figure 5-7 VLAN Configuration Wizard (Step 1) Window

The fields that can be configured are described below:

Parameter	Description
Create VLAN	Select this option to create a new VLAN. <ul style="list-style-type: none"> VID - Enter the VLAN ID here. The range is from 1 to 4094.
Configure VLAN	Select this option to configure an existing VLAN. <ul style="list-style-type: none"> VID - Enter the VLAN ID here. The range is from 1 to 4094.

Click the **Next** button to continue to the next step.

Create VLAN

After selecting the **Create VLAN** option and clicking the **Next** button, the following window will appear.

Figure 5-8 VLAN Configuration Wizard (Create VLAN) Window

The fields that can be configured are described below:

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

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

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

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

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

Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN
eth1/0/1	Hybrid	1	1	
eth1/0/2	Hybrid	1	1	
eth1/0/3	Hybrid	1	1	
eth1/0/4	Hybrid	1	1	
eth1/0/5	Hybrid	1	1	
eth1/0/6	Hybrid	1	1	
eth1/0/7	Hybrid	1	1	
eth1/0/8	Hybrid	1	1	
eth1/0/9	Hybrid	1	1	
eth1/0/10	Hybrid	1	1	

Figure 5-9 Allowed VLAN Window

Configure VLAN

After selecting the **Configure VLAN** option and clicking the **Next** button, the following window will appear.

VLAN Configuration Wizard

Configure VLAN

VID: 1

VLAN Name: default

Port	Select All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Untagged	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Native VLAN (PVID)	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VLAN Mode		H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	

A-Access; H-Hybrid; T-Trunk

View Allowed VLAN

Back Apply

Figure 5-10 VLAN Configuration Wizard (Configure VLAN) Window

The fields that can be configured are described below:

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

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

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

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

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

Allowed VLAN

Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN
eth1/0/1	Hybrid	1	1	
eth1/0/2	Hybrid	1	1	
eth1/0/3	Hybrid	1	1	
eth1/0/4	Hybrid	1	1	
eth1/0/5	Hybrid	1	1	
eth1/0/6	Hybrid	1	1	
eth1/0/7	Hybrid	1	1	
eth1/0/8	Hybrid	1	1	
eth1/0/9	Hybrid	1	1	
eth1/0/10	Hybrid	1	1	

Figure 5-11 Allowed VLAN Window

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:

The screenshot shows the '802.1Q VLAN' configuration window. At the top, there's a 'VID List' field containing '3 or 2-5' and 'Apply' and 'Delete' buttons. Below that is a 'Find VLAN' section with a 'VID (1-4094)' field and 'Find' and 'Show All' buttons. A table displays 'Total Entries: 2' with columns: VID, VLAN Name, Description, Tagged Member Ports, Untagged Member Ports, and VLAN Type. The table has two rows: one for VID 1 (default) and one for VID 2 (VLAN0002). Each row has 'Edit' and 'Delete' buttons. At the bottom right, there's a pagination bar showing '1/1' and a 'Go' button.

Figure 5-12 802.1Q VLAN Window

The fields that can be configured in **802.1Q VLAN** are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be created here.

Click the **Apply** button to create a new 802.1Q VLAN.

Click the **Delete** button to remove the 802.1Q VLAN specified.

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

Parameter	Description
VID	Enter the VLAN ID that will be displayed here.
VLAN Name	After clicking the Edit button, enter the name of the VLAN here.

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

Click the **Show All** button to locate all the entries.

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

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

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

VLAN Interface

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

To view the following window, click **L2 Features > VLAN > VLAN Interface** and select the **VLAN Interface Settings** tab, as shown below:

Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	Show Detail	Edit
eth1/0/1	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/2	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/3	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/4	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/5	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/6	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/7	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/8	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/9	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/10	Hybrid	Enabled	Admit-All	Show Detail	Edit

Figure 5-13 VLAN Interface Settings Window

Click the **Show Detail** button to view detailed information about the VLAN on the specific interface.

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

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

VLAN Interface Information	
Port	eth1/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	
Dynamic Tagged VLAN	
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All

Figure 5-14 VLAN Interface (VLAN Detail) Window

On this page, detailed information about the VLAN of the specific interface is displayed.

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

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

The screenshot shows the 'Configure VLAN Interface' window with the following settings:

- Port: eth1/0/1
- VLAN Mode: Access
- Acceptable Frame: Untagged Only
- Ingress Checking: Enabled
- VID (1-4094): 1
- Clone:
- From Port: eth1/0/1
- To Port: eth1/0/1

Figure 5-15 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 , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN ID	Enter the VLAN ID used for this configuration here. The range is from 1 to 4094.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the 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.

The screenshot shows the 'Configure VLAN Interface' window with the following settings:

- Port: eth1/0/1
- VLAN Mode: Hybrid
- Acceptable Frame: Admit All
- Ingress Checking: Enabled
- Native VLAN: Native VLAN
- VID (1-4094): 1
- Action: Add
- Add Mode: Untagged
- Allowed VLAN Range: [Empty]
- Current Hybrid Untagged VLAN Range: 1
- Current Hybrid Tagged VLAN Range: [Empty]
- Clone:
- From Port: eth1/0/1
- To Port: eth1/0/1

Figure 5-16 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 , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .

Parameter	Description
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. The range is from 1 to 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.

The screenshot shows the 'Configure VLAN Interface' window. The 'Port' is set to 'eth1/0/1'. The 'VLAN Mode' is set to 'Trunk'. The 'Acceptable Frame' is set to 'Admit All'. The 'Ingress Checking' is set to 'Enabled'. The 'Native VLAN' is checked. The 'Untagged' option is selected under the Native VLAN section. The 'VID (1-4094)' is set to '1'. The 'Action' is set to 'None'. The 'Allowed VLAN Range' is empty. There are also 'Clone', 'From Port', and 'To Port' options, all of which are currently empty or disabled.

Figure 5-17 VLAN Interface (Trunk) Window

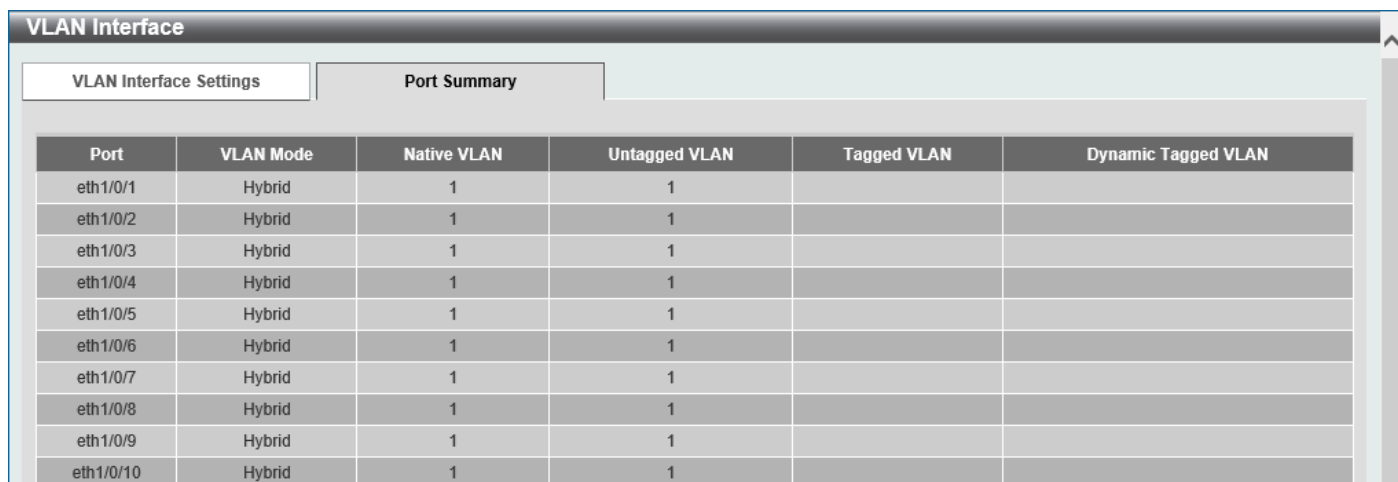
The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
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. The range is from 1 to 4094.
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.

To view the following window, select the **Port Summary** tab, as shown below:



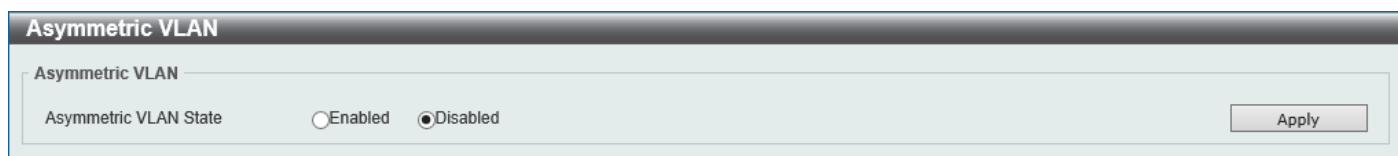
Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN	Dynamic Tagged VLAN
eth1/0/1	Hybrid	1	1		
eth1/0/2	Hybrid	1	1		
eth1/0/3	Hybrid	1	1		
eth1/0/4	Hybrid	1	1		
eth1/0/5	Hybrid	1	1		
eth1/0/6	Hybrid	1	1		
eth1/0/7	Hybrid	1	1		
eth1/0/8	Hybrid	1	1		
eth1/0/9	Hybrid	1	1		
eth1/0/10	Hybrid	1	1		

Figure 5-18 Port Summary Window

Asymmetric VLAN

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

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



Asymmetric VLAN

Asymmetric VLAN State Enabled Disabled

Figure 5-19 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.

L2VLAN Interface Description

This window is used to display and configure the Layer 2 VLAN interface description.

To view the following window, click **L2 Features > VLAN > L2VLAN Interface Description**, as shown below:

L2VLAN Interface Description

Create L2VLAN Interface Description

L2VLAN Interface:

Description:

Apply

Find L2VLAN Interface Description

L2VLAN Interface:

Find Show All

Total Entries: 2

Interface	Status	Administrative	Description	
L2VLAN 1	up	enabled		Delete Description
L2VLAN 2	down	enabled		Delete Description

1/1 < < 1 > > Go

Figure 5-20 L2VLAN Interface Description Window

The fields that can be configured are described below:

Parameter	Description
L2VLAN Interface	Enter the ID of the Layer 2 VLAN interface here.
Description	Enter the description for the Layer 2 VLAN interface here.

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

Click the **Find** button to generate the display based on the information entered.

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

Click the **Delete Description** button to remove the description from the specified Layer 2 VLAN.

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

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to display and configure the auto surveillance VLAN properties.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties**, as shown below:

Auto Surveillance Properties

Global Settings

Surveillance VLAN State Enabled Disabled

Surveillance VLAN ID (2-4094)

Surveillance VLAN CoS ▼

Aging Time (1-65535) min

ONVIF Discover Port (554, 1025-65535)

Note: Surveillance VLAN ID and Voice VLAN ID cannot be the same.

ONVIF Global Status

Surveillance Device Detected (OUI) 0

IP-Camera Detected (ONVIF) 0

NVR Detected (ONVIF) 0

Port Settings

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 5-21 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
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** and select the **User-defined MAC Settings** tab, as shown below:

MAC Settings and Surveillance Device

User-defined MAC Settings | Auto Surveillance VLAN Summary

To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.

Component Type: Description:

MAC Address: Mask:

Apply

Total Entries: 4

ID	Component Type	Description	MAC Address	Mask	
1	D-Link Device	IP Surveillance...	28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Delete
2	D-Link Device	IP Surveillance...	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Delete
3	D-Link Device	IP Surveillance...	B0-C5-54-00-00-00	FF-FF-FF-80-00-00	Delete
4	D-Link Device	IP Surveillance...	F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	Delete

Figure 5-22 MAC Settings and Surveillance Device Window

The fields that can be configured are described below:

Parameter	Description
Component Type	Select the component type here. Option to choose from are: <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.

Parameter	Description
Mask	Enter the matching bitmask for the OUI MAC address here.

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

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

To view the following window, select the **Auto Surveillance VLAN Summary** tab, as shown below:

Port	Component Type	Description	MAC Address	Start Time
Total Entries: 0				

Figure 5-23 MAC Settings and Surveillance Device (Auto Surveillance VLAN Summary) Window

ONVIF IP-Camera Information

This window is used to display ONVIF IP camera information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > ONVIF IP-Camera Information**, as shown below:

Port	IP Address	MAC Address	Model	Manufacturer	Traffic	Description	Throughput (Mbps)	More Detail	Edit
eth1/0/9	172.31.132.211	F0-7D-68-0C-CA-2B	DCS-5211L	DCS-5211L	Enabled		0	More Detail	Edit
eth1/0/11	172.31.132.210	F0-7D-68-0C-CA-CC	DCS-5222L	DCS-5222L	Enabled		0	More Detail	Edit

Note: System probes IP-Camera every 30s.

Figure 5-24 ONVIF IP-Camera Information Window

Click the IP address hyperlink to connect to the Web Interface of the IP camera.

Click the **More Detail** button to view detailed ONVIF IP camera information.

Click the **Edit** button to configure the state and description of the IP camera.

After click the **More Detail** button, the following window will appear.

Port	eth1/0/9
IP Address	172.31.132.211
MAC Address	F0-7D-68-0C-CA-2B
Model	DCS-5211L
Manufacturer	DCS-5211L
State	Enabled
Description	
Throughput	0 Mbps
Protocol	ONVIF

Back

Figure 5-25 ONVIF IP-Camera Information (More Detail) Window

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

Figure 5-26 ONVIF IP-Camera Information (Edit) Window

The fields that can be configured are described below:

Parameter	Description
IP-Camera State	Select to enable or disable the IP camera state here.
Description	Enter the description for this IP camera here.

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

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

ONVIF NVR Information

This window is used to display ONVIF Network Video Recorder (NVR) information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > ONVIF NVR Information**, as shown below:

Figure 5-27 ONVIF NVR Information Window

Click the IP address hyperlink to connect to the Web Interface of the NVR.

Click the **IP-Camera List** button to view the list of IP cameras that are connected to the NVR.

Click the **Edit** button to configure the description of the NVR.

After click the **IP-Camera List** button, the following window will appear.

Figure 5-28 ONVIF NVR Information (IP-Camera List) Window

Click the IP address hyperlink to connect to the Web Interface of the IP camera.

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

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

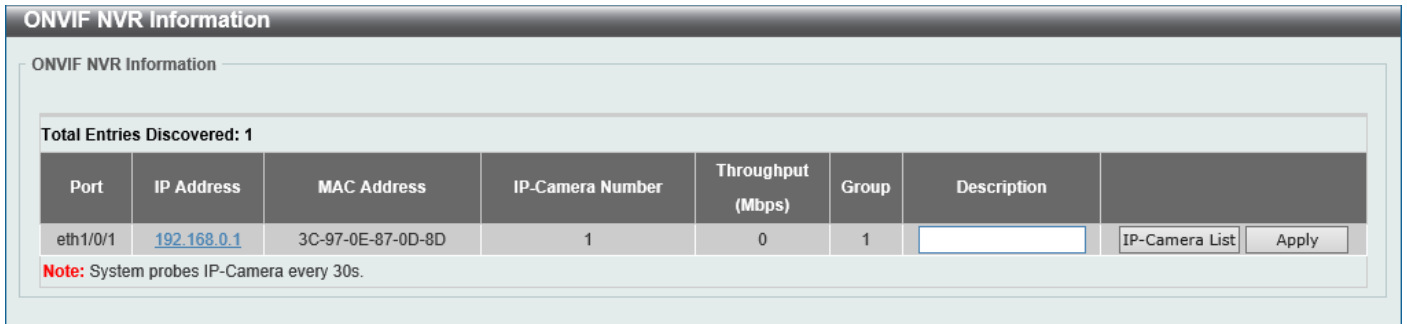


Figure 5-29 ONVIF NVR Information (Edit) Window

The additional fields that can be configured are described below:

Parameter	Description
Description	Enter the description for this NVR here.

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

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:

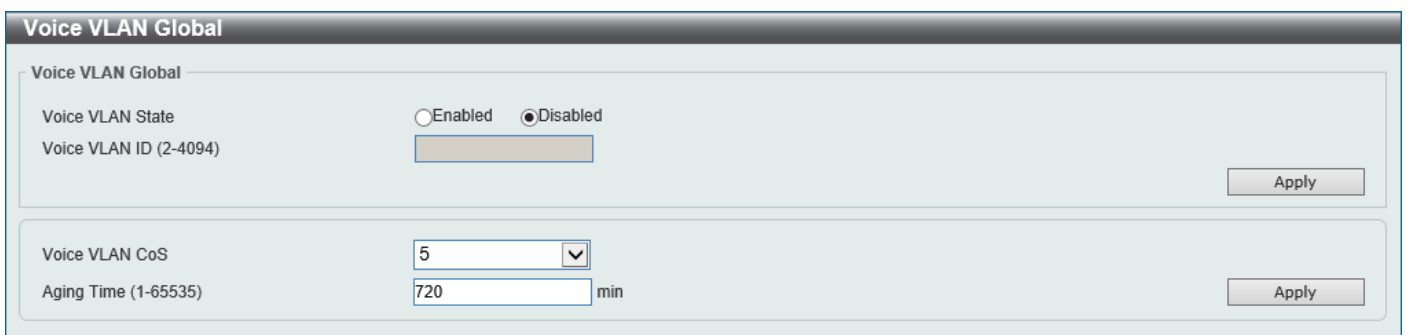


Figure 5-30 Voice VLAN Global Window

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

Parameter	Description
	here. The remarking of CoS packets allow the voice VLAN traffic to be distinguished from data traffic in Quality of Service.
Aging Time	Enter the aging time value here. This is used to configure the aging time for aging out the automatically learned voice device and voice VLAN information. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled. The range is from 1 to 65535 minutes.

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

Voice VLAN Port

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

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

Port	State	Mode
eth1/0/1	Disabled	Auto/Untag
eth1/0/2	Disabled	Auto/Untag
eth1/0/3	Disabled	Auto/Untag
eth1/0/4	Disabled	Auto/Untag
eth1/0/5	Disabled	Auto/Untag
eth1/0/6	Disabled	Auto/Untag
eth1/0/7	Disabled	Auto/Untag
eth1/0/8	Disabled	Auto/Untag
eth1/0/9	Disabled	Auto/Untag
eth1/0/10	Disabled	Auto/Untag

Figure 5-31 Voice VLAN Port Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the 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 comply 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</p>

Parameter	Description
	<p>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> <p>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.</p>

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:

Voice VLAN OUI

Voice VLAN OUI

OUI Address: 00-01-E3-00-00-00 Mask: FF-FF-FF-00-00-00 Description: 32 chars

Total Entries: 8

OUI Address	Mask	Description	
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	<input type="button" value="Delete"/>
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	<input type="button" value="Delete"/>
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	<input type="button" value="Delete"/>
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	<input type="button" value="Delete"/>
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	<input type="button" value="Delete"/>
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	<input type="button" value="Delete"/>
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	<input type="button" value="Delete"/>
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	<input type="button" value="Delete"/>

Figure 5-32 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.

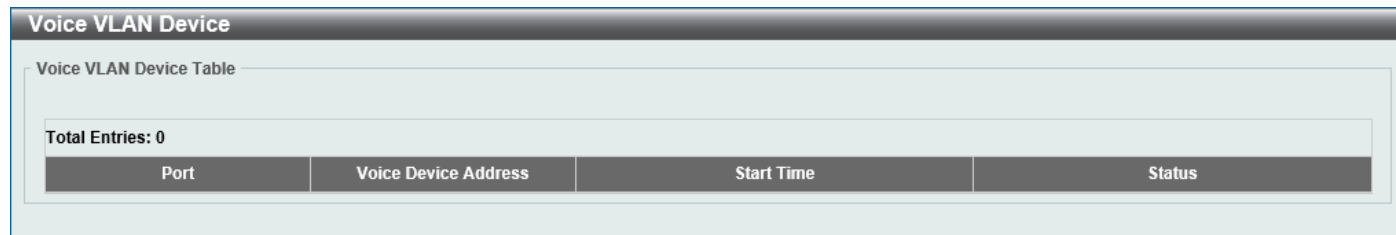
Click the **Apply** button to accept the changes made.

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:



The screenshot shows a web interface window titled "Voice VLAN Device". Inside, there is a section labeled "Voice VLAN Device Table" with a sub-header "Total Entries: 0". Below this is a table with four columns: "Port", "Voice Device Address", "Start Time", and "Status". The table is currently empty.

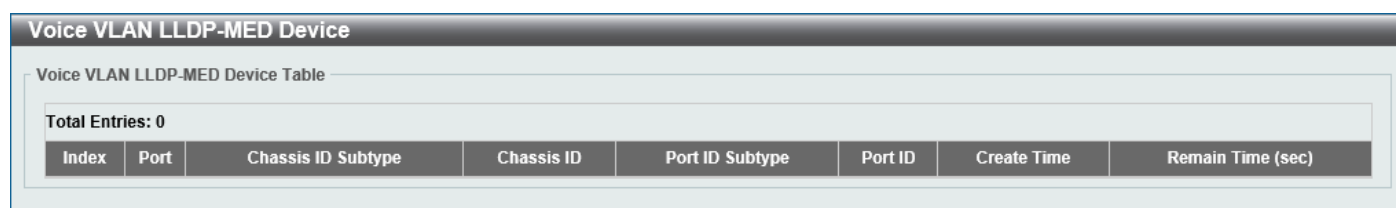
Port	Voice Device Address	Start Time	Status
Total Entries: 0			

Figure 5-33 Voice VLAN Device Window

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:



The screenshot shows a web interface window titled "Voice VLAN LLDP-MED Device". Inside, there is a section labeled "Voice VLAN LLDP-MED Device Table" with a sub-header "Total Entries: 0". Below this is a table with eight columns: "Index", "Port", "Chassis ID Subtype", "Chassis ID", "Port ID Subtype", "Port ID", "Create Time", and "Remain Time (sec)". The table is currently empty.

Index	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time	Remain Time (sec)
Total Entries: 0							

Figure 5-34 Voice VLAN LLDP-MED Device Window

STP

This Switch supports three versions of the Spanning Tree Protocol (STP): IEEE 802.1D-1998 STP, IEEE 802.1D-2004 Rapid STP, and IEEE 802.1Q-2005 MSTP. The IEEE 802.1D-1998 STP standard will be familiar to most networking professionals. However, as IEEE 802.1D-2004 RSTP and IEEE 802.1Q-2005 MSTP have been recently introduced to D-Link managed Ethernet Switches, a brief introduction to the technology is provided below followed by a description of how to set up IEEE 802.1D-1998 STP, IEEE 802.1D-2004 RSTP, and IEEE 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

The Multiple Spanning Tree Protocol (MSTP) is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance.

Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP, or MSTP).

A Multiple Spanning Tree Instance (MSTI) ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree instance. Frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each Switch utilizing the MSTP on a network will share a single MSTP configuration that will have the following three attributes:

- A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the **Configuration Name** field).
- A configuration revision number (named here as a **Revision Level** and found in the **MST Configuration Identification** window)
- A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

- The Switch must be set to the MSTP setting (found in the **STP Global Settings** window in the **STP Mode** field).
- The correct spanning tree priority for the MSTP instance must be entered (defined here as a **Priority** in the **MSTP Port Information** window when configuring MSTI ID settings).
- VLANs that will be shared must be added to the MSTP Instance ID (defined here as a **VID List** in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by IEEE 802.1D-2004 and a version compatible with IEEE 802.1D-1998. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998, however, the advantages of using RSTP will be lost. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way, this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states Disabled, Blocking, and Listening used in 802.1D-1998 and create a single state called Discarding. In either case, ports do not forward packets. In the STP port transition states Disabled, Blocking, or Listening or in the RSTP/MSTP port state Discarding there is no functional difference, the port is not active in the network topology. The table below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently, with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately, this difference results in faster detection of failed links, and therefore faster topology adjustment. A drawback of IEEE 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
<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:** Disabled (selected)
- STP Traps:** STP New Root Trap: Disabled (selected); STP Topology Change Trap: Disabled (selected)
- STP Mode:** RSTP
- STP Priority:** 32768
- STP Configuration:**
 - Bridge Max Age (6-40): 20 sec
 - Bridge Forward Time (4-30): 15 sec
 - Max Hops (1-40): 20 times
 - Bridge Hello Time (1-2): 2 sec
 - TX Hold Count (1-10): 6 times

Figure 5-35 STP Global Settings Window

The field that can be configured for **STP State** is described below:

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

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

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select to enable or disable the STP New Root Trap option here.
STP Topology Change Trap	Select to enable or disable the STP Topology Change Trap option here.

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

The fields that can be configured for **STP Mode** are described below:

Parameter	Description
STP Mode	Select the STP mode used here. Options to choose from are MSTP , RSTP , and STP .

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

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

Parameter	Description
Priority	Select the STP priority value here. The range is from 0 to 61440. By default, this value is 32768. The lower the value, the higher the priority.

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

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

Parameter	Description
Bridge Max Age	Enter the bridge Maximum Age value here. The range is from 6 to 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting RSTP/STP as the Spanning Tree Mode , this parameter will be available. Enter the bridge Hello Time value here. The range is from 1 to 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP version. For MSTP, the Hello Time must be set on a port per-port basis.
Bridge Forward Time	Enter the bridge Forwarding Time value here. The range is from 4 to 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
TX Hold Count	Enter the Transmit Hold Count value here. The range is from 1 to 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. The range is from 1 to 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out.

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:

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority
eth1/0/1	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/2	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/3	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/4	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/5	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/6	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/7	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/8	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/9	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/10	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128

Figure 5-36 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Cost	Enter the cost value here. The range is from 1 to 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. By default, this value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. By default, port cost for 100 Mbps is 200000, 1 Gbps is 20000, 10 Gbps is 2000, and 25 Gbps is 800. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.
Link Type	Select the link type here. Options to choose from are Auto , P2P , and Shared . A full-duplex port is considered to have a Point-to-Point (P2P) connection. The port cannot transit into the forwarding state rapidly by setting the link type to Shared . By default, the Auto option is used.
Port Fast	Select the Port Fast option here. Options to choose from are: <ul style="list-style-type: none"> • Network - The port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. • Disable - The port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. • Edge - The port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the

Parameter	Description
	interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this is Edge .
TCN Filter	Select to enable or disable the TCN Filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is disabled.
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is disabled.
Priority	Select the priority value here. Options to choose from are 0 to 240. By default, this value is 128. A lower value has higher priority.
Hello Time	Enter the hello time value here. The range is from 1 to 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.

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

MST Configuration Identification

This window is used to display and configure the MST configuration identification settings. These settings will uniquely identify an MSTI configured on the Switch. The Switch initially possesses one Common Internal Spanning Tree (CIST) of which the user may modify the parameters for but cannot change or delete the MSTI ID.

To view the following window, click **L2 Features > STP > MST Configuration Identification**, as shown below:

Figure 5-37 MST Configuration Identification Window

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

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	Enter the revision level value here. The range is from 0 to 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

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

The fields that can be configured for **Instance ID Settings** are described below:

Parameter	Description
Instance ID	Enter the instance ID here. The range is from 1 to 32.
Action	Select the action that will be taken here. Options to choose from are Add VID and Remove VID .
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

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

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

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

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

STP Instance

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

To view the following window, click **L2 Features > STP > STP Instance**, as shown below:

STP Instance			
Total Entries: 1			
Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	<input type="button" value="Edit"/>
		1/1	<input type="button" value="Go"/>
Instance CIST			
		CIST Global Info[Mode RSTP]	
Bridge Address		F0-7D-68-12-10-01	
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 5-38 STP Instance Window

The fields that can be configured are described below:

Parameter	Description
Instance Priority	After clicking the Edit button, enter the Instance Priority value here. The range is from 0 to 61440.

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

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

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

MSTP Port Information

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

To view the following window, click **L2 Features > STP > MSTP Port Information**, as shown below:

Figure 5-39 MSTP Port Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be cleared here.
Cost	After clicking the Edit button, enter the cost value here. The range is from 1 to 200000000.
Priority	After clicking the Edit button, select the priority value here. Options to choose from are 0 to 240. By default, this value is 128. A lower value has higher priority.

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

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

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

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

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 5-40 Loopback Detection Window

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

Parameter	Description
Loopback Detection State	Select to enable or disable loopback detection. By default, this option is disabled.
Mode	Select the loopback detection mode. Options to choose from are Port-based and VLAN-based .
Enabled VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when VLAN-based is selected in the Mode drop-down list.
Interval	Enter the interval in seconds that the device will use to transmit Configuration Test Protocol (CTP) packets to detect a loopback event. The range is from 1 to 32767 seconds. By default, this value is 10 seconds.
Trap State	Select to enable or disable the loopback detection trap state.
Action Mode	Select the action mode here. Option to choose from are: <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
From Port - To Port	Select the appropriate port range used for the configuration here.

Parameter	Description
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 8 port trunk groups with up to 8 ports in each group.

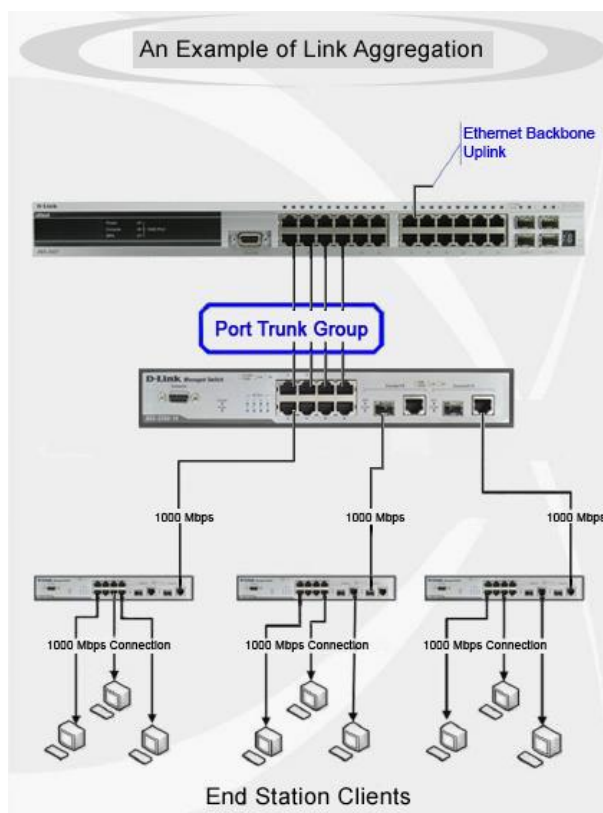


Figure 5-41 Example of Port Trunk Group

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 8 link aggregation groups, each group consisting of up to 8 links (ports). Each port can only belong to a single link aggregation group. Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group, in the same way, STP will block a single port that has a redundant link.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

This window is used to display and configure the link aggregation settings. To view the following window, click **L2 Features > Link Aggregation**, as shown below:

Link Aggregation

System Priority (1-65535)

Load Balance Algorithm

System ID

Channel Group Information

From Port To Port Group ID (1-8) Mode

Note: Each Channel Group supports up to 8 member ports.

Total Entries: 2

Channel Group	Protocol	Max Ports	Member Number	Member Ports	
Port-channel1	Static	8	4	1/0/10-1/0/13	<input type="button" value="Delete Channel"/> <input type="button" value="Show Detail"/>
Port-channel2	LACP	8	4	1/0/14-1/0/17	<input type="button" value="Delete Channel"/> <input type="button" value="Show Detail"/>

Figure 5-42 Link Aggregation Window

The fields that can be configured for **Link Aggregation** are described below:

Parameter	Description
System Priority	Enter the system priority value used here. The range is from 1 to 65535. By default, this value is 32768. The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load-balancing algorithm that will be used here. Options to choose from are Source MAC , Destination MAC , Source Destination MAC , Source IP , Destination IP , and Source Destination IP . By default, the Source Destination MAC option is used.

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

The fields that can be configured for **Channel Group Information** are described below:

Parameter	Description
From Port - To Port	Select the list of ports that will be associated with this configuration here.
Group ID	Enter the channel group number here. The range is from 1 to 8. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are Static , Active , and Passive . If the mode Static is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

Click the **Add** button to add a new channel group.

Click the **Delete Member Port** button, to delete the member port(s) specified from the group.

Click the **Delete Channel** button to delete the specified channel group.

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

After clicking the **Show Detail** button, the following page will be available.

Port Channel

Port Channel Information

Port Channel 2
Protocol LACP

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/14	Short	Active	down	32768	0	<input type="button" value="Edit"/>
eth1/0/15	Short	Active	down	32768	0	<input type="button" value="Edit"/>
eth1/0/16	Short	Active	down	32768	0	<input type="button" value="Edit"/>
eth1/0/17	Short	Active	down	32768	0	<input type="button" value="Edit"/>

Port Channel Neighbor Information

Port	Partner System ID	Partner Port Number	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/14	0,00-00-00-00-00-00	0	Long	Active	0
eth1/0/15	0,00-00-00-00-00-00	0	Long	Active	0
eth1/0/16	0,00-00-00-00-00-00	0	Long	Active	0
eth1/0/17	0,00-00-00-00-00-00	0	Long	Active	0

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.

Figure 5-43 Link Aggregation (Channel Detail) Window

The fields that can be configured are described below:

Parameter	Description
LACP Timeout	After clicking the Edit button, select the LACP timeout here. Options to choose from are Short and Long .
Working Mode	After clicking the Edit button, select the working mode here. Options to choose from are Active and Passive .
Port Priority	Enter the port priority value here.

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

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 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:

The screenshot shows the 'IGMP Snooping Settings' window. It has three main sections:

- Global Settings:** 'Global State' is set to 'Disabled' (radio button selected).
- VLAN Status Settings:** 'VID (1-4094)' is an empty text box. 'Status' is set to 'Disabled' (radio button selected).
- IGMP Snooping Table:** 'VID (1-4094)' is an empty text box. Below it, there is a table with one entry:

VID	VLAN Name	Status
1	default	Enabled

At the bottom right of the table, there are buttons for 'Show Detail', 'Edit', and 'Go'. There is also a pagination control showing '1/1' and navigation arrows.

Figure 5-44 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.

IGMP Snooping VLAN Parameters	
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (Port-based)
Report Suppression	Disabled
Suppression Time	10 sec
Querier State	Disabled
Query Version	v3
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Member Query Interval	1 sec

Figure 5-45 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	
VID (1-4094)	1
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Minimum Version	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)	10
Querier State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Query Version	3
Query Interval (1-31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Value (1-7)	2
Last Member Query Interval (1-25)	1 sec

Figure 5-46 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 from the last member. When fast leave is enabled, the Switch will not generate specific queries. When fast leave is disabled, the Switch will generate specific queries.
Report Suppression	Select this option to enable or disable the report suppression. The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expires. For report or leave messages to the same group, only

Parameter	Description
	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 query messages. The range is from 1 to 25.

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

IGMP Snooping Groups Settings

This window is used to display and configure the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:

IGMP Snooping Groups Settings

IGMP Snooping Static Groups Settings

VID (1-4094) Group Address From Port To Port

IGMP Snooping Static Groups Table

VID (1-4094) Group Address

Total Entries: 1

VID	Group Address	Ports
1	224.0.1.0	port-channel1

1/1 |< < 1 > >| Go

IGMP Snooping Groups Table

VID (1-4094) Group Address Detail

Total Entries: 0

VID	Group Address	Learned On Port
-----	---------------	-----------------

Figure 5-47 IGMP Snooping Groups Settings Window

The fields that can be configured in **IGMP Snooping Static Groups Settings/Table** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Enter an IP multicast group address.
From Port - To Port	Select the appropriate port range used for the configuration here.

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.

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 Mrouter Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings**, as shown below:

Figure 5-48 IGMP Snooping Mrouter Settings Window

The fields that can be configured in **IGMP Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID used here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are: <ul style="list-style-type: none"> Port - Select to have the configured ports to be static multicast router ports. Forbidden Port - Select to have the configured ports not to be multicast router ports.

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

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

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

The fields that can be configured in **IGMP Snooping Mrouter Table** are described below:

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

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

Click the **Show All** button to view all the entries.

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

IGMP Snooping Statistics Settings

This window is used to view and clear the IGMP snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings**, as shown below:

Figure 5-49 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 the VLAN ID here. The range is from 1 to 4094. This is available when VLAN is selected in the Statistics drop-down list.
From Port - To Port	Select the 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 the VLAN ID here. The range is from 1 to 4094. This is available when VLAN is selected in the Find Type drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Find Type drop-down list.

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

Click the **Show All** button to view all the entries.

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

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

These types of messages are transferred between devices using MLD snooping. These messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

- **Multicast Listener Query** - Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router: the General Query, which is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which is used to advertise a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
- **Multicast Listener Report, Version 1** - Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
- **Multicast Listener Done** - Similar to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is "done" with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.
- **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

MLD Snooping Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings**, as shown below:

Figure 5-50 MLD Snooping Settings Window

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

Parameter	Description
Global State	Select this option to enable or disable the global MLD snooping state.

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

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

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable MLD snooping on the VLAN.

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

The fields that can be configured in **MLD Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

Click the **Show All** button to view all the entries.

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

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

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

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

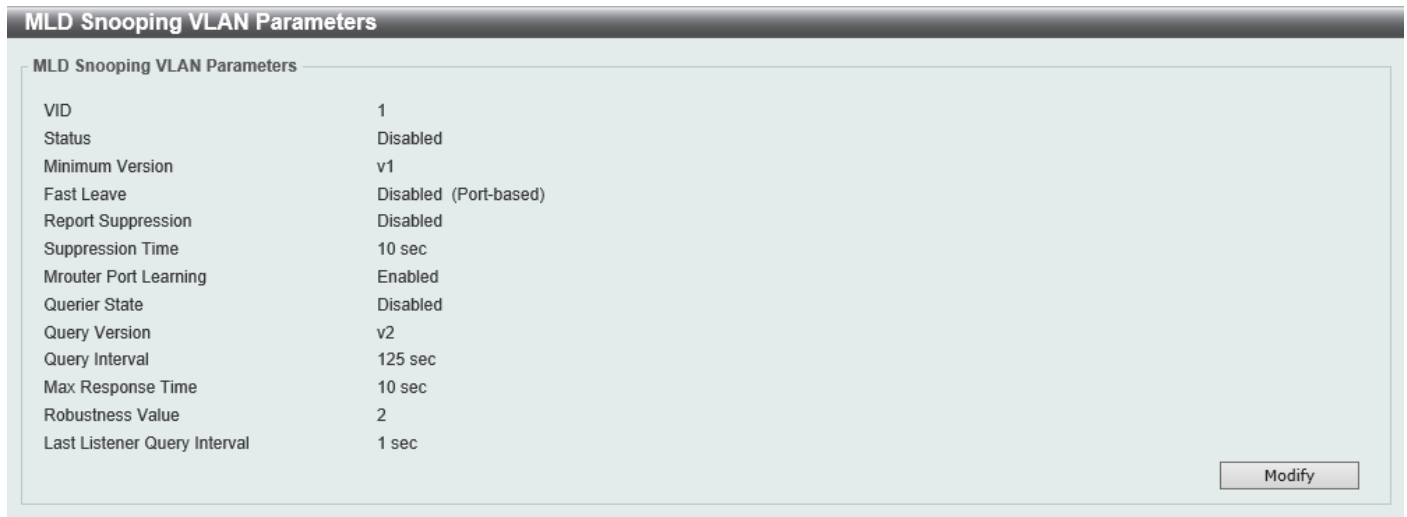


Figure 5-51 MLD Snooping Settings (Show Detail) Window

The window displays the detail information about MLD snooping VLAN.

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

After clicking the **Modify** or **Edit** button in MLD Snooping Settings window, the following window will appear.

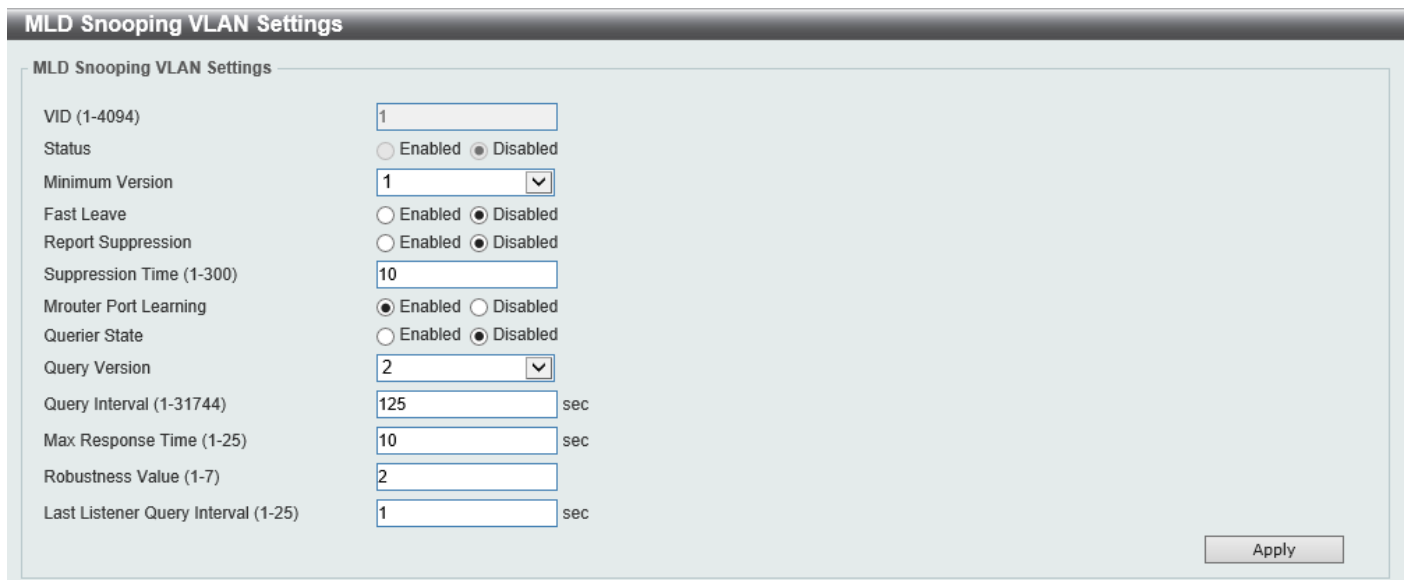


Figure 5-52 MLD Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN. Options to choose from are 1 and 2 .
Fast Leave	Select this option to enable or disable the MLD snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the MLD done message from the last member.
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.
Mrouter Port Learning	Select to enable or disable the multicast router port learning function here.

Parameter	Description
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.

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 5-53 MLD Snooping Groups Settings Window

The fields that can be configured in **MLD Snooping Static Groups Settings/Table** are described below:

Parameter	Description
VID	Enter the VLAN ID of the multicast group here. The range is from 1 to 4094.
Group Address	Enter the IPv6 multicast group address here.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.

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

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

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

Click the **Show All** button to view all the entries.

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

The fields that can be configured in **MLD Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.
Detail	Select this option to display the MLD 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 Mrouter 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 5-54 MLD Snooping Mrouter Settings Window

The fields that can be configured in **MLD Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are: <ul style="list-style-type: none"> • Port - Specifies that the configured ports are connected to multicast-enabled routers. • Forbidden Port - Specifies that the configured ports are not connected to multicast-enabled routers. • Learn PIMv6 - Specifies to enable the dynamic learning of multicast router ports on the specified VLAN.
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 the VLAN ID here. The range is from 1 to 4094.

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

Click the **Show All** button to view all the entries.

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

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 5-55 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 the VLAN ID here. The range is from 1 to 4094. This is available when VLAN is selected in the Statistics drop-down list.
From Port - To Port	Select the 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 the VLAN ID here. The range is from 1 to 4094. This is available when VLAN is selected in the Find Type drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here.

Parameter	Description
	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 Filtering Mode

This window is used to display and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering Mode**, as shown below:

Figure 5-56 Multicast Filtering Mode Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filtering Mode	<p>Select the multicast filtering mode here. Options to choose from are:</p> <ul style="list-style-type: none"> • Forward Unregistered - Registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. • Forward All - All multicast packets will be flooded based on the VLAN domain. • Filter Unregistered - Registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

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

LLDP

LLDP Global Settings

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

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:

Figure 5-57 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 the 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. The range is from 1 to 10. Select the Default option to use the default value.

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

The 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. Select the Default option to use the default value.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDU transmission interval that used to calculate the TTL value of an LLDPDU. The range is from 2 to 10. Select the Default option to use the default value.
Reinit Delay	Enter the delay value for LLDP initialization on an interface. The range is from 1 to 10 seconds. Select the Default option to use the default value.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer. Select the Default option to use the default value.

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

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

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.

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	
eth1/0/9	Disabled	Local	TX and RX	
eth1/0/10	Disabled	Local	TX and RX	

Figure 5-58 LLDP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select to enable or disable the notification feature here.
Subtype	Select the subtype of LLDP TLV(s). Options to choose from are MAC Address and Local .
Admin State	Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are: <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. By default, the TX and RX option is used.
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are Default , IPv4 , and IPv6 .
Action	Select the action that will be taken here. Options to choose from are Remove and Add .
Address	Enter the IP address that will be sent.

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



NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

This window is used to view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP Management Address List**, as shown below:

LLDP Management Address List				
All				Find
Subtype	Address	IF Type	OID	Advertising Ports
IPv4	10.90.90.90 (default)	lindex	1.3.6.1.4.1.171.10.1...	-
IPv4	10.90.90.90	lindex	1.3.6.1.4.1.171.10.1...	-

Figure 5-59 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: <ul style="list-style-type: none"> • All - Specifies to display all entries. • IPv4 - Enter the IPv4 address in the space provided. • IPv6 - Enter the IPv6 address in the space provided.

Click the **Find** button to locate a specific entry based on the selection made.

LLDP Basic TLVs Settings

The Type-Length-Value (TLV) field allows specific information to be sent within LLDP packets. This window is used to configure basic TLV settings. An active LLDP port on the Switch always includes mandatory data in its outbound advertisements. There are four optional data types that can be configured to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of TLVs: end of LLDPDU TLV, chassis ID TLV, port ID TLV, and TTL TLV. The mandatory data types cannot be disabled. There are also four data types, which can be optionally selected. These include Port Description, System Name, System Description, and System Capability.

To view the following window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**, as shown below:

Port	Port Description	System Name	System Description	System Capabilities
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled	Disabled

Figure 5-60 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

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

Port	Port VLAN ID	Enabled VLAN Name	Enabled Protocol Identity
eth1/0/1	Disabled		
eth1/0/2	Disabled		
eth1/0/3	Disabled		
eth1/0/4	Disabled		
eth1/0/5	Disabled		
eth1/0/6	Disabled		
eth1/0/7	Disabled		
eth1/0/8	Disabled		
eth1/0/9	Disabled		
eth1/0/10	Disabled		

Figure 5-61 LLDP Dot1 TLVs Settings Window

The fields that can be configured are described below:

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

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size
eth1/0/1	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled

Figure 5-62 LLDP Dot3 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
Link Aggregation	Select this option to enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
Maximum Frame Size	Select this option to enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.

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:

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
eth1/0/8	Disabled	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled	Disabled

Figure 5-63 LLDP-MED Port Settings Window

The fields that can be configured are described below:

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

LLDP Statistics Information

LLDP Statistics Information

Last Change Time 0 Clear Counter

Total Inserts 0

Total Deletes 0

Total Drops 0

Total Ageouts 0

LLDP Statistics Ports

Port Clear Counter Clear All

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
eth1/0/9	0	0	0	0	0	0	0
eth1/0/10	0	0	0	0	0	0	0

Figure 5-64 LLDP Statistics Information Window

The fields that can be configured are described below:

Parameter	Description
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:



The screenshot shows the 'LLDP Local Port Information' window. At the top, there is a 'Port' dropdown menu set to 'eth1/0/1'. To the right are 'Find' and 'Show Detail' buttons. Below is a table with the following columns: Port, Port ID Subtype, Port ID, and Port Description.

Port	Port ID Subtype	Port ID	Port Description
eth1/0/1	Local	eth1/0/1	D-Link Corporation DXS-1210-28...
eth1/0/2	Local	eth1/0/2	D-Link Corporation DXS-1210-28...
eth1/0/3	Local	eth1/0/3	D-Link Corporation DXS-1210-28...
eth1/0/4	Local	eth1/0/4	D-Link Corporation DXS-1210-28...
eth1/0/5	Local	eth1/0/5	D-Link Corporation DXS-1210-28...
eth1/0/6	Local	eth1/0/6	D-Link Corporation DXS-1210-28...
eth1/0/7	Local	eth1/0/7	D-Link Corporation DXS-1210-28...
eth1/0/8	Local	eth1/0/8	D-Link Corporation DXS-1210-28...
eth1/0/9	Local	eth1/0/9	D-Link Corporation DXS-1210-28...
eth1/0/10	Local	eth1/0/10	D-Link Corporation DXS-1210-28...

Figure 5-65 LLDP Local Port Information Window

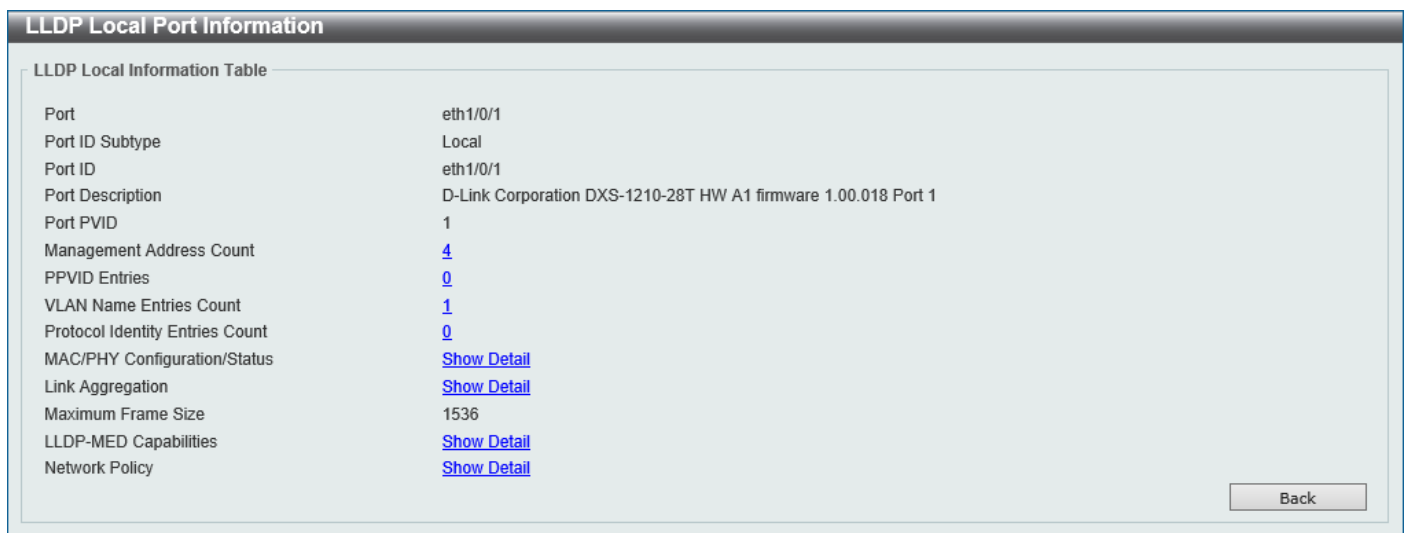
The fields that can be configured are described below:

Parameter	Description
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.



The screenshot shows the 'LLDP Local Port Information (Show Detail)' window. It displays a list of parameters and their values for port eth1/0/1. A 'Back' button is located at the bottom right.

Port	eth1/0/1
Port ID Subtype	Local
Port ID	eth1/0/1
Port Description	D-Link Corporation DXS-1210-28T HW A1 firmware 1.00.018 Port 1
Port PVID	1
Management Address Count	4
PPVID Entries	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail

Figure 5-66 LLDP Local Port Information (Show Detail) Window

Click the hyperlink next to the entry to view more information related to the topic.

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:

The screenshot shows the 'LLDP Neighbor Port Information' window. At the top, there is a search bar with a dropdown menu set to 'eth1/0/19'. To the right of the search bar are three buttons: 'Find', 'Clear', and 'Clear All'. Below the search bar, it says 'Total Entries: 1'. A table displays the following information:

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	
1	MAC Address	F0-7D-68-12-10-01	Local	eth1/0/18		Show Detail

Figure 5-67 LLDP Neighbor Port Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be displayed.

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

Click the **Clear** button to clear the specific port information.

Click the **Clear All** button to clear all the port information displayed.

Click the **Show Detail** button to view detailed information of the specific port.

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

The screenshot shows the 'LLDP Neighbor Port Information (Show Detail)' window. It displays the following information:

Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	F0-7D-68-12-10-01
Port ID Subtype	Local
Port ID	eth1/0/18
Port Description	
System Name	
System Description	
System Capabilities	
Management Address Entries	Show Detail
Port PVID	0
PPVID Entries	Show Detail
VLAN Name Entries	Show Detail
Protocol Identity Entries	Show Detail
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	0
Unknown TLVs	Show Detail
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Inventory Management	Show Detail

A 'Back' button is located at the bottom right of the window.

Figure 5-68 LLDP Neighbor Port Information (Show Detail) Window

Click the hyperlink next to the entry to view more information related to the topic.

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

6. Layer 3 Features

ARP

Gratuitous ARP

IPv6 Neighbor

Interface

IPv4 Static/Default Route

IPv4 Route Table

IPv6 Static/Default Route

IPv6 Route Table

IP Multicast Routing Protocol

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
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.
Timeout	After click the Edit button, enter the ARP aging timeout value here. The range is from 0 to 65535. If this value is 0, the entry never times out.

Click the **Find** button to find and display the entries, based on the information entered, in the **ARP Aging Time Table**.

Click the **Show All** button to display all the static ARP aging time entries in the **ARP Aging Time Table**.

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

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

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

Static ARP

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

To view the following window, click **L3 Features > ARP > Static ARP**, as shown below:

Figure 6-2 Static ARP Window

The fields that can be configured in the **Static ARP Setting** section are described below:

Parameter	Description
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

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

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

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

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

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 6-3 ARP Table Window

The fields that can be configured are described below:

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

Parameter	Description
IP Address	Select and enter the IP address to display here.
Mask	After the IP Address option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Type	Select the Type option here. Options to choose from are All and Dynamic .

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

Click the **Clear All** button to clear all dynamic ARP cache.

Click the **Clear** button to clear the dynamic ARP cache associated with the specific entry.

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

Gratuitous ARP

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

To view the following window, click **L3 Features > Gratuitous ARP**, as shown below:

The screenshot shows the 'Gratuitous ARP' configuration window. It is divided into two main sections:

- Gratuitous ARP Global Settings:** This section contains four rows of radio buttons:
 - IP Gratuitous ARP State: Enabled, Disabled
 - Gratuitous ARP Trap State: Enabled, Disabled
 - IP Gratuitous ARP Dad-Reply State: Enabled, Disabled
 - Gratuitous ARP Learning State: Enabled, Disabled
- Gratuitous ARP Send Interval:** This section shows a table with the following data:

Interface Name	Interval Time (sec)
vlan1	0

 Below the table is an 'Edit' button and a pagination control showing '1/1' entries.

Figure 6-4 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 6-5 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 by Interface** button to clear all the dynamic information for the specific interface.

Click the **Clear All** button to clear all the dynamic IPv6 neighbor information in this table.

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

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

Interface

IPv4 Interface

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

To view the following window, click **L3 Features > Interface > IPv4 Interface**, as shown below:

The screenshot shows the 'IPv4 Interface' window. At the top, there is a header 'IPv4 Interface' and a sub-header 'IPv4 Interface'. Below this, there is a form for 'Interface VLAN (1-4094)' with an empty text box and 'Apply' and 'Find' buttons. A table below shows 'Total Entries: 1' with the following data:

Interface	State	IP Address	Link Status	
vlan1	Enabled	10.90.90.90/255.0.0.0 Manual	Up	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

At the bottom of the table, there are navigation controls: '1/1', '<', '<', '1', '>', '>', and a 'Go' button.

Figure 6-6 IPv4 Interface Window

The fields that can be configured are described below:

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

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

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

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

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

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

After clicking the **Edit** button, the following page will be available.

The screenshot shows the 'IPv4 Interface Configure' window. It has a header 'IPv4 Interface Configure' and a sub-header 'IPv4 Interface Settings'. Below this, there is a form for 'DHCP Client' with 'Interface' set to 'vlan1' and a 'Back' button. The 'Settings' section has 'State' set to 'Enabled' with a dropdown arrow and an 'Apply' button. The 'Primary IP Settings' section has 'Get IP From' set to 'Static' with a dropdown arrow, 'IP Address' set to '10 . 90 . 90 . 90', and 'Mask' set to '255 . 0 . 0 . 0'. There are 'Apply' and 'Delete' buttons at the bottom right.

Figure 6-7 IPv4 Interface (Edit) Window

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

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.

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

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

The fields that can be configured in the **Primary IP Settings** section are described below:

Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are: <ul style="list-style-type: none"> • Static - Enter the IPv4 address of this interface manually in the fields provided. • DHCP - This interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the primary IPv4 address for this interface here.
Mask	Enter the primary IPv4 subnet mask for this interface here.

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

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

After selecting the **DHCP Client** tab, the following page will appear.

The screenshot shows the 'IPv4 Interface Configure' window with the 'DHCP Client' tab selected. The 'IPv4 Interface Settings' tab is also visible. The DHCP Client section contains the following fields:

- DHCP Client Client-ID (1-4094): A text input field.
- Class ID String: A text input field with '32 chars' and a 'Hex' checkbox.
- Host Name: A text input field with '64 chars'.
- Lease: A text input field with 'Days (0-10000)' and '00' in a dropdown, and 'Hours' and '00' in a dropdown, and 'Minutes' below it.

An 'Apply' button is located at the bottom right of the DHCP Client section.

Figure 6-8 IPv4 Interface (Edit, DHCP Client) Window

The fields that can be configured are described below:

Parameter	Description
DHCP Client Client-ID	Enter the DHCP Client ID here. The range is from 1 to 4094. This parameter is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message.
Class ID String	Enter the class ID string here. This string can be up to 32 characters long. Select the Hex option to enter the Class ID string in the hexadecimal format. This string can be up to 64 characters long. This parameter is used to specify the vendor class identifier used as the value of Option 60 in the DHCP discover message.
Host Name	Enter the host name here. This string can be up to 64 characters long. This parameter is used to specify the value of the host name option to be sent with the DHCP discover message.
Lease	Enter and optionally select the DHCP client lease time here. In the textbox, the lease time, in days, can be entered. The range is from 0 to 10000 days. Hours and Minutes can also be selected optionally.

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

IPv6 Interface

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

To view the following window, click **L3 Features > Interface > IPv6 Interface**, as shown below:

Interface	IPv6 State	Link Status
vlan1	Disabled	Up

Figure 6-9 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 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 6-10 IPv6 Interface (Detail, IPv6 Interface Settings) Window

The fields that can be configured for **IPv6 Interface Settings** are described below:

Parameter	Description
IPv6 State	Select to globally enable or disable the IPv6 interface 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 0 (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.

Parameter	Description
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.

IPv6 Interface			
IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	DHCPv6 Client
Total Entries: 2			
Address Type	IPv6 Address		
Link-Local Address	FE80::F27D:68FF:FE12:1001		Delete
Global Unicast Address	2020::20/64 (Manual)		Delete

Figure 6-11 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.

IPv6 Interface					
IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	DHCPv6 Client		
Total Entries: 1					
IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
2020::/64	604800	2592000	Enabled	Enabled	Edit

Figure 6-12 IPv6 Interface (Detail, Neighbor Discover) Window

IPv6 Interface					
IPv6 Interface Settings	Interface IPv6 Address	Neighbor Discover	DHCPv6 Client		
Total Entries: 1					
IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
2020::/64	604800	2592000	Enabled	Enabled	Apply

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

Click the **Edit** button to modify the entry. The fields that can be configured are described below:

Parameter	Description
Preferred Life Time	Enter the preferred lifetime value here. The range is from 0 to 4294967295 seconds. By default, this is 604800 seconds (7 days).
Valid Life Time	Enter the valid lifetime value here. The range is from 0 to 4294967295 seconds. By default, this is 2592000 seconds (30 days).
Link Flag	Select to enable or disable the link flag function here. By default, this is enabled.
Autoconfig Flag	Select to enable or disable the automatic configuration function here. By default, this is enabled.

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

After selecting the **DHCPv6 Client** tab option, at the top of the page, the following page will be available.

Figure 6-14 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.

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 128 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 6-15 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address for this route here. Tick the Default Route option to use the default route as the IPv4 address.
Mask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.
Backup State	Select the backup state option here. Options to choose from are: <ul style="list-style-type: none"> • Primary - Specifies the route as the primary route to the destination. • Backup - Specifies the route as the backup route to the destination.

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

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

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

IPv4 Route Table

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

To view the following window, click **L3 Features > IPv4 Route Table**, as shown below:

IPv4 Route Table

IPv4 Route Table

Show All
 IP Address
 Network Address
 Connected Hardware Summary

Find

Total Entries: 3

IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
0.0.0.0	0.0.0.0	10.90.90.10	vlan1	1/1	Static	Yes
10.0.0.0	255.0.0.0	Directly Connected	vlan1		Connected	-
192.168.70.0	255.255.255.0	Directly Connected	vlan1_1		Connected	-

1/1 < << 1 >> > Go

Figure 6-16 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
Show All	Select this option to display all available IPv4 route entries in the table.
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

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

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 6-17 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Select Default Route to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Backup State	Select the backup state option here. Options to choose from are: <ul style="list-style-type: none"> • Primary - The route is specified as the primary route to the destination. • Backup - The route is specified as the backup route to the destination.

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

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

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

IPv6 Route Table

This window is used to display and configure the IPv6 route table.

To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:

IPv6 Route Table

IPv6 Route Table

Please Select Database
 Hardware
 Summary

Find

Total Entries: 1 entries, 1 routes

IPv6 Address/Prefix Length	Next Hop	Interface	Distance/Metric	Protocol	Valid Route	Selected Route
2020::/64	Directly Connected	vlan1	0/1	Connected	-	-

1/1 < < 1 > > Go

Figure 6-18 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Select this option to display the IPv6 routes associated with the specified IPv6. Enter the IPv6 address in the textbox.
IPv6 Address/Prefix Length	Select this option to display the IPv6 routes associated with the specified IPv6 network. Enter the IPv6 address and prefix length in the textbox. Select the Longer Prefixes option to display IPv6 routes with prefixes greater than and equal to the prefix length.
Interface Name	Select this option to display the IPv6 routes associated with the specified interface. Enter the name of the interface in the textbox.
Connected	Select this option to display only connected routes.
Database	Select this option to display all the related entries in the routing database instead of just the best route.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

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

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

IP Multicast Routing Protocol

IPMC

IP Multicast Routing Forwarding Cache Table

This window is used to display the content of the IP multicast routing forwarding cache database.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Routing Forwarding Cache Table**, as shown below:

Figure 6-19 IP Multicast Routing Forwarding Cache Table Window

The fields that can be configured are described below:

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

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

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

IPv6MC

IPv6 Multicast Routing Forwarding Cache Table

This window is used to display the contents of the IPv6 multicast routing forwarding cache database.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table**, as shown below:

Figure 6-20 IPv6 Multicast Routing Forwarding Cache Table Window

The fields that can be configured are described below:

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

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

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

7. Quality of Service (QoS)

Basic Settings

Advanced Settings

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
eth1/0/7	0	No
eth1/0/8	0	No
eth1/0/9	0	No
eth1/0/10	0	No

Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
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
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
eth1/0/8	WRR
eth1/0/9	WRR
eth1/0/10	WRR

Figure 7-2 Port Scheduler Method Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Scheduler Method	<p>Select the scheduler method that will be applied to the specified port(s). Options to choose from are:</p> <ul style="list-style-type: none"> • SP (Strict Priority) - Specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest. • RR (Round-Robin) - 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. • WRR (Weighted Round-Robin) - Operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time. • WDRR (Weighted Deficit Round-Robin) - Operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration. <p>To set a CoS queue in the SP mode, any higher priority CoS queue must also be in the strict priority mode.</p>

Parameter	Description
	By default, the WRR option is used.

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
	7	0	1

Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Enter the queue ID value here. The range is from 0 to 7.
WRR Weight	Enter the WRR weight value here. The range is from 0 to 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. Therefore, the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. The range is from 0 to 127.

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

CoS to Queue Mapping

This window is used to display and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:

CoS	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7.

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

Port Rate Limiting

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

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:

Port	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
eth1/0/7	No Limit	No Limit	No Limit	No Limit
eth1/0/8	No Limit	No Limit	No Limit	No Limit
eth1/0/9	No Limit	No Limit	No Limit	No Limit
eth1/0/10	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
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: <ul style="list-style-type: none"> • Input - The rate limit for ingress packets is configured. • Output - The rate limit for egress packets is configured.
Rate Limit	Select and enter the rate limit value here. Options to choose from are: <ul style="list-style-type: none"> • Bandwidth - Enter the input/output bandwidth value used in the space provided. The range is from 64 to 10000000 kbps. Also, enter the Burst Size value in the space provided. The range is from 0 to 128000 kilobytes. • Percent - Enter the input/output bandwidth percentage value used in the space provided. The range is from 1 to 100 percent (%). Also, enter the Burst Size value in the space provided. The range is from 0 to 128000 kilobytes. • None - Specifies 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:

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...
eth1/0/7	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...
eth1/0/8	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...
eth1/0/9	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...
eth1/0/10	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
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.

Parameter	Description
Rate Limit	<p>Select and enter the queue rate limit settings here. Options to choose from are:</p> <ul style="list-style-type: none"> Min Bandwidth - Enter the minimum bandwidth rate limit value in the space provided. The range is from 64 to 10000000 kbps. Also, enter the maximum bandwidth (Max Bandwidth) rate limit in the space provided. The range is from 64 to 10000000 kbps. <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> Min Percent - Enter the minimum bandwidth percentage value in the space provided. The range is from 1 to 100 percent (%). Also, enter the maximum percentage value (Max Percent) in the space provided. The range is from 1 to 100 percent (%). None - Specifies to apply no rate limit.

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 original DSCP of the packet. 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: Input DSCP List (0-63): Output DSCP (0-63):

Total Entries: 1

Mutation Name	Digit in tens	Digit in ones										Delete
		0	1	2	3	4	5	6	7	8	9	
Mutation	00	0	1	2	3	4	5	6	7	8	9	Delete
	10	11	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 > >

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. The range is from 0 to 63.
Output DSCP List	Enter the output DSCP list value here. The range is from 0 to 63.

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

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

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

Port Trust State 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	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	
eth1/0/7	Trust CoS	
eth1/0/8	Trust CoS	
eth1/0/9	Trust CoS	
eth1/0/10	Trust CoS	

Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
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:

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
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. The range is from 0 to 63.

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 Name	Multiple Match Criteria	Match	Delete
class-map1	Match Any	Match	Delete
class-default	Match Any	Match	Delete

Figure 7-10 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 7-11 Class Map (Match) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. The range is from 0 to 7.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. The range is from 0 to 63. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. The range is from 0 to 7. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are ARP, BGP, DHCP, DNS, EGP, FTP, IPv4, IPv6, NetBIOS, NFS, NTP, OSPF, PPPOE, RIP, RTSP, SSH, Telnet, and TFTP .
VID List	Select and enter the VLAN list value that will be matched with the class map here. The range is from 1 to 4094.

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

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

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 7-12 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.

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 7-13 Policy Map (Set Action) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to specify that no action will be taken.
Specify	Select this option to specify that action will be taken based on the configurations made.
New Precedence	Select the new precedence value for the packet here. The range is from 0 to 7. Select the IPv4 only option to specify that IPv4 precedence will be marked only. If not selected, then both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of the traffic class of the IPv6 header. Setting the precedence will not affect the CoS queue selection.
New DSCP	Select the new DSCP value for the packet here. The range is from 0 to 63. Select the IPv4 only option to specify that the IPv4 DSCP will be marked only. If not selected, then both the IPv4 and IPv6 DSCP will be marked. Setting the DSCP will not affect the CoS queue selection.
New CoS	Select the new CoS value to the packet here. The range is from 0 to 7. Setting the CoS will affect the CoS queue selection while the policy map is applied on the ingress interface.
New Cos Queue	Select the new CoS queue value to the packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface.

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

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

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:

Port	Direction	Policy Map Name
eth1/0/1		
eth1/0/2		
eth1/0/3		
eth1/0/4		
eth1/0/5		
eth1/0/6		
eth1/0/7		
eth1/0/8		
eth1/0/9		
eth1/0/10		

Figure 7-14 Policy Binding Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are Input and Output . Input specified ingress traffic and output specifies egress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the None option to not tie a policy map to this entry.

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

8. Access Control List (ACL)

ACL Configuration Wizard
ACL Access List
ACL Interface Access Group

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:

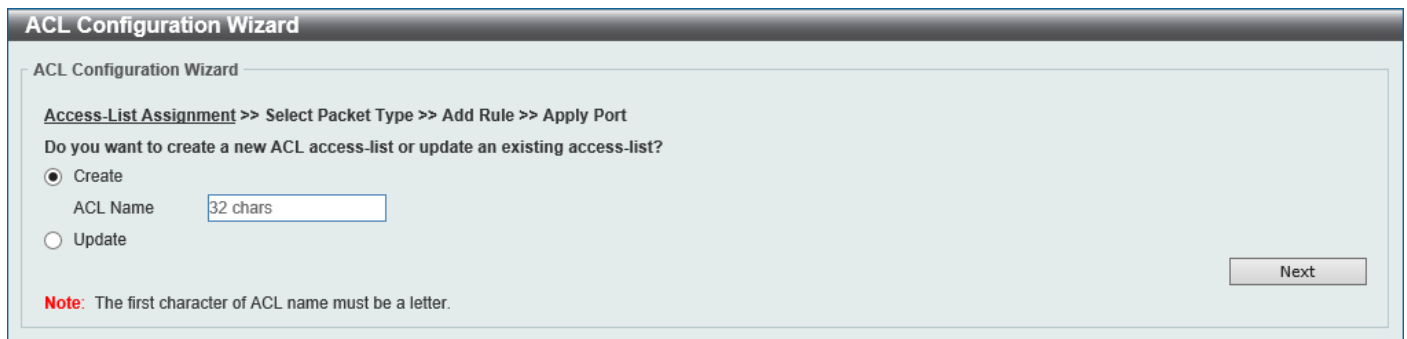
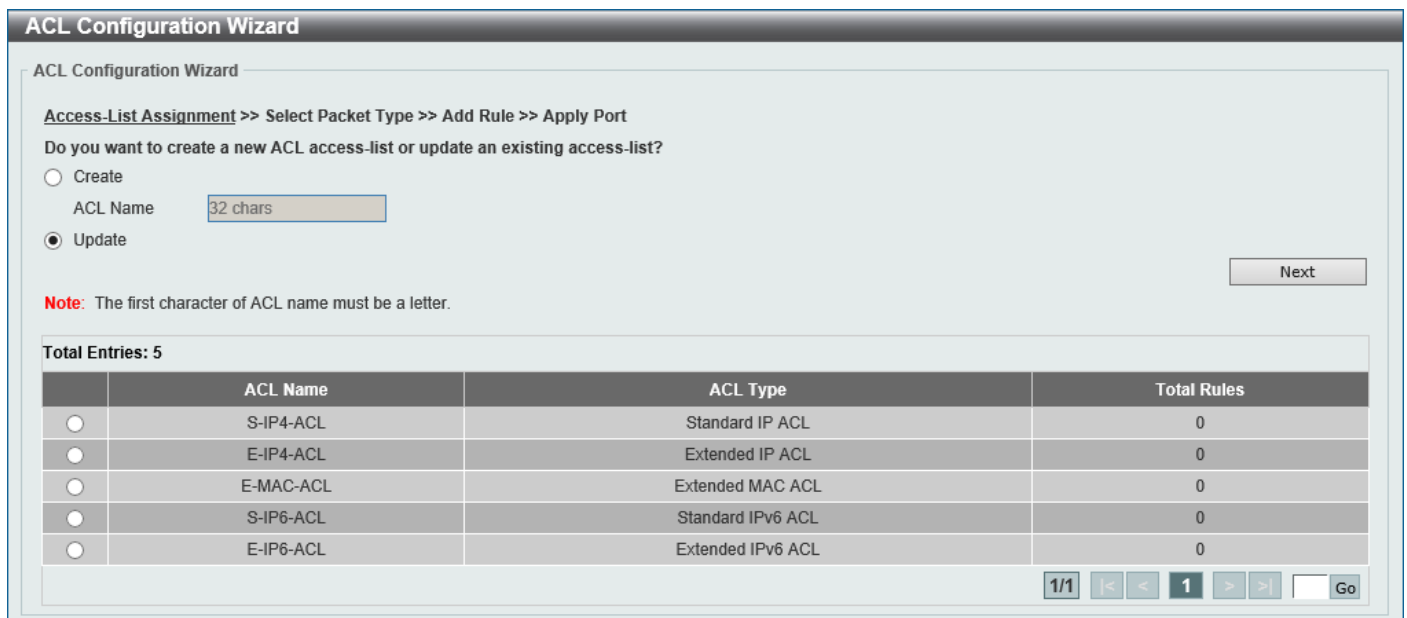


Figure 8-1 ACL Configuration Wizard (Create) Window



Total Entries: 5			
	ACL Name	ACL Type	Total Rules
<input type="radio"/>	S-IP4-ACL	Standard IP ACL	0
<input type="radio"/>	E-IP4-ACL	Extended IP ACL	0
<input type="radio"/>	E-MAC-ACL	Extended MAC ACL	0
<input type="radio"/>	S-IP6-ACL	Standard IPv6 ACL	0
<input type="radio"/>	E-IP6-ACL	Extended IPv6 ACL	0

Figure 8-2 ACL Configuration Wizard (Update) Window

The fields that can be configured are described below:

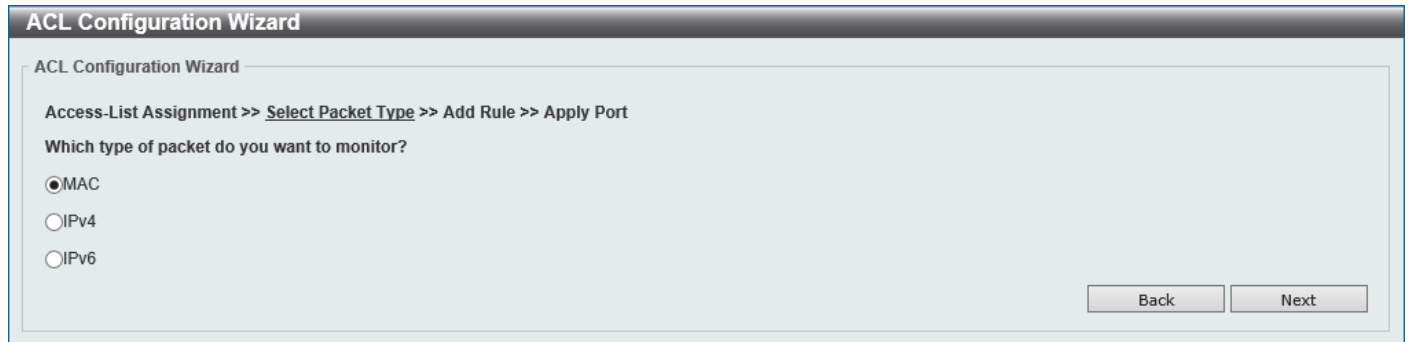
Parameter	Description
Create	Select this option to create a new ACL access list using the configuration wizard.
ACL Name	Enter the new ACL name here. This name can be up to 32 characters long.
Update	Select this option to update an existing ACL access list. Select the existing ACL in the table to process with the update.

Click the **Next** button to continue to the next step.

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

Step 2 - Select Packet Type

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



The screenshot shows a web browser window titled "ACL Configuration Wizard". The breadcrumb trail is "Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port". The main question is "Which type of packet do you want to monitor?". There are three radio button options: "MAC" (which is selected), "IPv4", and "IPv6". At the bottom right, there are two buttons: "Back" and "Next".

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

Extended MAC ACL

Selecting to **Create** or **Update** a **MAC ACL** and click the **Next** button to view the following window:

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> **Add Rule** >> Apply Port

Please assign a sequence number to create a new rule.

Sequence No. (1-65535) Auto Assign

Assign Rule Criteria

MAC Address **Ethernet Type** **802.1Q VLAN**

MAC Address

Any Host Any Host

Source MAC Destination MAC

Wildcard Wildcard

Ethernet Type

Specify Ethernet Type

Ethernet Type (0x0-0xFFFF)

Ethernet Type Mask (0x0-0xFFFF)

802.1Q VLAN

CoS Mask (0x0-0x7)

VID(1-4094) Mask (0x0-0xFFF)

VLAN Range ~

Time Range

Action Permit Deny

Figure 8-4 ACL Configuration Wizard (Extended MAC ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select Auto Assign to generate an ACL rule number automatically for this entry.
Source	Select and enter the source MAC address information here. Options to choose from are: <ul style="list-style-type: none"> Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host MAC address here. MAC - The Wildcard option will be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are: <ul style="list-style-type: none"> Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host MAC address here. MAC - The Wildcard option will be available. Enter the destination MAC address and wildcard value in the spaces provided.

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) Mask (0x0-0xFF) Fragments

Assign Rule Criteria

IPv4 Address **Port** **IPv4 DSCP** **TCP Flag**

IPv4 Address

Source Any Host IP Wildcard

Destination Any Host IP Wildcard

Port

Source Port (0-65535) (0-65535)

Destination Port (0-65535) (0-65535)

IPv4 DSCP

IP Precedence Value (0-7) Mask (0x0-0x7)

ToS Value (0-15) Mask (0x0-0xF)

DSCP (0-63) Value (0-63) Mask (0x0-0x3F)

TCP Flag

TCP Flag ack fin psh rst syn urg

Time Range

Action Permit Deny

Figure 8-6 ACL Configuration Wizard (Extended IPv4 ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select Auto Assign to generate an ACL rule number automatically for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID , and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Mask - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • Fragments - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host IP address here. • IP - The Wildcard option will be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

Parameter	Description
Destination	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host IP address here. • IP - The Wildcard option will be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified destination port number and mask will be used. Enter the destination port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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.</p> <p>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.</p> <p>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>
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. • Mask - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.

Parameter	Description
ToS	Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8). <ul style="list-style-type: none"> • Value - The ToS value can also manually be entered here. The range is from 0 to 15. • Mask - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> • Value - The DSCP value can also manually be entered here. The range is from 0 to 63. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available in the protocol type TCP .
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

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

Click the **Next** button to continue to the next step.

Extended/Standard IPv6 ACL

Selecting to **Create** or **Update** an **IPv6 ACL** and click the **Next** button to view the following window:

Figure 8-7 ACL Configuration Wizard (Standard IPv6 ACL) Window

Figure 8-8 ACL Configuration Wizard (Extended IPv6 ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select Auto Assign to generate an ACL rule number automatically for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50) , PCP (108) , SCTP (132) , and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Mask - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • Fragments - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host IPv6 address here. • IPv6 - The Prefix Length option will be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:

Parameter	Description
	<ul style="list-style-type: none"> • Any - Any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host IPv6 address here. • IPv6 - The Prefix Length option will be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified destination port number and mask will be used. Enter the destination port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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.</p> <p>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.</p> <p>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>
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. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Traffic Class	<p>Select and enter the traffic class value here. The range is from 0 to 255.</p>

Parameter	Description
	<ul style="list-style-type: none"> Mask - Enter the traffic class mask value here. The range is from 0x0 to 0xFF.
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. The range is from 0 to 1048575. <ul style="list-style-type: none"> Mask - Enter the flow label mask value here. The range is from 0x0 to 0xFFFFF.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

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

Click the **Next** button to continue to the next step.

Step 4 - Apply Port

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

Figure 8-9 ACL Configuration Wizard (Create, Port) Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are In and Out .

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

Click the **Apply** button to accept the changes made and return to the main ACL Wizard window.

ACL Access List

This window is used to display and configure the ACLs, ACL rules, and settings.

To view the following window, click **ACL > ACL Access List**, as shown below:

ACL Access List

ACL Access List

ACL Type: ID (1-14999) ACL Name

Total Entries: 5

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP4-ACL	Standard IP ACL	10	10	Disabled		Edit	Delete
2000	E-IP4-ACL	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		Edit	Delete
11000	S-IP6-ACL	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IP6-ACL	Extended IPv6 ACL	10	10	Disabled		Edit	Delete

1/1 < < 1 > >

S-IP4-ACL (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
1	Permit	any any			Delete

1/1 < < 1 > >

Figure 8-10 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 , and MAC ACL .
ID	Select and enter the access list ID here. The range is from 1 to 14999.
ACL Name	Select and enter the access list name here. This name can be up to 32 characters long.

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

Click the **Add ACL** button to create a new ACL.

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

Click the **Delete** button, next to the ACL, to remove the specific ACL.

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

Click the **Clear All Counter** button to clear all the counter information displayed.

Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the **Add Rule** button to create an ACL rule for the ACL selected.

Click the **Delete** button, next to the ACL rule, to remove the specific ACL rule.

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

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

ACL Access List

ACL Type: ID (1-14999) ACL Name

Total Entries: 5

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP4-ACL	Standard IP ACL	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="Disabled"/>	<input type="text"/>	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>
2000	E-IP4-ACL	Extended IP ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
11000	S-IP6-ACL	Standard IPv6 ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
13000	E-IP6-ACL	Extended IPv6 ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1 < < 1 > >

S-IP4-ACL (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
1	Permit	any any			<input type="button" value="Delete"/>

1/1 < < 1 > >

Figure 8-11 ACL Access List (Edit) Window

After clicking the **Edit** button, the fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number step here. The step range is from 1 to 32. This specifies the number that the sequence numbers step. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on. By default, this value is 10.
Counter State	Select to enable or disable the counter state option here. By default, this is disabled.
Remark	Enter an optional remark that will be associated with this ACL here.

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

After clicking the **Add ACL** button, the following page will appear.

Add ACL Access List

Add ACL Access List

ACL Type:

ID (1-1999):

ACL Name:

Note: The first character of ACL name must be a letter.

Figure 8-12 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 , and Extended MAC ACL .
ID	Enter the ID for the ACL here.

Parameter	Description
	<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.
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 8-13 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none"> Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host IP address here. IP - The Wildcard option will be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: <ul style="list-style-type: none"> Any - Any destination traffic will be evaluated according to the conditions of this rule. Host - Enter the destination host IP address here. IP - The Wildcard option will be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

Parameter	Description
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended IP ACL

After selecting an Extended IP ACL and clicking the **Add Rule** button, the following page will appear.

Figure 8-14 Extended IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID , and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Mask - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • Fragments - Select this option to include packet fragment filtering.

Parameter	Description
Source	<p>Select and enter the source information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host IP address here. • IP - The Wildcard option will be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	<p>Select and enter the destination information here. Options to choose from are:</p> <ul style="list-style-type: none"> • Any - Any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host IP address here. • IP - The Wildcard option will be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified destination port number and mask will be used. Enter the destination port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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.</p> <p>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.</p> <p>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
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available in the protocol type TCP .
IP Precedence	Select the IP precedence value used here. Options to choose from are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), and network (7). <ul style="list-style-type: none"> Value - The IP precedence value can also manually be entered here. The range is from 0 to 7. Mask - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
ToS	Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8). <ul style="list-style-type: none"> Value - The ToS value can also manually be entered here. The range is from 0 to 15. Mask - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63. Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Standard IPv6 ACL

After selecting a Standard IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

The screenshot shows the 'Add ACL Rule' configuration window. The fields are as follows:

- ID:** 11000
- ACL Name:** S-IP6-ACL
- ACL Type:** Standard IPv6 ACL
- Sequence No. (1-65535):** [Empty] (If it isn't specified, the system automatically assigns.)
- Action:** Permit Deny
- Match IPv6 Address:**
 - Source:** Any, Host (2012::1), IPv6 (2012::1). **Prefix Length:** [Empty]
 - Destination:** Any, Host (2012::1), IPv6 (2012::1). **Prefix Length:** [Empty]
- Time Range:** 32 chars

Buttons for **Back** and **Apply** are located at the bottom right.

Figure 8-15 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host IPv6 address here. • IPv6 - The Prefix Length option will be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host IPv6 address here. • IPv6 - The Prefix Length option will be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended IPv6 ACL

After selecting an Extended IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

The screenshot shows the 'Add ACL Rule' window with the following configuration:

- ID:** 13000
- ACL Name:** E-IP6-ACL
- ACL Type:** Extended IPv6 ACL
- Sequence No. (1-65535):** (Empty field, note: (If it isn't specified, the system automatically assigns.))
- Action:** Permit Deny
- Protocol Type:** TCP (dropdown), (0-255) Mask (0x0-0xFF) (Empty field) Fragments
- Match IPv6 Address:**
 - Source:** Any, Host (2012::1), IPv6 (2012::1) with Prefix Length (Empty field)
 - Destination:** Any, Host (2012::1), IPv6 (2012::1) with Prefix Length (Empty field)
- Match Port:**
 - Source Port:** Please Select (dropdown), (0-65535) Please Select (dropdown), (0-65535)
 - Destination Port:** Please Select (dropdown), (0-65535) Please Select (dropdown), (0-65535)
- TCP Flag:** ack fin psh rst syn urg
- DSCP (0-63):** Please Select (dropdown) Value (0-63) (Empty field) Mask (0x0-0x3F) (Empty field)
- Traffic Class (0-255):** (Empty field) Mask (0x0-0xFF) (Empty field)
- Flow Label (0-1048575):** (Empty field) Mask (0x0-0xFFFF) (Empty field)
- Time Range:** 32 chars

Buttons: Back, Apply

Figure 8-16 Extended IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50) , PCP (108) , SCTP (132) , and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Mask - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • Fragments - Select this option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Any source traffic will be evaluated according to the conditions of this rule. • Host - Enter the source host IPv6 address here. • IPv6 - The Prefix Length option will be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: <ul style="list-style-type: none"> • Any - Any destination traffic will be evaluated according to the conditions of this rule.

Parameter	Description
	<ul style="list-style-type: none"> • Host - Enter the destination host IPv6 address here. • IPv6 - The Prefix Length option will be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	<p>Select and enter the source port value here. Options to choose from are:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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:</p> <ul style="list-style-type: none"> • = - The specific selected port number will be used. • > - All ports greater than the selected port, will be used. • < - All ports smaller than the selected port, will be used. • ≠ - All ports, excluding the selected port, will be used. • Range - 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. • Mask - The specified destination port number and mask will be used. Enter the destination port mask value in the space provided. The range is from 0x0 to 0xFFFF. <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. The range is from 0 to 255.</p> <p>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.</p> <p>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>
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. • Mask - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Traffic Class	<p>Select and enter the traffic class value here. The range is from 0 to 255.</p>

Parameter	Description
	<ul style="list-style-type: none"> Mask - Enter the traffic class mask value here. The range is from 0x0 to 0xFF.
Flow Label	Enter the flow label value here. The range is from 0 to 1048575. <ul style="list-style-type: none"> Mask - Enter the flow label mask value here. The range is from 0x0 to 0xFFFFF.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended MAC ACL

After selecting an Extended MAC ACL and clicking the **Add Rule** button, the following page will appear.

The screenshot shows the 'Add ACL Rule' window with the following configuration details:

- ID:** 6000
- ACL Name:** E-MAC-ACL
- ACL Type:** Extended MAC ACL
- Sequence No. (1-65535):** [Empty field] (If it isn't specified, the system automatically assigns.)
- Action:** Permit Deny
- Match MAC Address:**
 - Source:** Any, Host (11-DF-36-4B-A7-CC), MAC (11-DF-36-4B-A7-CC), Wildcard (11-DF-36-4B-A7-CC)
 - Destination:** Any, Host (11-DF-36-4B-A7-CC), MAC (11-DF-36-4B-A7-CC), Wildcard (11-DF-36-4B-A7-CC)
- Match Ethernet Type:**
 - Specify Ethernet Type:** Please Select
 - Ethernet Type (0x0-0xFFFF):** [Empty field]
 - Ethernet Type Mask (0x0-0xFFFF):** [Empty field]
- CoS:** Please Select, Mask (0x0-0x7) [Empty field]
- VID (1-4094):** [Empty field], Mask (0x0-0xFFF) [Empty field]
- VLAN Range:** [Empty field] ~ [Empty field]
- Time Range:** 32 chars

Buttons: Back, Apply

Figure 8-17 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: <ul style="list-style-type: none"> Any - Any source traffic will be evaluated according to the conditions of this rule. Host - Enter the source host MAC address here.

Parameter	Description
	<ul style="list-style-type: none"> • MAC - The Wildcard option will 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:</p> <ul style="list-style-type: none"> • Any - Any destination traffic will be evaluated according to the conditions of this rule. • Host - Enter the destination host MAC address here. • MAC - The Wildcard option will be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	<p>Select the Ethernet type option here. Options to choose from are aarp, appletalk, decent-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, and arp.</p>
Ethernet Type	<p>Enter the Ethernet type hexadecimal value here. The range is from 0x0 to 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.</p>
Ethernet Type Mask	<p>Enter the Ethernet type mask hexadecimal value here. The range is from 0x0 to 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.</p>
CoS	<p>Select the CoS value that will be used here. The range is from 0 to 7.</p> <ul style="list-style-type: none"> • Mask - Enter the CoS mask value here. The range is from 0x0 to 0x7.
VID	<p>Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.</p> <ul style="list-style-type: none"> • Mask - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFFF.
VLAN Range	<p>Select and enter the VLAN range that will be associated with this ACL rule here. Enter the starting and ending VLANs in the spaces provided. The range is from 1 to 4094.</p>
Time Range	<p>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.</p>

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:

Port	In			Out		
	IP ACL	IPv6 ACL	MAC ACL	IP ACL	IPv6 ACL	MAC ACL
eth1/0/1						
eth1/0/2						
eth1/0/3						
eth1/0/4						
eth1/0/5						
eth1/0/6						
eth1/0/7						
eth1/0/8						
eth1/0/9						
eth1/0/10						

Figure 8-18 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
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:

ID	ACL Name	ACL Type
1	S-IP4-ACL	Standard IP ACL
2000	E-IP4-ACL	Extended IP ACL

Figure 8-19 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.

9. Security

Port Security

802.1X

AAA

RADIUS

IMPB

DHCP Server Screening

ARP Spoofing Prevention

Network Access Authentication

Safeguard Engine

Trusted Host

Traffic Segmentation Settings

Storm Control Settings

DoS Attack Prevention Settings

SSH

SSL

Network Protocol Port Protect 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:

Figure 9-1 Port Security Global Settings Window

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

Parameter	Description
Trap State	Select to enable or disable port security traps on the Switch.

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

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

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. By default, this value is 31. This indicates that an SNMP trap is generated for every security violation.

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

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

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. The range is from 1 to 1792. By default, there is no limit. Tick the No Limit checkbox to allow the maximum number of secure MAC address.

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

Port Security Port Settings

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

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

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
eth1/0/9	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/10	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
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. The range is from 0 to 64. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> • Protect - Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. • Restrict - Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. • Shutdown - Specifies to shut down the port if there is a security violation and record the system log.
Security Mode	Select the security mode option here. Options to choose from are: <ul style="list-style-type: none"> • Permanent - Specifies that under this mode, all learned MAC addresses are not be purged out unless the user manually deletes those entries.

Parameter	Description
	<ul style="list-style-type: none"> Delete-on-Timeout - Specifies that under this mode, all learned MAC addresses are purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. The range is from 0 to 1440 minutes.
Aging Type	Select the aging type here. Options to choose from are: <ul style="list-style-type: none"> 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. 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. By default, the Absolute option is used.

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
Port	Select the appropriate port range used for the configuration here.
MAC Address	Enter the MAC address here. Select Permanent to specify that all learned MAC addresses are purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID here. The range is from 1 to 4094.

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

Click the **Delete** button to remove a new entry based on the information entered.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

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

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

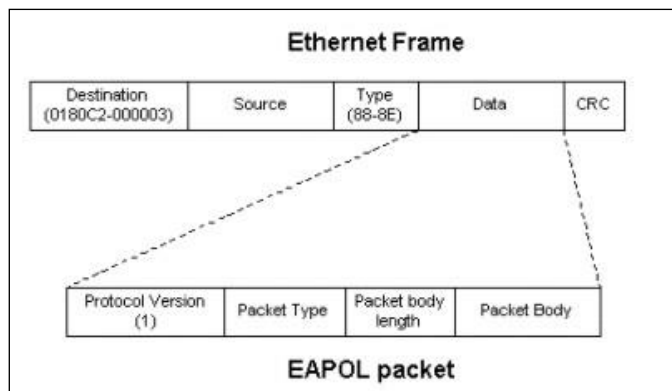


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

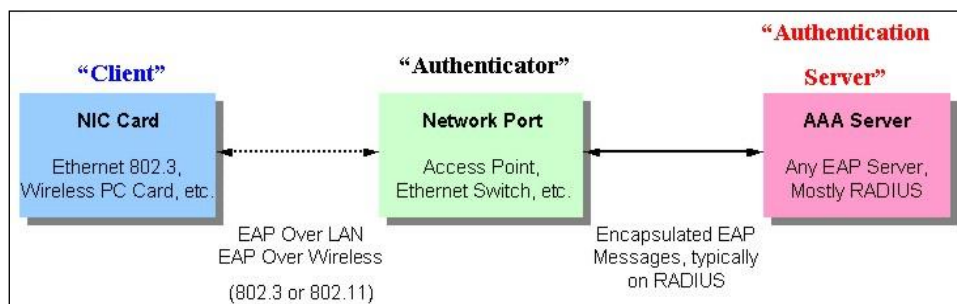


Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or Switches services.

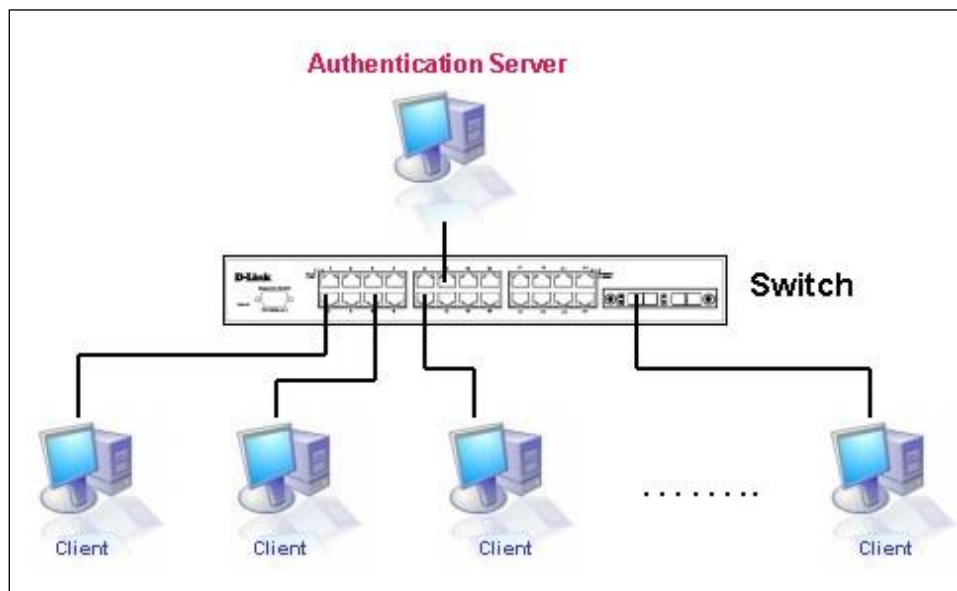


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

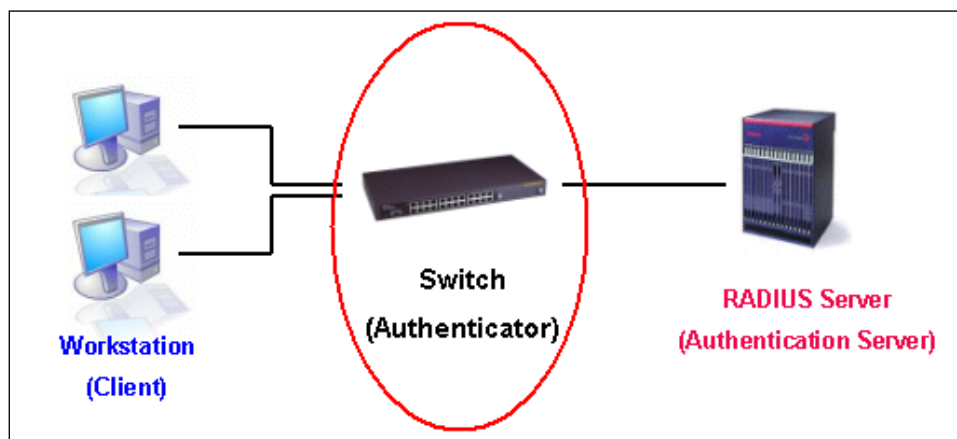


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X State must be Enabled. (**Security > 802.1X > 802.1X Global Settings**)
- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or Switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows 7 and later, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

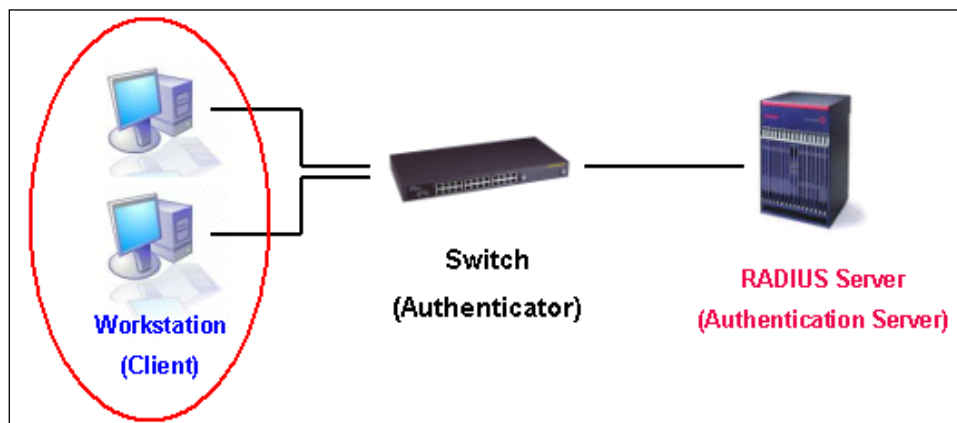


Figure 9-8 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is "locked" until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully "unlocks" the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a detailed explanation of how the authentication process is completed between the three roles stated above.

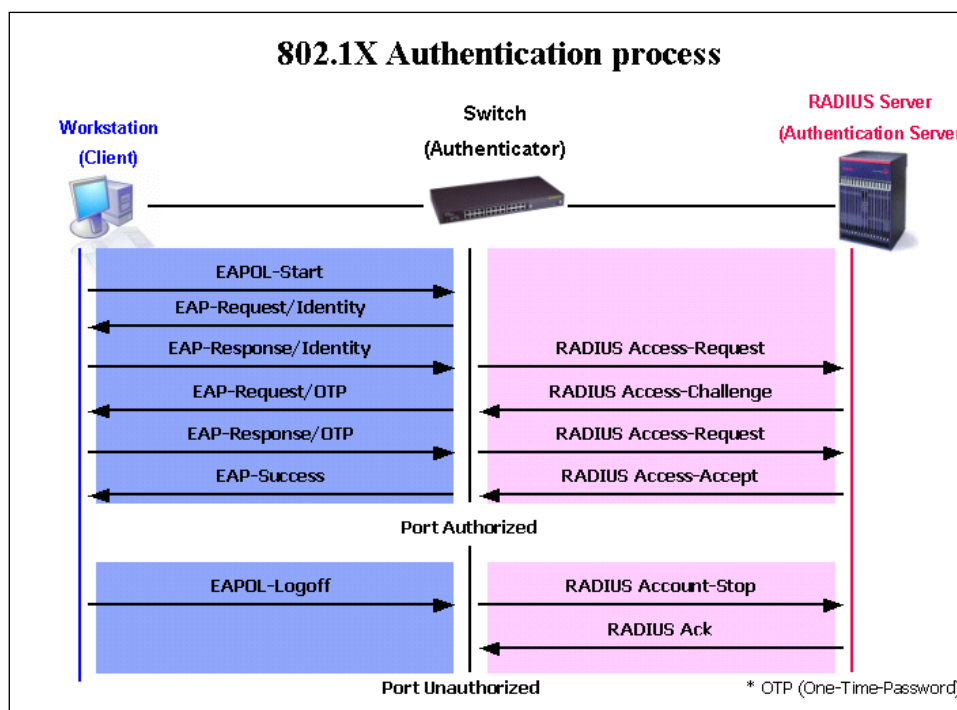


Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **Port-based Access Control** - This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
- **Host-based Access Control** - Using this method, the Switch will automatically learn up to a maximum of 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

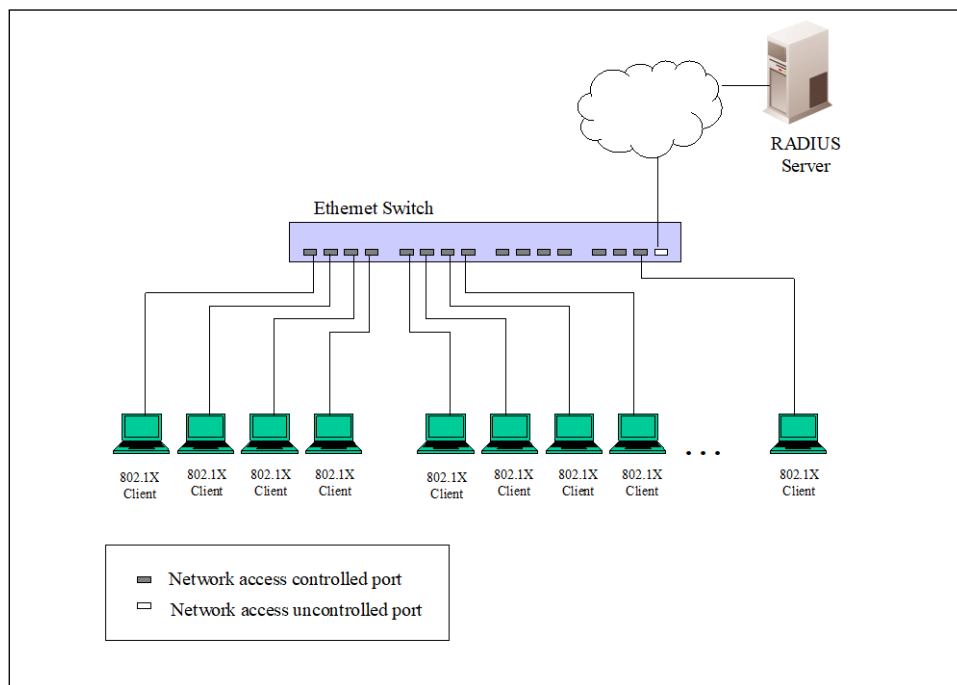


Figure 9-10 Example of Typical Port-based Configuration

Host-based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create "logical" Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices' individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

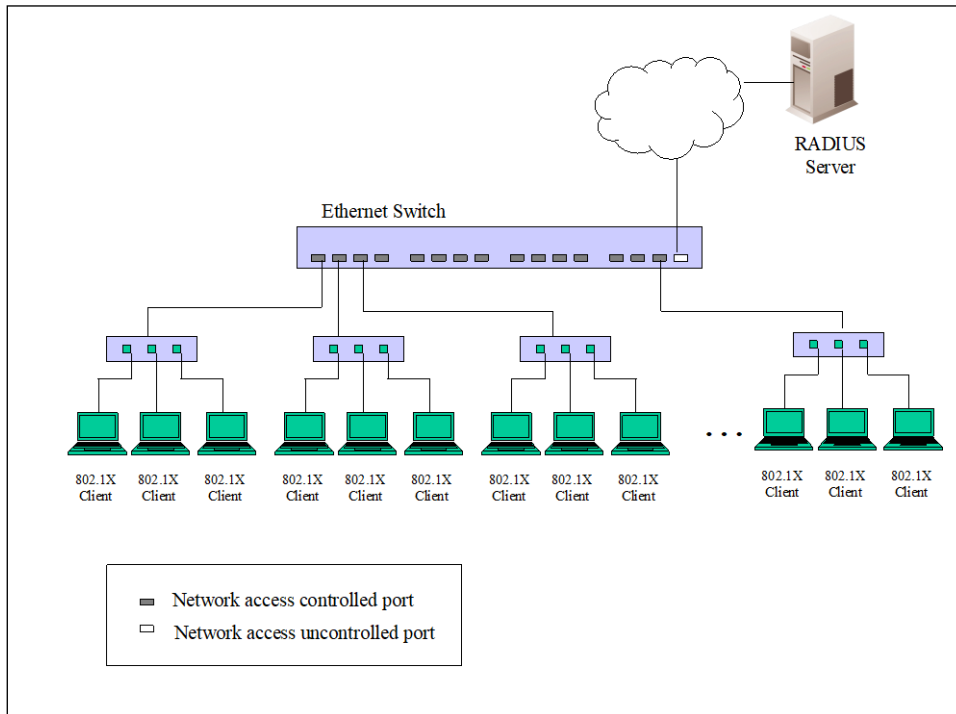


Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to display and configure the global 802.1X settings.

To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:

The screenshot shows the '802.1X Global Settings' window. It contains two settings: '802.1X State' and '802.1X Trap State', both set to 'Disabled'. An 'Apply' button is visible in the bottom right corner.

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:

The screenshot shows the '802.1X Port Settings' window. It contains several configuration fields and a table of port settings.

Configuration Fields:

- 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
- Server Timeout (1-65535):** 30 sec
- Supplicant Timeout (1-65535):** 30 sec
- TX Period (1-65535):** 30 sec

Table of Port Settings:

Port	Direction	Port Control	Forward PDU	MaxReq	PAE Authenticator	Server Timeout	Supplicant Timeout	TX Period
eth1/0/1	Both	Auto	Disabled	2	None	30	30	30
eth1/0/2	Both	Auto	Disabled	2	None	30	30	30
eth1/0/3	Both	Auto	Disabled	2	None	30	30	30
eth1/0/4	Both	Auto	Disabled	2	None	30	30	30
eth1/0/5	Both	Auto	Disabled	2	None	30	30	30
eth1/0/6	Both	Auto	Disabled	2	None	30	30	30
eth1/0/7	Both	Auto	Disabled	2	None	30	30	30
eth1/0/8	Both	Auto	Disabled	2	None	30	30	30
eth1/0/9	Both	Auto	Disabled	2	None	30	30	30
eth1/0/10	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
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are Both and In . This option configures the direction of the traffic on a controlled port as unidirectional (In) or bidirectional (Both).
Port Control	Select the port control option here. Options to choose from are ForceAuthorized , Auto , and ForceUnauthorized . If the port control is set to force-authorized, then the port is not controlled in both directions. If the port control is set to automatic, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to force-unauthorized, then the access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. The range is from 1 to 10. By default, this value is 2. This option configures the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. The range is from 1 to 65535 seconds. By default, this value is 30 seconds.
Supplicant Timeout	Enter the supplicant timeout value here. The range is from 1 to 65535 seconds. By default, this value is 30 seconds.
TX Period	Enter the transmission period value here. The range is from 1 to 65535 seconds. By default, this value is 30 seconds.

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

Authentication Sessions Information

This window is used to display and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Sessions Information**, as shown below:

Figure 9-14 Authentication Sessions Information Window

The fields that can be configured are described below:

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

Click the **Init by Port** button to initiate the session information based on the port selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the port selections made.

Click the **Init by MAC** button to initiate the session information based on the MAC address.

Click the **ReAuth by MAC** button to re-authenticate the session information based on the MAC address.

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

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:

Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
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:

The screenshot shows the 'Authenticator Session Statistics' window. At the top, there is a title bar. Below it, the window content includes a 'Port' dropdown menu with 'eth1/0/1' selected. To the right of the dropdown are three buttons: 'Find', 'Clear Counters', and 'Clear All'. Below these buttons, it displays 'Total Entries: 0'. At the bottom of the window is a table with the following columns: Port, Octets RX, Octets TX, Frames RX, Frames TX, ID, Authentic Method, Time, Terminate Cause, and User Name.

Figure 9-16 Authenticator Session Statistics Window

The fields that can be configured are described below:

Parameter	Description
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 screenshot shows the 'Authenticator Diagnostics' window. At the top, there is a 'Port' dropdown menu set to 'eth1/0/1'. To the right are buttons for 'Find', 'Clear Counters', and 'Clear All'. Below this is a table with the following data:

Total Entries: 1	
Port	eth1/0/2
EntersConnecting	1
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

At the bottom right of the table, there is a pagination control showing '1/1' and a 'Go' button.

Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
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:

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.

Authentication Settings

This window is used to display and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings** and select the **AAA Authentication Network** tab, as shown below:

Figure 9-19 Authentication Settings Window

The fields that can be configured in **AAA Authentication 802.1X** are described below:

Parameter	Description
Status	Select to enable or disable the AAA 802.1X authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: <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.

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 9-20 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. The range is from 1 to 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries.</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.

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:

IPv4/IPv6 Address	Authentication Port	Timeout	Retransmit	Key
10.90.90.254	1812	5	2	*****

Figure 9-21 RADIUS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server IPv4 address here.
IPv6 Address	Enter the RADIUS server IPv6 address here.
Authentication Port	Enter the authentication port number used here. The range is from 0 to 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Retransmit	Enter the retransmit value used here. The range is from 0 to 20. By default, this value is 2. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. The range is from 1 to 255 seconds. By default, this value is 5 seconds.
Key Type	Select to use the Plain Text key type that will be used here.
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 254 characters long.

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

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

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:

RADIUS Group Server Settings

RADIUS Group Server Settings

Group Server Name: 32 chars

IPv4 Address: . . .

IPv6 Address: 2013::1

Add

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
radius	10.90.90.2...	-	-	-	-	-	-	-	-
server1	10.90.90.2...	-	-	-	-	-	-	-	-

Show Detail Delete

Figure 9-22 RADIUS Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

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

Click the **Show Detail** button to view and configure detailed settings for the RADIUS group server.

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

After clicking the **Show Detail** button, the following page will be available.

IPv4/IPv6 Address	
10.90.90.254	Delete

Back

Figure 9-23 RADIUS Group Server Settings (Detail) Window

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

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

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:

RADIUS Server Address	Authentication Port	State
10.90.90.254	1812	Up

1/1 < < 1 > >| Go

Parameter	Authentication Port
Round Trip Time	0
Access Requests	0
Access Accepts	0
Access Rejects	0
Access Challenges	0
Acct Request	NA
Acct Response	NA
Retransmissions	0
Malformed Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Figure 9-24 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.

IMPB

The IP network layer uses a four-byte address. The Ethernet link-layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port Binding (IMPB) is to restrict the access to a Switch to a number of authorized users. Authorized clients can access a Switch's port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the Switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

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

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:

DHCP Snooping Global Settings		
DHCP Snooping Global Settings		
DHCP Snooping	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Information Option Allow Untrusted	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Source MAC Verification	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Station Move Deny	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
<input type="button" value="Apply"/>		

Figure 9-25 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
eth1/0/9	No	No Limit	No Limit
eth1/0/10	No	No Limit	No Limit

Figure 9-26 DHCP Snooping Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. The range is from 0 to 1024. Tick the No Limit option to disable the function.
Rate Limit	Enter the rate limit value here. The range is from 1 to 300. Tick the No Limit option to disable the function.
Trusted	Select the trusted option here. Options to choose from are No and Yes . Ports connected to the DHCP server or to other Switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping 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 9-27 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the DHCP snooping VLAN setting here.

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

DHCP Snooping Database

This window is used to display and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:

Figure 9-28 DHCP Snooping Database Window

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

Parameter	Description
Write Delay	Enter the write delay time value here. The range is from 60 to 86400 seconds. By default, this value is 300 seconds.

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

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be stored to here. Only TFTP is available for selection. 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. Only TFTP is available for selection. 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 9-29 DHCP Snooping Binding Entry Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID of the DHCP snooping binding entry here. The range is from 1 to 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. The range is from 60 to 4294967295 seconds.

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

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

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

Dynamic ARP Inspection

ARP Access List

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

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:

The screenshot shows the 'ARP Access List' configuration window. At the top, there is a header 'ARP Access List'. Below it, there is a section for adding a new entry with a text input field labeled 'ARP Access List Name' containing '32 chars' and an 'Add' button. Underneath, a table displays 'Total Entries: 1'. The table has a header row with 'ARP Access List Name' and a data row with 'access-list'. To the right of the data row are 'Edit' and 'Delete' buttons.

Figure 9-30 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)' configuration window. It features several configuration fields: 'Action' (dropdown menu set to 'Permit'), 'IP' (dropdown menu set to 'Any'), and 'MAC' (dropdown menu set to 'Any'). There are also input fields for 'Sender IP', 'Sender IP Mask', 'Sender MAC' (containing '00-50-54-00-00-00'), and 'Sender MAC Mask' (containing 'FF-FF-FF-FF-FF-FF'). 'Back' and 'Apply' buttons are located at the bottom right. Below the form, a table displays 'Total Entries: 1'. The table has a header row with columns: 'Action', 'IP Type', 'Sender IP', 'Sender IP Mask', 'MAC Type', 'Sender MAC', and 'Sender MAC Mask'. The data row contains: 'Permit', 'Any', '-', '-', 'Any', '-', and '-'. A 'Delete' button is positioned to the right of the data row.

Figure 9-31 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 .

Parameter	Description
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:

ARP Inspection Settings

ARP Inspection Validation

Src-MAC Enabled Disabled

Dst-MAC Enabled Disabled

IP Enabled Disabled Apply

ARP Inspection VLAN Logging

Total Entries: 1

VID	ACL Logging	DHCP Logging	
1	Deny	Deny	Edit

1/1 < < 1 > > Go

ARP Inspection Filter

ARP Access List Name

VID List

Static ACL Add Delete

Total Entries: 1

VID	ARP Access List Name	Static ACL
1	access-list	No

1/1 < < 1 > > Go

Figure 9-32 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, response packets, and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.

Parameter	Description
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.

Click the **Edit** button to configure the ACL/DHCP logging actions.

The fields that can be configured in **ARP Inspection VLAN Logging** are described below:

Parameter	Description
ACL Logging	After clicking the Edit button, select the ACL logging action here. Options to choose from are Deny , Permit , All , and None .
DHCP Logging	After clicking the Edit button, select the DHCP logging action here. Options to choose from are Deny , Permit , All , and None .

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

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

The fields that can be configured in **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting Yes or No .

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

Click the **Delete** button to remove an entry based on the information entered.

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

ARP Inspection Port Settings

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

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:

Port	Trust State	Rate Limit (pps)	Burst Interval
eth1/0/1	Untrusted	15	1
eth1/0/2	Untrusted	15	1
eth1/0/3	Untrusted	15	1
eth1/0/4	Untrusted	15	1
eth1/0/5	Untrusted	15	1
eth1/0/6	Untrusted	15	1
eth1/0/7	Untrusted	15	1
eth1/0/8	Untrusted	15	1
eth1/0/9	Untrusted	15	1
eth1/0/10	Untrusted	15	1

Figure 9-33 ARP Inspection Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. The range is from 1 to 150 packets per seconds.
Burst Interval	Enter the burst interval value here. The range is from 1 to 15. Tick the None option to disable the option.
Trust State	Select to enable or disable the trust state here.

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

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

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

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:

Figure 9-34 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:

Figure 9-35 ARP Inspection Statistics Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Click the **Clear by VLAN** button to clear the information based on the VLAN ID(s) entered.

Click the **Clear All** button to clear all the information in this table.

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

ARP Inspection Log

This window is used to view, configure, and clear the ARP inspection log information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log**, as shown below:

Figure 9-36 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
Log Buffer	Enter the log buffer value used here. The range is from 1 to 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to display and configure the IP Source Guard (IPSG) port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:

Port	Validation Type
eth1/0/10	ip

Figure 9-37 IP Source Guard Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IPSG's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are: <ul style="list-style-type: none"> • IP - Specifies that the IP address of the received packets will be checked. • IP-MAC - Specifies that the IP address and the MAC address of the received packets will be checked.

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

IP Source Guard Binding

This window is used to display and configure the IPSG binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:

Figure 9-38 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.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IP Source Binding Entry** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	Select the type of binding entry to find here. Options to choose from are: <ul style="list-style-type: none"> All - Specifies that all the DHCP binding entries will be displayed. DHCP Snooping - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. Static - Specifies to display the IP-source guard binding entry that is manually configured.

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

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

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

IP Source Guard HW Entry

This window is used to view the IPSG hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:

Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
eth1/0/10	ip	Active	10.90.90.100	-	1

Figure 9-39 IP Source Guard HW Entry Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the query here.

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

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
eth1/0/7	Disabled
eth1/0/8	Disabled

Figure 9-40 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. By default, this is disabled.

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

The fields that can be configured in **IP-MAC-Port Binding Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are: <ul style="list-style-type: none"> • Disabled - Specifies that IP-MAC-Port binding function is disabled on the specified port(s). • Strict - When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IPSPG static binding entry or the DHCP snooping learned dynamic binding entry. • Loose - When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IPSPG 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 9-41 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.
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.

Parameter	Description
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 9-42 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 . By default, this is Permit .

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. The range is from 0 to 511. Tick the No Limit option to disable this option.
Protocol	Select the protocol state here. Options to choose from are: <ul style="list-style-type: none"> DHCP - Specifies that addresses should be snooped in DHCPv6 packets. NDP - Specifies that addresses should be snooped in NDP packets. DHCPv6 snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database. ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping

Parameter	Description
	<p>detects DAD messages (DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA)) to build its binding database.</p> <p>The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.</p>
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 9-43 IPv6 ND Inspection Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name used here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Host and Router . By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.
Validate Source-MAC	Select to enable or disable the validation of the source MAC address option here. When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

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

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 9-44 IPv6 RA Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are Host and Router . By default, the device's role is Host , which will block all the RA packets. If the device's role is Router , RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the Please Select button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

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

After clicking the **Please Select** button, the following window will appear:

Figure 9-45 ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

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

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

IPv6 DHCP Guard

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

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:

Figure 9-46 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.
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 9-47 ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

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

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

IPv6 Source Guard

IPv6 Source Guard Settings

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

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:

Figure 9-48 IPv6 Source Guard Settings Window

The fields that can be configured in **IPv6 Source Guard Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to permit 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. By default, this is Permit .
Link Local Traffic	Select to permit or deny hardware permitted data traffic sent by the link-local address. By default, this is Deny .

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

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

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

The fields that can be configured in **IPv6 Source Guard Attach Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Target Port	Select this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

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

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

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 9-49 IPv6 Neighbor Binding Window

The fields that can be configured in **IPv6 Neighbor Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address used here.
VID	Enter the VLAN ID used here. The range is from 1 to 4094.
IPv6 Address	Enter the IPv6 address used here.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IPv6 Neighbor Binding Entry** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

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

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

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 9-50 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. By default, this is disabled.

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

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

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.

Click the **Create** button to create a new profile.

Click the **Binding** button to configure the client MAC address in the profile.

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

Click the **Delete Profile** button to remove the specified profile.

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

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. The range is from 10 to 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

After clicking the **Binding** button, the following window will appear:

Figure 9-51 Bind Client MAC Address Window

The fields that can be configured are described below:

Parameter	Description
Client MAC	Enter the MAC address used here.

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

DHCP Server Screening Port Settings

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

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:

Figure 9-52 DHCP Server Screening Port Settings Window

The fields that can be configured are described below:

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

Parameter	Description
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:

The screenshot shows the ARP Spoofing Prevention configuration window. The configuration fields are as follows:

From Port	eth1/0/1	To Port	eth1/0/1
Gateway IP		Gateway MAC	00-11-22-33-44-aa

Below the configuration fields, there is a table showing the total entries:

Gateway IP	Gateway MAC	Port	
10.90.90.1	00-11-22-33-44-99	eth1/0/20	Delete

Figure 9-53 ARP Spoofing Prevention Window

The fields that can be configured in **ARP Spoofing Prevention** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway IP address used here.
Gateway MAC	Enter the gateway MAC address used here.

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

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

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 9-54 Guest VLAN Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. The range is from 1 to 4094.

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

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

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

Network Access Authentication Global Settings

This window is used to display and configure the global Network Access Authentication settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:

Figure 9-55 Network Access Authentication Global Settings Window

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

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. The range is from 1 to 1000. By default, this value is 1000.
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) assigned by the RADIUS server, will be accepted if the authorization status is enabled.

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

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

Parameter	Description
User Name	Enter the user name used here. This name can be up to 32 characters long.
VID	Enter the VLAN ID used here.
Password Type	Specifies that the password encryption type is Plain Text .
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	Max Users	Periodic	ReAuth	Restart
eth1/0/1	Multi Auth	1000	Disabled	3600	60
eth1/0/2	Multi Auth	1000	Disabled	3600	60
eth1/0/3	Multi Auth	1000	Disabled	3600	60
eth1/0/4	Multi Auth	1000	Disabled	3600	60
eth1/0/5	Multi Auth	1000	Disabled	3600	60
eth1/0/6	Multi Auth	1000	Disabled	3600	60
eth1/0/7	Multi Auth	1000	Disabled	3600	60
eth1/0/8	Multi Auth	1000	Disabled	3600	60
eth1/0/9	Multi Auth	1000	Disabled	3600	60
eth1/0/10	Multi Auth	1000	Disabled	3600	60

Figure 9-56 Network Access Authentication Port Settings Window

The fields that can be configured are described below:

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

Parameter	Description
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are: <ul style="list-style-type: none"> • Multi Host - If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. • Multi Auth - If the port is operated in the multi-authenticated mode, then each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access. <p>By default, this is Multi Auth.</p>
Max Users	Enter the maximum users value used here. The range is from 1 to 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol. By default, this is disabled.
ReAuth Timer	Enter the re-authentication timer value here. The range is from 1 to 65535 seconds. By default, this value is 3600 seconds.
Restart	Enter the restart time value used here. The range is from 1 to 65535 seconds. By default, this is 60 seconds.

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

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:

Network Access Authentication Sessions Information

Network Access Authentication Sessions Information

Port: eth1/0/1

MAC Address: 00-84-57-00-00-00

Protocol: DOT1X

Clear by Port Find

Clear by MAC Find

Clear by Protocol Find

Clear All Show All

Authentication Sessions Total

Total Authenticating Hosts	0
Total Authenticated Hosts	0
Total Blocked Hosts	0

Authentication Sessions Information

Total Entries: 0

Figure 9-57 Network Access Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port for the query here.
MAC Address	Enter the MAC address used here.
Protocol	Select the protocol option used here. The only option available is 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
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet

Protocol Name	Sub-interface (Group)	Description
TFTP	Manage	Trivial File Transfer Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's sub-interfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.



NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to display and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:

Figure 9-58 Safeguard Engine Settings Window

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

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.
Trap State	Select to enable or disable the safeguard engine trap state here.

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

Parameter	Description
Rising Threshold	Enter the rising threshold value here. The range is from 20% to 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. The range is from 20% to 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

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

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:

Figure 9-59 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:

Figure 9-60 CPU Protect Sub-Interface Window

The fields that can be configured in **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , and Route .
Rate Limit	Enter the rate limit value used here. The range is from 0 to 1024 packets per second. 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:

CPU Protect Type	
Protocol Name	dhcp
Rate Limit (0-1024)	
pps <input type="checkbox"/> No Limit <input type="button" value="Apply"/>	
Protect Type Information	
Type	dhcp
Rate Limit	612 pps
<input type="button" value="Find"/>	
Total	Drop
0	0

Figure 9-61 CPU Protect Type Window

The fields that can be configured in **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here.
Rate Limit	Enter the rate limit value used here. The range is from 0 to 1024 packets per second. 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
Type	Select the protocol type here. After selecting the protocol type, the Rate Limit assigned to the protocol type will be displayed.

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

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:

Trusted Host

Trusted Host

ACL Name Type

Note: The first character of ACL name must be a letter.

Total Entries: 1

Type	ACL Name	
Telnet	ACL	<input type="button" value="Delete"/>

Figure 9-62 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:

Traffic Segmentation Settings

Traffic Segmentation Settings

From Port To Port From Forward Port To Forward Port

Port	Forwarding Domain
eth1/0/20	eth1/0/22-1/0/23
eth1/0/21	eth1/0/22-1/0/23

Figure 9-63 Traffic Segmentation Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the receiving port range used for the configuration here.
From Forward Port ~ To Forward Port	Select the forward port range used for the configuration here.

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

Click the **Delete** button to remove an entry based on the information entered.

Storm Control Settings

This window is used to display and configure the storm control settings.

To view the following window, click **Security > Storm Control Settings**, as shown below:

Storm Control Settings

Storm Control Trap Settings

Trap State:

Storm Control Polling Settings

Polling Interval (5-600): sec Shutdown Retries (0-360): times Infinite

Storm Control Port Settings

From Port	To Port	Type	Action	Level Type	PPS Rise (0-2147483647)	PPS Low (0-2147483647)
<input type="text" value="eth1/0/1"/>	<input type="text" value="eth1/0/1"/>	<input type="text" value="Broadcast"/>	<input type="text" value="Drop"/>	<input type="text" value="PPS"/>	<input type="text"/>	<input type="text"/>

Total Entries: 84

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 9-64 Storm Control Settings Window

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

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are: <ul style="list-style-type: none"> • None - No traps are sent. • Storm Occur - A trap notification is sent when a storm event is detected. • Storm Clear - A trap notification is sent when a storm event is cleared. • Both - A trap notification is sent when a storm event is detected and cleared.

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

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Polling Interval	Enter the interval value used here. The range is from 5 to 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. The range is from 0 to 360. By default, this value is 3. Tick the Infinite option to disable this feature.

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

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

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are Broadcast , Multicast , and 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: <ul style="list-style-type: none"> • None - Specifies not to filter the storm packets. • Shutdown - Specifies to shut down the port when the value specified for rise threshold is reached. • Drop - Specifies to discards packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are PPS , Kbps , and Level .
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. The range is from 0 to 2147483647 packets per second.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. The range is from 0 to 2147483647 packets per second. By default, this is 80% of the specified PPS Rise value.

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

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.

The screenshot shows the 'Storm Control Port Settings' window with the following configuration:

- From Port:** eth1/0/1
- To Port:** eth1/0/1
- Type:** Broadcast
- Action:** Drop
- Level Type:** Kbps
- KBPS Rise (0-2147483647):** [Empty text box] Kbps
- KBPS Low (0-2147483647):** [Empty text box] Kbps
- Apply** button is visible.

Figure 9-65 Storm Control Settings (Level Type - Kbps) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 0 to 2147483647 Kbps.
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 0 to 2147483647 Kbps. By default, this is 80% of the specified KBPS Rise value.

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

After selecting the **Level** option as the **Level Type**, the following parameters are available.

The screenshot shows the 'Storm Control Port Settings' window. It contains several configuration fields: 'From Port' and 'To Port' are both set to 'eth1/0/1'; 'Type' is set to 'Broadcast'; 'Action' is set to 'Drop'; 'Level Type' is set to 'Level'; 'Level Rise (0-100)' and 'Level Low (0-100)' are both empty text boxes followed by a '%' sign; and an 'Apply' button is located at the bottom right.

Figure 9-66 Storm Control Settings (Level Type - Level) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 0% to 100%.
Level Low	Enter the low-level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 0% to 100%. By default, this is 80% of the Level Rise value.

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

DoS Attack Prevention Settings

This window is used to display and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types, which can be detected by most Switches:

Type of Attack	Description
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.

Type of Attack	Description
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 9-67 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 that allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

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

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

Figure 9-68 SSH Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IP SSH Server State	Select to enable or disable the global SSH server state.
IP SSH Service Port	Enter the SSH service port number used here. The range is from 1 to 65535. By default, this value is 22.
Authentication Timeout	Enter the authentication timeout value here. The range is from 30 to 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. The range is from 1 to 32. By default, this value is 3.

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

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:

Figure 9-69 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 RSA (Rivest Shamir Adleman) and DSA (Digital Signature Algorithm).
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 RSA (Rivest Shamir Adleman) and DSA (Digital Signature Algorithm).

After clicking the **Generate** button, the following window will appear:

Figure 9-70 Host Key (Generating) Window

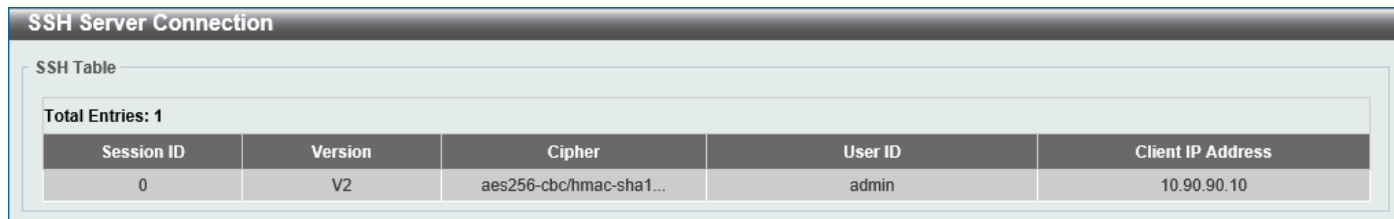
After the key was successfully generated, the following window will appear.

Figure 9-71 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:



The screenshot shows the 'SSH Server Connection' window. At the top, it says 'SSH Table' and 'Total Entries: 1'. Below this is a table with the following data:

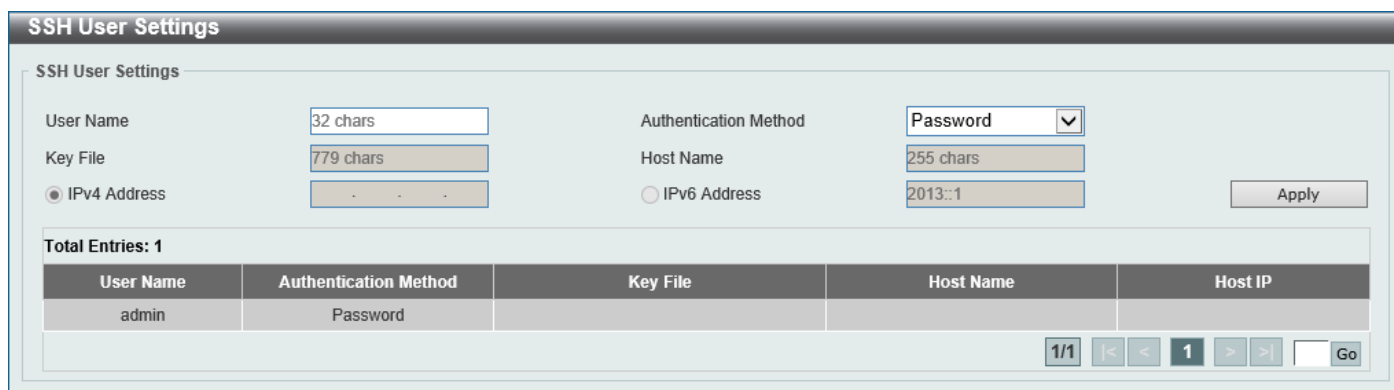
Session ID	Version	Cipher	User ID	Client IP Address
0	V2	aes256-cbc/hmac-sha1...	admin	10.90.90.10

Figure 9-72 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:



The screenshot shows the 'SSH User Settings' window. It contains several configuration fields:

- User Name: 32 chars
- Key File: 779 chars
- Authentication Method: Password (dropdown menu)
- Host Name: 255 chars
- IPv4 Address: (radio button selected)
- IPv6 Address: 2013::1

Below the fields is an 'Apply' button and a table showing the current settings:

User Name	Authentication Method	Key File	Host Name	Host IP
admin	Password			

At the bottom right, there is a pagination control showing '1/1' and a 'Go' button.

Figure 9-73 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 server and client through the use of authentication, digital signatures, and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms, and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and server as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
 - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys, and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
 - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) to create the encrypted text.
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function, which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA256.

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the client. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server or the Switch file system. The Switch supports TLS 1.0, TLS 1.1, and TLS 1.2. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to server.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web-based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https:// (Ex. https://xx.xx.xx.xx). Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

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

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:

Figure 9-74 SSL Global Settings Window

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

Parameter	Description
SSL Status	Select to enable or disable the global SSL status here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

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

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

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are Certificate and Private Key . After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the Browse button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

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

Click the **Generate** button in the **SSL-Self-signed Certificate** section to generate a new self-signed certificate, regardless if there is a built-in self-signed certificate or not. The certificate generated does not affect the user-downloaded certificates.



NOTE: The SSL self-signed certificate only supports self-signature RSA certificates with a key length of 2048 bits.

Crypto PKI Trustpoint

This window is used to display and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:

Figure 9-75 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server path here.
Type	Select the type of certificate that will be imported here. Options to choose from are: <ul style="list-style-type: none"> • Both - Specifies to import the CA certificate, local certificate, and key pairs. • CA - Specifies to import the CA certificate only. • Local - Specifies to import local certificate and key pairs only.

Click the **Apply** button to 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:

The screenshot shows the 'SSL Service Policy' configuration window. It includes the following fields and options:

- Policy Name:** 32 chars
- Version:**
 - TLS 1.0
 - TLS 1.1
 - TLS 1.2
- Session Cache Timeout (60-86400):** 600 sec
- Secure Trustpoint:** 32 chars
- Cipher Suites:**
 - DHE_DSS_WITH_3DES_EDE_CBC_SHA
 - RSA_WITH_3DES_EDE_CBC_SHA
 - RSA_WITH_RC4_128_SHA
 - RSA_EXPORT_WITH_RC4_40_MD5
 - RSA_WITH_RC4_128_MD5
 - RSA_WITH_AES_128_CBC_SHA
 - RSA_WITH_AES_256_CBC_SHA
 - RSA_WITH_AES_128_CBC_SHA256
 - RSA_WITH_AES_256_CBC_SHA256
 - DHE_DSS_WITH_AES_256_CBC_SHA
 - DHE_RSA_WITH_AES_256_CBC_SHA

At the bottom, there is a table with the following data:

Total Entries: 1					
Policy Name	Version	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint	
Policy	TLS 1.2	RSA_WITH_AES_256_CBC...	600	Trustpoint	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure 9-76 SSL Service Policy Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the SSL service policy name here. This name can be up to 32 characters long.
Version	Select the Transport Layer Security (TLS) version here. Options to choose from are TLS 1.0 , TLS 1.1 , and TLS 1.2 .
Session Cache Timeout	Enter the session cache timeout value used here. The range is from 60 to 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust point name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

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

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

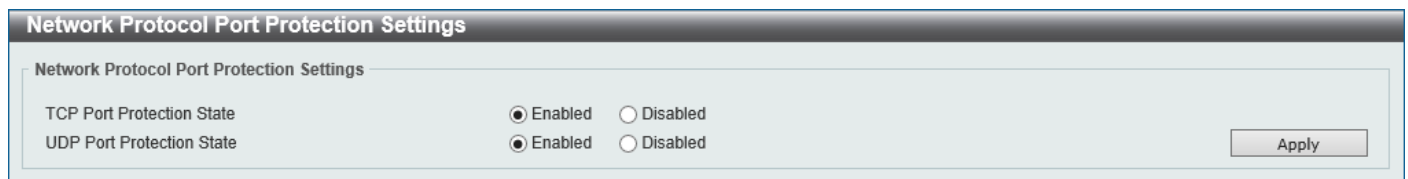
Click the **Edit** button to re-configure the specific entry.

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

Network Protocol Port Protect Settings

This window is used to display and configure the network protocol port protection settings.

To view the following window, click **Security > Network Protocol Port Protect Settings**, as shown below:



The screenshot shows a web interface window titled "Network Protocol Port Protection Settings". Inside the window, there are two rows of settings. The first row is "TCP Port Protection State" with radio buttons for "Enabled" (selected) and "Disabled". The second row is "UDP Port Protection State" with radio buttons for "Enabled" (selected) and "Disabled". An "Apply" button is located on the right side of the window.

Figure 9-77 Network Protocol Port Protect Settings Window

The fields that can be configured are described below:

Parameter	Description
TCP Port Protect State	Select to enable or disable the TCP port network protocol protection function here.
UDP Port Protect State	Select to enable or disable the UDP port network protocol protection function here.

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

10. OAM

Cable Diagnostics

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:

Port	Type	Link Status	Test Result	Cable Length (M)	
eth1/0/1	10GBASE-T	Link Up	Pair 1 Short at 2M	-	Clear
			Pair 2 Ok at 0M	-	
			Pair 3 Ok at 0M	-	
			Pair 4 Short at 1M	-	
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 Down	-	-	Clear
eth1/0/6	10GBASE-T	Link Down	-	-	Clear
eth1/0/7	10GBASE-T	Link Down	-	-	Clear
eth1/0/8	10GBASE-T	Link Down	-	-	Clear

Figure 10-1 Cable Diagnostics Window

The fields that can be configured are described below:

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

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.



NOTE: For more accurate test results, use the TIA/EIA-568B pin assignment on the RJ45 connectors.

Fault messages:

- **Open:** The cable in the error pair does not have a connection at the specified position.
- **Short:** The cable in the error pair has a short at the specified position.
- **Open or Short:** The cable has an open or a short problem, but the PHY has no capability to distinguish between them.
- **Crosstalk:** The cable in the error pair has a crosstalk problem at the specified position.
- **Shutdown:** The remote partner is powered off.
- **Unknown:** The test got an unknown status.
- **No cable:** The port does not have a cable connection to the remote partner.

11. Monitoring

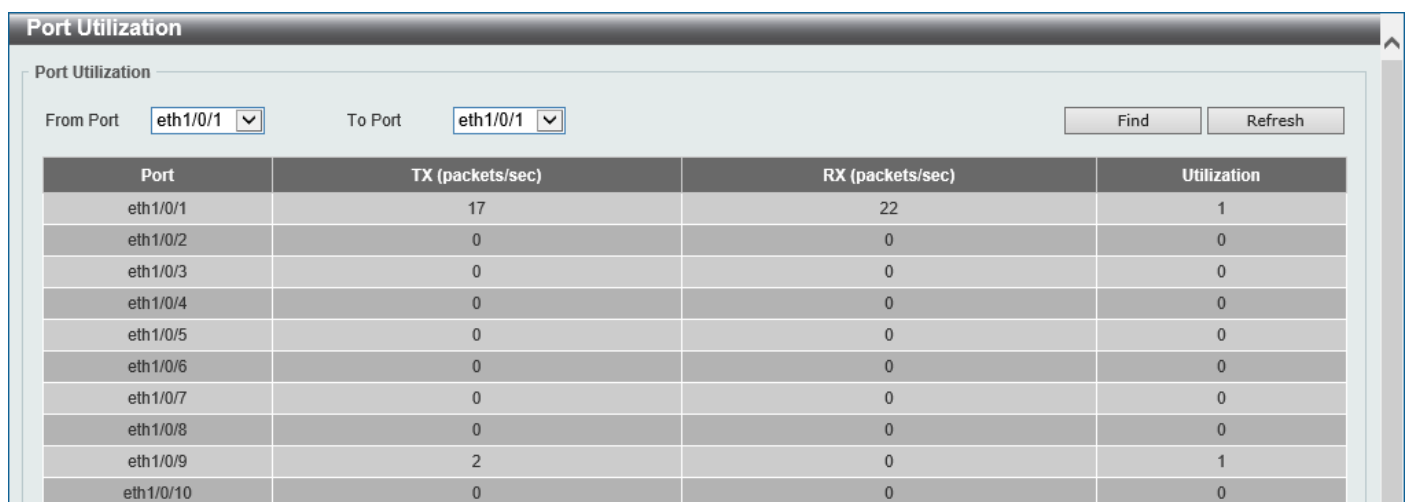
[Utilization](#)
[Statistics](#)
[Mirror Settings](#)
[Device Environment](#)

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 with the following data:

Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	17	22	1
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth1/0/4	0	0	0
eth1/0/5	0	0	0
eth1/0/6	0	0	0
eth1/0/7	0	0	0
eth1/0/8	0	0	0
eth1/0/9	2	0	1
eth1/0/10	0	0	0

Figure 11-1 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used 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	RX				TX				Show Detail
	Rate		Total		Rate		Total		
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets	
eth1/0/1	123	2	2972702	20806	0	0	4087203	7619	Show Detail
eth1/0/2	0	0	0	0	0	0	0	0	Show Detail
eth1/0/3	0	0	0	0	0	0	0	0	Show Detail
eth1/0/4	0	0	0	0	0	0	0	0	Show Detail
eth1/0/5	0	0	0	0	0	0	0	0	Show Detail
eth1/0/6	0	0	0	0	0	0	0	0	Show Detail
eth1/0/7	0	0	0	0	0	0	0	0	Show Detail
eth1/0/8	0	0	0	0	0	0	0	0	Show Detail
eth1/0/9	0	0	144157	888	123	2	1651816	13667	Show Detail
eth1/0/10	0	0	0	0	0	0	0	0	Show Detail

Figure 11-2 Port Window

The fields that can be configured are described below:

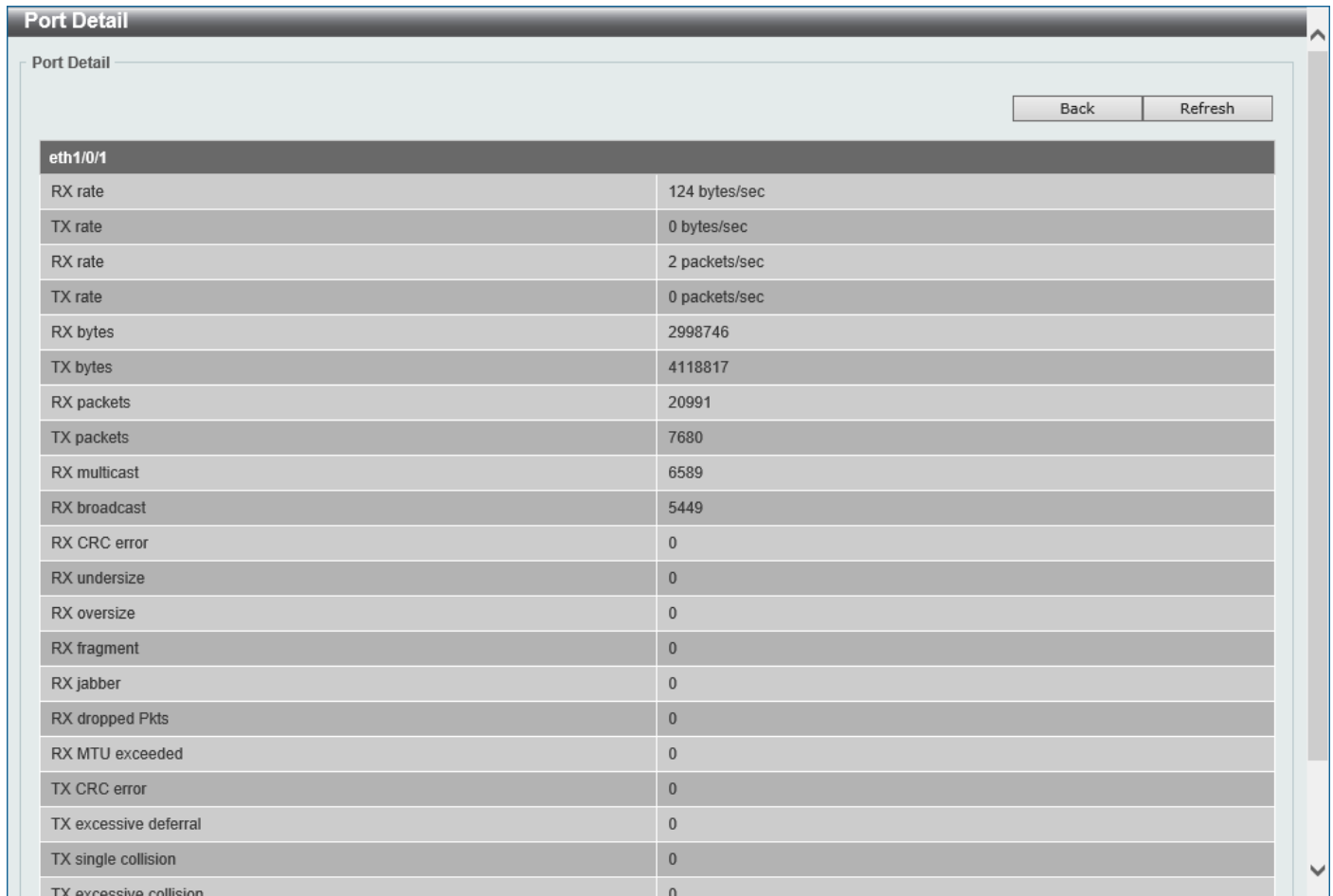
Parameter	Description
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Detail** button to view detailed statistics information on the specified port.

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



The screenshot shows a window titled "Port Detail" with a "Back" and "Refresh" button. Below the buttons is a table of statistics for the port "eth1/0/1".

eth1/0/1	
RX rate	124 bytes/sec
TX rate	0 bytes/sec
RX rate	2 packets/sec
TX rate	0 packets/sec
RX bytes	2998746
TX bytes	4118817
RX packets	20991
TX packets	7680
RX multicast	6589
RX broadcast	5449
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	0
RX MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0

Figure 11-3 Port (Show Detail) Window

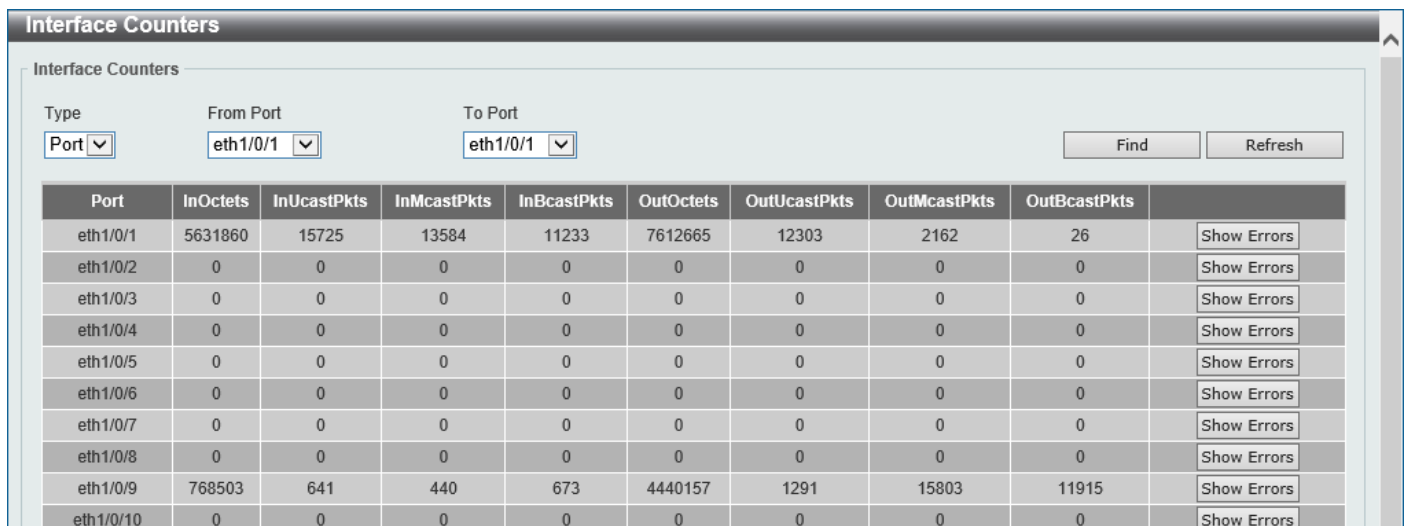
Click the **Back** button to return to the previous window.

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:



The screenshot shows a window titled "Interface Counters" with filters for "Type" (Port), "From Port" (eth1/0/1), and "To Port" (eth1/0/1). Below the filters is a table of interface statistics.

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	Show Errors
eth1/0/1	5631860	15725	13584	11233	7612665	12303	2162	26	Show Errors
eth1/0/2	0	0	0	0	0	0	0	0	Show Errors
eth1/0/3	0	0	0	0	0	0	0	0	Show Errors
eth1/0/4	0	0	0	0	0	0	0	0	Show Errors
eth1/0/5	0	0	0	0	0	0	0	0	Show Errors
eth1/0/6	0	0	0	0	0	0	0	0	Show Errors
eth1/0/7	0	0	0	0	0	0	0	0	Show Errors
eth1/0/8	0	0	0	0	0	0	0	0	Show Errors
eth1/0/9	768503	641	440	673	4440157	1291	15803	11915	Show Errors
eth1/0/10	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. The only option available here is Port .
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 detailed error information on the specified port.

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

eth1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Undersize	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Excess-Col	0
Multi-Col	0
Carri-Sen	0
Late-Col	0
Runts	0
Giants	0
DeferredTx	0
Symbol-Err	0
IntMacTx	0
SQETest-Err	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	3	Show Detail
eth1/0/2	0	Show Detail
eth1/0/3	0	Show Detail
eth1/0/4	0	Show Detail
eth1/0/5	0	Show Detail
eth1/0/6	0	Show Detail
eth1/0/7	0	Show Detail
eth1/0/8	0	Show Detail
eth1/0/9	1	Show Detail
eth1/0/10	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. The only option available here is Port .
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 detailed counter information on the specified port.

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

eth1/0/1 Counters	
rxHCTotalPkts	41288
txHCTotalPkts	14790
rxHCUnicastPkts	16038
txHCUnicastPkts	12553
rxHCMulticastPkts	13827
txHCMulticastPkts	2211
rxHCBroadcastPkts	11423
txHCBroadcastPkts	26
rxHCOctets	5739643
txHCOctets	7769448
rxHCPk64Octets	33392
rxHCPk65to127Octets	531
rxHCPk128to255Octets	1008
rxHCPk256to511Octets	3309
rxHCPk512to1023Octets	3048
rxHCPk1024to1518Octets	0
rxHCPk1519to1522Octets	0
rxHCPk1519to2047Octets	0
rxHCPk2048to4095Octets	0
rxHCPk4096to9216Octets	0
rxHCPk9217to16383Octets	0

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:

Figure 11-8 Mirror Settings Window

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

Parameter	Description
Session Number	Select the mirror session number for this entry here. The range is from 1 to 4.
Destination	Select the checkbox to configure the destination for this port mirror entry. <ul style="list-style-type: none"> • Type - Select Port here. • Port - Select the destination port for this configuration here.
Source	Select the checkbox to configure the source for this port mirror entry. <ul style="list-style-type: none"> • Port - Select Port here. • From Port - To Port - Select the source port(s) for this configuration here. • Frame Type - Select the frame type here. Options to choose from are Both, RX (received data), and TX (transmitted data).

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

The fields that can be configured for **Mirror Session Table** are described below:

Parameter	Description
Mirror Session Type	Select the mirror session type of information that will be displayed from the drop-down menu. Options to choose from are: <ul style="list-style-type: none"> • All Session - Specifies to display all mirror sessions in the table. • Session Number - Specifies to display only the specified mirror session in the table. Select the mirror session number here. The range is from 1 to 4.

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

Click the **Show Detail** button to view detailed information about the mirror session.

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

Mirror Session Detail	
Mirror Session Detail	
Session Number	1
Session Type	Local Session
Both Port	eth1/0/5-eth1/0/6
RX Port	
TX Port	
Destination Port	eth1/0/4

Figure 11-9 Mirror Settings (Show Detail) Window

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

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	
Temperature Description/ID	Current/Threshold Range
Central Temperature /1	42C/11~79C
Status code: * temperature is out of threshold range	
Detail Fan Status	
Items	Status
Right Fan 1	(OK)
Right Fan 2	(OK)
Detail Power Status	
Power Module	Power Status
Power 1	In-operation

Figure 11-10 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** and select the **Power Saving Global Settings** tab, 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 to enable or disable the link detection state. When enabled, a port, which has a link down status, will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Scheduled Port-shutdown Power Saving	Select to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Hibernation Power Saving	Select to enable or disable the scheduled hibernation power saving function here.
Scheduled Dim-LED Power Saving	Select to enable or disable applying the power saving by scheduled dimming LEDs.
Administrative Dim-LED	Select to enable or disable the port LED function.

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

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

Parameter	Description
Type	Select the type of power saving. Options to choose from are Dim-LED and Hibernation .
Time Range	Enter the name of the time range to associate with the power saving type.

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

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

To view the following window, select the **Power Saving Shutdown Settings** tab, as shown below:

Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
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 time range from the specified port.

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
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of this feature here.

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

13. Toolbar

[Save](#)
[Tools](#)
[Wizard](#)
[Online Help](#)
[Surveillance Mode](#)
[Logout](#)

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

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

The screenshot shows a web interface window titled "Save Configuration". Inside the window, there is a section labeled "Save Configuration" with a "File Path" dropdown menu set to "startup-config" and an "Apply" button on the right.

Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
File Path	Select the destination where the configuration will be saved here. Options to choose from are startup-config , Configuration 1 , and Configuration 2 .

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

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

The screenshot shows a web interface window titled "Firmware Upgrade from HTTP". It features a "Source File" input field with a "Browse..." button, a "Destination File" dropdown menu set to "Image 1", and an "Upgrade" button at the bottom.

Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button and navigate to the firmware file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are Image 1 and Image 2 .

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware 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
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. • IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the firmware file on the TFTP server here. This will be uploaded to the Switch. This field can be up to 64 characters long.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are Image 1 and Image 2 .

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Figure 13-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the firmware on the Switch that will be backed up to the local PC here. Options to choose from are Image 1 and Image 2 .

Click the **Backup** button to initiate the firmware backup.

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
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Select the firmware file on the Switch that will be backed up to the TFTP server here. Options to choose from are Image 1 and Image 2 .
Destination File	Enter the filename and path of the firmware file that will be stored on the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 13-6 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button and navigate to the configuration file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: <ul style="list-style-type: none"> • Configuration 1 - Select this option to use configuration 1 as the destination. • Configuration 2 - Select this option to use configuration 2 as the destination. • running-config - Select this option to use the running configuration as the destination. • startup-config - Select this option to use the start-up configuration as the destination.
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

Figure 13-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. • IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the configuration file on the TFTP server here. This will be uploaded to the Switch. This field can be up to 64 characters long.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: <ul style="list-style-type: none"> • Configuration 1 - Select this option to use configuration 1 as the destination. • Configuration 2 - Select this option to use configuration 2 as the destination. • running-config - Select this option to use the running configuration as the destination. • startup-config - Select this option to use the start-up configuration as the destination.

Parameter	Description
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 13-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the configuration on the Switch that will be backed up to the local PC here. Options to choose from are: <ul style="list-style-type: none"> • Configuration 1 - Select this option to backup configuration 1. • Configuration 2 - Select this option to backup configuration 2. • running-config - Select this option to backup the running configuration. • startup-config - Select this option to backup the start-up configuration.

Click the **Backup** button to initiate the configuration file backup.

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
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. • IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.

Parameter	Description
Source File	Select the configuration on the Switch that will be backed up to the TFTP server here. Options to choose from are: <ul style="list-style-type: none"> • Configuration 1 - Select this option to backup configuration 1. • Configuration 2 - Select this option to backup configuration 2. • running-config - Select this option to backup the running configuration. • startup-config - Select this option to backup the start-up configuration.
Destination File	Enter the filename and path of the configuration file that will be stored on the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Certificate & Key Restore & Backup

Certificate & Key Restore from HTTP

This window is used to initiate a certificate and key restore from a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP**, as shown below:

Figure 13-10 Certificate & Key Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button and navigate to the certificate and key file on the local PC here. This will be uploaded to the Switch.
Destination File	Enter the filename and path of the certificate and key file that will be stored on the Switch here. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from TFTP

This window is used to initiate a certificate and key restore from a TFTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP**, as shown below:

Figure 13-11 Certificate & Key Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. • IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the certificate and key file on the TFTP server here. This will be uploaded to the Switch. This field can be up to 64 characters long.
Destination File	Enter the filename and path of the certificate and key file that will be stored on the Switch here. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Public Key Backup to HTTP

This window is used to initiate a certificate and key backup to a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to HTTP**, as shown below:

Figure 13-12 Public Key Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the filename and path of the certificate and key file on the Switch here. This will be downloaded to the local PC using HTTP. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Public Key Backup to TFTP

This window is used to initiate a certificate and key backup to a TFTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to TFTP**, as shown below:

Figure 13-13 Public Key Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. • IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the certificate and key file on the Switch here. This will be downloaded to the TFTP server. This field can be up to 64 characters long.
Destination File	Enter the filename and path of the certificate and key file that will be stored on the TFTP sever here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

Figure 13-14 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	Select the log type on the Switch that will be backed up to the local PC here. Options to choose from are System Log and Attack Log .

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 13-15 Log Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. <ul style="list-style-type: none"> • IPv4 - Specifies to select and enter the IPv4 address of the TFTP server. • IPv6 - Specifies to select and enter the IPv6 address of the TFTP server.
Destination File	Enter the filename and path of the log file that will be stored on the TFTP sever here. This field can be up to 64 characters long.
Log Type	Select the log type on the Switch that will be backed up to the TFTP server here. Options to choose from are System Log and Attack Log .

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:

The screenshot shows the 'Ping' configuration window. It is divided into two main sections: 'IPv4 Ping' and 'IPv6 Ping'. Each section contains the following fields and controls:

- Target IPv4/IPv6 Address:** A radio button is selected, followed by an input field.
- Domain Name:** A radio button is unselected, followed by an input field labeled '255 chars'.
- Ping Times (1-255):** An input field with a '255' value and a checked 'Infinite' checkbox.
- Timeout (1-99):** An input field with a '1' value and the unit 'sec'.
- Source IPv4/IPv6 Address:** An input field.
- Start:** A button located at the bottom right of each section.

Figure 13-16 Ping Window

The fields that can be configured in **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. The range is from 1 to 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select the timeout period here. The range is from 1 to 99 seconds. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Source IPv4 Address	Enter the source IPv4 address. If the current Switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address

Parameter	Description
	will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the **Start** button to initiate the Ping Test for each individual section.

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

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. The range is from 1 to 255. Tick the Infinite check box to keep sending ICMPv6 Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select the timeout period here. The range is from 1 to 99 seconds. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
Source IPv6 Address	Enter the source IPv6 address. If the current Switch has more than one IPv6 address, you can enter one of them to this field. When entered, this IPv6 address will be used as the packets' source IPv6 address sent to the remote host, or as primary IPv6 address.

Click the **Start** button to initiate the Ping Test for each individual section.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

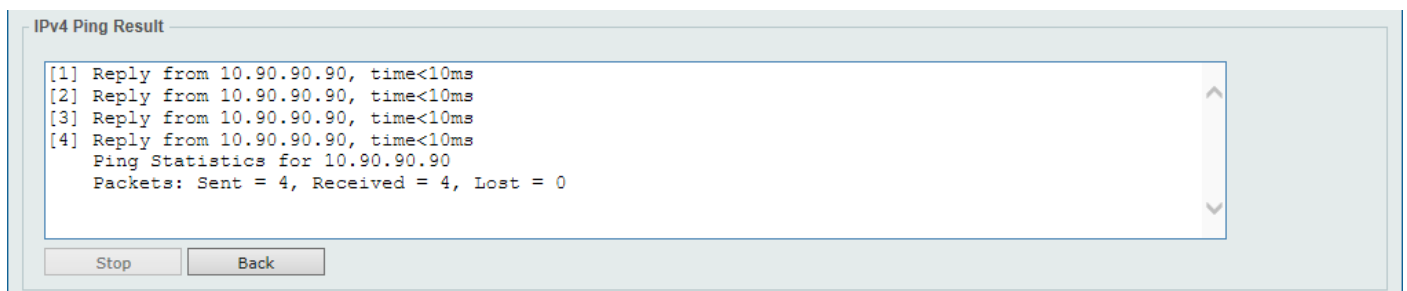


Figure 13-17 Ping (Start) Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

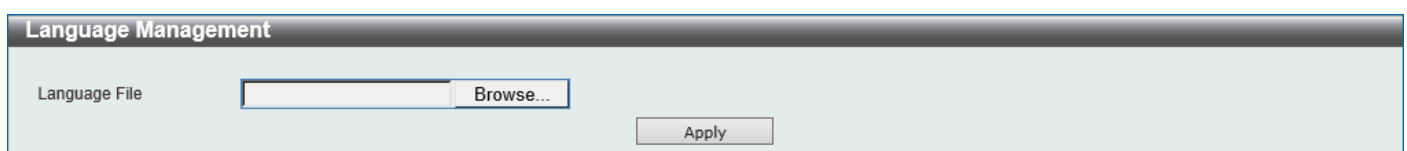


Figure 13-18 Language Management Window

The fields that can be configured are described below:

Parameter	Description
Language File	Click the Browse button and navigate to the language pack file on the local PC here. This file will be uploaded to the Switch.

Click the **Apply** button to initiate the language pack upload and installation.

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 13-19 Reset Window

Select one of the following options:

- Reset to factory default settings, save, and then reboot.
- Reset to factory default settings, save, and then reboot. This option excludes the IP address.
- Reset to factory default settings and do not reboot.

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:

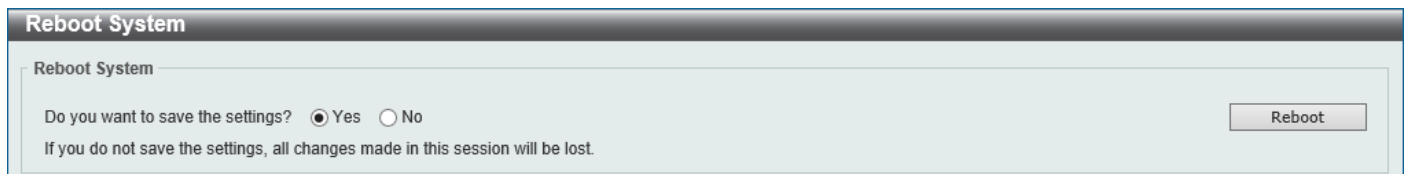


Figure 13-20 Reboot System Window

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.

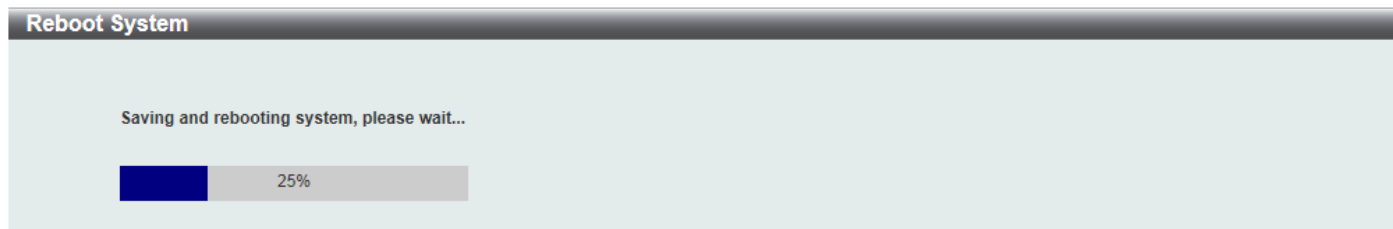


Figure 13-21 Reboot System (Rebooting) Window

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 3.

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Surveillance Mode

Click this option to change the Web UI mode and style from the **Standard Mode** to the **Surveillance Mode**. An unsuccessful change will display a warning message.



NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

After clicking the **Surveillance Mode** option in the **Toolbar**, the following window will appear.

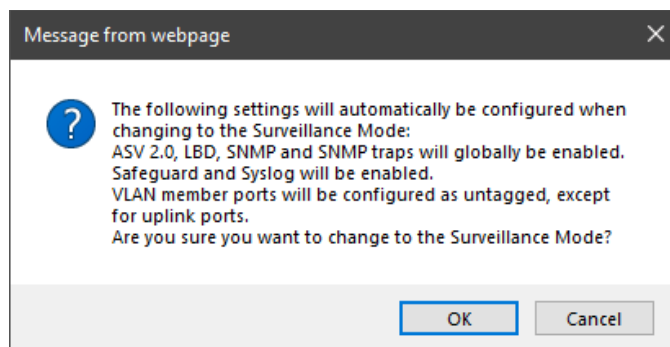


Figure 13-22 Surveillance Mode Confirmation Message

The window above displays a message that the abovementioned configurations need to be changed when access to the Surveillance Mode is given.

Click the **OK** button to continue.

Click the **Cancel** button to return to the **Standard Mode**.

After successfully switching to the Surveillance Mode on the Web UI of the Switch, the following window will appear.

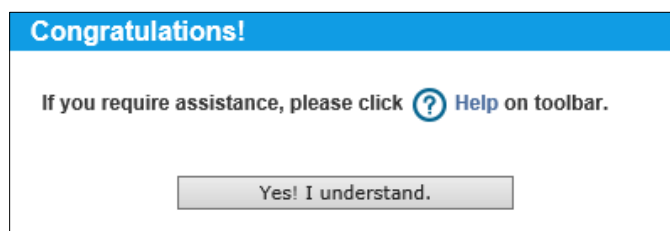


Figure 13-23 Surveillance Mode 'Congratulations' Message

Click the **Yes! I understand** button to continue.

Logout

Click this option to log out of the Web UI of the Switch

14. Surveillance Mode

[Surveillance Overview](#)
[Port Information](#)
[IP-Camera Information](#)
[NVR Information](#)
[Management](#)
[Time](#)
[Surveillance Settings](#)
[Surveillance Log](#)
[Health Diagnostic](#)
[Toolbar](#)

Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device.

To return to the Surveillance Overview window after viewing other windows, click the **DXS-1210-28T** link.

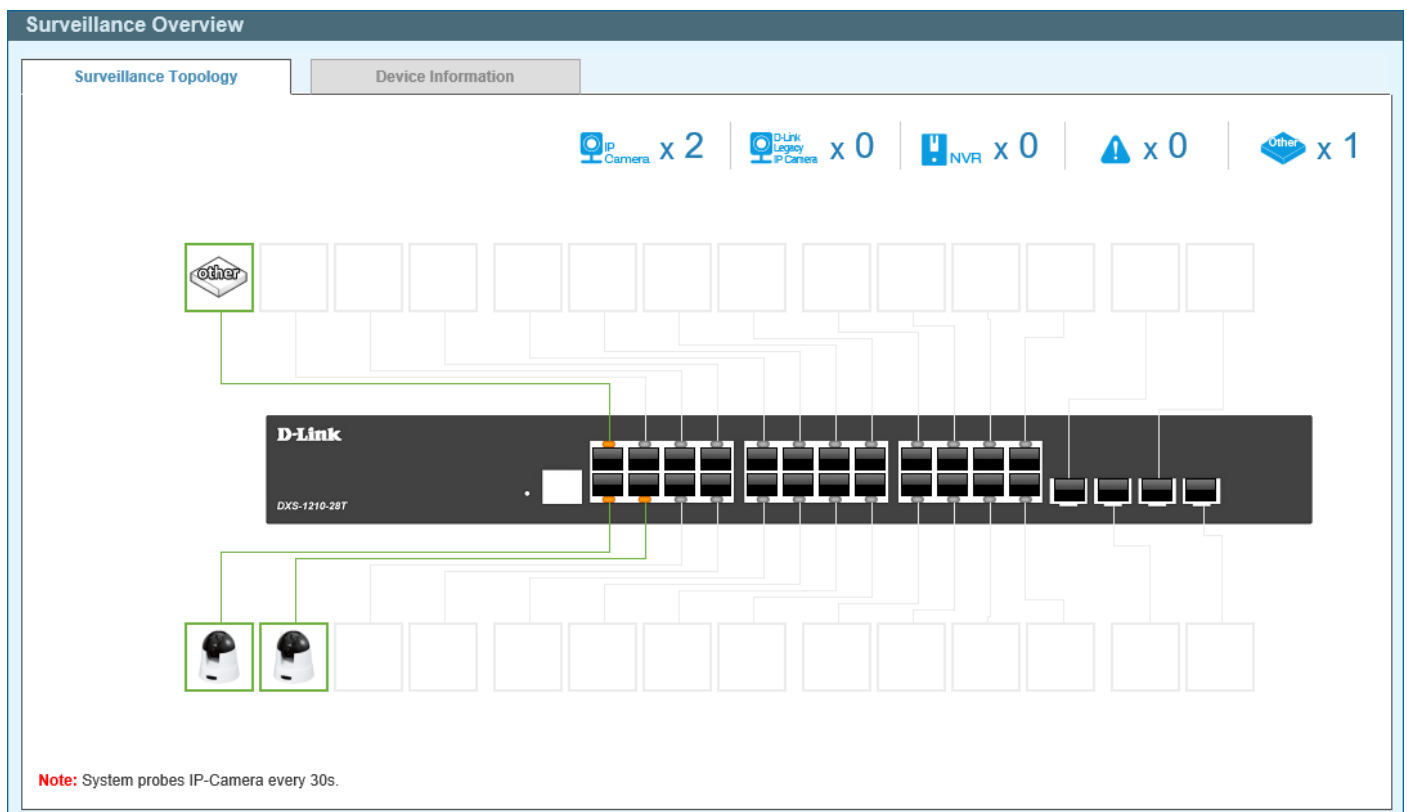








Figure 14-1 Surveillance Overview Window

The following icons are available in this window and are described below:

Icon	Description
 x 1	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.

Icon	Description
 x 0	This displays the total amount of D-Link legacy IP cameras (detected by ASV 1.0) connected to the Ethernet ports on the Switch.
 x 1	This displays the total amount of Network Video Recorders (NVRs) connected to the Ethernet ports on the Switch.
 x 0	This displays the amount of surveillance warnings generated on the Switch.
 x 1	This displays the amount of other devices connected to the Ethernet ports on the Switch.
	This displays the device connected to the Ethernet port on the Switch. The green border around the image indicates that the device is a non-PoE device.

After hovering (with the mouse pointer) over the network device icon, the following additional information will be displayed:

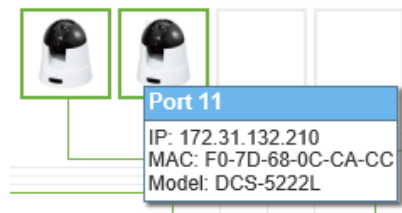


Figure 14-2 Additional Device Information



NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.



NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.

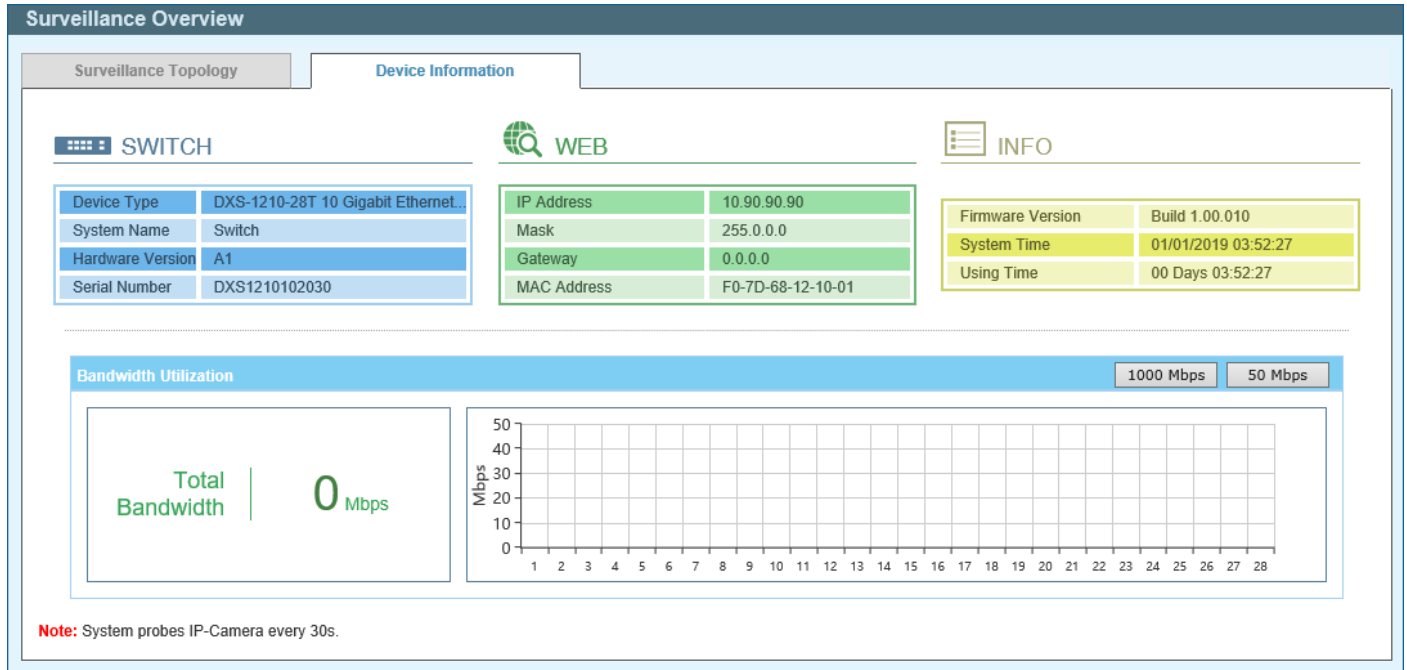


Figure 14-6 Device Information Window

Click the **1000 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 1 Gbps.

Click the **50 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 50 Mbps.

Port Information

This window is used to display port information like throughput, distance of the network cable, PoE provisioning status, power consumption, loopback detection status, group, and how many IP cameras, NVRs, and other devices are connected to the ports.

To view the following window, click **Port Information**, as shown below:

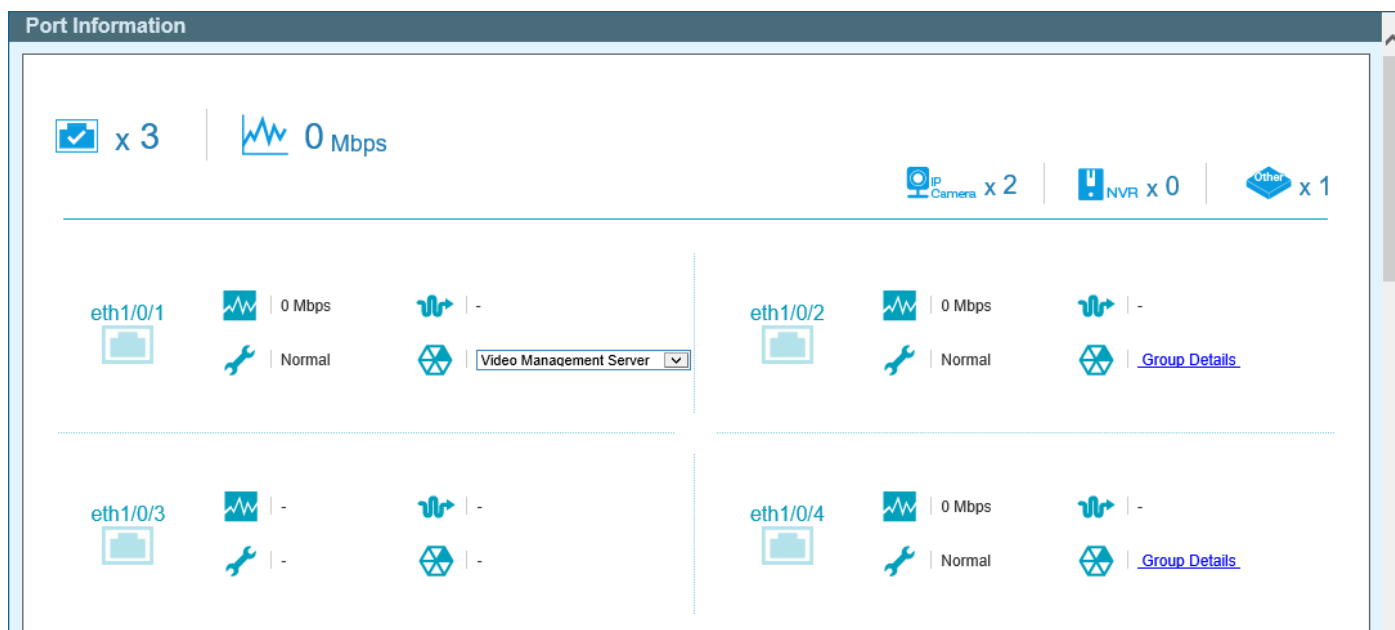














Figure 14-7 Port Information Window

The following icons are available in this window and are described below:

Icon	Description
 x 5	This displays the total amount of Ethernet devices connected to the Ethernet ports on the Switch.
 6 Mbps	The displays the total amount of inbound bandwidth that is being used by the Ethernet devices connected to the Ethernet ports on the Switch.
 x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
 x 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
 x 1	This displays the total amount of other Ethernet devices connected to the Ethernet ports on the Switch.
eth1/0/1 	This displays the Ethernet port number on the Switch.
 0 Mbps	This displays the amount of inbound bandwidth that is being used by the Ethernet device connected to the respective Ethernet port.
 -	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.
 Normal  <u>Loop</u>	This displays the Loopback Detection status on the Ethernet port. <ul style="list-style-type: none"> Normal - Specifies that there are no loops in the network. Loop - Specifies that there is a loop in the network. Click the Loop link to navigate to the Health Diagnostic window.
 Group Details	If an ONVIF IP camera or NVR is connected to the port, the Group Details link will be available. Select the Group Details link to access the Group Details window.

Icon	Description
 <input type="text" value="Video Management Server"/>	If a network device is connected to the port that is neither an ONVIF IP camera nor NVR, the device type can be selected. Options to choose from are Video Management Server , VMS Client/Remote Viewer , Video Encoder , Network Storage , and Other IP Surveillance Device .

Group Details

After clicking **Group Details** link, the following window will appear.

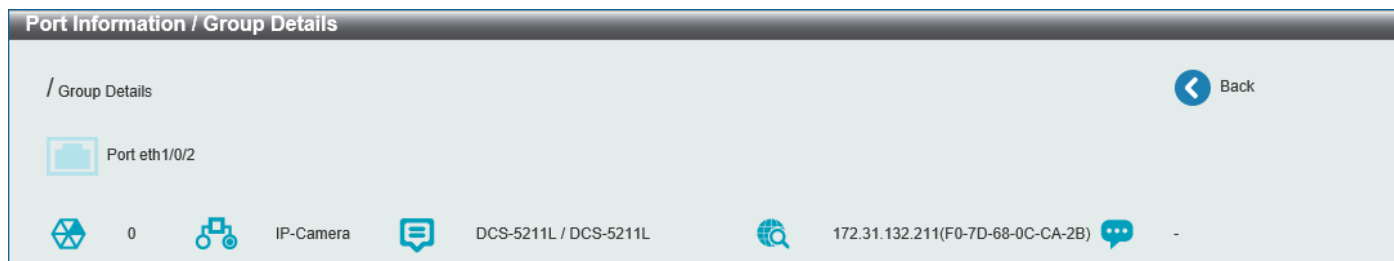








Figure 14-8 Port Information / Group Details Window

The following icons are available in this window and are described below:

Icon	Description
 Port eth1/0/5	This displays the Ethernet port number on the Switch.
 0	This displays the group ID of the IP camera or NVR on the port.
 IP-Camera	This displays the type of device connected to the port. The can be either IP-Camera or NVR .
 DCS-5211L / DCS-5211L	This displays the model name of the IP camera.
 192.168.0.23(28-10-7B-04-60-EC)	This displays the IP Address and MAC Address of the IP camera or NVR.
 DCS-942LB1	This displays the description of the device connected to the port.

Click the **< Back** option to return to the previous window.

IP-Camera Information

This window is used to display IP camera information.

To view the following window, click **IP-Camera Information**, as shown below:



Figure 14-9 IP-Camera Information Window

The following icons are available in this window and are described below:

Icon	Description
	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
	The displays the total amount of inbound bandwidth that is being used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
	This displays the Ethernet port number on the Switch.
 DCS-942LB1 DCS-942LB1	This displays a photo, manufacturer, and model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the IP camera.
192.168.0.21 (B0-C5-54-26-B7-A3)	This displays the IP address and MAC address of the IP camera.
DCS-942LB1	This displays the description for the IP camera. Click the icon to modify the description.
<input type="text"/>	Enter the description for the IP camera here. Click the icon to apply the modified description.

NVR Information

This window is used to display NVR information.

To view the following window, click **NVR Information**, as shown below:



Figure 14-10 NVR Information Window

The following icons are available in this window and are described below:

Icon	Description
	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
	The displays the total amount of inbound bandwidth that is being used by the NVRs connected to the Ethernet ports on the Switch.
	This displays the Ethernet port number on the Switch.
	This displays a generic photo of the NVR connected to the port.
	This displays the amount of inbound bandwidth that is being used by the NVR.
	This displays the IP address and MAC address of the NVR.
	This displays the description for the NVR. Click the icon to modify the description.
	Enter the description for the NVR here. Click the icon to apply the modified description.
	This displays the group ID of the NVR.
	This displays the number of ONVIF IP cameras managed by this NVR.
	This displays information about the ONVIF IP camera that is managed by this NVR.

Management

File System

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

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

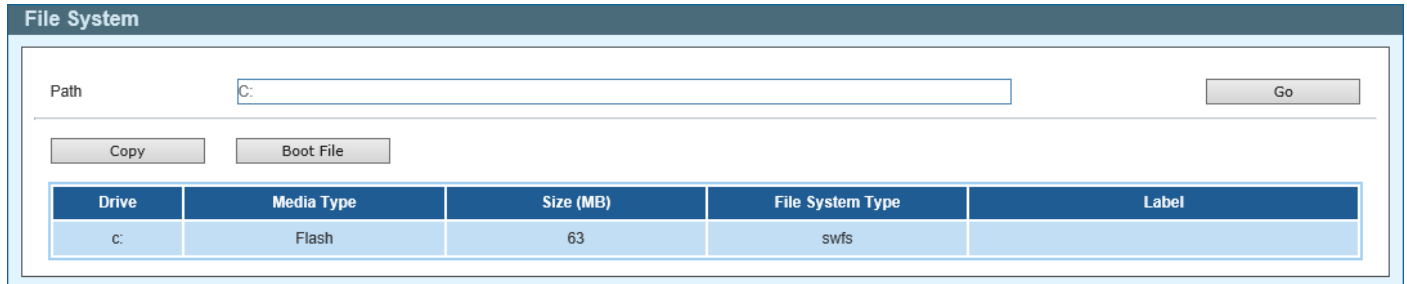


Figure 14-14 File System Window

The fields that can be configured are described below:

Parameter	Description
Path	Enter the path string here.

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

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

Click the **Boot File** button to configure the bootup image and configuration file settings.

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

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

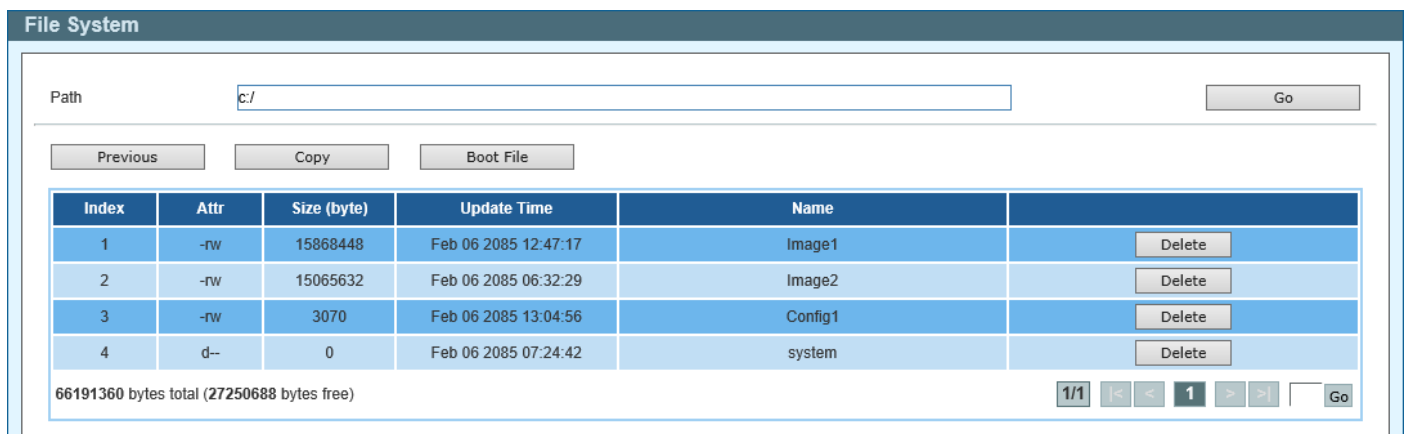


Figure 14-15 File System (c:) Window

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

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

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

Click the **Boot File** button to configure the bootup image and configuration file settings.

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

After clicking the **Copy** button, the following windows will appear.

Figure 14-16 File System (Copy) Window

The fields that can be configured are described below:

Parameter	Description
Source	Select the source for the copy here. Options to choose from are: <ul style="list-style-type: none"> • startup-config - Specifies to copy the startup configuration as the source. • Image 1 - Specifies to copy firmware "Image 1" as the source. • Image 2 - Specifies to copy firmware "Image 2" as the source. • Configuration 1 - Specifies to copy "Configuration 1" as the source. • Configuration 2 - Specifies to copy "Configuration 2" as the source.
Destination	Select the destination for the copy here. Options to choose from are: <ul style="list-style-type: none"> • running-config - Specifies to overwrite the running configuration with the source. • startup-config - Specifies to overwrite the start-up configuration with the source. • Image 1 - Specifies to overwrite "Image 1" with the source. • Image 2 - Specifies to overwrite "Image 2" with the source. • Configuration 1 - Specifies to overwrite "Configuration 1" with the source. • Configuration 2 - Specifies to overwrite "Configuration 2" with the source.
Replace	Specifies to replace the current running configuration with the indicated configuration file.

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

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

Time

Clock Settings

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

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

Figure 14-17 Clock Settings Window

The fields that can be configured are described below:

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

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

SNTP Settings

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

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

Figure 14-18 SNTP Settings Window

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

Parameter	Description
SNTP State	Select to enable or disable the SNTP feature here.
Poll Interval	Enter the poll interval value here. The range is from 30 to 99999 seconds. By default, this value is 720 seconds.

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

The fields that can be configured in the **SNTP Server Setting** section are described below:

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

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

Click the **Delete** button to remove the SNTP server from the configuration.

Surveillance Settings

This window is used to display and configure the surveillance settings. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

To view the following window, click **Surveillance Settings**, as shown below:

Figure 14-19 Surveillance Settings Window

The fields that can be configured in the **Surveillance VLAN Settings** section are described below:

Parameter	Description
VLAN ID	Enter the ID of the surveillance VLAN here. The range is from 2 to 4094.

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

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

Parameter	Description
Get IP From	Select the method used to configure the IP address settings on the Switch here. Options to choose from are: <ul style="list-style-type: none"> Static - Specifies that the IP address settings will be manually configured. DHCP - Specifies that the IP address settings will be automatically obtained from a DHCP server on the network.
IP Address	Enter the IPv4 address of the Switch here.
Mask	Enter the IPv4 subnet mask of the Switch here.

Parameter	Description
Gateway	Enter the IPv4 address of the default gateway here.

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

The fields that can be configured in the **SNMP Host Settings** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP host here.

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

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

The fields that can be configured in the **Log Server** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP server here.

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

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

The uplink ports join all surveillance VLANs since they forward surveillance traffic to other switches. It is recommended to connect uplink ports to the other switches because the discovery process is disabled on these ports.

The fields that can be configured in the **Uplink Port Settings** section are described below:

Parameter	Description
From Port / To Port	Select the uplink port range that will be used here.

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

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

Surveillance Log

This window is used to display the surveillance log.

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

Index	Time	Level	Log Description
1	2000-01-01 00:25:32	INFO(6)	ASV: Remove IPC(192.168.0.20, MAC:B0-C5-54-26-B7-8...
2	2000-01-01 00:13:01	INFO(6)	ASV: Remove IPC(192.168.0.30, MAC:28-10-7B-26-A7-E...
3	2000-01-01 00:08:12	INFO(6)	ASV: Add NVR(192.168.0.205, MAC:1C-BD-B9-E3-CE-25)...
4	2000-01-01 00:07:48	INFO(6)	ASV: Add IPC(192.168.0.20, MAC:B0-C5-54-26-B7-86)
5	2000-01-01 00:07:13	INFO(6)	ASV: Remove IPC(192.168.0.20, MAC:B0-C5-54-26-B7-8...
6	2000-01-01 00:06:41	INFO(6)	ASV: Mode change from (Standard Mode) to (Surveill...
7	2000-01-01 00:06:00	INFO(6)	ASV: Add IPC(192.168.0.20, MAC:B0-C5-54-26-B7-86)
8	2000-01-01 00:05:54	INFO(6)	ASV: Add NVR(192.168.0.202, MAC:00-0E-C6-C1-F6-02)...
9	2000-01-01 00:05:51	INFO(6)	ASV: Add IPC(192.168.0.30, MAC:28-10-7B-26-A7-EF)

Figure 14-20 Surveillance Log Window

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Backup** button to upload the surveillance log to the PC using HTTP.

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

Health Diagnostic

This window is used to display Health Diagnostics information, Discovered Surveillance Devices information, and initiate a cable distance test on all or selected ports on the Switch. For each link-up port, the system will check the link status, PoE status and error counters periodically. This page will refresh every 30s.

To view the following window, click **Health Diagnostic**, as shown below:

The screenshot shows the 'Health Diagnostic' window. At the top right, there is a 'Detect All' button. Below it is a table with the following columns: Port, Loopback Detection Status, Cable Link, Tx/Rx CRC Counter, Discovered Surveillance Devices, and Detect Distance. The table contains 10 rows of data for ports eth1/0/1 through eth1/0/10.

Port	Loopback Detection Status	Cable Link	Tx/Rx CRC Counter	Discovered Surveillance Devices	Detect Distance
eth1/0/1	Normal	Pass	0/0	0	Detect
eth1/0/2	-	-	-	-	Detect
eth1/0/3	Normal	Pass	0/0	0	Detect
eth1/0/4	-	-	-	-	Detect
eth1/0/5	-	-	-	-	Detect
eth1/0/6	-	-	-	-	Detect
eth1/0/7	-	-	-	-	Detect
eth1/0/8	-	-	-	-	Detect
eth1/0/9	-	-	-	-	Detect
eth1/0/10	-	-	-	-	Detect

Figure 14-21 Health Diagnostic Window

The fields that are displayed in the table are described below:

Parameter	Description
Port	This field displays the Ethernet port number.
Loopback Detection Status	This field displays the Loopback Detection status on the Ethernet port. It can be one of the following: <ul style="list-style-type: none"> • Normal - No loop is detected on the port. • Loop - A loop is detected on the port.
Cable Link	This field displays the cable link status. It can be the following: <ul style="list-style-type: none"> • Pass - The port link is up and operating in the full-duplex mode.
Tx/Rx CRC Counter	This field displays the TX/RX CRC counter.
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (1) to view the group details associated with IP camera or NVR connected to the port.
Detect Distance	Click the Detect button to initiate a cable distance test on the specified port.

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 3.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

Figure 14-22 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button and navigate to the firmware file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are Image 1 and Image 2 .

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Figure 14-23 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the firmware on the Switch that will be backed up to the local PC here. Options to choose from are Image 1 and Image 2 .

Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 14-24 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button and navigate to the configuration file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: <ul style="list-style-type: none"> • Configuration 1 - Select this option to use configuration 1 as the destination. • Configuration 2 - Select this option to use configuration 2 as the destination. • running-config - Select this option to use the running configuration as the destination. • startup-config - Select this option to use the start-up configuration as the destination.
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 14-25 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	<p>Select the configuration on the Switch that will be backed up to the local PC here. Options to choose from are:</p> <ul style="list-style-type: none"> • Configuration 1 - Select this option to backup configuration 1. • Configuration 2 - Select this option to backup configuration 2. • running-config - Select this option to backup the running configuration. • startup-config - Select this option to backup the start-up configuration.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

Figure 14-26 Language Management Window

The fields that can be configured are described below:

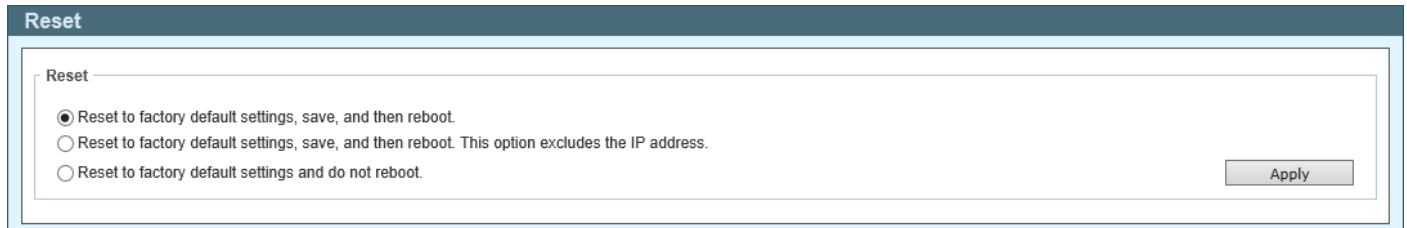
Parameter	Description
Language File	<p>Click the Browse button and navigate to the language pack file on the local PC here. This file will be uploaded to the Switch.</p>

Click the **Apply** button to initiate the language pack upload and installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:



Reset

Reset

- Reset to factory default settings, save, and then reboot.
- Reset to factory default settings, save, and then reboot. This option excludes the IP address.
- Reset to factory default settings and do not reboot.

Apply

Figure 14-27 Reset Window

Select one of the following options:

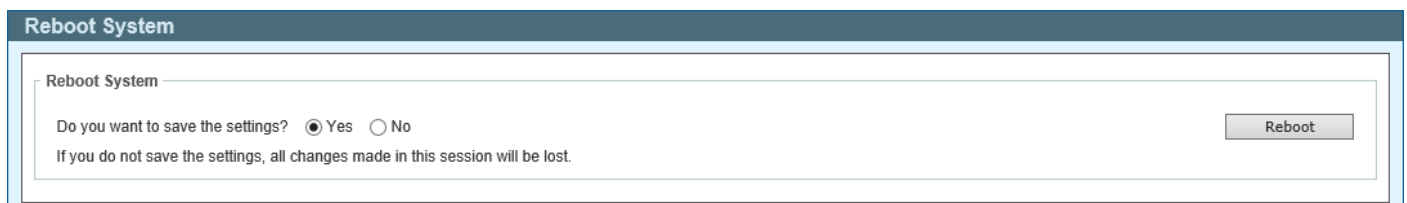
- Reset to factory default settings, save, and then reboot.
- Reset to factory default settings, save, and then reboot. This option excludes the IP address.
- Reset to factory default settings and do not reboot.

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

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

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



Reboot System

Reboot System

Do you want to save the settings? Yes No

If you do not save the settings, all changes made in this session will be lost.

Reboot

Figure 14-28 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

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



Figure 14-29 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
File Path	Select the destination where the configuration will be saved here. Options to choose from are startup-config , Configuration 1 , and Configuration 2 .

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

Help

Click this option to access the built-in Surveillance Help window.

After clicking the **Help** option, the following window will appear.

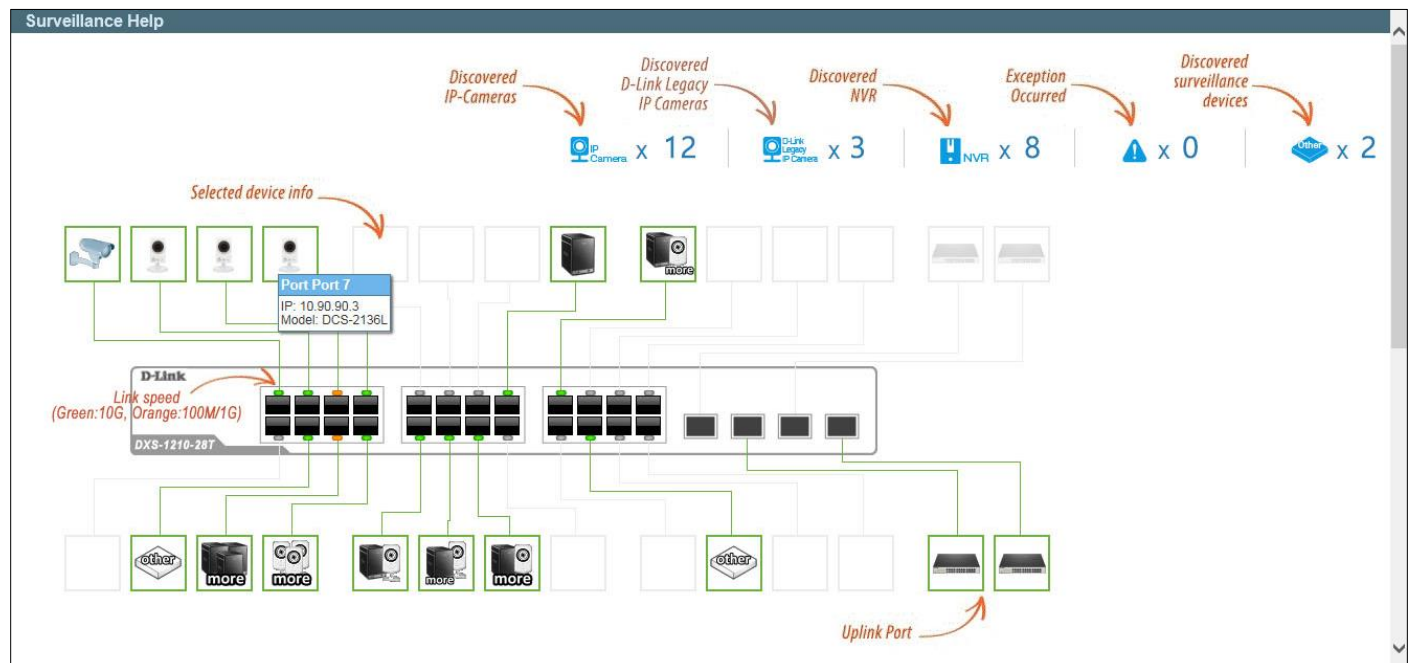


Figure 14-30 Help (Diagram) Window

Device Status					
Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.
IP-Camera/NVR Status					
Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.		Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.		Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
	Multiple ONVIF IP-Cameras and one NVR discovered on this port.		One ONVIF IP-Camera and multiple NVRs discovered on this port.		Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

Figure 14-31 Help (Table) Window

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Standard Mode

Click the **Standard Mode** button in the toolbar to change the Web UI mode and style from Surveillance Mode to Standard Mode.



NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

Logout

Click this option to log out of the Web UI of the Switch

Appendix A - System Log Entries

The System Log entries are listed in this appendix.

802.1X

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when IEEE 802.1X authentication failed.</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. The possible reason may be:</p> <ul style="list-style-type: none"> (1) user authentication failure (2) no server(s) responding (3) no servers configured (4) no resources (5) user timeout expired <p>username: The user being authenticated.</p> <p>interface-id: The switch interface number.</p> <p>mac-address: The MAC address of the authenticated device.</p>	Critical
<p>2</p> <p>Event Description: This log is recorded when IEEE 802.1X authentication is 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 being authenticated.</p> <p>interface-id: The interface name.</p> <p>mac-address: The MAC address of the authenticated device.</p>	Informational

AAA

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when the AAA global state is enabled or disabled.</p> <p>Log Message: AAA is <status></p> <p>Parameters Description:</p> <p>status: The AAA status.</p>	Informational
<p>2</p> <p>Event Description: This log is recorded when login is successful.</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: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).</p> <p>client-ip: The IP address of the client if valid through IP protocol.</p> <p>aaa-method: The authentication method, for example, none, local, or server.</p> <p>server-ip: The IP address of the AAA server if the authentication method is remote server.</p> <p>username: The username for authentication.</p>	Informational
<p>3</p> <p>Event Description: This log is recorded when the 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: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).</p> <p>client-ip: The IP address of the client if valid through IP protocol.</p> <p>aaa-method: The authentication method, for example, local or server.</p> <p>server-ip: The IP address of the AAA server if the authentication method is remote server.</p> <p>username: The username for authentication.</p>	Warning
<p>4</p> <p>Event Description: This log is recorded when RADIUS assigned valid VLAN ID attributes.</p>	Informational

Log Description	Severity
<p>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Parameters Description:</p> <p>server-ip: The IP address of the RADIUS server.</p> <p>vid: The assign VLAN ID authorized by the RADIUS server.</p> <p>interface-id: The port number of the authenticated client.</p> <p>username: The username for authentication.</p>	

ARP

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when gratuitous ARP detected a duplicate IP address.</p> <p>Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>)</p> <p>Parameters Description:</p> <p>ipaddr: The duplicated IP address.</p> <p>macaddr: The MAC address of the duplicated IP address.</p> <p>port-num: The port number of the device.</p> <p>ipif-name: The name of the interface on the switch that contains the duplicated IP address.</p>	Warning

Auto Image

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when the auto-image firmware upgraded successfully.</p> <p>Log Message: The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: The IP address of the TFTP server.</p>	Informational
<p>2</p> <p>Event Description: This log is recorded when the auto-image firmware failed to upgrade.</p> <p>Log Message: The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: The IP address of the TFTP server.</p>	Informational

Auto Save Config

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when the DDP configuration is saved automatically.</p> <p>Log Message: CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p>	Informational

Auto Surveillance VLAN

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when a new surveillance device is detected on an interface.</p> <p>Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>)</p> <p>Parameters Description:</p> <p>interface-id: The name of the interface.</p> <p>mac-address: The MAC address of the surveillance device.</p>	Informational
<p>2</p> <p>Event Description: This log is recorded when an interface, which is an enabled surveillance VLAN, joins the surveillance VLAN automatically.</p>	Informational

Log Description	Severity
<p>Log Message: <interface-id> add into surveillance VLAN <vid></p> <p>Parameters Description: interface-id: The name of the interface. vid: The VLAN ID.</p>	
<p>3</p> <p>Event Description: This log is recorded when an interface leaves the surveillance VLAN and at the same time no surveillance device is detected in the aging interval for that interface.</p> <p>Log Message: <interface-id> remove from surveillance VLAN <vid></p> <p>Parameters Description: interface-id: The name of the interface. vid: The VLAN ID.</p>	Informational
<p>4</p> <p>Event Description: This log is recorded when an IPC is added in the surveillance VLAN.</p> <p>Log Message: ASV: Add IPC (<ipaddr>, MAC:<mac-address>)</p> <p>Parameters Description: ipaddr: The IP address of the IPC. mac-address: The MAC address of the IPC.</p>	Informational
<p>5</p> <p>Event Description: This log is recorded when an IPC is removed from the surveillance VLAN.</p> <p>Log Message: ASV: Remove IPC (<ipaddr>, MAC:<mac-address>)</p> <p>Parameters Description: ipaddr: The IP address of the IPC. mac-address: The MAC address of the IPC.</p>	Informational
<p>6</p> <p>Event Description: This log is recorded when an NVR is added in the surveillance VLAN.</p> <p>Log Message: ASV: Add NVR (<ipaddr>, MAC:<mac-address>)</p> <p>Parameters Description: ipaddr: The IP address of the NVR. mac-address: The MAC address of the NVR.</p>	Informational
<p>7</p> <p>Event Description: This log is recorded when an NVR is removed from the surveillance VLAN.</p> <p>Log Message: ASV: Remove NVR (<ipaddr>, MAC:<mac-address>)</p> <p>Parameters Description: ipaddr: The IP address of the NVR. mac-address: The MAC address of the NVR.</p>	Informational
<p>8</p> <p>Event Description: This log is recorded when the mode of ASV 2.0 is changed through the Web.</p> <p>Log Message: ASV: Mode change from <mode> to <mode ></p> <p>Parameters Description: mode: The mode of ASV 2.0. This can be standard or surveillance.</p>	Informational

Configuration /Firmware

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when the firmware was upgraded successfully.</p> <p>Log Message: Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)</p> <p>Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.</p>	Informational
<p>2</p> <p>Event Description: This log is recorded when the firmware upgrade failed.</p> <p>Log Message: Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)</p> <p>Parameters Description: session: The user's session.</p>	Warning

Log Description	Severity
username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	
3 Event Description: This log is recorded when the firmware uploaded successfully. Log Message: Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
4 Event Description: This log is recorded when the firmware upload failed. Log Message: Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
5 Event Description: This log is recorded when the configuration downloaded successfully. Log Message: Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
6 Event Description: This log is recorded when the configuration download failed. Log Message: Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
7 Event Description: This log is recorded when the configuration uploaded successfully. Log Message: Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational

Log Description	Severity
<p>8</p> <p>Event Description: This log is recorded when the configuration upload failed.</p> <p>Log Message: Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p> <p>macaddr: The MAC address of the client.</p> <p>server-ip: The IP address of the server.</p> <p>pathfile: The path and file name on the server.</p>	Warning
<p>9</p> <p>Event Description: This log is recorded when the configuration is saved to the flash through the console.</p> <p>Log Message: Configuration saved to flash by console (Username: <username>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p>	Informational
<p>10</p> <p>Event Description: This log is recorded when the configuration is saved to the flash remotely.</p> <p>Log Message: Configuration saved to flash (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p>	Informational
<p>11</p> <p>Event Description: This log is recorded when a log message is uploaded successfully.</p> <p>Log Message: Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p> <p>macaddr: The MAC address of the client.</p>	Informational
<p>12</p> <p>Event Description: This log is recorded when a log message upload failed.</p> <p>Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>])</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p> <p>macaddr: The MAC address of the client.</p>	Warning
<p>13</p> <p>Event Description: This log is recorded when an unknown type file download failed.</p> <p>Log Message: Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p> <p>macaddr: The MAC address of the client.</p> <p>server-ip: The IP address of the server.</p> <p>pathfile: The path and file name on the server.</p>	Warning

NOTE:

- The user's session indicates Console, Web, SNMP, Telnet, or SSH.
- If the configuration/firmware is updated through the Console, there will be no IP and MAC information for logging.

DAD

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when the DUT receives a Neighbor Solicitation (NS) message with a duplicate address in the DAD duration, the DUT will add this log.</p> <p>Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages</p> <p>Parameters Description: ipv6address: The IPv6 address in NS messages interface-id: The interface name.</p>	Warning
<p>2</p> <p>Event Description: This log is recorded when the DUT receives a Neighbor Advertisement (NA) message with a duplicate address in the DAD duration, the DUT will add this log.</p> <p>Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages</p> <p>Parameters Description: ipv6address: The IPv6 address in NA messages. interface-id: The interface name.</p>	Warning

DAI

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when DAI detects invalid ARP packets.</p> <p>Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Parameters Description: type: The type of ARP packet. It indicates an ARP packet request or response. ip-address: The IP address. mac-address: The MAC address. vlan-id: The VLAN ID. interface-id: The name of the interface.</p>	Warning
<p>2</p> <p>Event Description: This log is recorded when DAI detects valid ARP packets.</p> <p>Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Parameters Description: type: The type of ARP packet. It indicates an ARP packet request or response. ip-address: The IP address. mac-address: The MAC address. vlan-id: The VLAN ID. interface-id: The name of the interface.</p>	Informational

DHCPv6 Client

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when the 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: ipif-name: The name of the DHCPv6 client interface.</p>	Informational
<p>2</p> <p>Event Description: This log is recorded when the 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: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.</p>	Informational
<p>3</p> <p>Event Description: This log is recorded when 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>	Informational

Log Description		Severity
	Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	
4	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, renews success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
5	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, starts rebinding. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
6	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, rebinds success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
7	Event Description: This log is recorded when the IPv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational

DHCPv6 Relay

Log Description		Severity
1	Event Description: This log is recorded when the DHCPv6 relay on the specified interface's administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] Parameters Description: <ipif-name>: The name of the DHCPv6 relay agent interface.	Informational

DNS Resolver

Log Description		Severity
1	Event Description: This log is recorded when a duplicate domain name is added to the cache and this leads to the deletion of the dynamic domain name cache. Log Message: Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domain-name: The domain name string. ipaddr: The static/dynamic IP address.	Informational

DoS Prevention

Log Description		Severity
1	Event Description: This log is recorded when a DoS attack is detected. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>) Parameters Description: dos-type: The DoS attack type.	Notification

Log Description	Severity
ip-address: The IP address. interface-id: The name of the interface.	

Interface

Log Description	Severity
1 Event Description: This log is recorded when the port link is down. Log Message: Port <port-type><interface-id> link down Parameters Description: port-type: The port type. interface-id: The interface name.	Informational
2 Event Description: This log is recorded when the port link is up. Log Message: Port <port-type><interface-id> link up, <link-speed> Parameters Description: port-type: The port type. interface-id: The interface name. link-speed: The port link speed.	Informational

IPSG

Log Description	Severity
1 Event Description: This log is recorded when there are no hardware rule resources to set the DHCP snooping entry into the IPSG table. Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) Parameters Description: ipaddr: The IP address. macaddr: The MAC address. vlanid: The VLAN ID. interface-id: The interface name.	Warning

IPv6SG

Log Description	Severity
1 Event Description: This log is recorded when there are no hardware rule resources to set the IPv6 snooping entry into the IPv6SG table. Log Message: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>) Parameters Description: ipaddr: The IPv6 address of the IPv6 snooping entry. macaddr: The MAC address of the IPv6 snooping entry. vlan-id: The VLAN ID of the IPv6 snooping entry. interface-id: The interface of the IPv6 snooping entry.	Warning

LACP

Log Description	Severity
1 Event Description: This log is recorded when the link aggregation group link is up. Log Message: Link Aggregation Group <group-id> link up Parameters Description: group-id: The group ID of the link down aggregation group.	Informational
2 Event Description: This log is recorded when the link aggregation group link is down. Log Message: Link Aggregation Group <group-id> link down	Informational

Log Description	Severity
Parameters Description: group-id: The group ID of the link down aggregation group.	
3 Event Description: This log is recorded when a member port is attached to the link aggregation group. Log Message: <iface> attach to Link Aggregation Group <group-id> Parameters Description: iface: The interface name of the port that is attached to the aggregation group. group-id: The group ID of the aggregation group that the port attached to.	Informational
4 Event Description: This log is recorded when a member port is detached from the link aggregation group. Log Message: <iface> detach from Link Aggregation Group <group-id> Parameters Description: iface: The interface name of the port that is detached from the aggregation group. group-id: The group ID of the aggregation group that the port detached from.	Informational

LBD

Log Description	Severity
1 Event Description: This log is recorded when an interface detects a loop. Log Message: <interface-id> LBD loop occurred Parameters Description: interface-id: The interface on which loop is detected.	Critical
2 Event Description: This log is recorded when an interface detects a loop in a VLAN. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Parameters Description: interface-id: The interface on which the loop is detected. vlan-id: The VLAN on which the loop is detected.	Critical
3 Event Description: This log is recorded when an interface loop is recovered. Log Message: <interface-id> LBD loop recovered Parameters Description: interface-id: The interface on which the loop is recovered.	Critical
4 Event Description: This log is recorded when an interface loop is recovered in a VLAN. Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered Parameters Description: interface-id: The interface on which the loop is recovered. vlan-id: The VLAN on which the loop is recovered.	Critical
5 Event Description: This log is recorded when the number of VLANs that loop back exceeds the reserved number. Log Message: Loop VLAN numbers overflow	Critical

LLDP/LLDP-MED

Log Description	Severity
1 Event Description: This log is recorded when an LLDP-MED topology change is detected. Log Message: LLDP-MED topology change detected (on port <portNum>. chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7). portID: The port ID. deviceClass: The LLDP-MED device type.	Notification

Log Description	Severity
<p>2</p> <p>Event Description: This log is recorded when an LLDP-MED device type conflict is 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: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7).</p> <p>chassisID: The chassis ID.</p> <p>portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7).</p> <p>portID: The port ID.</p> <p>deviceClass: The LLDP-MED device type.</p>	Notification
<p>3</p> <p>Event Description: This log is recorded when an incompatible LLDP-MED TLV set is 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.</p> <p>chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7).</p> <p>chassisID: The chassis ID.</p> <p>portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7).</p> <p>portID: The port ID.</p> <p>deviceClass: The LLDP-MED device type.</p>	Notification

Login/Logout CLI

Log Description	Severity
<p>1</p> <p>Event Description: This log is recorded when login through the console is successful.</p> <p>Log Message: Successful login through Console (Username: <username>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p>	Informational
<p>2</p> <p>Event Description: This log is recorded when login through the console failed.</p> <p>Log Message: Login failed through Console (Username: <username>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p>	Warning
<p>3</p> <p>Event Description: This log is recorded when the console session timed out.</p> <p>Log Message: Console session timed out (Username: <username>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p>	Informational
<p>4</p> <p>Event Description: This log is recorded when logout from the console occurred.</p> <p>Log Message: Logout through Console (Username: <username>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p>	Informational
<p>5</p> <p>Event Description: This log is recorded when login through Telnet is successful.</p> <p>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p>	Informational
<p>6</p> <p>Event Description: This log is recorded when login through Telnet failed.</p> <p>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The current login user.</p> <p>ipaddr: The IP address of the client.</p>	Warning

Log Description	Severity
7 Event Description: This log is recorded when the Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
8 Event Description: This log is recorded when logout from Telnet occurred. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
9 Event Description: This log is recorded when login through SSH is successful. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
10 Event Description: This log is recorded when login through SSH failed. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Critical
11 Event Description: This log is recorded when the SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
12 Event Description: This log is recorded when logout from SSH occurred. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational

MSTP Debug Enhancement

Log Description	Severity
1 Event Description: This log is recorded when the Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
2 Event Description: This log is recorded when the Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
3 Event Description: This log is recorded when an MSTP instance topology change event occurs. Log Message: Topology changed (Instance: <instance-id>, <interface-id>, MAC: <macaddr>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. macaddr: The MAC address of the bridge.	Notification
4 Event Description: This log is recorded when a new MSTP instance root bridge is selected. Log Message: [CIST CIST Region MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority: <priority>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. macaddr: The MAC address of the bridge. priority: The bridge priority value. This is divisible by 4096.	Informational
5 Event Description: This log is recorded when a new MSTP instance root port is selected.	Notification

Log Description	Severity
<p>Log Message: New root port selected (Instance:<instance-id>, <interface-id>)</p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p> <p>interface-id: The port number that detects or receives topology change information.</p>	
<p>6</p> <p>Event Description: This log is recorded when an MSTP instance port state change event occurs.</p> <p>Log Message: Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status></p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p> <p>interface-id: The port number that detects or receives topology change information.</p> <p>old-status: The old status of the port. This can be Disable, Discarding, Learning, or Forwarding.</p> <p>new-status: The new status of the port. This can be Disable, Discarding, Learning, or Forwarding.</p>	Notification
<p>7</p> <p>Event Description: This log is recorded when an MSTP instance port role change event occurs.</p> <p>Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role></p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p> <p>interface-id: The port number that detects or receives topology change information.</p> <p>old-role: The old STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.</p> <p>new-role: The new STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.</p>	Informational
<p>8</p> <p>Event Description: This log is recorded when an MST instance is created.</p> <p>Log Message: Spanning Tree instance created (Instance:<instance-id>)</p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p>	Informational
<p>9</p> <p>Event Description: This log is recorded when an MST instance is deleted.</p> <p>Log Message: Spanning Tree instance deleted (Instance:<instance-id>)</p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p>	Informational
<p>10</p> <p>Event Description: This log is recorded when STP version changes.</p> <p>Log Message: Spanning Tree version change (new version:<new-version>)</p> <p>Parameters Description:</p> <p>new-version: The active STP version.</p>	Informational
<p>11</p> <p>Event Description: This log is recorded when the configuration name and revision level changed in the MST configuration identification.</p> <p>Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name>, revision level <revision-level>)</p> <p>Parameters Description:</p> <p>name: The name given for the specified MST region.</p> <p>revision-level: The revision level. Switches using the same given name but with a different revision level are considered members of different MST regions.</p>	Informational
<p>12</p> <p>Event Description: This log is recorded when a VLAN is mapped to an MST instance.</p> <p>Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>])</p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p> <p>startvlanid: The starting VLAN ID in the VLAN range to be added.</p> <p>endvlanid: The ending VLAN ID in the VLAN range to be added.</p>	Informational
<p>13</p> <p>Event Description: This log is recorded when a VLAN is deleted from an MST instance.</p> <p>Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>])</p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p> <p>startvlanid: The starting VLAN ID in the VLAN range to be deleted.</p>	Informational

Log Description		Severity
	endvlanid: The ending VLAN ID in the VLAN range to be deleted.	
14	<p>Event Description: This log is recorded when the port role changes to alternate due to guard root.</p> <p>Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root</p> <p>Parameters Description:</p> <p>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.</p> <p>interface-id: The port number which detects the event.</p>	Informational

Peripheral

Log Description		Severity
1	<p>Event Description: This log is recorded when the fan is recovered.</p> <p>Log Message: <fan-descr> back to normal</p> <p>Parameters Description:</p> <p>fan-descr: The fan ID and position.</p>	Critical
2	<p>Event Description: This log is recorded when a fan failed.</p> <p>Log Message: <fan-descr> failed</p> <p>Parameters Description:</p> <p>fan-descr: The fan ID and position.</p>	Critical
3	<p>Event Description: This log is recorded when the temperature sensor enters the alarm state.</p> <p>Log Message: <thermal-sensor-descr> detects abnormal temperature <degree></p> <p>Parameters Description:</p> <p>thermal-sensor-descr: The sensor ID and position.</p> <p>degree: The current temperature.</p>	Critical
4	<p>Event Description: This log is recorded when the temperature recovers to normal.</p> <p>Log Message: <thermal-sensor-descr> temperature back to normal</p> <p>Parameters Description:</p> <p>thermal-sensor-descr: The sensor ID and position.</p>	Critical
5	<p>Event Description: This log is recorded when factory reset button is pressed.</p> <p>Log Message: Factory reset button pressed</p>	Critical

Port Security

Log Description		Severity
1	<p>Event Description: This log is recorded when a MAC address causes a port security violation.</p> <p>Log Message: MAC address <macaddr> causes port security violation on <interface-id></p> <p>Parameters Description:</p> <p>macaddr: The violation MAC address.</p> <p>interface-id: The interface name.</p>	Warning
2	<p>Event Description: This log is recorded when the address table is full on the system</p> <p>Log Message: Limit on system entry number has been exceeded</p>	Warning

Safeguard

Log Description		Severity
1	<p>Event Description: This log is recorded when the host enters the exhausted mode.</p> <p>Log Message: Safeguard Engine enters EXHAUSTED mode</p>	Warning
2	<p>Event Description: This log is recorded when the host enters the normal mode.</p> <p>Log Message: Safeguard Engine enters NORMAL mode</p>	Informational

SNMP

Log Description		Severity
1	<p>Event Description: This log is recorded when an SNMP request is received with an invalid community string.</p> <p>Log Message: SNMP request received from <ipaddr> with invalid community string</p> <p>Parameters Description:</p> <p>ipaddr: The IP address.</p>	Informational

SSH

Log Description		Severity
1	<p>Event Description: This log is recorded when the SSH server is enabled.</p> <p>Log Message: SSH server is enabled</p>	Informational
2	<p>Event Description: This log is recorded when the SSH server is disabled.</p> <p>Log Message: SSH server is disabled</p>	Informational

Storm Control

Log Description		Severity
1	<p>Event Description: This log is recorded when a storm is occurring.</p> <p>Log Message: <Broadcast Multicast Unicast> storm is occurring on <interface-id></p> <p>Parameters Description:</p> <p>Broadcast: A broadcast storm is occurring. Broadcast packets (DA = FF:FF:FF:FF:FF:FF).</p> <p>Multicast: A multicast storm is occurring. Multicast packets may include unknown L2 multicast, known L2 multicast, unknown IP multicast, and known IP multicast.</p> <p>Unicast: A unicast storm is occurring. Unicast packets may include both known and unknown unicast packets.</p> <p>interface-id: The interface ID on which a storm is occurring.</p>	Warning
2	<p>Event Description: This log is recorded when the storm is cleared.</p> <p>Log Message: <Broadcast Multicast Unicast> storm is cleared on <interface-id></p> <p>Parameters Description:</p> <p>Broadcast: The broadcast storm is cleared.</p> <p>Multicast: The multicast storm is cleared.</p> <p>Unicast: The unicast storm is cleared. This includes both known and unknown unicast packets.</p> <p>interface-id: The interface ID on which a storm is cleared.</p>	Informational
3	<p>Event Description: This log is recorded when a port is shut down due to a packet storm.</p> <p>Log Message: <interface-id> is currently shut down due to the <Broadcast Multicast Unicast> storm</p> <p>Parameters Description:</p> <p>interface-id: The interface ID that was error-disabled because of the storm.</p> <p>Broadcast: The interface is disabled due to a broadcast storm occurrence.</p> <p>Multicast: The interface is disabled due to a multicast storm occurrence.</p> <p>Unicast: The interface is disabled due to a unicast storm occurrence. This includes both known and unknown unicast packets.</p>	Warning

System

Log Description		Severity
1	<p>Event Description: This log is recorded when the system warm start.</p> <p>Log Message: System warm start</p>	Critical
2	<p>Event Description: This log is recorded when the system cold start.</p> <p>Log Message: System cold start</p>	Critical
3	<p>Event Description: This log is recorded when the system starts up.</p> <p>Log Message: System started up</p>	Critical

Telnet

Log Description	Severity
1 Event Description: This log is recorded when login through Telnet is successful. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational
2 Event Description: This log is recorded when login through Telnet failed. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Warning
3 Event Description: This log is recorded when logout from Telnet is successful. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational
4 Event Description: This log is recorded when the Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of Telnet client.	Informational

Voice VLAN

Log Description	Severity
1 Event Description: This log is recorded when a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: The interface name. mac-address: The MAC address of the voice device.	Informational
2 Event Description: This log is recorded when an interface, in the auto-voice VLAN mode, joins the voice VLAN. Log Message: <interface-id> add into voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational
3 Event Description: This log is recorded when an interface leaves the voice VLAN and no voice device is detected in the aging interval for that interface. Log Message: <interface-id> remove from voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational

Web

Log Description	Severity
1 Event Description: This log is recorded when login through the Web is successful. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.	Informational

Log Description	Severity
<p>2</p> <p>Event Description: This log is recorded when login through the Web failed. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.</p>	Warning
<p>3</p> <p>Event Description: This log is recorded when the Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.</p>	Informational
<p>4</p> <p>Event Description: This log is recorded when logout through the Web is successful. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.</p>	Informational
<p>5</p> <p>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.</p>	Informational
<p>6</p> <p>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.</p>	Warning
<p>7</p> <p>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.</p>	Informational
<p>8</p> <p>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.</p>	Informational

Appendix B - Trap Entries

The Trap Log entries are listed in this appendix.

802.1X

Trap Name	Description	OID
1	dDot1xExtLoggedSuccess This trap is sent when a host passed IEEE 802.1X authentication (login successful). Binding Objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
2	dDot1xExtLoggedFail This trap is sent when a host failed to pass IEEE 802.1X authentication (login failed). Binding Objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.14.30.0.2

Authentication Fail

Trap Name	Description	OID
1	authenticationFailure This 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 SNMPv2 must be capable to generate this trap, the <i>snmpEnableAuthenTraps</i> object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

DHCP Server Screen Prevention

Trap Name	Description	OID
1	dDhcpFilterAttackDetected This trap is sent when DHCP server screen is enabled and the switch received a forged DHCP Server packet. Binding Objects: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1

DoS Prevention

Trap Name	Description	OID
1	dDosPreveAttackDetectedPacket This trap is sent when a DoS attack is detected. Binding Objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.59.0.2

ErrDisable

Trap Name	Description	OID
1 dErrDisNotifyPortDisabledAss ert	This trap is sent when a port enters the error-disabled state. Binding Objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
2 dErrDisNotifyPortDisabledCle ar	This trap is sent when a port-loop restarts after the interval time. Binding Objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2

General Management

Trap Name	Description	OID
1 dGenMgmtLoginFail	This trap is sent when the user login failed to the switch. Binding Objects: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.14.165.0.1

Gratuitous ARP

Trap Name	Description	OID
1 agentGratuitousARPTrap	This trap is sent when an IP address conflict occurred. Binding Objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.14.75.0.1

IMPB

Trap Name	Description	OID
1 dImpbViolationTrap	This trap is sent when the switch detects an IPMB address violation. Binding Objects: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.171.14.22.0.1

LACP

Trap Name	Description	OID
1 linkUp	This trap signifies that the SNMP entity, acting in an agent role, has detected that the <i>ifOperStatus</i> object for one of its communication links left the down state and transitioned into another state (not the <i>notPresent</i> state). The new state is indicated in <i>ifOperStatus</i> . Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4

Trap Name	Description	OID
2	linkDown This trap signifies that the SNMP entity, acting in an agent role, has detected that the <i>ifOperStatus</i> object for one of its communication links is about to enter the down state from another state (not from the <i>notPresent</i> state). This old state is indicated in <i>ifOperStatus</i> . Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

LBD

Trap Name	Description	OID
1	dLbdLoopOccurred This trap is sent when an interface loop occurs. Binding Objects: (1) dLbdNotifyInfolIndex	1.3.6.1.4.1.171.14.46.0.1
2	dLbdLoopRestart This trap is sent when an interface loop restarts after the interval time. Binding Objects: (1) dLbdNotifyInfolIndex	1.3.6.1.4.1.171.14.46.0.2
3	dLbdVlanLoopOccurred This trap is sent when an interface with a VID loop occurs. Binding Objects: (1) dLbdNotifyInfolIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.3
4	dLbdVlanLoopRestart This trap is sent when an interface loop with a VID restarts after the interval time. Binding Objects: (1) dLbdNotifyInfolIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4

LLDP/LLDP-MED

Trap Name	Description	OID
1	lldpRemTablesChange This trap is sent when the value in <i>lldpStatsRemTableLastChangeTime</i> changes. Binding Objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2	lldpXMedTopologyChangeDetected This trap is sent by the local device sensing a change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding Objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1

MAC Notification

Trap Name	Description	OID
1	swL2macNotification This trap indicates a MAC address variation in the MAC address table. Binding Objects:	1.3.6.1.4.1.171.14.3.0.1

Trap Name	Description	OID
	(1) swL2macNotifyInfo	
2	dL2FdbMacNotificationWithVID This trap indicates a MAC address variation in the MAC address table. Binding Objects: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2

MSTP

Trap Name	Description	OID
1	newRoot This trap indicates that the sending agent has become the new root of the Spanning Tree. This trap is sent by a bridge after its election as the new root. For example, upon the expiration of the Topology Change Timer or immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
2	topologyChange This trap is sent by a bridge when any of its configured ports transitions from the <i>Learning</i> state to the <i>Forwarding</i> state, or from the <i>Forwarding</i> state to the <i>Blocking</i> state. This trap is not sent if a <i>newRoot</i> trap is sent for the same transition. Implementation of this trap is optional	1.3.6.1.2.1.17.0.2

Peripheral

Trap Name	Description	OID
1	dEntityExtFanStatusChg This trap is sent from the commander switch when a fan fails (<i>dEntityExtEnvFanStatus</i> is 'fault') or recovers (<i>dEntityExtEnvFanStatus</i> is 'ok'). Binding Objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171.14.5.0.1
2	dEntityExtThermalStatusChg This trap is sent from the commander switch when a thermal alarms (<i>dEntityExtEnvTempStatus</i> is 'abnormal') or recovers (<i>dEntityExtEnvTempStatus</i> is 'ok'). Binding Objects: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2

Port

Trap Name	Description	OID
1	linkUp This trap is generated when the port link status changes to up. Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown This trap is generated when the port link status changes to down. Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

Port Security

Trap Name	Description	OID
1	dPortSecMacAddrViolation This trap is sent when new MAC addresses violate the pre-defined port security configuration. Binding Objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfLastMacAddress	1.3.6.1.4.1.171.14.8.0.1

RMON

Trap Name	Description	OID
1	risingAlarm This trap is sent when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding Objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2	fallingAlarm This trap is sent 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
1	dSafeguardChgToExhausted This trap indicates a change in the system operation mode from normal to exhaust. Binding Objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
2	dSafeguardChgToNormal This trap indicates a change in the system operation mode from exhausted to normal. Binding Objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2

Start

Trap Name	Description	OID
1	coldStart This trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
2	warmStart This 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
1	dStormCtrlOccurred	This trap is sent when <i>dStormCtrlNotifyEnable</i> is <i>stormOccurred</i> or 'both', and a storm is detected. Binding Objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
2	dStormCtrlStormCleared	This trap is sent when <i>dStormCtrlNotifyEnable</i> is <i>stormCleared</i> or 'both', and a storm is cleared. Binding Objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2

System File

Trap Name		Description	OID
1	dsfUploadImage	This trap is sent when the user uploaded an image file successfully.	1.3.6.1.4.1.171.14.14.0.1
2	dsfDownloadImage	This trap is sent when the user downloaded an image file successfully.	1.3.6.1.4.1.171.14.14.0.2
3	dsfUploadCfg	This trap is sent when the user uploaded a configuration file successfully.	1.3.6.1.4.1.171.14.14.0.3
4	dsfDownloadCfg	This trap is sent when the user downloaded a configuration file successfully.	1.3.6.1.4.1.171.14.14.0.4
5	dsfSaveCfg	This trap is sent when the user saved the configuration file successfully.	1.3.6.1.4.1.171.14.14.0.5

Appendix C - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the 802.1X module.

The description that follows explains the following RADIUS Attributes Assignment types:

- VLAN

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 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.

Appendix D - 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 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