



Web UI Reference Guide

Product Model: DGS-1250 Series

Gigabit Ethernet Smart Managed Switch

Release 2.01

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

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

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

© 2020 D-Link Corporation. All rights reserved.

January, 2020 P/N 651GS1250025G

Table of Contents

1.	Introduction	1
	Audience	1
	Other Documentation.....	1
	Conventions	1
	Notes, Notices, and Cautions	2
2.	Web-based Switch Configuration	3
	Management Options	3
	Logging into the Web UI	4
	Smart Wizard	5
	Step 1 - Web Mode.....	5
	Step 2 - System IP Information.....	6
	Step 3 - User Accounts Settings	7
	Step 4 - SNMP Settings.....	8
	Web User Interface (Web UI)	9
	Areas of the User Interface.....	9
	Standard Mode.....	9
	Surveillance Mode.....	10
3.	System	12
	Device Information	12
	System Information Settings.....	13
	Peripheral Settings	13
	Port Configuration.....	14
	Port Settings	14
	Port Status	16
	Port Auto Negotiation	16
	Error Disable Settings.....	17
	Jumbo Frame	18
	Interface Description.....	19
	PoE	19
	PoE System.....	20
	PoE Status.....	21
	PoE Configuration	21
	PD Alive	23
	PoE Statistics	24
	PoE Measurement.....	24
	PoE LLDP Classification.....	25
	System Log	25
	System Log Settings.....	25
	System Log Discriminator Settings	26
	System Log Server Settings.....	27
	System Log	28
	System Attack Log.....	29
	Time and SNTP	29
	Clock Settings.....	29
	Time Zone Settings	30
	SNTP Settings	32
	Time Range	33
4.	Management	34
	User Accounts Settings	34
	SNMP.....	35
	SNMP Global Settings.....	36
	SNMP Linkchange Trap Settings	37
	SNMP View Table Settings	38

SNMP Community Table Settings	38
SNMP Group Table Settings	40
SNMP Engine ID Local Settings.....	41
SNMP User Table Settings.....	41
SNMP Host Table Settings.....	43
RMON	44
RMON Global Settings	44
RMON Statistics Settings	44
RMON History Settings	45
RMON Alarm Settings	46
RMON Event Settings	47
Telnet/Web.....	48
Session Timeout	48
DHCP	49
Service DHCP	49
DHCP Class Settings	50
DHCP Relay	51
DHCP Relay Global Settings	51
DHCP Relay Pool Settings.....	51
DHCP Relay Information Settings.....	54
DHCP Relay Information Option Format Settings.....	55
DHCP Local Relay VLAN Settings.....	56
DHCPv6 Relay	57
DHCPv6 Relay Global Settings.....	57
DHCPv6 Relay Interface Settings	58
DHCPv6 Relay Remote ID Profile Settings.....	59
DHCPv6 Relay Format Type Settings.....	61
DHCPv6 Local Relay VLAN Settings	61
DHCP Auto Configuration.....	62
DNS	62
DNS Global Settings.....	62
DNS Name Server Settings.....	63
DNS Host Settings.....	64
File System	64
D-Link Discovery Protocol	67
5. Layer 2 Features	68
FDB.....	68
Static FDB.....	68
Unicast Static FDB	68
MAC Address Table Settings	69
MAC Address Table	70
MAC Notification.....	71
VLAN.....	72
VLAN Configuration Wizard.....	72
Create/Configure VLAN.....	72
802.1Q VLAN	75
VLAN Interface	76
VLAN Interface Settings	76
Port Summary	79
Asymmetric VLAN	79
L2VLAN Interface Description	80
Auto Surveillance VLAN	80
Auto Surveillance Properties	80
MAC Settings and Surveillance Device.....	82
ONVIF IP-Camera Information	83
ONVIF NVR Information.....	85
Voice VLAN	86
Voice VLAN Global.....	86

Voice VLAN Port	87
Voice VLAN OUI	88
Voice VLAN Device	88
Voice VLAN LLDP-MED Device	89
STP	89
STP Global Settings	91
STP Port Settings	93
MST Configuration Identification	94
STP Instance	95
MSTP Port Information	96
Loopback Detection	96
Link Aggregation	97
L2 Multicast Control	102
IGMP Snooping	102
IGMP Snooping Settings	102
IGMP Snooping Groups Settings	104
IGMP Snooping Mrouter Settings	105
IGMP Snooping Statistics Settings	106
MLD Snooping	107
MLD Snooping Settings	108
MLD Snooping Groups Settings	110
MLD Snooping Mrouter Settings	111
MLD Snooping Statistics Settings	112
Multicast Filtering Mode	113
LLDP	114
LLDP Global Settings	114
LLDP Port Settings	115
LLDP Management Address List	116
LLDP Basic TLVs Settings	116
LLDP Dot1 TLVs Settings	118
LLDP Dot3 TLVs Settings	119
LLDP-MED Port Settings	120
LLDP Statistics Information	121
LLDP Local Port Information	122
LLDP Neighbor Port Information	123
6. Layer 3 Features	126
ARP	126
ARP Aging Time	126
Static ARP	127
ARP Table	127
Gratuitous ARP	128
IPv6 Neighbor	129
Interface	129
IPv4 Interface	129
IPv6 Interface	131
IPv4 Static/Default Route	134
IPv4 Route Table	136
IPv6 Static/Default Route	136
IPv6 Route Table	137
IP Multicast Routing Protocol	138
IPMC	138
IP Multicast Routing Forwarding Cache Table	138
IPv6MC	138
IPv6 Multicast Routing Forwarding Cache Table	138
7. Quality of Service (QoS)	140
Basic Settings	140
Port Default CoS	140

Port Scheduler Method	141
Queue Settings	142
CoS to Queue Mapping	143
Port Rate Limiting	143
Queue Rate Limiting	144
Advanced Settings	145
DSCP Mutation Map	145
Port Trust State and Mutation Binding	147
DSCP CoS Mapping	148
Class Map	148
Policy Map	150
Policy Binding	152
8. Access Control List (ACL)	153
ACL Configuration Wizard	153
Step 1 - Create/Update	153
Step 2 - Select Packet Type	154
Step 3 - Add Rule	155
MAC	155
IPv4	157
IPv6	160
Step 4 - Apply Port	162
ACL Access List	163
Standard IP ACL	165
Extended IP ACL	166
Standard IPv6 ACL	168
Extended IPv6 ACL	169
Extended MAC ACL	171
ACL Interface Access Group	173
9. Security	175
Port Security	175
Port Security Global Settings	175
Port Security Port Settings	176
Port Security Address Entries	177
802.1X	177
802.1X Global Settings	182
802.1X Port Settings	183
Authentication Sessions Information	184
Authenticator Statistics	184
Authenticator Session Statistics	185
Authenticator Diagnostics	186
AAA	187
AAA Global Settings	187
Authentication Settings	187
RADIUS	188
RADIUS Global Settings	188
RADIUS Server Settings	188
RADIUS Group Server Settings	189
RADIUS Statistic	190
IMPB	191
IPv4	191
DHCPv4 Snooping	191
Dynamic ARP Inspection	195
IP Source Guard	200
Advanced Settings	202
IPv6	204
IPv6 Snooping	204
IPv6 ND Inspection	205
IPv6 RA Guard	206
IPv6 DHCP Guard	207

IPv6 Source Guard.....	208
DHCP Server Screening.....	210
DHCP Server Screening Global Settings	210
DHCP Server Screening Port Settings.....	211
ARP Spoofing Prevention	212
Network Access Authentication	213
Guest VLAN.....	213
Network Access Authentication Global Settings	213
Network Access Authentication Port Settings	215
Network Access Authentication Sessions Information	216
Safeguard Engine	216
Safeguard Engine Settings.....	218
CPU Protect Counters	218
CPU Protect Sub-Interface	219
CPU Protect Type.....	220
Trusted Host	220
Traffic Segmentation Settings.....	221
Storm Control Settings.....	222
DoS Attack Prevention Settings	224
SSH.....	225
SSH Global Settings.....	226
Host Key	227
SSH Server Connection	228
SSH User Settings.....	228
SSL	229
SSL Global Settings	230
Crypto PKI Trustpoint	231
SSL Service Policy	232
Network Protocol Port Protect Settings	233
10. OAM.....	234
Cable Diagnostics.....	234
11. Monitoring	236
Utilization	236
Port Utilization	236
Statistics.....	237
Port	237
Interface Counters	238
Counters	240
Mirror Settings	241
Device Environment.....	243
12. Green.....	244
Power Saving.....	244
EEE.....	246
13. Toolbar.....	247
Save	247
Save Configuration	247
Tools	247
Firmware Upgrade & Backup	247
Firmware Upgrade from HTTP	247
Firmware Upgrade from TFTP	248
Firmware Backup to HTTP	248
Firmware Backup to TFTP	249
Configuration Restore & Backup	249
Configuration Restore from HTTP.....	249
Configuration Restore from TFTP	250

Configuration Backup to HTTP	251
Configuration Backup to TFTP	251
Certificate & Key Restore & Backup.....	252
Certificate & Key Restore from HTTP	252
Certificate & Key Restore from TFTP.....	252
Public Key Backup to HTTP	253
Public Key Backup to TFTP	253
Log Backup.....	254
Log Backup to HTTP	254
Log Backup to TFTP	254
Ping.....	255
Language Management.....	256
Reset	257
Reboot System	257
Wizard.....	258
Online Help	258
D-Link Support Site	258
User Guide	258
Surveillance Mode	258
Logout.....	259
14. Surveillance Mode	260
Surveillance Overview	260
Surveillance Topology	260
Device Information.....	263
Port Information	264
Group Details.....	265
IP-Camera Information	266
NVR Information	267
PoE Information	268
PoE Scheduling	269
Management.....	270
File System.....	270
Time	272
Clock Settings.....	272
SNTP Settings	273
Surveillance Settings	274
Surveillance Log	275
Health Diagnostic.....	276
Toolbar.....	277
Wizard.....	277
Tools	277
Firmware Upgrade & Backup	277
Configuration Restore & Backup.....	278
Language Management	279
Reset	280
Reboot System.....	280
Save.....	281
Save Configuration.....	281
Help	282
Online Help	283
D-Link Support Site	283
User Guide	283
Standard Mode	283
Logout.....	283
Appendix A - System Log Entries	284

Appendix B - Trap Entries	302
Appendix C - RADIUS Attributes Assignment	310
Appendix D - IETF RADIUS Attributes Support	311

1. Introduction

This manual's software descriptions are based on the software release **2.01**. The features listed here are the subset of features that are supported by the DGS-1250 Series Switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the Switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DGS-1250 Series Switch, which will be generally be referred to simply as the "Switch" within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

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

- *DGS-1250 Series Hardware Installation Guide*
- *DGS-1250 Series CLI Reference Guide*

Conventions

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

Notes, Notices, and Cautions

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



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



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



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

2. Web-based Switch Configuration

Management Options

Logging into the Web UI

Smart Wizard

Web User Interface (Web UI)

Management Options

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

Command Line Interface (CLI)

The Switch can be managed, out-of-band, by using the console port on the front panel of the Switch. Alternatively, the Switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on the Switch.

For more information about the CLI, refer to the *DGS-1250 Series CLI Reference Guide*.

SNMP-based Management

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

Web User Interface (Web UI)

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

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

Logging into the Web UI

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



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

NOTE: The factory default username is *admin* and password is *admin*.

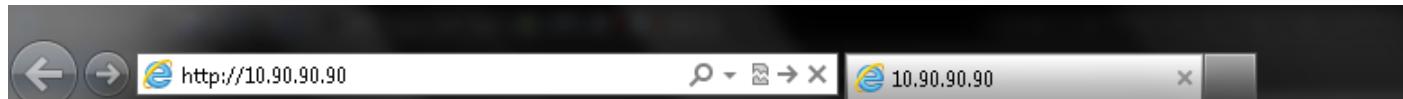


Figure 2-1 Displays entering the IP address in Internet Explorer

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

User Name	admin
Password	*****
Language	English
<input type="button" value="Login"/> <input type="button" value="Reset"/>	

Figure 2-2 Web UI Login Window

Enter the **User Name** and **Password** in the corresponding fields and click the **Login** button.

After clicking the **Login** button, the Web UI opens.

The management features available in the Web UI of the Switch are explained in the chapters below.



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** and **Surveillance Mode**.

- The **Standard Mode** is used to configure, manage, and monitor most of the software features on the Switch.
- The **Surveillance Mode** is an additional web mode specifically designed to assist the user with surveillance features supported by the Switch.



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

The screenshot shows the 'Welcome to Smart Wizard' interface. At the top, it says 'Welcome to Smart Wizard'. Below that is a message: '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.' A blue circular icon with a star and gear is displayed. The main area is titled 'Step 1 of 4: Choose the web interface mode.' It shows a 'Web Mode' section with two radio buttons: 'Standard Mode' (selected) and 'Surveillance Mode'. At the bottom left is a checkbox 'Ignore the wizard next time'. At the bottom right are 'Exit' and 'Next' buttons.

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.

The screenshot shows the 'Welcome to Smart Wizard' interface. At the top, it says 'Welcome to Smart Wizard' and 'Step 2 of 4: The wizard will help to complete settings for System IP address, Netmask, and Gateway.' Below this, there is a decorative icon of a wizard's hat. The main section is titled 'System IP Information'. It contains two radio buttons: 'Static' (selected) and 'DHCP'. Under 'Static', there are three input fields: 'IP Address' (10 . 90 . 90 . 90), 'Netmask' (8 (255.0.0.0)), and 'Gateway' (0 . 0 . 0 . 0). At the bottom of the wizard window, there is a checkbox labeled 'Ignore the wizard next time' and three buttons: 'Exit', 'Back', and 'Next'.

Figure 2-4 System IP Information

The fields that can be configured are described below:

Parameter	Description
Static	Select this option to manually assign and configure the IP address settings for the Switch.
DHCP	Select this option to obtain IP address settings automatically from a DHCP server for the Switch.
IP Address	After selecting the Static option, manually enter the IP address of the Switch here.
Netmask	After selecting the Static option, manually select the Netmask option here.
Gateway	After selecting the Static option, manually enter the IP address of the default gateway 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 **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.

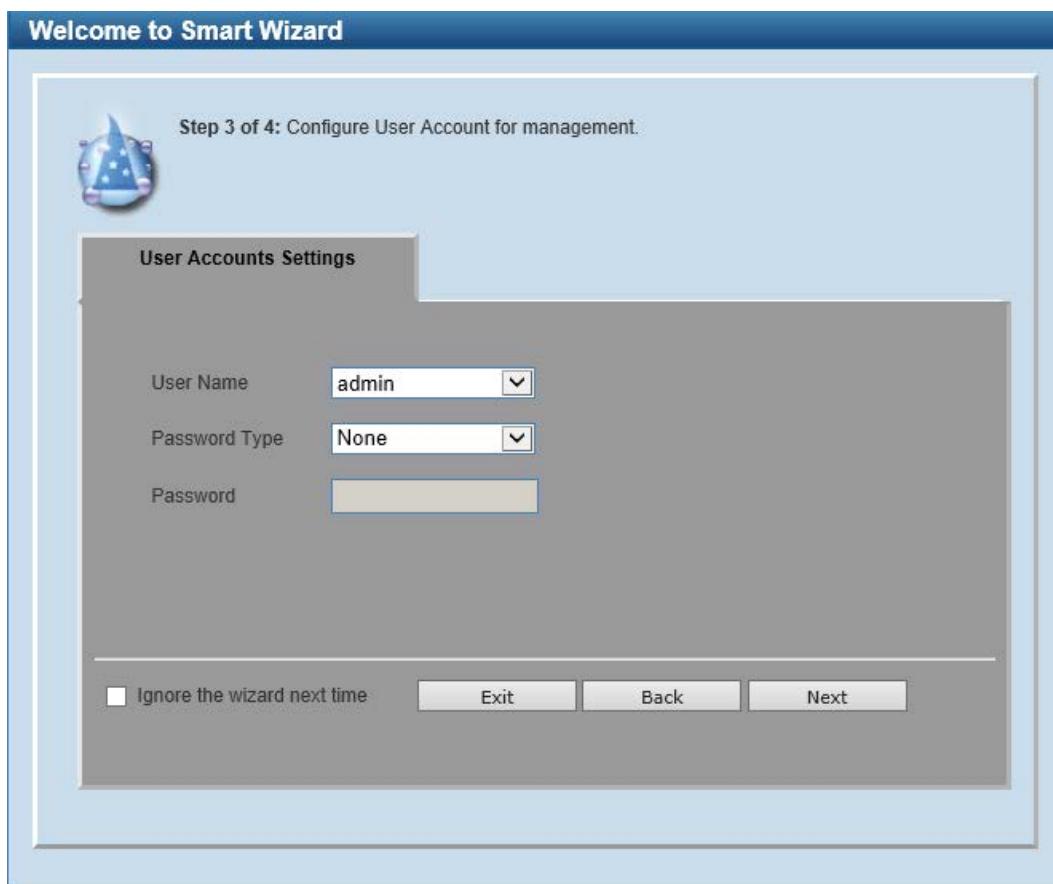


Figure 2-5 User Account Settings

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user name here.
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	After selecting Plain Text as the Password Type , 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.

Step 4 - SNMP Settings

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

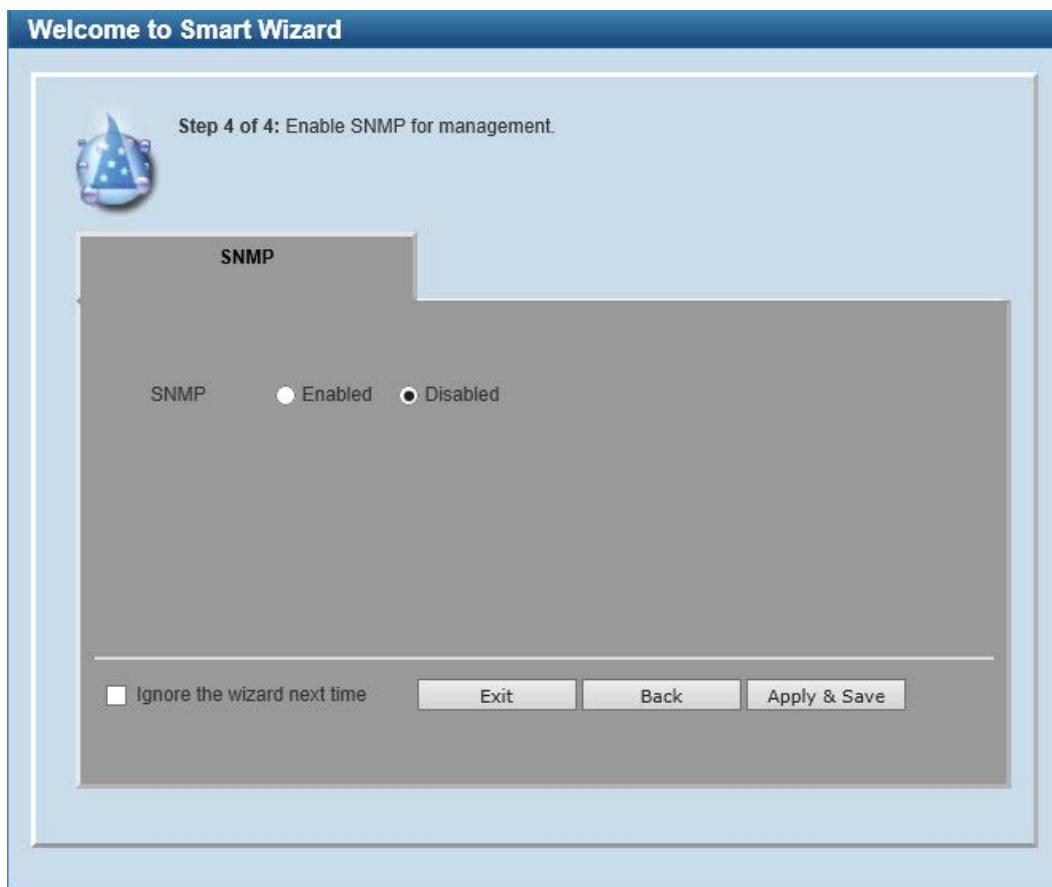


Figure 2-6 SNMP Window

The fields that can be configured are described below:

Parameter	Description
SNMP	Select to enable or disable the SNMP function 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 User Interface (Web UI)

Areas of the User Interface

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

Standard Mode

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



Figure 2-7 Web UI (Standard Mode)

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

Area Number	Description
AREA 4	In this area, configuration and monitoring window frames are available based on the selections made in Area 3.

Surveillance Mode

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

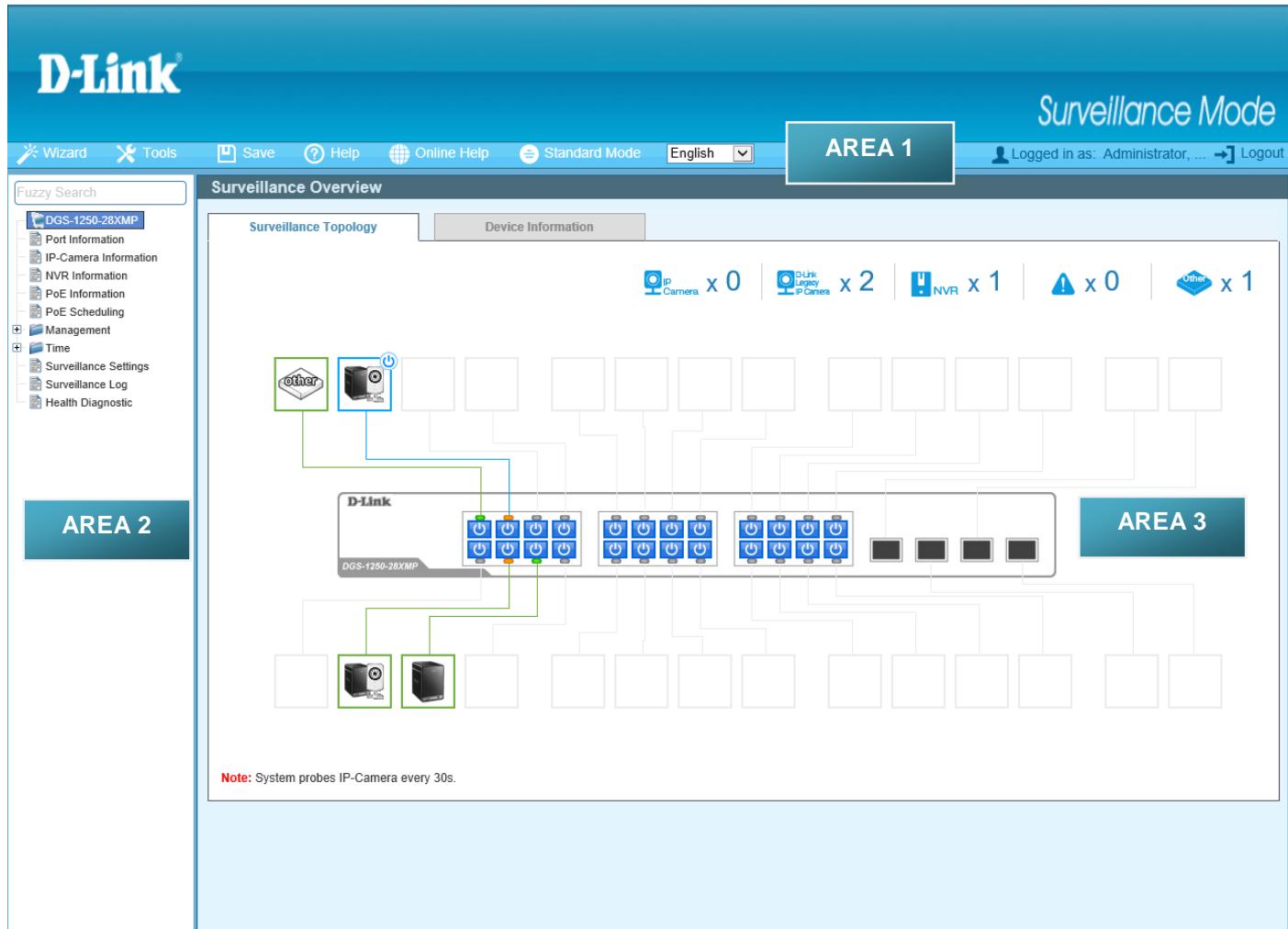


Figure 2-8 Web UI (Surveillance Mode)

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

Area Number	Description
	The status of devices, IP cameras, and NVRs discovered on the switch will also be displayed in this area.



NOTE: For more information about the Surveillance Mode, refer to **Surveillance Mode** on page 260.

3. System

Device Information

System Information Settings

Peripheral Settings

Port Configuration

PoE

System Log

Time and SNTP

Time Range

Device Information

In the Device Information section, the user can view a list of basic information regarding the Switch. It appears automatically when you log on to the Switch. To return to the Device Information window after viewing other windows, click the **DGS-1250-28XMP** link.

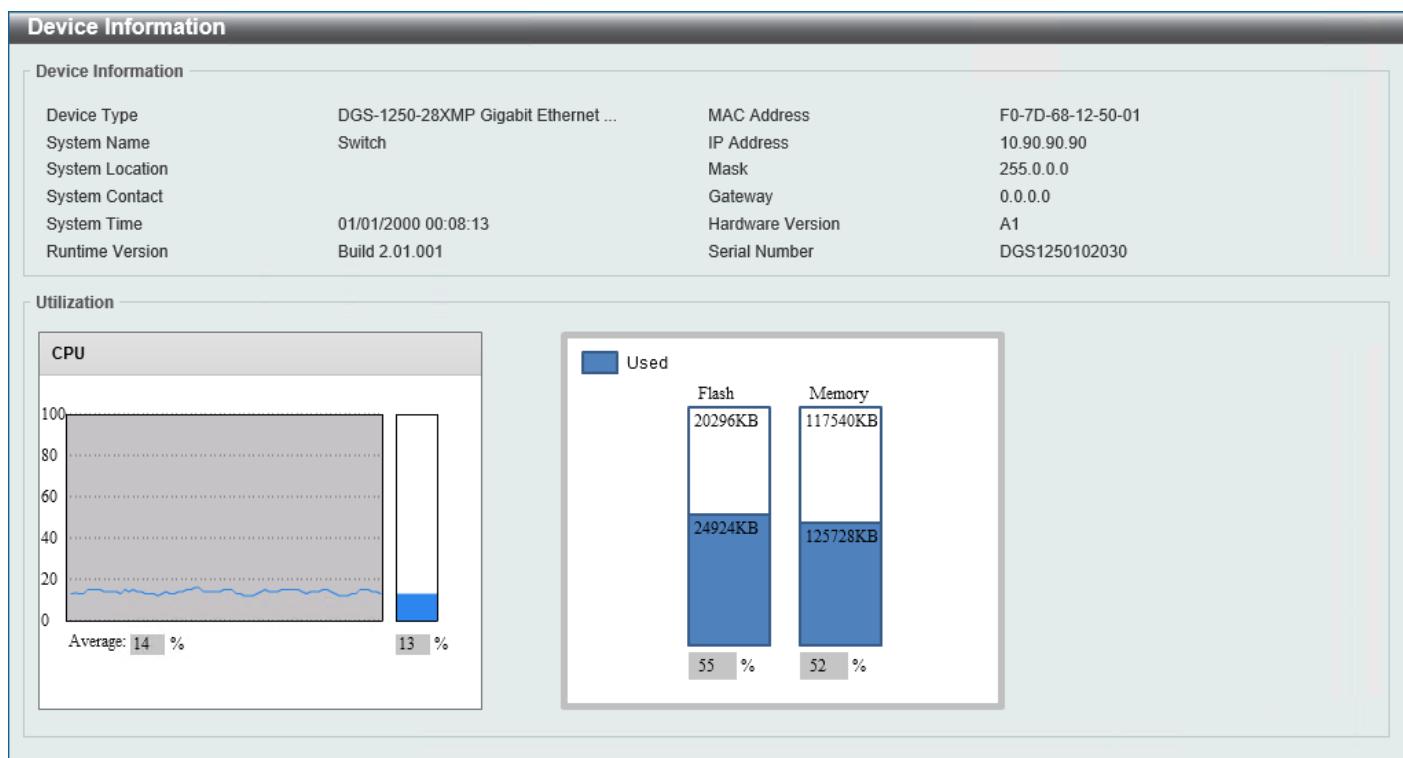


Figure 3-1 Device Information Window

System Information Settings

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

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

System Information Settings	
System Name	Switch
System Location	255 chars
System Contact	255 chars
Apply	

Figure 3-2 System Information Settings Window

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

Parameter	Description
System Name	Enter the system name for the Switch here. This name will identify it in the Switch network.
System Location	Enter the location description of the Switch here.
System Contact	Enter the contact information for the Switch here.

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

Peripheral Settings

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

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

Peripheral Settings	
Environment Trap Settings	
Fan Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Power Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Temperature Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Apply	
Environment Temperature Threshold Settings	
High Threshold (-100-200)	79 <input type="checkbox"/> Default
Low Threshold (-100-200)	11 <input type="checkbox"/> Default
Apply	

Figure 3-3 Peripheral Settings Window

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

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

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

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

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

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

Port Configuration

Port Settings

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

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

The screenshot shows the 'Port Settings' window with the following details:

- From Port:** eth1/0/1
- To Port:** eth1/0/1
- State:** Enabled
- MDIX:** Auto
- Flow Control:** Off
- Duplex:** Auto
- Speed:** Auto
- Capability Advertised:** 10M, 100M, 1000M
- Description:** 64 chars
- Buttons:** Apply

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 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.
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.

Parameter	Description
	<ul style="list-style-type: none"> 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. <p>Note: This option is only available on the 10/100/1000 Mbps RJ45 ports.</p>
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 , Half , and Full .
Speed	<p>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.</p> <p>The Master setting will allow the port to advertise capabilities related to duplex, speed, and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source.</p> <p>The Slave setting uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for master, the other side of the connection must be set for slave. Any other configuration will result in a 'link down' status for both ports.</p> <p>Options to choose from are:</p> <ul style="list-style-type: none"> Auto - Specifies that for copper ports, auto-negotiation will start to negotiate the speed and flow control with its link partner. For fiber ports, auto-negotiation will start to negotiate the clock and flow control with its link partner. 10M - Specifies to force the port speed to 10 Mbps. 100M - Specifies to force the port speed to 100 Mbps. 1000M - Specifies to force the port speed to 1 Gbps. 1000M Master - Specifies to force the port speed to 1 Gbps and operates as the master, to facilitate the timing of transmit and receive operations. 1000M Slave - Specifies to force the port speed to 1 Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. 10G - Specifies to force the port speed to 10 Gbps.
Capability Advertised	When the Speed is set to Auto , 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.

Port Status

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

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

Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	F0-7D-68-12-50-02	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
eth1/0/2	Not-Connected	F0-7D-68-12-50-03	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/3	Not-Connected	F0-7D-68-12-50-04	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/4	Not-Connected	F0-7D-68-12-50-05	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/5	Not-Connected	F0-7D-68-12-50-06	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/6	Not-Connected	F0-7D-68-12-50-07	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/7	Not-Connected	F0-7D-68-12-50-08	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/8	Not-Connected	F0-7D-68-12-50-09	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/9	Not-Connected	F0-7D-68-12-50-0A	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/10	Not-Connected	F0-7D-68-12-50-0B	1	Off	Off	Auto	Auto	1000BASE-T

Figure 3-5 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:

Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
eth1/0/1	Enabled	-	Complete	10M_Half, ...	10M_Half, ...	10M_Half, ...	-	-
eth1/0/2	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/3	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/4	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/5	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/6	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/7	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/8	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/9	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/10	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-

Figure 3-6 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:

The screenshot shows the 'Error Disable Settings' configuration page. It includes sections for 'Error Disable Trap Settings' and 'Error Disable Recovery Settings'. In the trap settings, 'Asserted' and 'Cleared' are both set to 'Disabled'. The notification rate is set to 0. In the recovery settings, 'ErrDisable Cause' is set to 'All', and the state is 'Disabled'. The recovery interval is set to 300 seconds. A table lists five error causes: Port Security, Storm Control, Dynamic ARP Inspection, DHCP Snooping, and Loopback Detect, all with a state of 'Disabled' and an interval of 300 seconds. Below this is a table for interfaces that will be recovered at the next timeout, with columns for Interface, VLAN, ErrDisable Cause, and Time Left (sec).

Figure 3-7 Error Disable Settings Window

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

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

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

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

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

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

Jumbo Frame

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

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

The screenshot shows the 'Jumbo Frame' configuration window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1') and 'To Port' (set to 'eth1/0/1'), and an input field for 'Maximum Receive Frame Size (64-12288) bytes' (set to '1536'). An 'Apply' button is located to the right of the input field. Below this, a table lists the current maximum receive frame size for each port from eth1/0/1 to eth1/0/10, all of which are set to 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 3-8 Jumbo Frame 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.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 12288 bytes. By default, this value is 1536 bytes.

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

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:

The screenshot shows a table titled "Interface Description" with the following data:

Total Entries: 30			
Interface	Status	Administrative	Description
eth1/0/1	up	enabled	
eth1/0/2	down	enabled	
eth1/0/3	down	enabled	
eth1/0/4	down	enabled	
eth1/0/5	down	enabled	
eth1/0/6	down	enabled	
eth1/0/7	down	enabled	
eth1/0/8	down	enabled	
eth1/0/9	down	enabled	
eth1/0/10	down	enabled	

At the bottom right of the table are navigation buttons: 1/3, <, <, 1, 2, 3, >, >, and Go.

Figure 3-9 Interface Description Window

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

PoE

The **DGS-1250-28XMP** and **DGS-1250-52XMP** switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All PoE-supported ports can supply up to 30 Watts of power. The Switch ports can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The Switch follows the standard Power Sourcing Equipment (PSE) pin-out Alternative A, whereby power is sent out over pins 1, 2, 3, and 6. The Switches work with all D-Link 802.3af capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD and automatically sends power to it.
- The auto-disable feature occurs under two conditions:
 - If the total power consumption exceeds the system power limit
 - If the per-port power consumption exceeds the per port power limit
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

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

Class	Maximum power used by the PD	Maximum power supplied by the Switch
0	12.95 Watts	15.4 Watts
1	3.84 Watts	4 Watts
2	6.49 Watts	7 Watts
3	12.95 Watts	15.4 Watts
4	25.5 Watts	30 Watts

PoE System

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

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

The screenshot shows the PoE System configuration window. At the top, there are three input fields: 'Usage Threshold (1-99)' with value '99', 'Policy Preempt' set to 'Disabled', and 'Trap State' set to 'Disabled'. Below these are two buttons: 'Apply' and 'Show Detail'. A summary table follows, containing five columns: Delivered (W), Power Budget (W), Usage Threshold (%), Policy Preempt, and Trap State. The values are 0, 370, 99, Disabled, and Disabled respectively.

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

Figure 3-10 PoE System Window

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

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

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

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

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

The screenshot shows the PoE System configuration window with the 'Show Detail' button clicked. It includes the same top-level fields as Figure 3-10, plus a new section titled 'PoE System Parameters' containing a table with three columns: Max Ports (24), Device ID (E121), and SW Version (30).

Max Ports	Device ID	SW Version
24	E121	30

Figure 3-11 PoE System (Show Detail) Window

PoE Status

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

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

PoE Status						
PoE Status						
From Port	To Port	Description				
eth1/0/1	eth1/0/1	32 chars				Apply
Port	State	Class	Max (W)	Used (W)	Description	
eth1/0/1	Searching	N/A	0.0	0.0	Server	Delete Description
eth1/0/2	Searching	N/A	0.0	0.0		Delete Description
eth1/0/3	Searching	N/A	0.0	0.0		Delete Description
eth1/0/4	Searching	N/A	0.0	0.0		Delete Description
eth1/0/5	Searching	N/A	0.0	0.0		Delete Description
eth1/0/6	Searching	N/A	0.0	0.0		Delete Description
eth1/0/7	Searching	N/A	0.0	0.0		Delete Description
eth1/0/8	Searching	N/A	0.0	0.0		Delete Description
eth1/0/9	Searching	N/A	0.0	0.0		Delete Description
eth1/0/10	Searching	N/A	0.0	0.0		Delete Description

Figure 3-12 PoE Status Window

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

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

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

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

PoE Configuration

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



NOTE: If the Switch failed to supply power to the IEEE 802.3at PD,

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

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

The screenshot shows the PoE Configuration window with the following settings:

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

Figure 3-13 PoE Configuration Window

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

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are Critical , High and Low .
Legacy Support	Select this option to enable or disable the support of legacy PD.
Mode	Select the power management mode for the PoE ports. Options to choose from are Auto and Never .
Max Wattage	When selecting Auto in the Mode drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage that can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW.
Time Range	When selecting Auto in the Mode drop-down list, this option appears. Tick the check box and enter the name of the time range to determine the activation period.

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

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

PD Alive

This window is used to configure the PD Alive function for PDs connected to the PoE ports. The ping function is used to check if PDs, connected to the PoE ports, are active or not. When PDs appear to be inactive, the specified action (Reset, Notify, or Both) will be taken.

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

The screenshot shows the 'PD Alive' configuration window. At the top, there are dropdown menus for 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), and 'PD Alive State' (Disabled). Below these are input fields for 'Poll Interval (10-300)' (30 sec) and 'Retry Count (0-5)' (2). To the right are fields for 'Waiting Time (30-300)' (90 sec) and 'Action' (Both). An 'Apply' button is located at the bottom right. Below the configuration area is a table listing 10 ports (eth1/0/1 to eth1/0/10) with their respective configurations.

Port	PD Alive State	PD IP Address	Poll Interval	Retry Count	Waiting Time	Action
eth1/0/1	Disabled	0.0.0.0	30	2	90	Both
eth1/0/2	Disabled	0.0.0.0	30	2	90	Both
eth1/0/3	Disabled	0.0.0.0	30	2	90	Both
eth1/0/4	Disabled	0.0.0.0	30	2	90	Both
eth1/0/5	Disabled	0.0.0.0	30	2	90	Both
eth1/0/6	Disabled	0.0.0.0	30	2	90	Both
eth1/0/7	Disabled	0.0.0.0	30	2	90	Both
eth1/0/8	Disabled	0.0.0.0	30	2	90	Both
eth1/0/9	Disabled	0.0.0.0	30	2	90	Both
eth1/0/10	Disabled	0.0.0.0	30	2	90	Both

Figure 3-14 PD Alive 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.
PD Alive State	Select to enable or disable the PD Alive function on the specified port(s).
PD IP Address	Enter the IP address of the PD here.
Poll Interval	Enter the poll interval here. This is the interval between ping messages from the system to PDs connected to the PoE port(s). By default, this value is 30 seconds. The range is from 10 to 300 seconds.
Retry Count	Enter the retry count here. This is the amount of ping messages that will be sent (at each interval) when PDs are not responding. By default, this value is 2. The range is from 0 to 5.
Waiting Time	Enter the waiting time here. This is how long the system will wait before sending ping messages to the PD connected to the PoE port after the Reset action was taken. By default, this value is 90 seconds. The range is from 30 to 300 seconds.
Action	Select the action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> • Reset - Specifies to reset the PoE port state (turn PoE off and on). • Notify - Specifies to send logs and traps to notify the administrator. • Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

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

PoE Statistics

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

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

The screenshot shows a table titled "PoE Statistics" with a header "PoE Statistics Table". The table has columns for Port, MPS Absent, Overload, Short, Power Denied, Invalid Signature, and a "Clear All" button. Each row corresponds to a port from eth1/0/1 to eth1/0/10, with all values in the first six columns being 0. The "Invalid Signature" column contains values ranging from 118 to 238. Each row also has a "Clear" button in the last column.

Port	MPS Absent	Overload	Short	Power Denied	Invalid Signature	Clear All
eth1/0/1	0	0	0	0	173	<input type="button" value="Clear"/>
eth1/0/2	0	0	0	0	151	<input type="button" value="Clear"/>
eth1/0/3	0	0	0	0	170	<input type="button" value="Clear"/>
eth1/0/4	0	0	0	0	172	<input type="button" value="Clear"/>
eth1/0/5	0	0	0	0	172	<input type="button" value="Clear"/>
eth1/0/6	0	0	0	0	171	<input type="button" value="Clear"/>
eth1/0/7	0	0	0	0	238	<input type="button" value="Clear"/>
eth1/0/8	0	0	0	0	118	<input type="button" value="Clear"/>
eth1/0/9	0	0	0	0	146	<input type="button" value="Clear"/>
eth1/0/10	0	0	0	0	192	<input type="button" value="Clear"/>

Figure 3-15 PoE Statistics Window

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

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

PoE Measurement

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

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

The screenshot shows a table titled "PoE Measurement" with a header "PoE Measurement Table". The table has columns for Port, Voltage (V), Current (mA), Temperature (C), and Power (W). Each row corresponds to a port from eth1/0/1 to eth1/0/10, with all values in the first four columns being N/A. The "Power (W)" column also contains N/A.

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

Figure 3-16 PoE Measurement Window

PoE LLDP Classification

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

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

The screenshot shows a table with three rows, each representing a port. The columns are labeled "Port" and "PoE LLDP Classification Table".

Port	PSE TX information	Information from PD
Port eth1/0/1	None	None
Port eth1/0/2	None	None
Port eth1/0/3	None	None

Figure 3-17 PoE LLDP Classification Window

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 two main sections: "Log State" and "Buffer Log Settings".

Log State	
Log State	Enabled <input type="button" value="▼"/>
<input type="button" value="Apply"/>	

Buffer Log Settings	
Buffer Log State	Enabled <input type="button" value="▼"/>
Severity	4(Warnings) <input type="button" value="▼"/>
Discriminator Name	15 chars <input type="text"/>
Write Delay (0-65535)	300 sec <input type="checkbox"/> Infinite
<input type="button" value="Apply"/>	

Figure 3-18 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. This value must be between 0 and 65535 seconds. By default, this value is 300 seconds. Tick the Infinite option, to disable the write delay feature.

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

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:

The screenshot shows the 'System Log Discriminator Settings' window. At the top, it says 'Discriminator Log Settings'. Below that, there's a form for creating a new discriminator entry:

- Discriminator Name:** A text input field containing '15 chars'.
- Action:** A dropdown menu set to 'Drops', with other options like 'Includes' available.
- Severity:** A dropdown menu set to 'Drops', with other options like 'Emergency', 'Alert', etc., available.
- Facility List:** A list of checkboxes for various facility types, including PORT, STP, LAC, VOICE_VL..., and many others.
- Severity List:** A list of checkboxes for severity levels 0 through 7.
- Buttons:** An 'Apply' button at the bottom right and a 'Delete' button for the current entry.

At the bottom, there's a summary table showing the total entries (1) and the details of the single entry:

Name	Action	Facility List	Severity	Severity List
Name	Drops	DAI	Drops	7

Figure 3-19 System Log Discriminator Settings Window

The fields that can be configured are described below:

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

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

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

System Log Server Settings

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

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

The screenshot shows the 'System Log Server Settings' window. At the top, there are fields for 'Host IPv4 Address' (radio button selected), 'Host IPv6 Address' (radio button unselected), 'UDP Port (514,1024-65535)' (set to 514), 'Facility' (set to 23), 'Severity' (set to 4(Warnings)), and 'Discriminator Name' (set to 15 chars). Below these are 'Apply' and 'Delete' buttons. A table titled 'Total Entries: 1' lists one entry: Server IP 10.90.90.1, Severity Warnings, Facility 23, Discriminator Name (empty), UDP Port 514, and a 'Delete' button.

Figure 3-20 System Log Server Settings Window

The fields that can be configured are described below:

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

Parameter	Description		
14	logalert	Log alert	
15	clock2	Clock daemon	
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.		

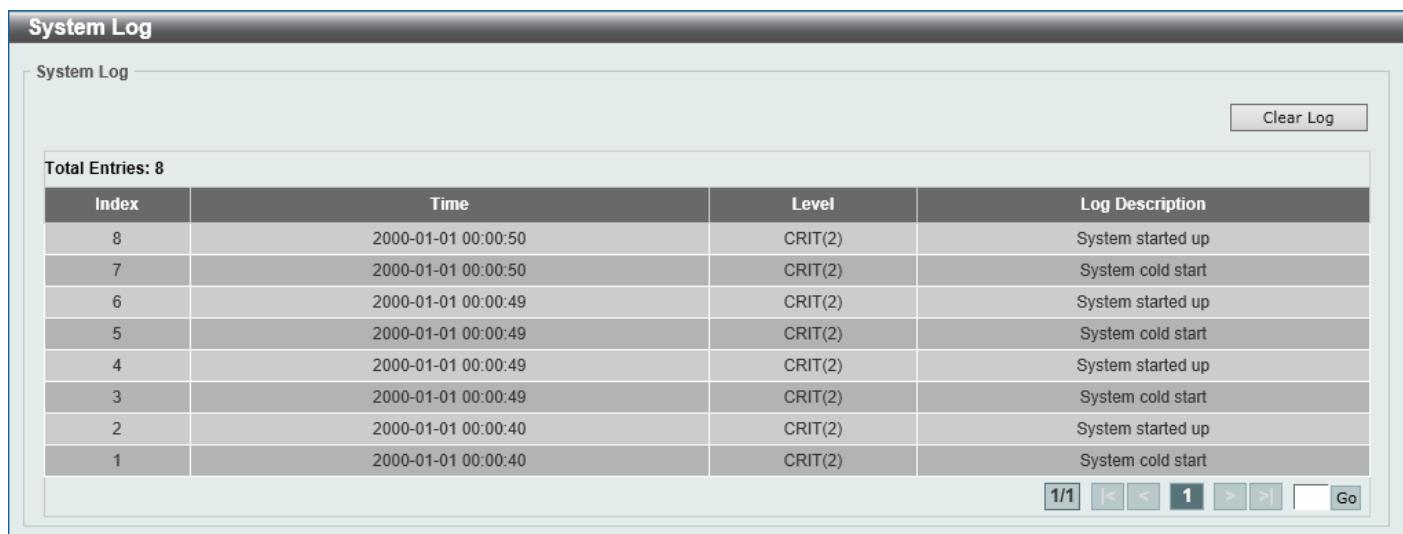
Click the **Apply** button to accept the changes made.

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 a web-based interface for viewing system logs. The title bar says "System Log". Below it is a sub-header "System Log". On the right side, there is a "Clear Log" button. The main area contains a table with 8 entries. The table has columns for Index, Time, Level, and Log Description. The entries are as follows:

Index	Time	Level	Log Description
8	2000-01-01 00:00:50	CRIT(2)	System started up
7	2000-01-01 00:00:50	CRIT(2)	System cold start
6	2000-01-01 00:00:49	CRIT(2)	System started up
5	2000-01-01 00:00:49	CRIT(2)	System cold start
4	2000-01-01 00:00:49	CRIT(2)	System started up
3	2000-01-01 00:00:49	CRIT(2)	System cold start
2	2000-01-01 00:00:40	CRIT(2)	System started up
1	2000-01-01 00:00:40	CRIT(2)	System cold start

At the bottom right of the table, there are navigation buttons: "1/1", '<', '<', '1', '>', '>', and a "Go" input field.

Figure 3-21 System Log Window

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

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

System Attack Log

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

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

System Attack Log			
Total Entries: 0			
Index	Time	Level	Log Description

Clear Attack Log

Figure 3-22 System Attack Log Window

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

Time and SNTP

Clock Settings

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

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

Clock Settings	
Time (HH:MM:SS)	00:06:10
Date (DD / MM / YYYY)	01/01/2000

Apply

Figure 3-23 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, 30/09/2019.

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:

The screenshot shows the 'Time Zone Settings' window with the following configuration fields:

- Summer Time State:** Set to **Disabled**.
- Time Zone:** Set to **+ 0 0 0**.
- Recurring Setting:**
 - From: Week of the Month - Last
 - From: Day of the Week - Sun
 - From: Month - Jan
 - From: Time (HH:MM) - 00 00
 - To: Week of the Month - Last
 - To: Day of the Week - Sun
 - To: Month - Jan
 - To: Time (HH:MM) - 00 00
 - Offset - 60
- Date Setting:**
 - From: Date of the Month - 01
 - From: Month - Jan
 - From: Year - (disabled)
 - From: Time (HH:MM) - 00 00
 - To: Date of the Month - 01
 - To: Month - Jan
 - To: Year - (disabled)
 - To: Time (HH:MM) - 00 00
 - Offset - 60

An **Apply** button is located at the bottom right of the window.

Figure 3-24 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.

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

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

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

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

SNTP Settings

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

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

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

The screenshot shows the 'SNTP Settings' window. The 'SNTP Global Settings' section contains fields for 'Current Time Source' (System Clock), 'SNTP State' (Disabled), and 'Poll Interval (30-99999)' (720 sec). The 'SNTP Server Setting' section shows a table with one entry: 'Total Entries: 1'. The table columns are 'SNTP Server', 'Version', and 'Last Receive'. The entry shows '10.90.90.1' in the 'SNTP Server' column. Buttons for 'Apply', 'Add', and 'Delete' are visible.

Figure 3-25 SNTP Settings Window

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

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

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

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

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

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

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

Time Range

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

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

Total Entries: 1					
Range Name	Start Weekday	Start Time	End Weekday	End Time	
Weekdays	Mon	00:00	Fri	23:59	<input type="button" value="Delete Periodic"/> <input type="button" value="Delete"/>

1/1 |< < 1 > >| Go

Figure 3-26 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

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.

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.

The screenshot shows a web-based configuration interface for managing user accounts. At the top, there are two tabs: "User Management Settings" (selected) and "Session Table". Below the tabs, there are input fields for "User Name" (32 chars) and "Password Type" (set to "None"). To the right of these fields is a "Password" input field and an "Apply" button. A message "Total Entries: 1" is displayed above a table. The table has columns for "User Name" and "Password". One entry is listed: "admin" with a password of "*****". To the right of the table are buttons for "Delete", "1/1", and navigation arrows. At the bottom right are buttons for "Go" and "1".

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	After selecting Plain Text as the password type, enter the password for this user account here.

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

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

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

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

Total Entries: 2			
Type	User Name	Login Time	IP Address
console	admin	2H15M27S	
* web	admin	9M12S	10.90.90.14
		1/1	< < < 1 > > Go

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 that 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:

The screenshot shows the 'SNMP Global Settings' window. It has two main sections: 'SNMP Global Settings' and 'Trap Settings'. Under 'SNMP Global Settings', there are three radio buttons: 'Enabled' (selected), 'Disabled', and another 'Enabled' button which is grayed out. Below these are two checkboxes: 'SNMP Response Broadcast Request' (selected) and 'SNMP UDP Port (1-65535)' with the value '161' entered. Under 'Trap Settings', there is a radio button for 'Trap Global State' (disabled) and a list of five checkboxes for trap types: 'SNMP Authentication Trap', 'Port Link Up', 'Port Link Down', 'Coldstart', and 'Warmstart'. A 'Apply' button is located at the bottom right of the window.

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 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:

SNMP Linkchange Trap Settings			
SNMP Linkchange Trap Settings			
From Port	To Port	Trap Sending	Trap State
eth1/0/1	eth1/0/1	Disabled	Disabled
<input type="button" value="Apply"/>			
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:

The screenshot shows the 'SNMP View Table Settings' window. At the top, there are input fields for 'View Name' (32 chars), 'Subtree OID' (N.N.N...N), and 'View Type' (Included). Below these are buttons for 'Add' and 'Delete'. A message indicates there are 'Total Entries: 8'. The main area is a table with columns: View Name, Subtree OID, View Type, and Delete button. The entries are:

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

Figure 4-5 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:

The screenshot shows the 'SNMP Community Table Settings' window. At the top, there are input fields for 'Key Type' (Plain Text), 'Community Name' (32 chars), 'View Name' (32 chars), 'Access Right' (Read Only), and 'IP Access-List Name' (32 chars). Below these is an 'Add' button. A table section displays 'Total Entries: 2' with columns: Community Name, View Name, Access Right, and IP Access-List Name. The entries are:

Community Name	View Name	Access Right	IP Access-List Name
public	CommunityView	ro	<button>Delete</button>
private	CommunityView	rw	<button>Delete</button>

Figure 4-6 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Key Type	The only supported key type 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. At the top, there's a form for creating a new group with fields for 'Group Name' (32 chars), 'User-based Security Model' (SNMPv1 selected), 'Security Level' (NoAuthNoPriv selected), and 'IP Access-List Name'. Below this is a table titled 'Total Entries: 5' containing five rows of group configurations. Each row includes columns for Group Name, Read View Name, Write View Name, Notify View Name, Security Model, Security Level, IP Access-List Name, and a Delete button.

Total Entries: 5							
Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level	IP Access-List Name	
public	CommunityV...		CommunityV...	v1			<input type="button" value="Delete"/>
public	CommunityV...		CommunityV...	v2c			<input type="button" value="Delete"/>
initial	restricted		restricted	v3	NoAuthNoPriv		<input type="button" value="Delete"/>
private	CommunityV...	CommunityV...	CommunityV...	v1			<input type="button" value="Delete"/>
private	CommunityV...	CommunityV...	CommunityV...	v2c			<input type="button" value="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 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:

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	Select the SNMP version. Options to choose from are v1 , v2c , and v3 .
SNMP V3 Encryption	When selecting v3 in the SNMP Version drop-down list, this option is available. Options to choose from are None , Password , and Key .
Auth-Protocol by Password	When selecting v3 in the SNMP Version drop-down list, and selecting Password in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are: <ul style="list-style-type: none"> • MD5 - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or key. • SHA - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or key.
Password	Enter the Auth-Protocol password here. For MD5 this password must be between 8 and 16 characters long. For SHA this password must be between 8 and 20 characters long.
Priv-Protocol by Password	When selecting v3 in the SNMP Version drop-down list, and selecting Password in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are: <ul style="list-style-type: none"> • None - Specify that no authorization protocol is in use. • DES56 - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
Password	Enter the Priv-Protocol password here. For none , this field will be disabled. For DES56 the password must be between 8 and 16 characters long.
Auth-Protocol by Key	When selecting v3 in the SNMP Version drop-down list, and selecting Key in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are: <ul style="list-style-type: none"> • MD5 - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. • SHA - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.
Key	Enter the Auth-Protocol key here. For MD5 this key must be 32 characters long. For SHA this key must be 40 characters long.
Priv-Protocol by Key	When selecting v3 in the SNMP Version drop-down list, and selecting Key in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are: <ul style="list-style-type: none"> • None - Specify that no authorization protocol is in use. • DES56 - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
Key	Enter the Priv-Protocol key here. For none , this field will be disabled. For DES56 the key must be 32 characters long.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the user.

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

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

SNMP Host Table Settings

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

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

The screenshot shows the 'SNMP Host Table Settings' window. At the top, there are configuration fields for a single host entry:

- Host IPv4 Address:** Selected (radio button).
- Host IPv6 Address:** Not selected (radio button).
- User-based Security Model:** SNMPv1 (selected from a dropdown).
- Security Level:** NoAuthNoPriv (selected from a dropdown).
- UDP Port (1-65535):** 162 (entered in a text field).
- Community String / SNMPv3 User Name:** private (entered in a text field).

Below these fields is a button labeled 'Add'.

A table titled 'Total Entries: 1' displays the current configuration:

Host IP Address	SNMP Version	UDP Port	Community String / SNMPv3 User Name	
10.90.90.123	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 default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string or SNMPv3 user name to be sent with the notification packet.

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

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

RMON

RMON Global Settings

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

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

RMON Global Settings		
RMON Global Settings RMON Rising Alarm Trap <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled RMON Falling Alarm Trap <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<input type="button" value="Apply"/>		

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:

RMON Statistics Settings										
RMON Statistics Settings Port * Index (1-65535) * Owner eth1/0/1 <input type="text"/> 127 chars										
<table border="1"> <thead> <tr> <th>Index</th> <th>Port</th> <th>Owner</th> <th>Owner</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>eth1/0/2</td> <td>Owner</td> <td><input type="button" value="Delete"/></td> </tr> </tbody> </table>			Index	Port	Owner	Owner	1	eth1/0/2	Owner	<input type="button" value="Delete"/>
Index	Port	Owner	Owner							
1	eth1/0/2	Owner	<input type="button" value="Delete"/>							
Add <input type="button" value="Delete"/> <input type="button" value="Show Detail"/>										
1/1 << < > >> 1 Go										

Figure 4-12 RMON Statistics Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

RMON Statistics Table																		
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	eth1/0/2	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)		Owner						
		Port	Index (1-65535)	Bucket Number (1-65535)	Interval (1-3600)			Owner						
<input type="button" value="Add"/>														
Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	<input type="button" value="Delete"/>	<input type="button" value="Show Detail"/>							
1	eth1/0/2	50	50	1800	Owner	<input type="button" value="Delete"/>	<input type="button" value="Show Detail"/>	1/1	<input type="button" value="<"/>	<input type="button" value="<"/>	<input type="button" value="1"/>	<input type="button" value=">"/>	<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. The default value is 50.
Interval	Enter the time in seconds in each polling cycle. The range is from 1 to 3600.
Owner	Enter the owner string. The string can be up to 127 characters.

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

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

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

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

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

Figure 4-15 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:

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

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

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

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

RMON Event Settings

This window is used to display and configure event entries.

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

The screenshot shows the 'RMON Event Settings' window. At the top, there are input fields for 'Index (1-65535)', 'Description' (1-127 chars), 'Type' (None selected), 'Community' (1-127 chars), and 'Owner' (1-127 chars). Below these is an 'Add' button. A table titled 'Total Entries: 1' displays one entry: Index 1, Description Event, Community blank, Event Trigger blank, Owner Owner, Last Trigger Time 0d:0h:0m:0s. Buttons for 'Delete' and 'View Logs' are next to the table, along with navigation buttons (1/1, <<, <, >, >>) and a 'Go' button.

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.

The screenshot shows the 'Event Logs Table' window. It displays a table with 'Total Entries: 0'. The table has columns for 'Log Index', 'Log Time', and 'Log Description'. A 'Back' button is located at the bottom right of the table area.

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:

The screenshot shows the 'Telnet/Web' configuration window. It has two main sections: 'Telnet Settings' and 'Web Settings'. In the 'Telnet Settings' section, 'Telnet State' is set to 'Enabled' and 'Port (1-65535)' is set to '23'. In the 'Web Settings' section, 'Web State' is set to 'Enabled' and 'Port (1-65535)' is set to '80'. Both sections have an 'Apply' button at the bottom right.

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. The range is from 1 to 65535.

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. The range is from 1 to 65535.

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:

The screenshot shows the 'Session Timeout' configuration window. It has four sections: 'Web Session Timeout (60-36000)', 'Console Session Timeout (0-1439)', 'Telnet Session Timeout (0-1439)', and 'SSH Session Timeout (0-1439)'. Each section has a text input field for the timeout value and a checkbox for 'Default'. The 'Apply' button is located at the bottom right.

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. The default 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. The default 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. The default 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. The default value is 3 minutes. Select the Default option to use the default value.

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

DHCP

Service DHCP

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

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

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

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:

The screenshot shows the 'DHCP Class Settings' window. At the top, there is a 'Class Name' input field with '32 chars' and an 'Apply' button. Below that is a table with one entry. The table has columns for 'Class Name' and 'Class'. The first row contains 'Class Name' and 'Class'. To the right of the table are 'Edit' and 'Delete' buttons. At the bottom are navigation buttons: '1/1', '<', '<', '1', '>', '>', and 'Go'.

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.

The screenshot shows the 'DHCP Class Option Settings' window. It includes fields for 'Class Name', 'Option (1-254)', 'Hex', and 'Bitmask'. There is also an 'Apply' button. Below these is a table with one entry. The table has columns for 'Option', 'Hex', and 'Bitmask'. To the right of the table is a 'Back' button.

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 Global Settings

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

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

DHCP Relay Global Settings	
DHCP Relay Global Settings DHCP Smart Relay State <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
<input type="button" value="Apply"/>	

Figure 4-24 DHCP Relay Global Settings Window

The fields that can be configured are described below:

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

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

DHCP Relay Pool Settings

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

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

DHCP Relay Pool Settings									
DHCP Relay Pool Settings Pool Name 32 chars <input type="button" value="Apply"/>									
Total Entries: 1 <table border="1"> <thead> <tr> <th>Pool Name</th> <th>Source</th> <th>Destination</th> <th>Class</th> </tr> </thead> <tbody> <tr> <td>Pool</td> <td><input type="button" value="Edit"/></td> <td><input type="button" value="Edit"/></td> <td><input type="button" value="Edit"/></td> </tr> </tbody> </table>		Pool Name	Source	Destination	Class	Pool	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>
Pool Name	Source	Destination	Class						
Pool	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>						
1/1 <input type="button" value="<"/> <input type="button" value="<"/> 1 <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>									

Figure 4-25 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

Source IP Address	Subnet Mask
10.90.90.254	255.0.0.0

Figure 4-26 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.

Destination Address
10.90.90.251

Figure 4-27 DHCP Relay Pool Destination Settings Window

The fields that can be configured are described below:

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

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

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

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

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

DHCP Relay Pool Class Settings	
Pool Name	Pool
Class Name	Please Select
Total Entries: 1	
Class Name	
Class	
<input type="button" value="Edit"/> <input type="button" value="Delete"/>	
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

Figure 4-28 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	
Pool Name	Pool
Class Name	Class
Relay Target	<input type="text"/>
Total Entries: 1	
Target Address	10.90.90.250
<input type="button" value="Delete"/> <input type="button" value="Apply"/> <input type="button" value="Back"/>	

Figure 4-29 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:

Figure 4-30 DHCP Relay Information Settings Window

The fields that can be configured are described below:

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

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

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

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

DHCP Relay Information Option Format Settings

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

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

Figure 4-31 DHCP Relay Information Option Format Settings Window

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

Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: <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.
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are: <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.

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 vendor 3 format will be used.

Parameter	Description
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 Settings

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

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

DHCP Local Relay VLAN Settings			
DHCP Local Relay VID List	<input type="text" value="1,3-5"/> <input type="checkbox"/> All VLANs	State	Disabled <input type="button" value="▼"/>
DHCP Local Relay VID List	1		<input type="button" value="Apply"/>

Figure 4-32 DHCP Local Relay VLAN Settings Window

The fields that can be configured are described below:

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

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



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

DHCPv6 Relay

DHCPv6 Relay Global Settings

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

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

Figure 4-33 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 remote ID. Options to choose from are: <ul style="list-style-type: none"> ASCII - Select to enter the ASCII string with a maximum of 128 characters in the text box. HEX - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are: <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: <ul style="list-style-type: none"> Lowercase - Specifies that the MAC format will be lowercase.

Parameter	Description
	<ul style="list-style-type: none"> ○ For example, aa-bb-cc-dd-ee-ff. ● Uppercase - Specifies that the MAC format will be uppercase. ○ For example, AA-BB-CC-DD-EE-FF.
Delimiter	Select the delimiter that will be used here. Options to choose from are: <ul style="list-style-type: none"> ● Hyphen - Specifies that the MAC address format will contain hyphens. For example, AA-BB-CC-DD-EE-FF. ● Colon - Specifies that the MAC address format will contain colons. For example, AA:BB:CC:DD:EE:FF. ● Dot - Specifies that the MAC address format will contain dots. For example, AA.BB.CC.DD.EE.FF. ● None - Specifies that the MAC address format will contain no delimiters. For example, AABBCCDDEEFF.
Delimiter Number	Specifies the delimiter number that will be used in the MAC address format here. Options to choose from are: <ul style="list-style-type: none"> ● 1 - Specifies to use a single delimiter. For example, AABBCC.DDEEFF. ● 2 - Specifies to use two delimiters. For example, AABB.CCDD.EEFF ● 5 - Specifies to use multiple delimiters. For example, AA.BB.CC.DD.EE.FF

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

DHCPv6 Relay Interface Settings

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

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

DHCPv6 Relay Interface Settings											
Interface VLAN (1-4094)	<input type="button" value="Apply"/> <input type="button" value="Find"/>										
Destination IPv6 Address	2012::100										
Output Interface VLAN (1-4094)	<input type="button" value="Delete"/>										
Interface VLAN (1-4094)	<input type="button" value="Find"/>										
Total Entries: 1 <table border="1"> <thead> <tr> <th>Interface</th> <th>Destination IPv6 Address</th> <th>Output Interface</th> <th></th> </tr> </thead> <tbody> <tr> <td>vlan1</td> <td>2019::10</td> <td>vlan1</td> <td><input type="button" value="Delete"/></td> </tr> </tbody> </table>				Interface	Destination IPv6 Address	Output Interface		vlan1	2019::10	vlan1	<input type="button" value="Delete"/>
Interface	Destination IPv6 Address	Output Interface									
vlan1	2019::10	vlan1	<input type="button" value="Delete"/>								
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">>"/> <input type="button" value="Go"/>											

Figure 4-34 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 4-35 DHCPv6 Relay Remote ID Profile Settings Window

The fields that can be configured are described below:

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

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. <ul style="list-style-type: none"> ● 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	Format Type Expert UDF
eth1/0/1	32 chars
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 4-36 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	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 Settings

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

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

DHCPv6 Local Relay VID List	All VLANs	State	Apply
1,3,5	<input type="checkbox"/>	Disabled	

Figure 4-37 DHCPv6 Local Relay VLAN Settings 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.

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:

The screenshot shows the 'DHCP Auto Configuration' window. It has a title bar 'DHCP Auto Configuration'. Below it, there's a section titled 'DHCP Auto Configuration' with a radio button group for 'Auto Configuration State'. The 'Enabled' radio button is selected. To the right of the radio buttons is an 'Apply' button. Below the radio buttons is a note: 'Note: If autoconfig state enabled, it won't take effect until reboot.'

Figure 4-38 DHCP Auto Configuration Window

The fields that can be configured are described below:

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

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

DNS

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

DNS Global Settings

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

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

The screenshot shows the 'DNS Global Settings' window. It has a title bar 'DNS Global Settings'. Below it, there's a section titled 'DNS Global Settings' with two configuration items: 'IP Domain Lookup' (set to 'Disabled') and 'IP Name Server Timeout (1-60)' (set to '3 sec'). To the right of these settings is an 'Apply' button.

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. This value is between 1 and 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:

DNS Name Server Settings	
<input checked="" type="radio"/> Name Server IPv4 <input type="text"/> <input type="radio"/> Name Server IPv6 <input type="text" value="2233::1"/> Apply	
Total Entries: 1	
Name Server	172.1.1.1
Delete	

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

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

DNS Host Settings

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

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

The screenshot shows the 'DNS Host Settings' window. At the top left is a 'Static Host Settings' section with fields for 'Host Name' (255 chars) and 'IP Address' (IPv4 or IPv6). Below this is a table header: 'Static Total Entries: 1' and 'Dynamic Total Entries: 0'. The table has columns: 'Host Name', 'IPv4/IPv6 Address', and 'Aging Time'. A single entry 'Host' maps to '172.2.2.2' with an 'Aging Time' of 'forever'. Navigation buttons at the bottom include 'Apply', 'Clear All', and page navigation (1/1, <, >, 1, Go).

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

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

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

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

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:

The screenshot shows the 'File System' window. At the top left is a 'Path' field set to 'C:' and a 'Go' button. Below this are buttons for 'Copy' and 'Boot File'. The main area is a table with columns: 'Drive', 'Media Type', 'Size (MB)', 'File System Type', and 'Label'. One entry is listed: 'C:' is the Drive, 'Flash' is the Media Type, '44' is the Size (MB), 'swfs' is the File System Type, and there is no Label.

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 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:

The screenshot shows a 'File System' window with the path 'C:/'. It includes a Go button, Previous, Copy, and Boot File buttons. A table lists files with columns: Index, Attr, Size (byte), Update Time, Name, and Delete buttons. The table contains the following data:

Index	Attr	Size (byte)	Update Time	Name	Delete
1	-rw	122858	Jan 01 2000 00:45:43	tech-support.log	Delete
2	-rw	8488464	Jan 01 2000 17:50:00	Image1	Delete
3	-rw	8486640	Jan 01 2000 01:08:30	Image2	Delete
4	-rw	1585	Jan 01 2000 00:01:30	Config1	Delete
5	-rw	29076	Jan 01 2000 00:04:25	Config2	Delete
6	d-	1360	Jan 01 2000 00:00:10	system	Delete

46305280 bytes total (20783104 bytes free)

Navigation buttons: 1/1, <, <, 1, >, >, Go

Figure 4-43 File System (Drive) Window

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

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

Click the **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.



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.

The screenshot shows a 'File System' window with the path 'C:/'. It includes a Go button, Previous, Copy, and Boot File buttons. A 'Copy File' dialog is open with Source set to 'startup-config' and Destination set to 'running-config'. There is a Replace checkbox, an Apply button, and a Cancel button.

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 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.

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

File System	
Path	C:
Boot File	
Boot Image	Image 1
Boot Configuration	Configuration 1
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Boot Image	Boot Configuration
/c:/Image1	/c:/Config1

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 Image 1 and Image 2 .
Boot Configuration	Select the boot configuration here. Options to choose from are Configuration 1 and Configuration 2 .

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

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

D-Link Discovery Protocol

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

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

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

Figure 4-46 D-Link Discovery Protocol Window

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

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

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

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

Parameter	Description
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.

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:

Unicast Static FDB			
Port	eth1/0/1	VID (1-4094)	MAC Address
Total Entries: 1			
VID	MAC Address	Port	
1	00-11-22-33-44-55	eth1/0/2	<input type="button" value="Delete"/>
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>			

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. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

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

After selecting the **MAC Address Learning** 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:

The screenshot shows the 'MAC Address Table' configuration window. At the top, there are three input fields: 'Port' (set to 'eth1/0/1'), 'VID (1-4094)' (empty), and 'MAC Address' (empty). To the right of these are three 'Clear Dynamic' buttons (by Port, VLAN, or MAC) and two 'Find' buttons. Below this is a table header row with columns: VID, MAC Address, Type, and Port. The table contains six entries:

VID	MAC Address	Type	Port
1	00-11-22-33-44-55	Static	eth1/0/2
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/1
1	10-BF-48-D6-E3-3B	Dynamic	eth1/0/1
1	5C-33-8E-43-B3-68	Dynamic	eth1/0/1
1	D0-AE-EC-D9-9E-5E	Dynamic	eth1/0/1
1	F0-7D-68-12-50-01	Static	CPU

At the bottom right are navigation buttons for pages 1/1, previous, next, and Go.

Figure 5-4 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port that will be used 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:

The screenshot shows the 'MAC Notification' configuration page. At the top, there are two tabs: 'MAC Notification Settings' (selected) and 'MAC Notification History'. The 'MAC Notification Global Settings' section contains fields for 'MAC Address Notification' (radio buttons for Enabled and Disabled, with Disabled selected), 'Interval (1-2147483647)' (text input field containing '1'), 'History Size (0-500)' (text input field containing '1'), 'MAC Notification Trap State' (radio buttons for Enabled and Disabled, with Disabled selected), and 'Trap Type' (dropdown menu set to 'Without VID'). Below this is an 'Apply' button. The main area displays port trap status for ports eth1/0/1 to eth1/0/14. It includes four dropdown menus: 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Added Trap' (Disabled), and 'Removed Trap' (Disabled). A large table lists the trap status for each port. The table has three columns: 'Port' (listing ports eth1/0/1 through eth1/0/14), 'Added Trap' (all set to 'Disabled'), and 'Removed Trap' (all set to 'Disabled').

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 globally enable or disable the MAC notification function.
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
Trap Type	Specifies the trap type. Options to choose from are Without VID and With VID .
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.

The screenshot shows a web-based configuration interface for a switch. At the top, there's a header bar with the title 'MAC Notification'. Below it is a navigation bar with two tabs: 'MAC Notification Settings' (which is currently selected) and 'MAC Notification History'. Underneath the tabs, there are two buttons: 'History Index' and 'MAC Changed Message'. A message box indicates 'Total Entries: 0'.

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:

The screenshot shows the first step of the VLAN Configuration Wizard. It has a title bar 'VLAN Configuration Wizard'. Below it is a list of options under 'VLAN Configuration Wizard': 'Create VLAN' (radio button selected) and 'Configure VLAN'. For 'Create VLAN', there is a text input field labeled 'VID (1-4094)' which is empty. For 'Configure VLAN', there is also a text input field labeled 'VID (1-4094)' which is also empty. In the bottom right corner, there is a 'Next' button.

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	
eth1/0/11	Hybrid	1	1	
eth1/0/12	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.

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.

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	2
eth1/0/11	Hybrid	1	1-2	
eth1/0/12	Hybrid	2	1	2
eth1/0/13	Hybrid	2	1-2	
eth1/0/14	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:

802.1Q VLAN						
802.1Q VLAN						
VID List	3 or 2-5					<input type="button" value="Apply"/> <input type="button" value="Delete"/>
Find VLAN						
VID (1-4094)				<input type="button" value="Find"/> <input type="button" value="Show All"/>		
Total Entries: 2						
VID	VLAN Name	Description	Tagged Member Ports	Untagged Member Ports	VLAN Type	
1	default			1/0/1-1/0/28		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	VLAN0002		1/0/10,1/0/12	1/0/11,1/0/13		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">>"/> <input type="button" value="Go"/>						

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.

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 modify the VLAN name.

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

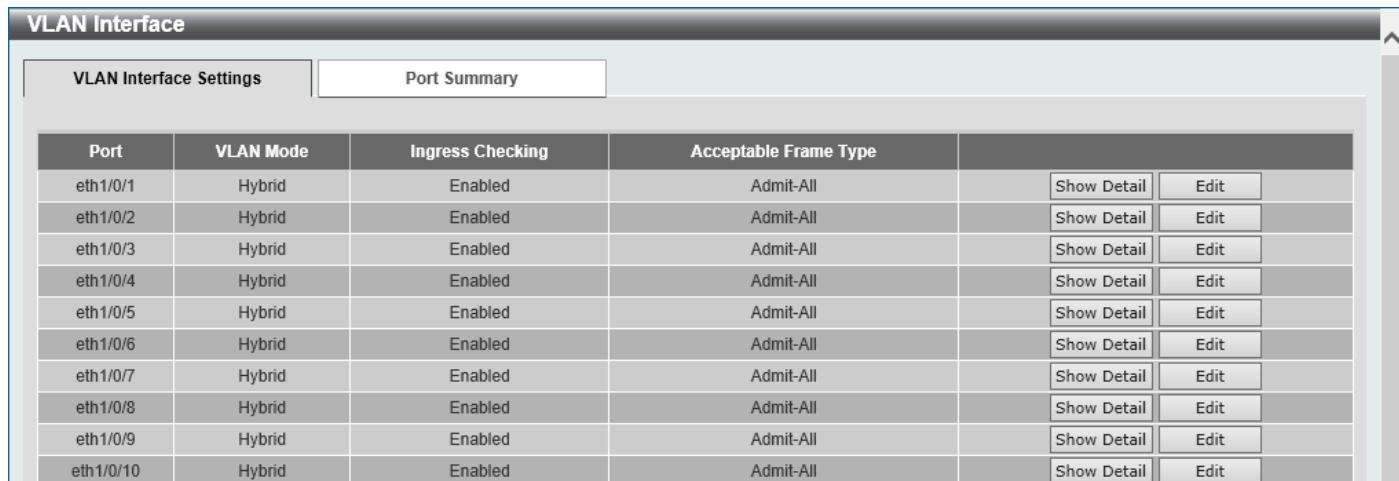
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

VLAN Interface

VLAN Interface Settings

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

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



The screenshot shows a web-based configuration interface for VLAN settings. At the top, there are two tabs: "VLAN Interface Settings" (selected) and "Port Summary". Below the tabs is a table with the following columns: Port, VLAN Mode, Ingress Checking, Acceptable Frame Type, Show Detail, and Edit. The table lists ten ports (eth1/0/1 to eth1/0/10), all configured in Hybrid mode with Ingress Checking enabled and Acceptable Frame Type set to Admit-All. Each row contains a "Show Detail" button and an "Edit" button.

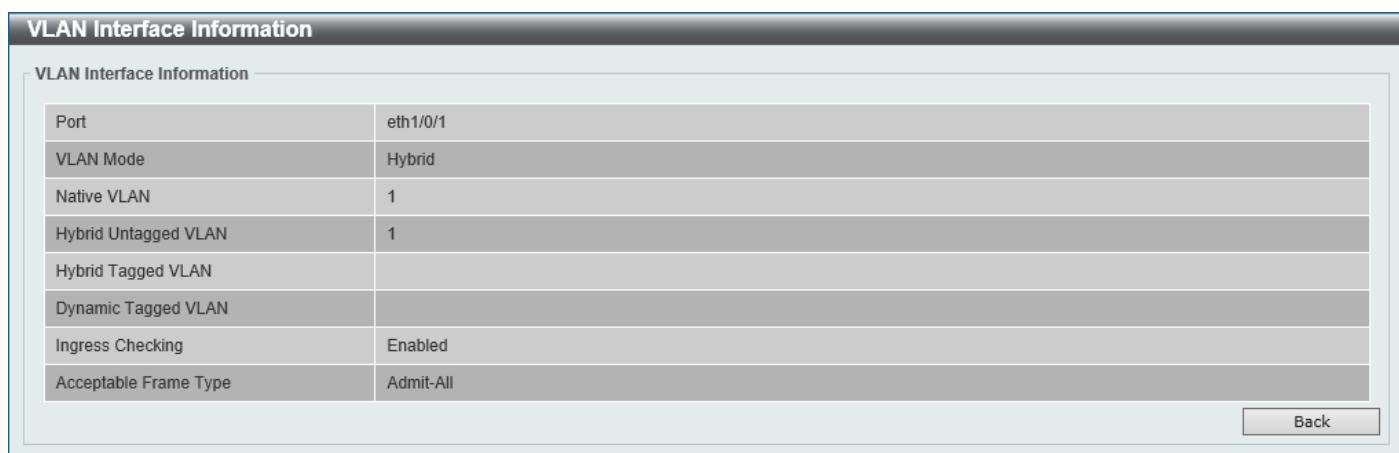
Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	Show Detail	Edit
eth1/0/1	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/2	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/3	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/4	Hybrid	Enabled	Admit-All	Show Detail	Edit
eth1/0/5	Hybrid	Enabled	Admit-All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



The screenshot shows a detailed configuration page for the VLAN interface of port eth1/0/1. The page title is "VLAN Interface Information". It displays the following settings for port eth1/0/1:

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

At the bottom right of the page is a "Back" button.

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.

Configure VLAN Interface

Configure VLAN Interface

Port	eth1/0/2	<input type="checkbox"/> Clone
VLAN Mode	Access	From Port
Acceptable Frame	Untagged Only	To Port
Ingress Checking	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	eth1/0/1
VID (1-4094)	1	eth1/0/1
Back Apply		

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.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.

Configure VLAN Interface

Configure VLAN Interface

Port	eth1/0/2	<input type="checkbox"/> Clone
VLAN Mode	Hybrid	From Port
Acceptable Frame	Admit All	To Port
Ingress Checking	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	eth1/0/1
Native VLAN	<input checked="" type="checkbox"/> Native VLAN	eth1/0/1
VID (1-4094)	1	
Action	Add	
Add Mode	<input checked="" type="radio"/> Untagged <input type="radio"/> Tagged	
Allowed VLAN Range	1	
Current Hybrid Untagged VLAN Range	1	
Current Hybrid Tagged VLAN Range		
Back Apply		

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 .

Parameter	Description
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the Native VLAN option, the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are Add , Remove , Tagged , and Untagged .
Add Mode	Select whether to add an Untagged or Tagged parameters.
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

When **Trunk** was selected as the **VLAN Mode**, the following page will appear.

The screenshot shows the 'Configure VLAN Interface' window for Trunk mode. The 'VLAN Mode' dropdown is set to 'Trunk'. Under 'Acceptable Frame', 'Admit All' is selected. 'Ingress Checking' is enabled. 'Native VLAN' is unchecked. 'VID (1-4094)' is set to 1. 'Action' is set to 'None'. There is an empty 'Allowed VLAN Range' input field. On the right, there are 'Clone' checkboxes for 'From Port' (set to eth1/0/1) and 'To Port' (set to eth1/0/1). At the bottom are 'Back' and 'Apply' buttons.

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. This value must be between 1 and 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.

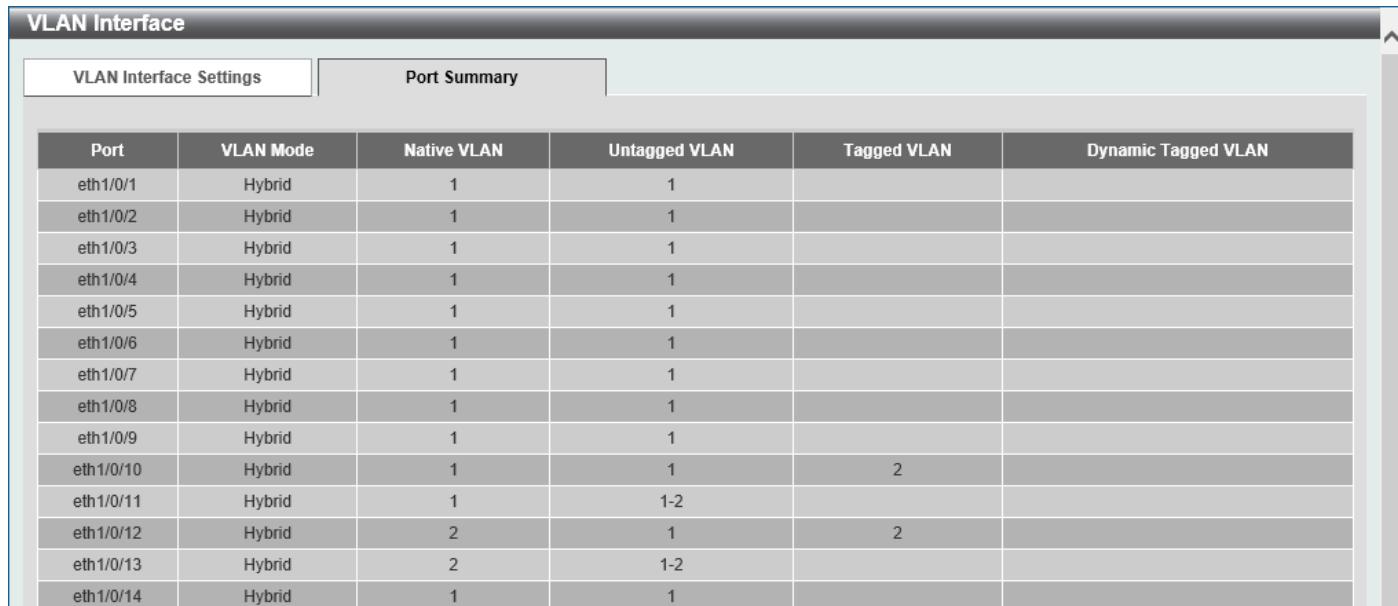
Parameter	Description
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

Port Summary

After selecting the **Port Summary** tab, the following page will be available.



The screenshot shows a table titled "VLAN Interface" with a "Port Summary" tab selected. The table has columns for Port, VLAN Mode, Native VLAN, Untagged VLAN, Tagged VLAN, and Dynamic Tagged VLAN. The rows list ports eth1/0/1 through eth1/0/14, all configured in Hybrid mode. The "Native VLAN" column shows values 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1-2, 1, 1-2, and 1 respectively. The "Untagged VLAN" column shows values 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1-2, 1, 1-2, and 1 respectively. The "Tagged VLAN" column shows values blank, 2, blank, blank, and blank respectively. The "Dynamic Tagged VLAN" column shows values blank, and blank respectively.

VLAN Interface					
VLAN Interface Settings		Port Summary			
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	2	
eth1/0/11	Hybrid	1	1-2		
eth1/0/12	Hybrid	2	1	2	
eth1/0/13	Hybrid	2	1-2		
eth1/0/14	Hybrid	1	1		

Figure 5-18 VLAN Interface 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:



The screenshot shows the "Asymmetric VLAN" configuration window. It has a title bar "Asymmetric VLAN" and a main area with a tree view "Asymmetric VLAN". Underneath, there is a section for "Asymmetric VLAN State" with two radio buttons: "Enabled" (unchecked) and "Disabled" (checked). A "Apply" button is located in the bottom right corner.

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:

The screenshot shows the 'L2VLAN Interface Description' window. It has two main sections: 'Create L2VLAN Interface Description' and 'Find L2VLAN Interface Description'.

Create L2VLAN Interface Description:

- L2VLAN Interface: A text input field.
- Description: A text input field with placeholder '64 chars'.
- Apply: A button to save changes.

Find L2VLAN Interface Description:

- L2VLAN Interface: A text input field.
- Find: A button to search.
- Show All: A button to view all entries.

Total Entries: 2

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

Navigation buttons at the bottom include: 1/1, <, <, 1, >, >, and 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 configure the auto-surveillance VLAN global settings and display the ports surveillance VLAN information.

The Switch regards a host as an NVR once it connects to the IPC via HTTP, HTTPS, or RTSP. The Switch will learn the NVR on this port and move it into the surveillance VLAN until the triggered aging mechanism age-out or the LAN cable is removed.

When the host sends an ARP request to an IPC, the Switch still regards the host as an NVR but only temporarily move it into the surveillance VLAN. The host will automatically be moved out of the surveillance VLAN after about 30 seconds if it is not recognized as an NVR anymore.



NOTE: The same PC, or PCs connected to the same LAN port on the Switch, cannot simultaneously manage the Switch and the IP cameras connected to the Switch.

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):
- 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
eth1/0/1	eth1/0/1	Disabled

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled

Figure 5-21 Auto Surveillance Properties Window

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

Parameter	Description
Surveillance VLAN State	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.
ONVIF Discover Port	Enter the TCP/UDP port number here. The range is either 554, or from 1025 to 65535. This is used to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.

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**, as shown below:

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	<input type="button" value="Delete"/>
2	D-Link Device	IP Surveillance...	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	<input type="button" value="Delete"/>
3	D-Link Device	IP Surveillance...	B0-C5-54-00-00-00	FF-FF-FF-80-00-00	<input type="button" value="Delete"/>
4	D-Link Device	IP Surveillance...	F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	<input type="button" value="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.
Mask	Enter the matching bitmask for the OUI MAC address here.

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

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

After selecting the **Auto Surveillance VLAN Summary** tab option, at the top of the page, the following page will be available.

Total Entries: 1				
Port	Component Type	Description	MAC Address	Start Time
eth1/0/3	D-Link Device	IP Surveillance...	28-10-7B-04-60-EE	2000-01-01 00:05

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:

Total Entries Discovered: 1								
Port	IP Address	MAC Address	Model	Manufacturer	Traffic	Description	Throughput (Mbps)	
eth1/0/3	192.168.70.110	28-10-7B-04-60-EE	DCS-5211L	DCS-5211L	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.

This screenshot shows the 'ONVIF IP-Camera Information' window with the title bar 'ONVIF IP-Camera Information'. It displays various parameters of an IP camera:

Port	eth1/0/3
IP Address	192.168.70.110
MAC Address	28-10-7B-04-60-EE
Model	DCS-5211L
Manufacturer	DCS-5211L
State	Enabled
Description	
Throughput	0 Mbps
Protocol	ONVIF
Power Consumption	3.7 (W) /15.4 (W)
PoE	802.3af
PoE Status	delivering

Buttons at the bottom right include 'Back' and 'Apply'.

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

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

This screenshot shows the 'ONVIF IP-Camera Settings' window with the title bar 'ONVIF IP-Camera Settings'. It includes fields for configuration:

Port	eth1/0/3
IP Address	192.168.70.110
MAC Address	28-10-7B-04-60-EE
IP-Camera State	Enabled <input type="button" value="▼"/>
Description	<input type="text"/>

Buttons at the bottom right include 'Back' and 'Apply'.

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:

ONVIF NVR Information																							
ONVIF NVR Information																							
Total Entries Discovered: 1																							
<table border="1"> <thead> <tr> <th>Port</th><th>IP Address</th><th>MAC Address</th><th>IP-Camera Number</th><th>Throughput (Mbps)</th><th>Group</th><th>Description</th><th></th></tr> </thead> <tbody> <tr> <td>eth1/0/6</td><td>192.168.70.13</td><td>10-BF-48-D6-E3-3B</td><td>1</td><td>2</td><td>1</td><td></td><td>IP-Camera List Edit</td></tr> </tbody> </table>								Port	IP Address	MAC Address	IP-Camera Number	Throughput (Mbps)	Group	Description		eth1/0/6	192.168.70.13	10-BF-48-D6-E3-3B	1	2	1		IP-Camera List Edit
Port	IP Address	MAC Address	IP-Camera Number	Throughput (Mbps)	Group	Description																	
eth1/0/6	192.168.70.13	10-BF-48-D6-E3-3B	1	2	1		IP-Camera List Edit																
Note: System probes IP-Camera every 30s.																							

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.

ONVIF IP-Camera List																	
ONVIF IP-Camera List																	
<table border="1"> <thead> <tr> <th>Port</th><th>IP Address</th><th>MAC Address</th><th>Group</th><th>Description</th><th></th></tr> </thead> <tbody> <tr> <td>eth1/0/6</td><td>192.168.70.110</td><td>28-10-7B-04-60-EE</td><td>1</td><td></td><td>Back</td></tr> </tbody> </table>						Port	IP Address	MAC Address	Group	Description		eth1/0/6	192.168.70.110	28-10-7B-04-60-EE	1		Back
Port	IP Address	MAC Address	Group	Description													
eth1/0/6	192.168.70.110	28-10-7B-04-60-EE	1		Back												
Port	IP Address	MAC Address	Group	Description													
eth1/0/6	192.168.70.110	28-10-7B-04-60-EE	1		Back												

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.

ONVIF NVR Information																							
ONVIF NVR Information																							
Total Entries Discovered: 1																							
<table border="1"> <thead> <tr> <th>Port</th><th>IP Address</th><th>MAC Address</th><th>IP-Camera Number</th><th>Throughput (Mbps)</th><th>Group</th><th>Description</th><th></th></tr> </thead> <tbody> <tr> <td>eth1/0/6</td><td>192.168.70.13</td><td>10-BF-48-D6-E3-3B</td><td>1</td><td>0</td><td>1</td><td><input type="text"/></td><td>IP-Camera List Apply</td></tr> </tbody> </table>								Port	IP Address	MAC Address	IP-Camera Number	Throughput (Mbps)	Group	Description		eth1/0/6	192.168.70.13	10-BF-48-D6-E3-3B	1	0	1	<input type="text"/>	IP-Camera List Apply
Port	IP Address	MAC Address	IP-Camera Number	Throughput (Mbps)	Group	Description																	
eth1/0/6	192.168.70.13	10-BF-48-D6-E3-3B	1	0	1	<input type="text"/>	IP-Camera List Apply																
Note: System probes IP-Camera every 30s.																							

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 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 complies with the OUI addresses.
Mode	<p>Select the mode here. Options to choose from are:</p> <ul style="list-style-type: none"> • Auto Untagged - Specifies that voice VLAN untagged membership will be automatically learned. • Auto Tagged - Specifies that voice VLAN tagged membership will be automatically learned. • Manual - Specifies that voice VLAN membership will be manually configured. <p>If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will automatically be aged out. When the port is working in the auto-tagged mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the Port VLAN ID (PVID).</p> <p>When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the voice VLAN.</p> <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			
OUI Address	Mask	Description	Apply
00-01-E3-00-00-00	FF-FF-FF-00-00-00	32 chars	
Total Entries: 8			
OUI Address	Mask	Description	Delete
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Delete
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Delete
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	Delete
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	Delete

Figure 5-32 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:

Voice VLAN Device			
Voice VLAN Device Table			
Total Entries: 0			
Port	Voice Device Address	Start Time	Status

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:

Voice VLAN LLDP-MED Device						
Voice VLAN LLDP-MED Device Table						
Total Entries: 0						
Index	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time
						Remain Time (sec)

Figure 5-34 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 creates a single state called Discarding. In either case, ports do not forward packets. In the STP port, transition states Disabled, Blocking or Listening or in the RSTP/MSTP port state Discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

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

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Blocking</i>	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Listening</i>	No	No
<i>Learning</i>	<i>Learning</i>	<i>Learning</i>	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

RSTP is capable of a more rapid transition to the Forwarding state. RSTP no longer relies on timer configurations and RSTP-compliant bridges are sensitive to feedback from other RSTP-compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a Forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the Edge Port and the Point-to-Point (P2P) port.

Edge Port

A port can be configured as an Edge Port if it is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the Listening and Learning states. An Edge Port loses its status if it receives a BPDU packet, after which it immediately becomes a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and are capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also includes a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

- On the Switch level, the settings are globally implemented.
- On the port level, the settings are implemented on a user-defined group of ports.

STP Global Settings

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

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

The screenshot shows the 'STP Global Settings' configuration window. It includes sections for STP State (Enabled), STP Traps (New Root Trap and Topology Change Trap both disabled), STP Mode (RSTP selected), STP Priority (Priority 32768), and STP Configuration (Bridge Max Age 20, Bridge Forward Time 15, Bridge Hello Time 2, TX Hold Count 6). Each section has an 'Apply' button.

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. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

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

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

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

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:

The screenshot shows the 'STP Port Settings' window. At the top, there are configuration fields for a single port: 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Cost' (0/20000000, 0=Auto), 'State' (Enabled), 'Guard Root' (Disabled), 'Link Type' (Auto), 'Port Fast' (Network), 'TCN Filter' (Disabled), 'BPDU Forward' (Disabled), and 'Priority' (128). Below these fields is a 'Hello Time (1-2)' input field with a 'sec' unit and an 'Apply' button. Below the configuration fields is a table listing port settings for all eight ports (eth1/0/1 to eth1/0/8). The table columns are: Port, State, Cost, Guard Root, Link Type, Port Fast, TCN Filter, BPDU Forward, and Priority. All ports are set to Enabled, Auto/P2P, Edge/Non-Edge, Disabled, and Priority 128.

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

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. This value must be between 1 and 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000, a Gigabit port is 20000, and a 10 Gigabit port is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.
Link Type	Select the link type 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, this option is Auto .
Port Fast	<p>Select the Port Fast option here. Options to choose from are:</p> <ul style="list-style-type: none"> In the Network mode, the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the Disable mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. <p>By default, this option is Network.</p>

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

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:

The screenshot shows the 'MST Configuration Identification' window. It includes fields for Configuration Name (F0:7D:68:12:50:01), Revision Level (0-65535) (0), and Digest (AC36177F50283CD4B83821D8AB26DE62). Below these are Instance ID Settings for Instance ID (1-32), Action (Add VID), and VID List (1 or 3-5). A table displays one entry: Total Entries: 1, Instance ID: CIST, VID List: 1-4094. Navigation buttons at the bottom include 1/1, <, <, 1, >, >, and Go.

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. This value must be between 0 and 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

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

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

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 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"/> <input type="button" value="1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>
Instance CIST			CIST Global Info[Mode RSTP]
Bridge Address		F0-7D-68-12-50-01	
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:

The screenshot shows the 'MSTP Port Information' window. At the top left is a dropdown menu set to 'Port eth1/0/1'. To its right are 'Clear Detected Protocol' and 'Find' buttons. Below this is a table titled 'eth1/0/1 Settings' with one row. The table has columns for 'Instance ID' (CIST), 'Cost' (200000), 'Priority' (128), 'Status' (Forwarding), and 'Role' (NonStp). An 'Edit' button is located in the last column of this row. At the bottom of the table are navigation buttons: '1/1', '<', '<', '1', '>', '>', and 'Go'.

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. This value must be between 1 and 200000000.
Priority	After clicking the Edit button, select the priority value here. Options to choose from are 0 to 240 . By default, this option is 0 . A lower value has higher priority.

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

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

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

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

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out.

The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:

Loopback Detection

Loopback Detection Global Settings

Loopback Detection State	Disabled	Mode	Port-based
Enabled VLAN ID List	1-4094	Interval (1-32767)	10 sec
Trap State	Disabled		
Function Version	v4.05	Apply	

Loopback Detection Port Settings

From Port	eth1/0/1	To Port	eth1/0/1	State	Disabled	Apply
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. The default is Disabled .
Mode	Select the loopback detection mode. Options to choose from are Port-based and VLAN-based .
Enabled VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when VLAN-based is selected in the Mode drop-down list.
Interval	Enter the interval in seconds that the device will use to transmit Configuration Test Protocol (CTP) packets to detect a loopback event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.
Trap State	Select to enable or disable the loopback detection trap state.

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.
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.

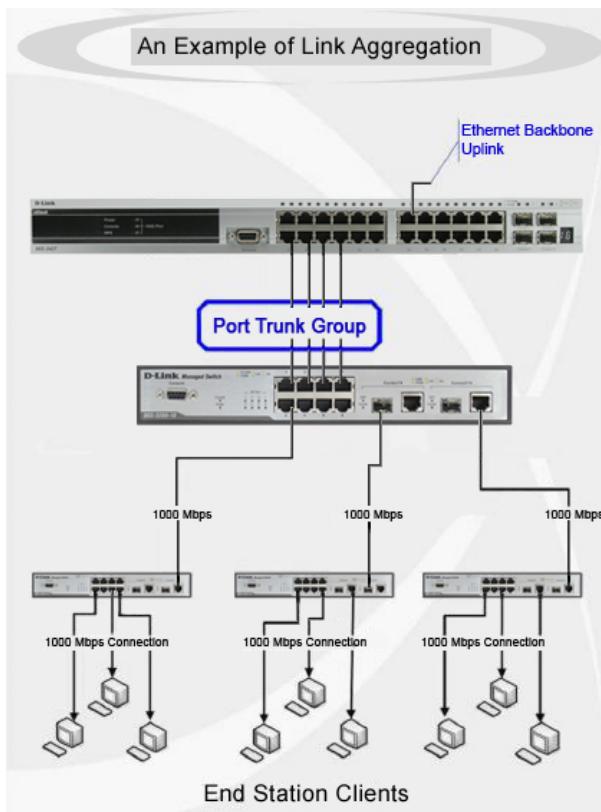


Figure 5-41 Example of Port Trunk Group

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:

The screenshot shows the 'Link Aggregation' configuration page. At the top, there are fields for 'System Priority (1-65535)' set to 32768, 'Load Balance Algorithm' set to 'Source Destination MAC', and 'System ID' set to 32768,F0-7D-68-12-50-01. Below these are two 'Apply' buttons. The main area is titled 'Channel Group Information' and contains fields for 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Group ID (1-8)' (empty), 'Mode' (On), and buttons for 'Add' and 'Delete Member Port'. A note states: 'Note: Each Channel Group supports up to 8 member ports.' Below this is a table titled 'Total Entries: 2' showing two entries:

Channel Group	Protocol	Max Ports	Member Number	Member Ports	
Port-channel1	Static	8	4	1/0/10-1/0/13	<button>Delete Channel</button> <button>Show Detail</button>
Port-channel2	LACP	8	2	1/0/14-1/0/15	<button>Delete Channel</button> <button>Show Detail</button>

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

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

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

Parameter	Description
From Port - To Port	Select the list of ports that will be associated with this configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 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 On , Active , and Passive . If the mode On is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

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

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

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

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

After clicking the **Show Detail** button at an entry that uses the **Static Protocol**, the following page will be available.

This screenshot shows the configuration details for Port Channel 1 using the Static Protocol. It includes sections for Port Channel Information, Port Channel Detail Information, Port Channel Neighbor Information, and a Note section.

Port Channel Information:

Port Channel	1
Protocol	Static

Port Channel Detail Information:

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	Edit
eth1/0/10	None	None	down	None	None	Edit
eth1/0/11	None	None	down	None	None	Edit
eth1/0/12	None	None	down	None	None	Edit
eth1/0/13	None	None	down	None	None	Edit

Port Channel Neighbor Information:

Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/10	None	None	None	None	None
eth1/0/11	None	None	None	None	None
eth1/0/12	None	None	None	None	None
eth1/0/13	None	None	None	None	None

Note:

LACP State:
 bndl: Port is attached to an aggregator and bundled with other ports.
 indep: Port is in an independent state(not bundled but able to switch data traffic).
 hot-sby: Port is in a hot-standby state.
 down: Port is down.

[Back](#)

Figure 5-43 Link Aggregation (Channel 1 Detail) Window

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

After clicking the **Show Detail** button at an entry that uses the **LACP Protocol**, the following page will be available.

This screenshot shows the configuration details for Port Channel 2 using the LACP Protocol. It includes sections for Port Channel Information, Port Channel Detail Information, Port Channel Neighbor Information, and a Note section.

Port Channel Information:

Port Channel	2
Protocol	LACP

Port Channel Detail Information:

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	Edit
eth1/0/14	Short	Active	down	32768	0	Edit
eth1/0/15	Short	Active	down	32768	0	Edit

Port Channel Neighbor Information:

Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/14	0,00-00-00-00-00-00	0	Long	Passive	0
eth1/0/15	0,00-00-00-00-00-00	0	Long	Passive	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.

[Back](#)

Figure 5-44 Link Aggregation (Channel 2 Detail) Window

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

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

After clicking the **Edit** button, the 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 <input type="button" value="▼"/>	Active <input type="button" value="▼"/>	down	32768	0	<input type="button" value="Apply"/>
eth1/0/15	Short	Active	down	32768	0	<input type="button" value="Edit"/>
Port Channel Neighbor Information						
Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority	
eth1/0/14	0,00-00-00-00-00-00	0	Long	Passive	0	<input type="button" value="Back"/>
eth1/0/15	0,00-00-00-00-00-00	0	Long	Passive	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 5-45 Link Aggregation (Channel 2 Detail, Edit) Window

The fields that can be configured are described below:

Parameter	Description
LACP Timeout	Select the LACP timeout option here. Options to choose from are: <ul style="list-style-type: none"> • Short - Specifies that there is 3 seconds before received LACPDU information is declared as invalid. Once the partner recognizes the information in the received PDU, periodic transmissions of LACP PDUs are sent at 1-second intervals on the interface. This is the default option. • Long - Specifies that there is 90 seconds before received LACPDU information is declared as invalid. Once the partner recognizes the information in the received PDU, periodic transmissions of LACP PDUs are sent at 30-second intervals on the interface.
Working Mode	Select the working mode here. Options to choose from are: <ul style="list-style-type: none"> • Passive - Specifies to operate in the LACP passive mode. • Active - Specifies to operate in the LACP active mode.
Port Priority	Enter the port priority value here. This determines which port can join the port-channel and which port operates in the stand-alone mode. A lower value carries a higher priority. The range is from 1 to 65535. By default, this value is 32768.

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

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', 'VLAN Status Settings', and 'IGMP Snooping Table'.
Global Settings: Contains a 'Global State' section with 'Enabled' selected. An 'Apply' button is located to the right.
VLAN Status Settings: Contains a 'VID (1-4094)' input field, an 'Enabled' radio button (selected), and an 'Apply' button.
IGMP Snooping Table: Shows a table with one entry:

Total Entries: 1			
VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit

Below the table are navigation buttons: 1/1, <, <, 1, >, >, and Go.

Figure 5-46 IGMP Snooping Settings Window

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

Parameter	Description
Global State	Select to globally enable or disable IGMP snooping here. By default, this is disabled.

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 the VLAN ID here. The range is from 1 to 4094. 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 the VLAN ID from 1 to 4094.

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

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

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

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

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

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

The screenshot shows the 'IGMP Snooping VLAN Parameters' window. It displays the following configuration for VLAN 1:

VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (port-based)
Querier State	Disabled
Query Version	v3
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Member Query Interval	1 seconds

A 'Modify' button is located in the bottom right corner of the window.

Figure 5-47 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.

The screenshot shows the 'IGMP Snooping VLAN Settings' window for VLAN 1. The configuration fields are as follows:

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
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

An 'Apply' button is located in the bottom right corner of the window.

Figure 5-48 IGMP Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum IGMP host version that is allowed on the VLAN. Options to choose from are 1 , 2 , and 3 .
Fast Leave	Select this option to enable or disable the IGMP snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the IGMP done message from the last member. When fast leave is enabled, the Switch will not generate specific queries. When fast leave is disabled, the Switch will generate specific queries.
Querier State	Select this option to enable or disable the querier state.

Parameter	Description
Query Version	Select the general query packet version sent by the IGMP snooping querier. Options to choose from are 1 , 2 , and 3 .
Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically. The range is from 1 to 31744.
Max Response Time	Enter the maximum response time, in seconds, advertised in IGMP snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable used in IGMP snooping. The range is from 1 to 7.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.

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:

The screenshot shows the 'IGMP Snooping Groups Settings' window with two main sections:

- IGMP Snooping Static Groups Settings:** This section contains fields for configuring a static group. It includes:
 - VID (1-4094) input field.
 - Group Address input field.
 - From Port dropdown menu set to 'eth1/0/1'.
 - To Port dropdown menu set to 'eth1/0/1'.
 - Apply and Delete buttons.
 - VID (1-4094) radio button group with one selected.
 - Group Address radio button group with one selected.
 - Total Entries: 1 table with one entry: VID 1, Group Address 224.0.1.0, Ports 1/0/10.
 - Pagination controls: 1/1, <, <, 1, >, >, Go.
- IGMP Snooping Groups Table:** This section displays a table of existing groups:
 - VID (1-4094) radio button group with one selected.
 - Group Address radio button group with one selected.
 - Total Entries: 0 table.
 - Columns: VID, Group Address, Source Address, FM, Exp(sec), Ports.

Figure 5-49 IGMP Snooping Groups Settings Window

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

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

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

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

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

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

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

The fields that can be configured or displayed for **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.
FM	Displays the filter mode. The following can be displayed: <ul style="list-style-type: none"> EX (Exclude) - The filter mode is Exclude. IN (Include) - The filter mode is Include.
Exp (sec)	Displays the time left in seconds before the entry expires.

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 5-50 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.
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 5-51 IGMP Snooping Statistics Settings Window

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

Parameter	Description
Statistics	Select the interface here. Options to choose from are All , VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Statistics drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Statistics drop-down list.

Click the **Clear** button to clear the IGMP snooping related statistics.

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

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Find Type drop-down list.
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:

The screenshot shows the 'MLD Snooping Settings' window with three main sections: Global Settings, VLAN Status Settings, and MLD Snooping Table.

- Global Settings:** Contains a 'Global State' section with radio buttons for 'Enabled' (selected) and 'Disabled'. An 'Apply' button is located to the right.
- VLAN Status Settings:** Contains a 'VID (1-4094)' input field, a radio button for 'Enabled' (selected), another for 'Disabled', and an 'Apply' button.
- MLD Snooping Table:** Shows a table with one entry:

VID	VLAN Name	Status	Show Detail	Edit
1	default	Enabled		

 Buttons for 'Find', 'Show All', and navigation (1/1, Go) are at the bottom.

Figure 5-52 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.

This screenshot shows the 'MLD Snooping VLAN Parameters' configuration page. It lists various parameters with their current values:

MLD Snooping VLAN Parameters	
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (port-based)
Mrouter Port Learning	Enabled
Querier State	Disabled
Query Version	v2
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Listener Query Interval	1 seconds

A 'Modify' button is located in the bottom right corner of the window.

Figure 5-53 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.

This screenshot shows the 'MLD Snooping VLAN Settings' configuration page. It contains several input fields for modifying parameters:

MLD Snooping VLAN Settings	
VID (1-4094)	<input type="text" value="1"/>
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Minimum Version	<input type="text" value="1"/>
Fast Leave	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Mrouter Port Learning	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Querier State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Query Version	<input type="text" value="2"/>
Query Interval (1-31744)	<input type="text" value="125"/> sec
Max Response Time (1-25)	<input type="text" value="10"/> sec
Robustness Value (1-7)	<input type="text" value="2"/>
Last Listener Query Interval (1-25)	<input type="text" value="1"/> sec

An 'Apply' button is located in the bottom right corner of the window.

Figure 5-54 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.
Mrouter Port Learning	Select this option to enable or disable Mrouter port learning.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the MLD snooping querier. Options to choose from are 1 , and 2 .
Query Interval	Enter the interval at which the MLD snooping querier sends MLD general query messages periodically. The range is from 1 to 31744.

Parameter	Description
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:

MLD Snooping Static Groups Settings																							
VID (1-4094)	Group Address	From Port	To Port	Apply	Delete																		
<input type="text"/>	FF11::11	eth1/0/1	eth1/0/1	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>																		
VID (1-4094)	Group Address	<input checked="" type="radio"/> <input type="text"/> <input type="radio"/> FF11::11 <input type="button" value="Find"/> <input type="button" value="Show All"/>																					
Total Entries: 1 <table border="1"> <thead> <tr> <th>VID</th> <th>Group Address</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>FF11::11</td> <td>1/0/10</td> </tr> </tbody> </table>						VID	Group Address	Ports	1	FF11::11	1/0/10												
VID	Group Address	Ports																					
1	FF11::11	1/0/10																					
MLD Snooping Groups Table <table border="1"> <thead> <tr> <th>VID</th> <th>Group Address</th> <th>Source Address</th> <th>FM</th> <th>Exp(sec)</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/></td> <td>FF11::11</td> <td></td> <td></td> <td></td> <td><input type="button" value="Find"/> <input type="button" value="Show All"/></td> </tr> <tr> <td colspan="6"> Total Entries: 0 </td> </tr> </tbody> </table>						VID	Group Address	Source Address	FM	Exp(sec)	Ports	<input checked="" type="radio"/>	FF11::11				<input type="button" value="Find"/> <input type="button" value="Show All"/>	Total Entries: 0					
VID	Group Address	Source Address	FM	Exp(sec)	Ports																		
<input checked="" type="radio"/>	FF11::11				<input type="button" value="Find"/> <input type="button" value="Show All"/>																		
Total Entries: 0																							

Figure 5-55 MLD Snooping Groups Settings Window

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

Parameter	Description
VID	Enter the VLAN ID of the multicast group here. The range is from 1 to 4094.
Group Address	Enter the IPv6 multicast group address here.
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 or displayed for **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.
FM	Displays the filter mode. The following can be displayed: <ul style="list-style-type: none"> EX (Exclude) - The filter mode is Exclude. IN (Include) - The filter mode is Include.
Exp (sec)	Displays the time left in seconds before the entry expires.

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

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

MLD Snooping Mrouter Settings

This window is used to display and configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports on the VLAN interface on the Switch.

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

MLD Snooping Mrouter Settings	
VID (1-4094)	Configuration
<input type="text"/>	<input type="button" value="Port"/> <input type="button" value="Port"/>
From Port	To Port
<input type="button" value="eth1/0/1"/>	<input type="button" value="eth1/0/1"/>
<input type="button" value="Apply"/> <input type="button" value="Delete"/>	
MLD Snooping Mrouter Table	
VID (1-4094)	<input type="button" value="Find"/> <input type="button" value="Show All"/>
Total Entries: 1	
VID	Ports
1	1/0/10 (Static)
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>	

Figure 5-56 MLD Snooping Mrouter Settings Window

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

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are: <ul style="list-style-type: none"> Port - Select to have the configured ports as being connected to multicast-enabled routers. Forbidden Port - Select to have the configured ports as being not connected to multicast-enabled routers. Learn pimv6 - Select to enable dynamic learning of multicast router port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

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

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

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

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

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

MLD Snooping Statistics Settings

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

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

Figure 5-57 MLD Snooping Statistics Settings Window

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

Parameter	Description
Statistics	Select the interface here. Options to choose from are All , VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Statistics drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Statistics drop-down list.

Click the **Clear** button to clear the MLD snooping related statistics.

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

Parameter	Description
Find Type	Select the interface type. Options to choose from are VLAN , and Port .
VID	Enter a VLAN ID between 1 and 4094. This is available when VLAN is selected in the Find Type drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when Port is selected in the Find Type drop-down list.

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

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

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

Multicast 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:

The screenshot shows the 'Multicast Filtering Mode' configuration window. At the top, there are fields for 'VID List' (set to '3 or 1-5') and 'Multicast Filtering Mode' (set to 'Forward Unregistered'). A note states that reserved destination IP and IPv6 addresses cannot be filtered in this mode. Below this is a table titled 'Total Entries: 2' with two rows. The first row has 'VLAN' set to 'default' and 'Multicast Filtering Mode' set to 'Forward Unregistered Groups'. The second row has 'VLAN' set to 'VLAN0002' and 'Multicast Filtering Mode' set to 'Forward Unregistered Groups'. At the bottom right are navigation buttons for pages 1/1, back, forward, and a 'Go' search bar.

Figure 5-58 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 Filter Mode	Select the multicast filter mode here. Options to choose from are: <ul style="list-style-type: none"> Forward Unregistered - Specifies that 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 - Specifies that all multicast packets will be flooded based on the VLAN domain. Filter Unregistered - Specifies that 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:

The screenshot shows the 'LLDP Global Settings' window with the following sections and configurations:

- LLDP Global Settings:**
 - LLDP State: Enabled (radio button selected)
 - LLDP Forward State: Enabled (radio button selected)
 - LLDP Trap State: Enabled (radio button selected)
 - LLDP-MED Trap State: Enabled (radio button selected)
- LLDP-MED Configuration:**
 - Fast Start Repeat Count (1-10): 4 times
- LLDP Configurations:**
 - Message TX Interval (5-32768): 30 sec
 - Message TX Hold Multiplier (2-10): 4 sec
 - RelInit Delay (1-10): 2 sec
 - TX Delay (1-8192): 2 sec
- LLDP System Information:**

Chassis ID Subtype	MAC Address
Chassis ID	F0-7D-68-12-50-01
System Name	Switch
System Description	Gigabit Ethernet Smart Managed Switch
System Capabilities Supported	Repeater, Bridge
System Capabilities Enabled	Repeater, Bridge
- LLDP-MED System Information:**

Device Class	Network Connectivity Device
Hardware Revision	A1
Software Revision	2.01.001
Serial Number	DGS1250102030
Manufacturer Name	D-Link Corporation

Figure 5-59 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. By default, this is disabled.
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the LLDP State is disabled and LLDP Forward State is enabled, the received LLDPDU packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the LLDP-MED trap state.

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

The fields that can be configured in **LLDP-MED Settings** are described below:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

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

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

Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDUs transmission interval that used to calculate the TTL value of an LLDPDU. This value must be between 2 and 10.
RelInit Delay	Enter the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

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

LLDP Port Settings

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

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

The screenshot shows the 'LLDP Port Settings' window. At the top, there are dropdown menus for 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Notification' (Disabled), 'Subtype' (Local), 'Admin State' (TX and RX), 'IP Subtype' (Default), 'Action' (Remove), and an 'Address' field. A note says 'The address should be the switch's address.' An 'Apply' button is at the bottom right. Below this is a table with columns: Port, Notification, Subtype, Admin State, and IPv4/IPv6 Address. The table lists ports eth1/0/1 through eth1/0/10, all set to 'Disabled' notification, 'Local' subtype, and 'TX and RX' admin state. There is a blank row for the 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 5-60 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. This is the default option.

Parameter	Description
	<ul style="list-style-type: none"> Disabled - The local LLDP agent can neither transmit nor receive LLDP frames.
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are Default , IPv4 , and IPv6 .
Action	Select the action that will be taken here. Options to choose from are Remove and Add .
Address	Enter the IP address that will be sent.

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



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

LLDP Management Address List

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

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

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

Figure 5-61 LLDP Management Address List Window

The fields that can be configured are described below:

Parameter	Description
Subtype	Select the subtype. Options to choose from are All , IPv4 and IPv6 . After selecting the IPv4 option, enter the IPv4 address in the space provided. After selecting the IPv6 option, enter the IPv6 address in the space provided.

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

LLDP Basic TLVs Settings

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

data types that 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:

The screenshot shows the 'LLDP Basic TLVs Settings' window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1'), 'To Port' (set to 'eth1/0/1'), and three checkboxes for 'Port Description' (disabled), 'System Name' (disabled), and 'System Description' (disabled). A 'System Capabilities' checkbox is also disabled. An 'Apply' button is located to the right of the checkboxes. Below this is a table with 10 rows, each representing a port from 'eth1/0/1' to 'eth1/0/10'. All ports have their 'Port Description', 'System Name', 'System Description', and 'System Capabilities' set to 'Disabled'.

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 5-62 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:

The screenshot shows the 'LLDP Dot1 TLVs Settings' window. At the top, there are four dropdown menus: 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'Port VLAN' (Disabled), and 'VLAN Name' (Disabled). To the right of these are 'Protocol Identity' (Disabled) and 'None'. An 'Apply' button is located at the bottom right of the header. Below the header is a table with ten rows, each representing a port from eth1/0/1 to eth1/0/10. The columns are 'Port', 'Port VLAN ID' (all set to 'Disabled'), 'Enabled VLAN Name' (empty), and 'Enabled Protocol Identity' (empty).

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 5-63 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:

The screenshot shows the 'LLDP Dot3 TLVs Settings' window. At the top, there are dropdown menus for 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'MAC/PHY Configuration/Status' (Disabled), 'Link Aggregation' (Disabled), 'Maximum Frame Size' (Disabled), and 'Power Via MDI' (Disabled). Below these are two buttons: 'Apply' and 'Cancel'. The main area is a table with 11 rows, one for each port from eth1/0/1 to eth1/0/10. Each row contains five columns corresponding to the settings above. All ports are currently set to 'Disabled' for all categories.

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Power Via MDI
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 5-64 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.
Power Via MDI	Select this option to enable or disable the power via MDI TLV to send. IEEE 802.3 PMD implementations allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

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:

The screenshot shows the 'LLDP-MED Port Settings' window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1'), 'To Port' (set to 'eth1/0/1'), 'Notification' (set to 'Disabled'), 'Capabilities' (set to 'Disabled'), 'Inventory' (set to 'Disabled'), 'Network Policy' (set to 'Disabled'), and 'PSE' (set to 'Disabled'). Below these are two buttons: 'Apply' and a vertical scroll bar. The main area contains a table with 11 rows, one for each port from eth1/0/1 to eth1/0/10. Each row has columns for Port, Notification, Capabilities, Inventory, Network Policy, and PSE, all set to 'Disabled'.

Port	Notification	Capabilities	Inventory	Network Policy	PSE
eth1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 5-65 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.
PSE	Select this option to enable or disable transmitting the LLDP-MED extended power via MDI TLV, if the local device is PSE device or PD device.

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:

The screenshot shows the 'LLDP Statistics Information' window. It has two main sections: 'LLDP Statistics Information' and 'LLDP Statistics Ports'. In the 'LLDP Statistics Information' section, there are five counters: Last Change Time (0), Total Inserts (0), Total Deletes (0), Total Drops (0), and Total Ageouts (0). There is also a 'Clear Counter' button. In the 'LLDP Statistics Ports' section, a dropdown menu shows 'Port' and 'eth1/0/1'. Below this is a table with columns: Port, Total Transmits, Total Discards, Total Errors, Total Receives, Total TLV Discards, Total TLV Unknowns, and Total Ageouts. The table lists ports from eth1/0/1 to eth1/0/10, all of which have 0 values in every column. There are also 'Clear Counter' and 'Clear All' buttons at the bottom of this section.

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 5-66 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 a web-based management interface for a DGS-1250 switch. The title bar says "LLDP Local Port Information". Below it is a sub-header "LLDP Local Port Brief Table". A dropdown menu under "Port" is set to "eth1/0/1". To the right are "Find" and "Show Detail" buttons. The main area is a table with the following columns: Port, Port ID Subtype, Port ID, and Port Description. The table contains 10 rows, each corresponding to a port from eth1/0/1 to eth1/0/10. All ports are listed as "Local". The Port ID column lists the port numbers. The Port Description column shows "D-Link Corporation DGS-1250-28..." repeated for each row.

Port	Port ID Subtype	Port ID	Port Description
eth1/0/1	Local	eth1/0/1	D-Link Corporation DGS-1250-28...
eth1/0/2	Local	eth1/0/2	D-Link Corporation DGS-1250-28...
eth1/0/3	Local	eth1/0/3	D-Link Corporation DGS-1250-28...
eth1/0/4	Local	eth1/0/4	D-Link Corporation DGS-1250-28...
eth1/0/5	Local	eth1/0/5	D-Link Corporation DGS-1250-28...
eth1/0/6	Local	eth1/0/6	D-Link Corporation DGS-1250-28...
eth1/0/7	Local	eth1/0/7	D-Link Corporation DGS-1250-28...
eth1/0/8	Local	eth1/0/8	D-Link Corporation DGS-1250-28...
eth1/0/9	Local	eth1/0/9	D-Link Corporation DGS-1250-28...
eth1/0/10	Local	eth1/0/10	D-Link Corporation DGS-1250-28...

Figure 5-67 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 a detailed configuration window for port "eth1/0/1". It includes fields for Port ID Subtype (Local), Port ID (eth1/0/1), Port Description (D-Link Corporation DGS-1250-28XMP HW A1 firmware 2.01.001 Port 1), Port PVID (1), Management Address Count (0), PPVID Entries (0), VLAN Name Entries Count (1), Protocol Identity Entries Count (0), MAC/PHY Configuration/Status (with a "Show Detail" link), Power Via MDI (with a "Show Detail" link), Link Aggregation (with a "Show Detail" link), Maximum Frame Size (1536), LLDP-MED Capabilities (with a "Show Detail" link), Network Policy (with a "Show Detail" link), and Extended Power Via MDI (with a "Show Detail" link). At the bottom right is a "Back" button.

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

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the [Show Detail](#) hyperlink.

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

After clicking the [Show Detail](#) hyperlink, a new section will appear at the bottom of the window.

LLDP Local Port Information	
LLDP Local Information Table	
Port	eth1/0/1
Port ID Subtype	Local
Port ID	eth1/0/1
Port Description	D-Link Corporation DGS-1250-28XMP HW A1 firmware 2.01.001 Port 1
Port PVID	1
Management Address Count	0
PPVID Entries	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Back	
MAC/PHY Configuration/Status	
Auto-Negotiation Support	Supported
Auto-Negotiation Enabled	Enabled
Auto-Negotiation Advertised Capability	6c01(hex)
Auto-Negotiation Operational MAU Type	001e(hex)

Figure 5-69 LLDP Local Port Information (Show Detail) Window

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

LLDP Neighbor Port Information

This window is used to display the LLDP information learned from neighboring switches. The Switch receives packets from a remote station but is able to store the information locally.

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

LLDP Neighbor Port Information						
LLDP Neighbor Port Brief Table						
Port	eth1/0/1	<input type="button" value="▼"/>	<input type="button" value="Find"/>	<input type="button" value="Clear"/>	<input type="button" value="Clear All"/>	
Total Entries: 1						
Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Detail
1	MAC Address	D0-AE-EC-D9-9E-5E	Local	1/15		

Figure 5-70 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.

LLDP Neighbor Information Table	
Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	D0-AE-EC-D9-9E-5E
Port ID Subtype	Local
Port ID	1/15
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

[Back](#)

Figure 5-71 LLDP Neighbor Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the [Show Detail](#) hyperlink.

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

After clicking the [Show Detail](#) hyperlink, a new section will appear at the bottom of the window.

LLDP Neighbor Information Table	
Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	D0-AE-EC-D9-9E-5E
Port ID Subtype	Local
Port ID	1/15
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

MAC/PHY Configuration/Status
None

[Back](#)

Figure 5-72 LLDP Neighbor Port Information (Show Detail) Window

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:

ARP Aging Time		
ARP Aging Time		
Total Entries: 1		
Interface Name	Timeout (min)	
vlan1	240	<input type="button" value="Edit"/>
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>		

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	After click the Edit button, enter the ARP aging timeout value here. The range is from 0 to 65535. If this is 0, entries will never timeout.

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

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

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

Static ARP

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

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

Static ARP					
IP Address	Hardware Address		00-11-22-33-44-AA		
Total Entries: 1					
Interface Name	IP Address	Hardware Address	Aging Time	Type	
vlan1	10.90.90.90	F0-7D-68-12-50-01	Forever		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>					

Figure 6-2 Static ARP Window

The fields that can be configured are described below:

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

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

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

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

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

ARP Table

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

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

ARP Table					
ARP Search					
<input checked="" type="radio"/> Interface VLAN (1-4094)	<input type="text"/>	<input type="radio"/> IP Address	<input type="text"/>	Mask	<input type="text"/>
<input type="radio"/> Hardware Address	<input type="text" value="00-11-22-33-44-55"/>	<input type="radio"/> Type	<input type="text" value="All"/>	<input type="button" value="Find"/>	<input type="button" value="Clear All"/>
Total Entries: 2					
Interface Name	IP Address	Hardware Address	Aging Time (min)	Type	
vlan1	10.90.90.14	10-BF-48-D6-E2-E2	20	<input type="button" value="Clear"/>	<input type="button" value="Clear"/>
vlan1	10.90.90.90	F0-7D-68-12-50-01	Forever	<input type="button" value="Clear"/>	<input type="button" value="Clear"/>
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>					

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. This value must be between 1 and 4094.
IP Address	Select and enter the IP address to display here.

Parameter	Description
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 a web-based configuration interface for 'Gratuitous ARP'. At the top, a navigation bar has 'Gratuitous ARP' selected. Below it, a section titled 'Gratuitous ARP Global Settings' contains a 'Gratuitous ARP Trap State' field. This field includes two radio buttons: 'Enabled' (unchecked) and 'Disabled' (checked). To the right of the field is an 'Apply' button. The overall background is light grey with dark blue header bars.

Figure 6-4 Gratuitous ARP Window

The fields that can be configured are described below:

Parameter	Description
Gratuitous ARP Trap State	Select to enable or disable the gratuitous ARP feature trap state 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:

The screenshot shows the 'IPv6 Neighbor' configuration window. At the top, there are two sets of input fields for 'Interface VLAN (1-4094)' and 'IPv6 Address' (2013::1) and 'MAC Address' (11-22-33-44-AA-FF), with an 'Apply' button. Below this is a search bar for 'Interface VLAN (1-4094)' and 'IPv6 Address' (2013::1), with 'Find' and 'Clear' buttons. A table titled 'Total Entries: 1' displays one entry: IPv6 Address 2019::1, Link-Layer Addr 00-11-22-33-44-55, Interface vlan1, Type Static, State Up. Buttons for 'Delete' and navigation (1/1, Go) are also present.

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** 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' configuration window. At the top, there is an input field for 'Interface VLAN (1-4094)' and buttons for 'Apply' and 'Find'. Below this is a table titled 'Total Entries: 1' with one entry: Interface vlan1, State Enabled, IP Address 10.90.90.90/255.0.0.0 Manual, Link Status Up. Buttons for 'Edit' and 'Delete' are also present.

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. This value must be between 1 and 4094.

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

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

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

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

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

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

Figure 6-7 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"> When the Static option is selected, users can enter the IPv4 address of this interface manually in the fields provided. When the DHCP option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the 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. It includes fields for 'Client-ID' (text input), 'Class ID String' (text input with 'Hex' checkbox), and 'Lease' (text input with dropdowns for 'Days', 'Hours', and 'Minutes'). An 'Apply' button is at the bottom right.

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.
Lease	Enter and optionally select the DHCP client lease time here. In the text box, the lease time, in days, can be entered. The range is from 0 to 10000 days. Hours and Minutes can also be selected optionally.

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

IPv6 Interface

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

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

The screenshot shows the 'IPv6 Interface' window. It includes a 'Interface VLAN' selection field, 'Apply' and 'Find' buttons, a table header 'Total Entries: 1', and a table row for 'vlan1' with columns 'Interface', 'IPv6 State', and 'Link Status'. At the bottom are navigation buttons for pages 1/1, and buttons for 'Show Detail', 'Go', and page numbers 1, <, >, and >>.

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 are described below:

Parameter	Description
IPv6 State	Select to enable or disable the IPv6 interface global state here.

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

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

The fields that can be configured for **IPv6 Address Autoconfig** are described below:

Parameter	Description
State	Select to enable or disable the automatic configuration of the IPv6 address using stateless auto-configuration here. Select the Default option to insert the default route to the IPv6 routing table based on the received router advertisement. The type of the default route is SLAAC.

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

Parameter	Description
	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.
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: 0				
Address Type	IPv6 Address			

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	Edit
3FFE:501:FFFF::/64	604800	2592000	Enabled	Enabled	

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

Click the **Edit** button to configure the following parameters:

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
3FFE:501:FFFF::/64		604800	2592000	Enabled	Enabled
<input type="button" value="Apply"/>					

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

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. The default value is 604800 seconds (7 days).
Valid Life Time	Enter the valid lifetime value here. The range is from 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).
Link Flag	Select to enable or disable the on-link flag here. The default option is Enabled .
Autoconfig Flag	Select to enable or disable the auto-configure flag here. The default option 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.

IPv6 Interface					
IPv6 Interface Settings		Interface IPv6 Address		Neighbor Discover	
DHCPv6 Client					
DHCPv6 Client					
DHCPv6 Client Settings					
Client State		Disabled	<input type="checkbox"/> Rapid Commit	<input type="button" value="Restart"/>	
<input type="button" value="Apply"/>					

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 124 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:

IP Address	Mask	Gateway	Interface Name	
0.0.0.0	0.0.0.0	10.90.90.1		<input type="button" value="Delete"/> <input type="button" value="Go"/>

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:

IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
10.0.0.0	255.0.0.0	Directly Connected	vlan1		Connected	-

Figure 6-16 IPv4 Route Table Window

The fields that can be configured are described below:

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

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

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

IPv6 Static/Default Route

This window is used to display and configure the IPv6 static or default routes.

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

IPv6 Address/Prefix Length	Next Hop	Interface Name	Protocol	Active	Delete
::/0	3FE1::1		Static	No	<input type="button" value="Delete"/>

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. Tick the Default Route option to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Backup State	Select the backup state option here. Options to choose from are Primary , and Backup . When the Primary option is selected, the route is specified as the primary route to the destination. When the Backup option is selected, the route is specified as the backup route to the destination.

Click the **Apply** button to 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:

The screenshot shows the 'IPv6 Route Table' window with the following interface elements and data:

- Filter:** A dropdown menu set to 'Connected' and a checked checkbox for 'Database'.
- Search:** A 'Find' button.
- Summary Table:**

Route Source	Count
Connected	0
Static	0
SLAAC	0
Total	0
- Pagination:** Page number '1/1' and navigation buttons for first, previous, next, last, and Go.

Figure 6-18 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
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.
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:

Source Address	Group Address	Incoming Interface	Outgoing Interface List
----------------	---------------	--------------------	-------------------------

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:

Source Address	Group Address	Interface Name	Outgoing Interface List
----------------	---------------	----------------	-------------------------

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) - Specifies to transmit 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. This is the default option. WDRR (Weighted Deficit Round-Robin) - Specifies to serve an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration. <p>To set a CoS queue in the SP mode, any higher priority CoS queue must also be in the strict priority mode.</p>

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

Queue Settings

This window is used to display and configure the queue settings.

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

The screenshot shows the 'Queue Settings' window with the following configuration:

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. This value must be between 0 and 7.
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. Therefore, the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0 and 127.

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

CoS to Queue Mapping

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

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

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

Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

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

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

Port Rate Limiting

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

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

Port Rate Limiting					
From Port To Port Direction Rate Limit					
eth1/0/1	eth1/0/1	Input	<input checked="" type="radio"/> Bandwidth (64-10000000) <input type="radio"/> Percent (1-100) <input type="radio"/> None	Kbps	Burst Size (0-128000)
				%	Burst Size (0-128000)
					Kbyte
					Kbyte
					<input type="button" value="Apply"/>
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. <ul style="list-style-type: none"> When Bandwidth is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes. When Percent is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes. Select the None option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

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

Queue Rate Limiting

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

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

The window title is "Queue Rate Limiting". It has a header with "Queue Rate Limiting" and several dropdown menus for "From Port" (eth1/0/1), "To Port" (eth1/0/1), and "Queue ID" (0). Below these are three radio buttons for "Rate Limit": "Min Bandwidth (64-10000000)" (selected), "Min Percent (1-100)", and "None". There are also two input fields for "Kbps" and "Max Bandwidth (64-10000000)" and "Max Percent (1-100)". An "Apply" button is located at the bottom right. The main area contains a table with columns for Port, Queue0, Queue1, Queue2, Queue3, Queue4, Queue5, Queue6, and Queue7. Each row represents a port (e.g., eth1/0/1 to eth1/0/10) and shows the current rate limit settings for each queue.

Port	Queue0		Queue1		Queue2		Queue3		Queue4		Queue5		Queue6		Queue7	
	Min Rate	Max Rate														
	Rate															
eth1/0/1	No Li...															
eth1/0/2	No Li...															
eth1/0/3	No Li...															
eth1/0/4	No Li...															
eth1/0/5	No Li...															
eth1/0/6	No Li...															
eth1/0/7	No Li...															
eth1/0/8	No Li...															
eth1/0/9	No Li...															
eth1/0/10	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.

Parameter	Description
Queue ID	Select the queue ID that will be configured here. Options to choose from are 0 to 7.
Rate Limit	<p>Select and enter the queue rate limit settings here.</p> <ul style="list-style-type: none"> When the Min Bandwidth option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the maximum bandwidth (Max Bandwidth) rate limit in the space provided. This value must be between 64 and 10000000 kbps. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied. The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports. <ul style="list-style-type: none"> When the Min Percent option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also, enter the maximum percentage value (Max Percent) in the space provided. This value must be between 1 and 100 percent (%). Select the None option to remove the rate limit on the specified port(s).

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 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:

		Digit in ones									
Mutation Name	Digit in tens	0	1	2	3	4	5	6	7	8	9
Mutation	00	0	2	2	3	4	5	6	7	8	9
	10	10	11	12	13	14	15	16	17	18	19
	20	20	21	22	23	24	25	26	27	28	29
	30	30	31	32	33	34	35	36	37	38	39
	40	40	41	42	43	44	45	46	47	48	49
	50	50	51	52	53	54	55	56	57	58	59
	60	60	61	62	63						

1/1 |< < 1 > >| Go

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63.
Output DSCP List	Enter the output DSCP list value here. This value must be between 0 and 63.

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

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

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

Port Trust State and Mutation Binding

This window is used to display and configure the port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:

Port	Trust State	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:

The screenshot shows the 'DSCP CoS Mapping' configuration window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1') and 'To Port' (set to 'eth1/0/1'), a 'CoS' dropdown set to '0', and a 'DSCP List (0-63)' input field. A large table below lists the mapping for both ports. For port 'eth1/0/1', CoS values 0 through 7 map to DSCP ranges 0-7, 8-15, 16-23, 24-31, 32-39, 40-47, 48-55, and 56-63 respectively. For port 'eth1/0/2', the same mapping applies. An 'Apply' button is located at the top right of the table area.

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. This value must be between 0 and 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:

The screenshot shows the 'Class Map' configuration window. At the top, there is a 'Class Map Name' input field (set to '32 chars') and a 'Multiple Match Criteria' dropdown set to 'Match Any'. A large table below lists the entries. There is one entry named 'class-default' with 'Match Any' criteria. Navigation buttons at the bottom include '1/1', '<', '<', '1', '>', '>', and 'Go'.

Class Map Name	Multiple Match Criteria	
Total Entries: 2	Match Any	Apply
Class Map Name	Multiple Match Criteria	
Class	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.

Match Rule	
Class Map Name	Class
Match:	
<input type="radio"/> None	
<input checked="" type="radio"/> Specify	
<input checked="" type="radio"/> ACL Name	32 chars
<input type="radio"/> CoS List (0-7)	0,5-7
<input type="radio"/> DSCP List (0-63)	1,2,61-63
<input type="radio"/> Precedence List (0-7)	0,5-7
<input type="radio"/> Protocol Name	None
<input type="radio"/> VID List (1-4094)	1,3-5
	<input type="checkbox"/> IPv4 only
	<input type="checkbox"/> IPv6 only
	<input type="button" value="Back"/>
	<input type="button" value="Apply"/>

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. This value must be between 0 and 7.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7. Tick the IPv4 only option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are ARP , BGP , DHCP , DNS , EGP , FTP , IPv4 , IPv6 , NetBIOS , NFS , NTP , OSPF , PPPOE , RIP , RTSP , SSH , Telnet , and TFTP .
VLAN List	Select and enter the VLAN list value that will be matched with the class map here. This value must be between 1 and 4094.

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

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:

The screenshot shows the 'Policy Map' configuration window. At the top left is a link to 'Create/Delete Policy Map'. Below it is a 'Traffic Policy' section with fields for 'Policy Map Name' (32 chars) and 'Class Map Name' (32 chars), both with 'Apply' buttons. A table titled 'Total Entries: 1' lists one entry: 'Policy Map Name' (Policy) with a 'Delete' button. Navigation buttons at the bottom include '1/1', '<', '<', '1', '>', '>', and 'Go'.

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 name of the policy map that will be created here. This name can be up to 32 characters long.

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

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.

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

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

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

To view the **Class Rules** assigned to a Policy, select the **Policy Map** entry in the Policy Map table. The class rules assigned to the Policy will be displayed in the **Class Rules** table, as shown below:

The screenshot shows the 'Policy Map' configuration page. At the top, there's a 'Create/Delete Policy Map' section with a 'Policy Map Name' input field (32 chars) and an 'Apply' button. Below it is a 'Traffic Policy' section with similar fields. A message 'Total Entries: 1' is displayed above a table. The table has two columns: 'Policy Map Name' and 'Policy'. It contains one entry: 'Policy' under 'Policy Map Name' and 'Class' under 'Policy'. To the right of the table are buttons for 'Delete', '1/1', and navigation arrows. Below the table is another section titled 'Policy Rules' with a similar table structure, showing one entry: 'Class' under 'Class Map Name' and 'Class' under 'Class'. Navigation buttons like 'Set Action', 'Delete', '1/1', and 'Go' are also present.

Figure 7-13 Policy Map (Class Rules) Window

Click the **Set Action** button to configure the set action settings for the specified entry.

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

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.

The screenshot shows the 'Set Action' configuration page. It starts with 'Policy Map Name' (Policy) and 'Class Map Name' (Class). Below is a 'Set Action' section with a radio button group for 'None' (selected) and 'Specify'. Under 'Specify', there are four options: 'New Precedence (0-7)', 'New DSCP (0-63)', 'New CoS (0-7)', and 'New CoS Queue (0-7)'. Each option has a dropdown menu and an 'IPv4 only' checkbox. At the bottom are 'Back' and 'Apply' buttons.

Figure 7-14 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

Parameter	Description
	selected, then both the IPv4 and IPv6 DSCP will be marked. Setting the DSCP will not affect the CoS queue selection.
New CoS	Select the new CoS value to packets here. The range is from 0 to 7. Setting the CoS will not affect the CoS queue selection. The CoS will only be marked.
New Cos Queue	Select the new CoS queue value to packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will take effect if the policy map is applied on the interface.

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

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

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:

The screenshot shows the 'Policy Binding' configuration window. At the top, there are four dropdown menus: 'From Port' (set to 'eth1/0/1'), 'To Port' (set to 'eth1/0/1'), 'Direction' (set to 'Input'), and 'Policy Map Name' (set to '32 chars'). To the right of these is a radio button for 'None' and an 'Apply' button. Below this is a table with three columns: 'Port', 'Direction', and 'Policy Map Name'. The table lists ports eth1/0/1 through eth1/0/10, all set to 'Input' direction and 'None' policy map.

Port	Direction	Policy Map Name
eth1/0/1	Input	None
eth1/0/2	Input	None
eth1/0/3	Input	None
eth1/0/4	Input	None
eth1/0/5	Input	None
eth1/0/6	Input	None
eth1/0/7	Input	None
eth1/0/8	Input	None
eth1/0/9	Input	None
eth1/0/10	Input	None

Figure 7-15 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. Input specifies ingress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the None option to not tie a policy map to this entry.

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

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:

ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

Create

Update

Note: The first character of ACL name must be a letter.

Next

Figure 8-1 ACL Configuration Wizard (Create) Window

ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

Create

Update

Note: The first character of ACL name must be a letter.

Total Entries: 5			
	ACL Name	ACL Type	Total Rules
<input type="radio"/>	S-IP	Standard IP ACL	1
<input type="radio"/>	E-IP	Extended IP ACL	0
<input type="radio"/>	E-MAC	Extended MAC ACL	0
<input type="radio"/>	S-IP6	Standard IPv6 ACL	0
<input type="radio"/>	E-IP6	Extended IPv6 ACL	0

1/1 < < 1 > > Go

Figure 8-2 ACL Configuration Wizard (Update) Window

The fields that can be configured are described below:

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

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

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

Step 2 - Select Packet Type

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

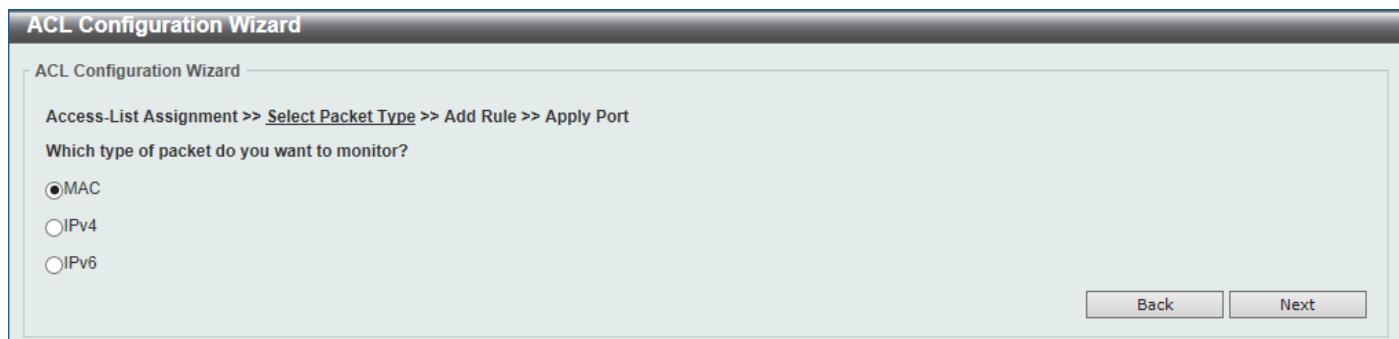


Figure 8-3 ACL Configuration Wizard (Create, Packet Type) Window

The fields that can be configured are described below:

Parameter	Description
MAC	Select to create/update a MAC ACL.
IPv4	Select to create/update an IPv4 ACL.
IPv6	Select to create/update an IPv6 ACL.

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

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

Step 3 - Add Rule

MAC

After clicking the **MAC** radio button and the **Next** button, the following window will appear.

The screenshot shows the 'ACL Configuration Wizard' window. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. Below that, it says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' (selected) and 'Auto Assign'. Under 'Assign Rule Criteria', there are three tabs: 'MAC Address' (selected), 'Ethernet Type', and '802.1Q VLAN'. In the 'MAC Address' tab, there are sections for 'Source' and 'Destination'. Under 'Source', 'Any' is selected. Under 'Destination', 'Any' is also selected. Both sections have dropdown menus for 'Host' and 'MAC' and a 'Wildcard' field. In the 'Ethernet Type' tab, there are fields for 'Specify Ethernet Type' (dropdown menu 'Please Select'), 'Ethernet Type (0x0-0xFFFF)', and 'Ethernet Type Mask (0x0-0xFFFF)'. In the '802.1Q VLAN' tab, there are fields for 'CoS' (dropdown menu 'Please Select') and 'VID(1-4094)'. At the bottom, there is a 'Time Range' field ('32 chars') and an 'Action' section with radio buttons for 'Permit' (selected) and 'Deny'. At the very bottom right are 'Back' and 'Next' buttons.

Figure 8-4 ACL Configuration Wizard (Create, Packet Type, MAC) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Source	Select and enter the source MAC address information here. Options to choose from are: <ul style="list-style-type: none"> Any - When this option is selected, any source traffic will be evaluated according to the conditions of this rule. Host - When this option is selected, enter the source host MAC address here. MAC - When this option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are: <ul style="list-style-type: none"> Any - When this option is selected, any destination traffic will be evaluated according to the conditions of this rule. Host - When this option is selected, enter the destination host MAC address here. MAC - When this option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.

Parameter	Description
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decent-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the Specify Ethernet Type drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094 .
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

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

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

IPv4

After clicking the **IPv4** radio button and the **Next** button, the following window will appear.

The screenshot shows the 'ACL Configuration Wizard' window. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. Below that, it asks 'Please assign a sequence number to create a new rule.' There are two options: 'Sequence No. (1-65535)' (selected) and 'Auto Assign'. Under 'Protocol Type', 'TCP' is selected. The main area is titled 'Assign Rule Criteria' and contains four tabs: 'IPv4 Address' (selected), 'Port', 'IPv4 DSCP', and 'TCP Flag'. The 'IPv4 Address' tab has sections for 'Source' and 'Destination'. Under 'Source', 'Any' is selected. Under 'Destination', 'Any' is also selected. The 'Port' tab shows 'Source Port' and 'Destination Port' both set to 'Please Select'. The 'IPv4 DSCP' tab shows three options: 'IP Precedence' (selected), 'ToS' (selected), and 'DSCP (0-63)'. The 'TCP Flag' tab shows several checkboxes for TCP flags: ack, fin, psh, rst, syn, and urg. The 'Time Range' field is set to '32 chars'. The 'Action' field has 'Permit' selected. At the bottom right are 'Back' and 'Next' buttons.

Figure 8-5 ACL Configuration Wizard (Create, Packet Type, IPv4) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID , and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Fragments - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , and IP . <ul style="list-style-type: none"> • When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the Host option is selected, enter the source host IP address here.

Parameter	Description
	<ul style="list-style-type: none"> When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	<p>Select and enter the destination information here. Options to choose from are Any, Host, and IP.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	<p>Select and enter the source port value here. Options to choose from are =, >, <, #, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the # option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are =, >, <, #, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the # option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available in the protocol type ICMP.</p>
ICMP Message Type	<p>When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available in the protocol type ICMP.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <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>

Parameter	Description
	<ul style="list-style-type: none"> Value - The IP precedence value can also manually be entered here. The range is from 0 to 7.
ToS	Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8). <ul style="list-style-type: none"> Value - The ToS value can also manually be entered here. The range is from 0 to 15.
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available in the protocol type TCP .
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .

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

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

IPv6

After clicking the **IPv6** radio button and the **Next** button, the following window will appear.

The screenshot shows the 'ACL Configuration Wizard' window. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port'. Below that, it says 'Please assign a sequence number to create a new rule.' There are two radio button options: '(1-65535)' and '(Auto Assign)'. The '(1-65535)' option is selected. Under 'Protocol Type', 'TCP' is selected from a dropdown menu. To the right of the dropdown is a range '(0-255)' and a checkbox for 'Fragments'. Below these settings is a section titled 'Assign Rule Criteria' with tabs for 'IPv6 Address', 'Port', 'IPv6 DSCP', 'TCP Flag', and 'Flow Label'. The 'IPv6 Address' tab is active. It contains fields for 'Source' and 'Destination'. Under 'Source', there are three options: 'Any' (selected), 'Host', and 'IPv6'. Under 'Destination', there are also three options: 'Any' (selected), 'Host', and 'IPv6'. There are also fields for 'Prefix Length' and 'Prefix Length'. The 'Port' tab shows 'Source Port' and 'Destination Port' both set to 'Please Select'. The 'IPv6 DSCP' tab shows 'DSCP (0-63)' (selected) and 'Traffic Class (0-255)'. The 'TCP Flag' tab shows 'TCP Flag' with checkboxes for ack, fin, psh, rst, syn, and urg. The 'Flow Label' tab shows 'Flow Label (0-1048575)'. The 'Time Range' tab shows '32 chars'. The 'Action' tab shows 'Permit' (selected) and 'Deny'.

Figure 8-6 ACL Configuration Wizard (Create, Packet Type, IPv6) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50), PCP (108), SCTP (132), and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Fragments - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are Any , Host , and IPv6 . <ul style="list-style-type: none"> • When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the Host option is selected, enter the source host IPv6 address here.

Parameter	Description
	<ul style="list-style-type: none"> When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	<p>Select and enter the destination information here. Options to choose from are Any, Host, and IPv6.</p> <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	<p>Select and enter the source port value here. Options to choose from are =, >, <, #, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the # option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	<p>Select and enter the destination port value here. Options to choose from are =, >, <, #, and Range.</p> <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the # option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Specify ICMP Message Type	<p>Select the ICMP message type used here.</p> <p>This parameter is only available in the protocol type ICMP.</p>
ICMP Message Type	<p>When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <p>This parameter is only available in the protocol type ICMP.</p>
Message Code	<p>When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered.</p> <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.

Parameter	Description
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg . This parameter is only available in the protocol type TCP .
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are Permit 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 8-7 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	Specifies that the In direction is used.

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

Click the **Apply** button to accept the changes made and return to the main ACL Wizard window.

ACL Access List

This window is used to display and configure the ACLs, ACL rules, and settings.

To view the following window, click **ACL > ACL Access List**, as shown below:

The screenshot shows the 'ACL Access List' window with the following details:

- Header:** ACL Access List, Filter dropdown (All), ID input (1-14999), ACL Name input (32 chars), Find button.
- Total Entries:** 5
- Table Headers:** ID, ACL Name, ACL Type, Start Sequence No., Step, Counter State, Remark.
- Table Data:**

1	S-IP	Standard IP ACL	10	10	Disabled		Edit	Delete
2000	E-IP	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	E-MAC	Extended MAC ACL	10	10	Disabled		Edit	Delete
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		Edit	Delete
- Pagination:** 1/1, Go button.
- Selected Rule View:** S-IP (ID: 1) Rule table with columns: Sequence No., Action, Rule, Time Range, Counter.
- Buttons:** Clear All Counter, Clear Counter, Add Rule, Delete, Go.

Figure 8-8 ACL Access List Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type to find here. Options to choose from are All , IP ACL , IPv6 ACL , 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.

The screenshot shows the 'ACL Access List' configuration page. At the top, there are search filters for 'ACL Type' (set to 'All'), 'ID (1-14999)' (set to '1'), 'ACL Name' (empty), and a 'Find' button. Below this is a table titled 'Total Entries: 5' with columns: ID, ACL Name, ACL Type, Start Sequence No., Step, Counter State, Remark, Apply, and Delete. The entries listed are:

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Apply	Delete
1	S-IP	Standard IP ACL	10	10	Disabled		Apply	Delete
2000	E-IP	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	E-MAC	Extended MAC ACL	10	10	Disabled		Edit	Delete
11000	S-IPv6	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IPv6	Extended IPv6 ACL	10	10	Disabled		Edit	Delete

Below the main table is a 'S-IP (ID: 1) Rule' section with columns: Sequence No., Action, Rule, Time Range, Counter, and Delete. It contains one rule:

Sequence No.	Action	Rule	Time Range	Counter	Delete
1	Permit	any any			Delete

Pagination controls at the bottom include '1/1', '<', '>', '1', 'Go', 'Clear All Counter', 'Clear Counter', and 'Add Rule' buttons.

Figure 8-9 ACL Access List (Edit) Window

After clicking the **Edit** button, the fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number step here. The step range is from 1 to 32. This specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this ACL here.

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

After clicking the **Add ACL** button, the following page will appear.

The screenshot shows the 'Add ACL Access List' configuration page. It has fields for 'ACL Type' (set to 'Standard IP ACL'), 'ID (1-1999)' (empty), and 'ACL Name' (empty). A note at the bottom states: 'Note: The first character of ACL name must be a letter.' An 'Apply' button is located on the right.

Figure 8-10 ACL Access List (Add ACL) Window

After clicking the **Add ACL** button, the fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are Standard IP ACL , Extended IP ACL , Standard IPv6 ACL , Extended IPv6 ACL , and Extended MAC ACL .
ID	Enter the ID for the ACL here. <ul style="list-style-type: none"> For a Standard IP ACL, the range from 1 to 1999. For an Extended IP ACL, the range from 2000 to 3999.

Parameter	Description
	<ul style="list-style-type: none"> 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.

The screenshot shows the 'Add ACL Rule' configuration window. It includes fields for the rule's ID (set to 1), its name (S-IP-ACL), and its type (Standard IP ACL). The sequence number is optional and set to 1-65535. The action is set to Permit. The 'Match IP Address' section allows specifying source and destination addresses using Any, Host, IP, or Wildcard options. A time range can also be defined. At the bottom, there are 'Back' and 'Apply' buttons.

Figure 8-11 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source information here. Options to choose from are Any , Host , IP , and Wildcard . <ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are Any , Host , IP , and Wildcard . <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

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.

The screenshot shows the 'Add ACL Rule' configuration interface for an Extended IP ACL. It includes fields for:

- ID:** 2000
- ACL Name:** E-IP-ACL
- ACL Type:** Extended IP ACL
- Action:** Permit (selected)
- Protocol Type:** TCP
- Match IP Address:** Fields for Source (Any, Host, IP, Wildcard) and Destination (Any, Host, IP, Wildcard).
- Match Port:** Fields for Source Port and Destination Port, each with a dropdown menu labeled 'Please Select'.
- TCP Flag:** Checkboxes for ack, fin, psh, rst, syn, urg.
- IP Precedence:** Please Select dropdown.
- ToS:** Please Select dropdown.
- DSCP (0-63):** Please Select dropdown.
- Time Range:** Input field for 32 chars.

Figure 8-12 Extended IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , EIGRP (88), ESP (50), GRE (47), IGMP (2), OSPF (89), PIM (103), VRRP (112), IP-in-IP (94), PCP (108), Protocol ID , and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Fragments - Select this option to include packet fragment filtering.
Source	Select and enter the source IP information here. Options to choose from are Any , Host , and IP .

Parameter	Description
	<ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination IP information here. Options to choose from are Any , Host , and IP . <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IP address here. When the IP option is selected, the Wildcard option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are = , > , < , # , and Range . <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the # option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	Select and enter the destination port value here. Options to choose from are = , > , < , # , and Range . <ul style="list-style-type: none"> When selecting the = option, the specific selected port number will be used. When selecting the > option, all ports greater than the selected port, will be used. When selecting the < option, all ports smaller than the selected port, will be used. When selecting the # option, all ports, excluding the selected port, will be used. When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type ICMP .
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are ack , fin , psh , rst , syn , and urg .

Parameter	Description
	This parameter is only available in the protocol type TCP .
IP Precedence	Select the IP precedence value used here. Options to choose from are routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), and network (7). <ul style="list-style-type: none"> Value - The IP precedence value can also manually be entered here. The range is from 0 to 7.
ToS	Select the Type-of-Service (ToS) value that will be used here. Options to choose from are normal (0), min-monetary-cost (1), max-reliability (2), max-throughput (4), and min-delay (8). <ul style="list-style-type: none"> Value - The ToS value can also manually be entered here. The range is from 0 to 15.
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
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. It includes fields for ID (set to 11000), ACL Name (S-IP6-ACL), and ACL Type (Standard IPv6 ACL). The Sequence No. field is empty, indicating automatic assignment. The Action is set to Permit. Under 'Match IPv6 Address', both Source and Destination fields have 'Any' selected. The Source field contains '2012::1' and the Destination field contains '2012::1'. Both have 'Prefix Length' fields set to 128. A 'Time Range' field is set to '32 chars'. At the bottom are 'Back' and 'Apply' buttons.

Figure 8-13 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source IPv6 information here. Options to choose from are Any , Host , IPv6 , and Prefix Length .

Parameter	Description
	<ul style="list-style-type: none"> When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the source host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination IPv6 information here. Options to choose from are Any , Host , IPv6 , and Prefix Length . <ul style="list-style-type: none"> When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the Host option is selected, enter the destination host IPv6 address here. When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended IPv6 ACL

After selecting an Extended IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

Add ACL Rule

ID	13000								
ACL Name	E-IP6-ACL								
ACL Type	Extended IPv6 ACL								
Sequence No. (1-65535)	<input type="text"/> (If it isn't specified, the system automatically assigns.)								
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny								
Protocol Type	TCP <input type="button" value="▼"/> (0-255) <input type="checkbox"/> Fragments								
Match IPv6 Address <table border="1"> <tr> <td>Source</td> <td><input checked="" type="radio"/> Any <input type="radio"/> Host 2012::1 <input type="radio"/> IPv6 2012::1 Prefix Length</td> <td>Destination</td> <td><input checked="" type="radio"/> Any <input type="radio"/> Host 2012::1 <input type="radio"/> IPv6 2012::1 Prefix Length</td> </tr> </table>		Source	<input checked="" type="radio"/> Any <input type="radio"/> Host 2012::1 <input type="radio"/> IPv6 2012::1 Prefix Length	Destination	<input checked="" type="radio"/> Any <input type="radio"/> Host 2012::1 <input type="radio"/> IPv6 2012::1 Prefix Length				
Source	<input checked="" type="radio"/> Any <input type="radio"/> Host 2012::1 <input type="radio"/> IPv6 2012::1 Prefix Length	Destination	<input checked="" type="radio"/> Any <input type="radio"/> Host 2012::1 <input type="radio"/> IPv6 2012::1 Prefix Length						
Match Port <table border="1"> <tr> <td>Source Port</td> <td>Please Select <input type="button" value="▼"/></td> <td>Please Select <input type="button" value="▼"/> (0-65535)</td> <td>Please Select <input type="button" value="▼"/> (0-65535)</td> </tr> <tr> <td>Destination Port</td> <td>Please Select <input type="button" value="▼"/></td> <td>Please Select <input type="button" value="▼"/> (0-65535)</td> <td>Please Select <input type="button" value="▼"/> (0-65535)</td> </tr> </table>		Source Port	Please Select <input type="button" value="▼"/>	Please Select <input type="button" value="▼"/> (0-65535)	Please Select <input type="button" value="▼"/> (0-65535)	Destination Port	Please Select <input type="button" value="▼"/>	Please Select <input type="button" value="▼"/> (0-65535)	Please Select <input type="button" value="▼"/> (0-65535)
Source Port	Please Select <input type="button" value="▼"/>	Please Select <input type="button" value="▼"/> (0-65535)	Please Select <input type="button" value="▼"/> (0-65535)						
Destination Port	Please Select <input type="button" value="▼"/>	Please Select <input type="button" value="▼"/> (0-65535)	Please Select <input type="button" value="▼"/> (0-65535)						
TCP Flag <input type="checkbox"/> ack <input type="checkbox"/> fin <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> urg									
<input checked="" type="radio"/> DSCP (0-63)	Please Select <input type="button" value="▼"/> Value (0-63) <input type="text"/>								
<input type="radio"/> Traffic Class (0-255)	<input type="text"/>								
Flow Label (0-1048575) <input type="text"/>									
Time Range <input type="text"/> 32 chars									
<input type="button" value="Back"/> <input type="button" value="Apply"/>									

Figure 8-14 Extended IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Protocol Type	Select the protocol type option here. Options to choose from are TCP , UDP , ICMP , Protocol ID , ESP (50), PCP (108), SCTP (132), and None . <ul style="list-style-type: none"> • Value - The protocol ID can also manually be entered here. The range is from 0 to 255. • Fragments - Select this option to include packet fragment filtering.
Source	Select and enter the source IPv6 information here. Options to choose from are Any , Host , and IPv6 . <ul style="list-style-type: none"> • When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the Host option is selected, enter the source host IPv6 address here. • When the IPv6 option is selected, the Prefix Length option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination IPv6 information here. Options to choose from are Any , Host , and IPv6 . <ul style="list-style-type: none"> • When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the Host option is selected, enter the destination host IPv6 address here. • When the IPv6 option is selected, the Prefix Length option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are = , > , < , # , and Range . <ul style="list-style-type: none"> • When selecting the = option, the specific selected port number will be used. • When selecting the > option, all ports greater than the selected port, will be used. • When selecting the < option, all ports smaller than the selected port, will be used. • When selecting the # option, all ports, excluding the selected port, will be used. • When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>
Destination Port	Select and enter the destination port value here. Options to choose from are = , > , < , # , and Range . <ul style="list-style-type: none"> • When selecting the = option, the specific selected port number will be used. • When selecting the > option, all ports greater than the selected port, will be used. • When selecting the < option, all ports smaller than the selected port, will be used. • When selecting the # option, all ports, excluding the selected port, will be used. • When selecting the Range option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. <p>This parameter is only available in the protocol type TCP and UDP.</p>

Parameter	Description
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 .
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type ICMP .
ICMP Message Type	When the ICMP Message Type is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
Message Code	When the ICMP Message Type is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the ICMP Message Type is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type ICMP .
DSCP	Select the DSCP value that will be used here. Options to choose from are default (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), and ef (46). <ul style="list-style-type: none"> Value - The DSCP value can also manually be entered here. The range is from 0 to 63.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended MAC ACL

After selecting an Extended MAC ACL and clicking the **Add Rule** button, the following page will appear.

Add ACL Rule

Add ACL Rule

ID	6000	ACL Name	E-MAC-ACL	ACL Type	Extended MAC ACL										
Sequence No. (1-65535)	<input type="text"/> (If it isn't specified, the system automatically assigns.)														
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny														
Match MAC Address <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input checked="" type="radio"/> Any <input type="radio"/> Host <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> MAC <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> Wildcard <input type="text" value="11-DF-36-4B-A7-CC"/> </div> </td> <td style="width: 50%;"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input checked="" type="radio"/> Any <input type="radio"/> Host <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> MAC <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> Wildcard <input type="text" value="11-DF-36-4B-A7-CC"/> </div> </td> </tr> </table>						<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input checked="" type="radio"/> Any <input type="radio"/> Host <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> MAC <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> Wildcard <input type="text" value="11-DF-36-4B-A7-CC"/> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input checked="" type="radio"/> Any <input type="radio"/> Host <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> MAC <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> Wildcard <input type="text" value="11-DF-36-4B-A7-CC"/> </div>								
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input checked="" type="radio"/> Any <input type="radio"/> Host <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> MAC <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> Wildcard <input type="text" value="11-DF-36-4B-A7-CC"/> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input checked="" type="radio"/> Any <input type="radio"/> Host <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> MAC <input type="text" value="11-DF-36-4B-A7-CC"/> <input type="radio"/> Wildcard <input type="text" value="11-DF-36-4B-A7-CC"/> </div>														
Match Ethernet Type <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Specify Ethernet Type <input style="width: 100%;" type="text" value="Please Select"/> </div> </td> <td style="width: 50%;"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Ethernet Type (0x0-0xFFFF) <input type="text"/> </div> </td> </tr> <tr> <td colspan="2"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Ethernet Type Mask (0x0-0xFFFF) <input type="text"/> </div> </td> </tr> <tr> <td colspan="2"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> CoS <input type="text" value="Please Select"/> </div> </td> </tr> <tr> <td colspan="2"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> VID(1-4094) <input type="text"/> </div> </td> </tr> <tr> <td colspan="2"> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Time Range <input type="text" value="32 chars"/> </div> </td> </tr> </table>						<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Specify Ethernet Type <input style="width: 100%;" type="text" value="Please Select"/> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Ethernet Type (0x0-0xFFFF) <input type="text"/> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Ethernet Type Mask (0x0-0xFFFF) <input type="text"/> </div>		<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> CoS <input type="text" value="Please Select"/> </div>		<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> VID(1-4094) <input type="text"/> </div>		<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Time Range <input type="text" value="32 chars"/> </div>	
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Specify Ethernet Type <input style="width: 100%;" type="text" value="Please Select"/> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Ethernet Type (0x0-0xFFFF) <input type="text"/> </div>														
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Ethernet Type Mask (0x0-0xFFFF) <input type="text"/> </div>															
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> CoS <input type="text" value="Please Select"/> </div>															
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> VID(1-4094) <input type="text"/> </div>															
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Time Range <input type="text" value="32 chars"/> </div>															

Figure 8-15 Extended MAC ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit and Deny .
Source	Select and enter the source MAC address information here. Options to choose from are Any , Host , MAC , and Wildcard . <ul style="list-style-type: none"> • When the Any option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the Host option is selected, enter the source host MAC address here. • When the MAC option is selected, the Wildcard option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are Any , Host , MAC , and Wildcard . <ul style="list-style-type: none"> • When the Any option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the Host option is selected, enter the destination host MAC address here. • When the MAC option is selected, the Wildcard option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are aarp , appletalk , decent-iv , etype-6000 , etype-8042 , lat , lavc-sca , mop-console , mop-dump , vines-echo , vines-ip , xns-idp , and arp .
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7 .
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

ACL Interface Access Group

This window is used to display and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:

Port	In			
	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
eth1/0/1				
eth1/0/2				
eth1/0/3				
eth1/0/4				
eth1/0/5				
eth1/0/6				
eth1/0/7				
eth1/0/8				
eth1/0/9				
eth1/0/10				

Figure 8-16 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	Specifies that the In direction is used.
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:

Total Entries: 2			
ID	ACL Name	ACL Type	
1	S-IP-ACL	Standard IP ACL	
2000	E-IP-ACL	Extended IP ACL	

Figure 8-17 ACL Interface Access Group (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

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

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

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:

Port Security Global Settings		
Port Security Trap Settings <div style="display: flex; justify-content: space-between;"> Trap State <div style="display: flex; align-items: center;"> <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled </div> Apply </div>		
Port Security Trap Rate Settings <div style="display: flex; justify-content: space-between;"> Trap Rate (0-1000) <input type="text" value="0"/> Apply </div>		
Port Security System Settings <div style="display: flex; justify-content: space-between;"> System Maximum Address (1-3328) <div style="display: flex; align-items: center;"> <input style="width: 50px; height: 20px; margin-right: 10px;" type="text"/> <input checked="" type="checkbox"/> No Limit </div> Apply </div>		

Figure 9-1 Port Security Global Settings Window

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

Parameter	Description
Trap State	Select to enable or disable port security traps on the Switch.

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

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

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 0 indicates an SNMP trap to be generated for every security violation.

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

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

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit. The valid range is from 1 to 3328. 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 port settings.

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

The screenshot shows the 'Port Security Port Settings' window. At the top, there are dropdown menus for 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'State' (Disabled), 'Maximum (0-64)' (32), 'Violation Action' (Protect), 'Security Mode' (Delete-on-TIMEOUT), 'Aging Time (0-1440)', and 'Aging Type' (Absolute). Below these are two buttons: 'Apply' and 'Cancel'. A large table lists port settings for ports eth1/0/1 through eth1/0/10. Each row includes columns for Port, Maximum, Current No., Violation Action, Violation Count, Security Mode, Admin State, Current State, Aging Time, and Aging Type. All ports are set to Maximum 32, Violation Action Protect, and Security Mode Delete-on-TIMEOUT.

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. This value must be between 0 and 64. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are: <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 would 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 would be purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.
Aging Type	Specifies that Absolute is used. All the secure addresses on this port age out exactly after the time specified and is removed from the secure address list.

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:

The screenshot shows the 'Port Security Address Entries' configuration page. At the top, there are input fields for 'Port' (set to 'eth1/0/1'), 'MAC Address' (set to '00-84-57-00-00-00'), and 'VID (1-4094)' (set to '1'). Below these are buttons for 'Add', 'Delete', 'Clear by Port', and 'Clear by MAC'. A message 'Total Entries: 1' is displayed above a table. The table has columns: Port, VID, MAC Address, Address Type, and Remaining Time (mins). One entry is listed: Port 'eth1/0/10', VID '1', MAC Address '00-11-22-33-44-55', Address Type 'Permanent', and Remaining Time '—'. At the bottom right are navigation buttons for pages 1/1, and a 'Go' button.

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 the Permanent option to specify that all learned MAC addresses would not be purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID here. This value must be between 1 and 4094.

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

Click the **Delete** button to remove a new entry based on the information entered.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

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

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

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control

model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

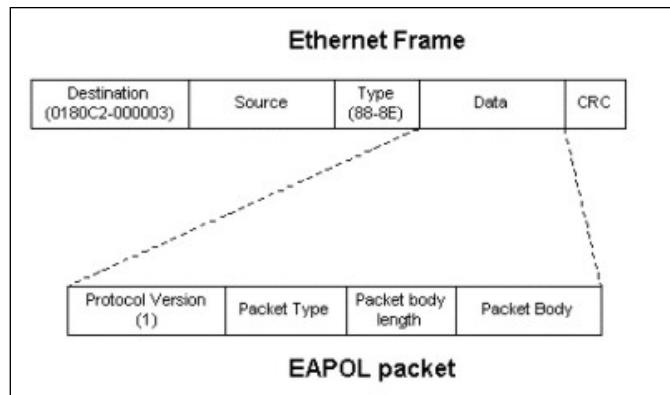


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

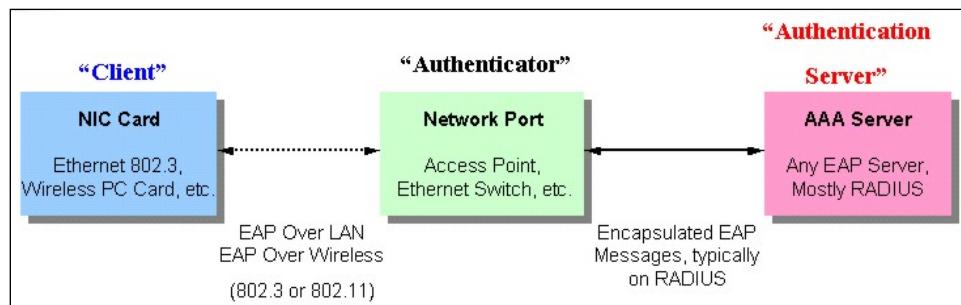


Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

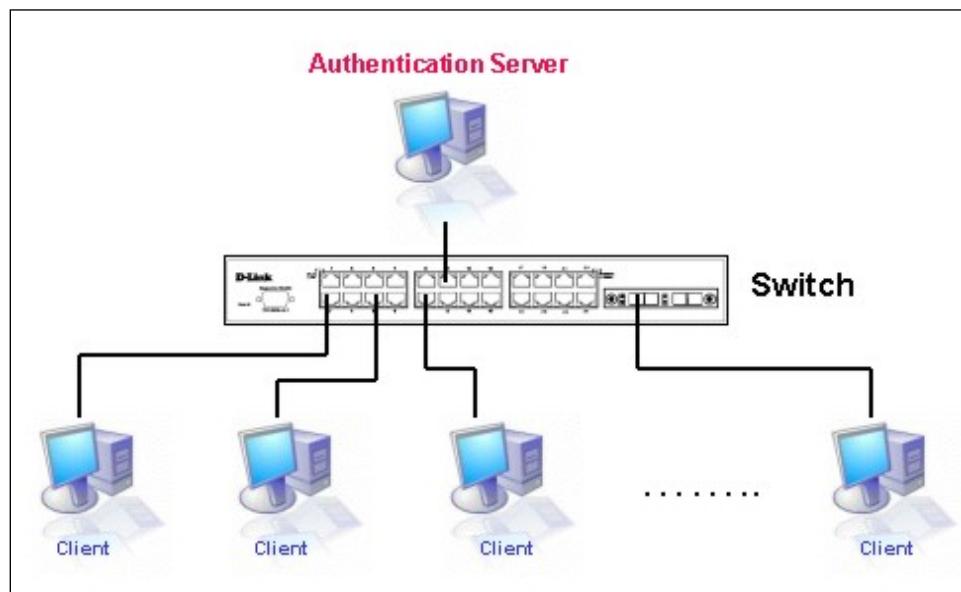


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

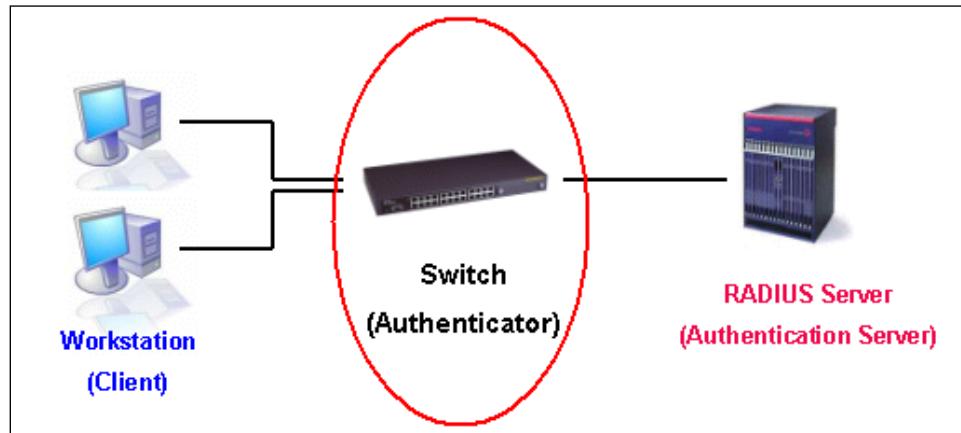


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X State must be Enabled. (**Security > 802.1X > 802.1X Global Settings**)
- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running windows XP and windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

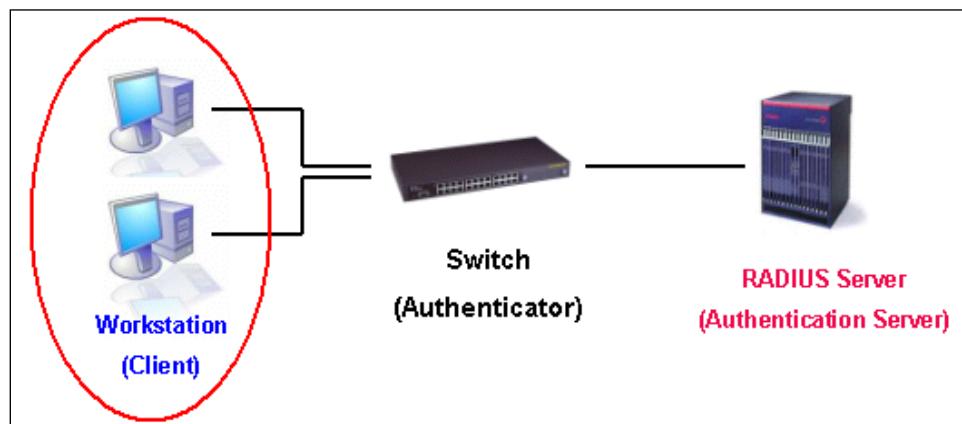


Figure 9-8 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

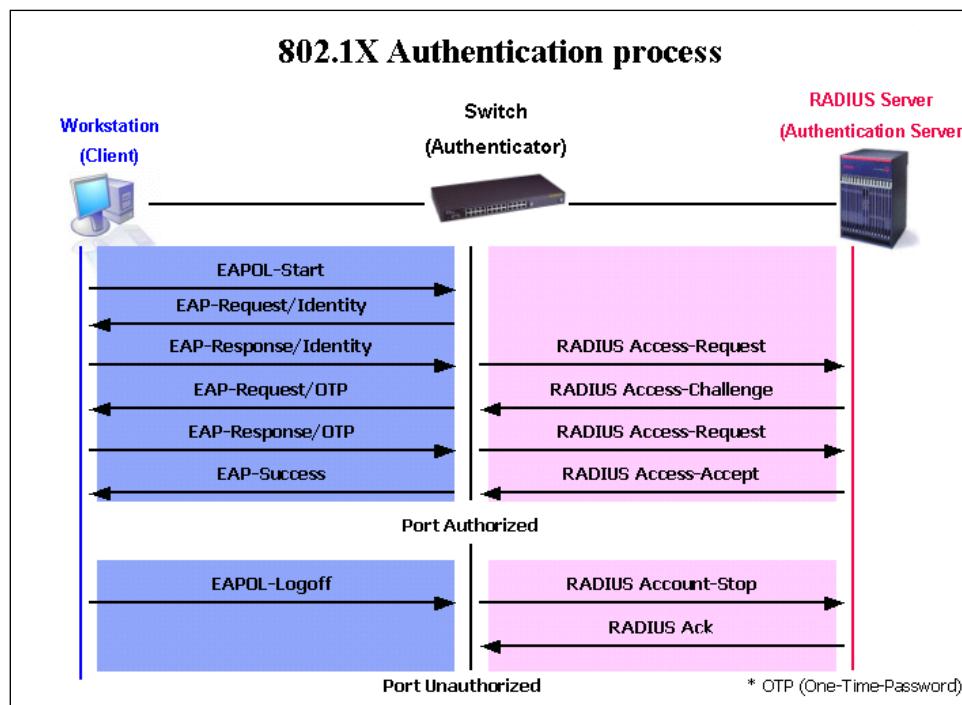


Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **Port-based Access Control** - This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
- **Host-based Access Control** - Using this method, the Switch will automatically learn up to a maximum of 1000 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

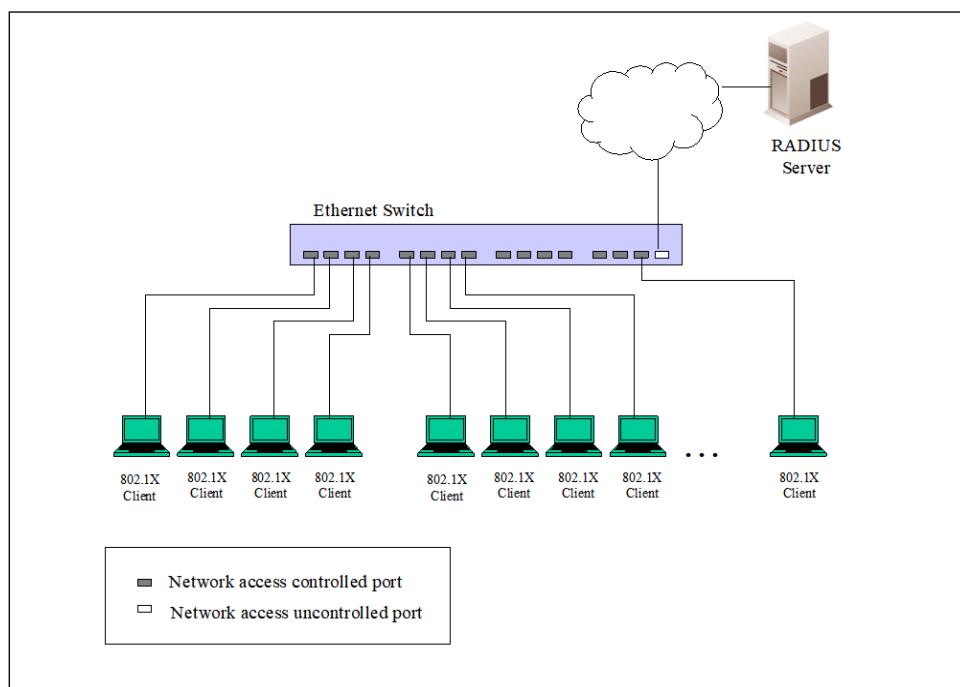


Figure 9-10 Example of Typical Port-based Configuration

Host-based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

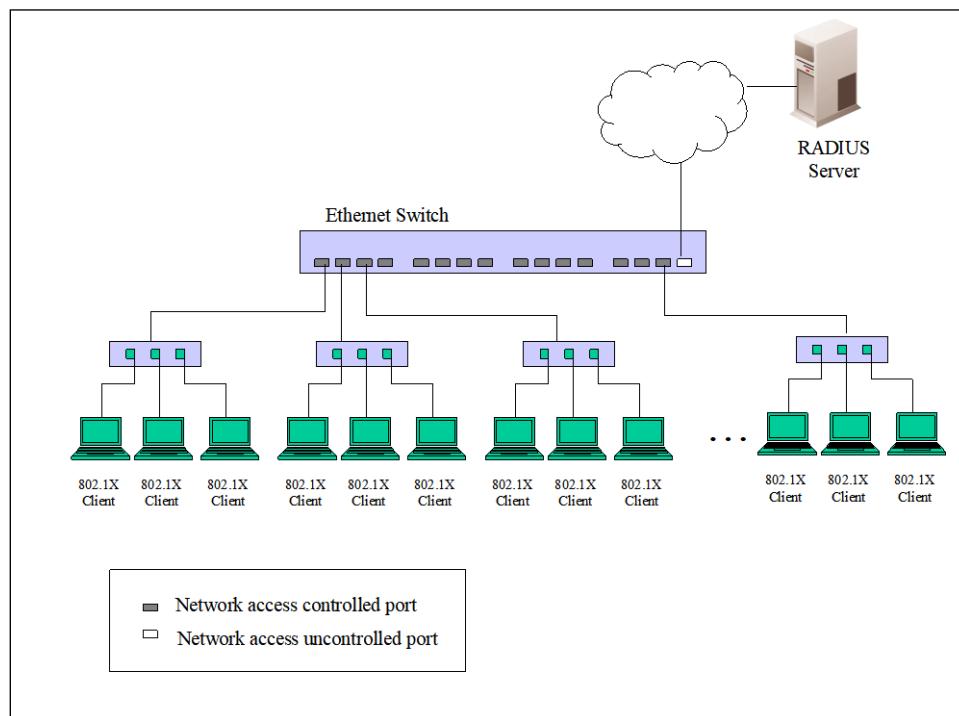


Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to display and configure the global 802.1X settings.

To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:

802.1X Global Settings	
802.1X State	Disabled <input type="button" value="▼"/>
802.1X Trap State	Disabled <input type="button" value="▼"/>
Apply	

Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

Parameter	Description
802.1X State	Select to enable or disable the global 802.1X state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

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

802.1X Port Settings

This window is used to display and configure the 802.1X port settings.

To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:

The screenshot shows the '802.1X Port Settings' window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1'), 'To Port' (set to 'eth1/0/1'), and 'Direction' (set to 'Both'). Below these are 'Port Control' (set to 'Auto'), 'Forward PDU' (set to 'Disabled'), 'MaxReq (1-10)' (set to '2'), 'PAE Authenticator' (set to 'Disabled'), 'ServerTimeout (1-65535)' (set to '30 sec'), 'SuppTimeout (1-65535)' (set to '30 sec'), and 'TX Period (1-65535)' (set to '30 sec'). An 'Apply' button is at the bottom right. Below the configuration area is a table with 11 rows, each representing a port from eth1/0/1 to eth1/0/10. The columns are: Port, Direction, Port Control, Forward PDU, MaxReq, PAE Authenticator, ServerTimeout, SuppTimeout, and TX Period. All ports are set to 'Both' direction, 'Auto' control, 'Disabled' PDU, '2' MaxReq, 'None' PAE, '30' ServerTimeout, '30' SuppTimeout, and '30' TX Period.

Port	Direction	Port Control	Forward PDU	MaxReq	PAE Authenticator	ServerTimeout	SuppTimeout	TX Period
eth1/0/1	Both	Auto	Disabled	2	None	30	30	30
eth1/0/2	Both	Auto	Disabled	2	None	30	30	30
eth1/0/3	Both	Auto	Disabled	2	None	30	30	30
eth1/0/4	Both	Auto	Disabled	2	None	30	30	30
eth1/0/5	Both	Auto	Disabled	2	None	30	30	30
eth1/0/6	Both	Auto	Disabled	2	None	30	30	30
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). The In control direction is only valid when the Host Mode is configured as Multi Host in the Network Access Authentication Port Settings window.
Port Control	Select the port control option here. Options to choose from are ForceAuthorized , Auto , and ForceUnauthorized . If the port control is set to force-authorized, then the port is not controlled in both directions. If the port control is set to automatic, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to force-unauthorized, then the access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. This value must be between 1 and 10. By default, this 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. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
SuppTimeout	Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

Parameter	Description
TX Period	Enter the transmission period value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

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

Authentication Sessions Information

This window is used to display and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Sessions Information**, as shown below:

The screenshot shows a table with one row. The columns are labeled "Port" and "MAC Address". The "Port" column contains "eth1/0/1". The "MAC Address" column contains "BC-AE-C5-75-97-72". Below the table are buttons for "Init by Port", "ReAuth by Port", "Init by MAC", and "ReAuth by MAC". At the bottom are navigation buttons for page 1/1, previous, next, last, first, and a "Go" button.

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 MAC address.

Click the **ReAuth by MAC** button to re-authenticate the session information based on MAC address.

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

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:

The screenshot shows a table with 14 columns. The columns are labeled: Port, Frames RX, Frames TX, Start RX, ReqID TX, LogOff RX, Req RX, RespID RX, Resp RX, Invalid RX, Error RX, Last Version, and Last Source. The "Port" column contains "eth1/0/6". The "Frames RX" column contains "0". The "Frames TX" column contains "3". The "Start RX" column contains "0". The "ReqID TX" column contains "2". The "LogOff RX" column contains "0". The "Req RX" column contains "0". The "RespID RX" column contains "0". The "Resp RX" column contains "0". The "Invalid RX" column contains "0". The "Error RX" column contains "0". The "Last Version" column contains "0". The "Last Source" column contains "00-00-00-00-00-0...". Below the table are buttons for "Find", "Clear Counters", "Clear All", and navigation buttons for page 1/1, previous, next, last, first, and a "Go" button.

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:

Authenticator Session Statistics									
Authenticator Session Statistics									
Port	Octets RX	Octets TX	Frames RX	Frames TX	ID	AuthenticMethod	Time	TerminateCause	User Name
Total Entries: 0									

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:

Authenticator Diagnostics	
Authenticator Diagnostics	
Port	eth1/0/1 <input type="button" value="▼"/>
	<input type="button" value="Find"/> <input type="button" value="Clear Counters"/> <input type="button" value="Clear All"/>
Total Entries: 1	
Port	eth1/0/6
EntersConnecting	3
EAP-LogoffsWhileConnecting	0
EntersAuthenticating	0
SuccessesWhileAuthenticating	0
TimeoutsWhileAuthenticating	0
FailsWhileAuthenticating	0
ReauthsWhileAuthenticating	0
EAP-StartsWhileAuthenticating	0
EAP-LogoffsWhileAuthenticating	0
ReauthsWhileAuthenticated	0
EAP-StartsWhileAuthenticated	0
EAP-LogoffsWhileAuthenticated	0
BackendResponses	0
BackendAccessChallenges	0
BackendOtherRequestsToSupplicant	0
BackendNonNakResponsesFromSupplicant	0
BackendAuthSuccesses	0
BackendAuthFails	0
<input type="button" value="1/1"/> <input type="button" value=" <"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=" >"/> <input type="text"/> Go	

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:

The screenshot shows a window titled "AAA Global Settings". Under the "AAA State Settings" section, there is a radio button labeled "Enabled" which is selected. An "Apply" button is located in the bottom right corner of this section.

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. By default, this is disabled.

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

Authentication Settings

This window is used to display and configure the AAA network settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:

The screenshot shows a window titled "Authentication Settings". Under the "AAA Authentication Network" section, there is a "AAA Authentication 802.1X" group. It contains a "Status" dropdown set to "Disabled", four "Method" dropdowns all set to "Please Select", and an "Apply" button in the bottom right corner.

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:

RADIUS Global Settings		
RADIUS Global Settings Dead Time (0-1440) <input type="text" value="0"/> min <input type="button" value="Apply"/>		

Figure 9-20 RADIUS Global Settings Window

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

Parameter	Description
Dead Time	Enter the dead time value here. This value must be between 0 and 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries. When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

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

RADIUS Server Settings

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

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:

RADIUS Server Settings																	
RADIUS Server Settings IP Address <input checked="" type="radio"/> <input type="radio"/> IPv6 Address Authentication Port (0-65535) <input type="text" value="1812"/> Timeout (1-255) <input type="text" value="5"/> sec Key <input type="text" value="32 chars"/>																	
Retransmit (0-20) <input type="text" value="2"/> times Key Type <input type="text" value="Plain Text"/>																	
Total Entries: 1 <table border="1"> <thead> <tr> <th>IPv4/IPv6 Address</th> <th>Authentication Port</th> <th>Timeout</th> <th>Retransmit</th> <th>Key</th> <th></th> </tr> </thead> <tbody> <tr> <td>10.90.90.1</td> <td>1812</td> <td>5</td> <td>2</td> <td>*****</td> <td><input type="button" value="Delete"/></td> </tr> </tbody> </table>						IPv4/IPv6 Address	Authentication Port	Timeout	Retransmit	Key		10.90.90.1	1812	5	2	*****	<input type="button" value="Delete"/>
IPv4/IPv6 Address	Authentication Port	Timeout	Retransmit	Key													
10.90.90.1	1812	5	2	*****	<input type="button" value="Delete"/>												

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. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 2. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Specifies that the Plain Text key type is used.
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

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

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

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:

The screenshot shows the 'RADIUS Group Server Settings' window. At the top, there's a 'Group Server Name' field with a '32 chars' limit, an 'IP Address' input field with a dropdown menu, and an 'IPv6 Address' input field with a dropdown menu. Below these are buttons for 'Add', 'Show Detail', and 'Delete'. A message 'Total Entries: 2' is displayed above a table. The table has columns for 'Group Server Name' and 'IPv4/IPv6 Address'. It contains two rows: one for 'group' with IP 10.90.90.2... and one for 'radius' with IP 10.90.90.2.... Each row has 'Show Detail' and 'Delete' buttons at the end.

Group Server Name	IPv4/IPv6 Address	Show Detail	Delete
group	10.90.90.2...	-	-
radius	10.90.90.2...	-	-

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.
IP Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

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

Click the **Show Detail** button to view and configure 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 Statistic		
Group Server Name	Please Select	Clear Clear All
Total Entries: 1		
RADIUS Server Address	Authentication Port	State
10.90.90.1	1812	Up
1/1 < < 1 > > Go		

RADIUS Server Address: 10.90.90.1		Clear
Parameter	Authentication Port	
Round Trip Time	0	
Access Requests	0	
Access Accepts	0	
Access Rejects	0	
Access Challenges	0	
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	<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
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 belongs 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. This value must be between 0 and 1024. Tick the No Limit option to disable the function.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 300. Tick the No Limit option to disable the function.
Trusted	Select the trusted option here. Options to choose from are No and Yes . Ports connected to the DHCP server or to other Switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

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

DHCP Snooping VLAN Settings

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

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:

DHCP Snooping VLAN Settings			
VID List	1, 4-6	State	Enabled <input type="button" value="▼"/>
DHCP Snooping Enabled VID :			

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:

DHCP Snooping Database			
DHCP Snooping Database			
Write Delay (60- 86400)	<input type="text" value="300"/> sec	<input type="checkbox"/> Default	<input type="button" value="Apply"/>
Store DHCP Snooping Database			
URL	<input type="button" value="TFTP"/> <input type="text"/>	<input type="button" value="Apply"/>	<input type="button" value="Clear"/>
A URL beginning with this prefix //location/filename			
Load DHCP Snooping Database			
URL	<input type="button" value="TFTP"/> <input type="text"/>	<input type="button" value="Apply"/>	
A URL beginning with this prefix //location/filename			
Last ignored Bindings counters			
Binding Collisions	0	Expired Lease	0
Invalid Interfaces	0	Unsupported VLAN	0
Parse Failures	0	Checksum Errors	0
<input type="button" value="Clear"/>			

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. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds.

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

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	Specifies to store the DHCP snooping database on a TFTP server. Enter the URL in the space provided.

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

The fields that can be configured in **Load DHCP Snooping Database** are described below:

Parameter	Description
URL	Specifies to load the DHCP snooping database from a TFTP server. Enter the URL in the space provided.

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

Click the **Clear** button to clear all the counter information.

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:

The screenshot shows the 'DHCP Snooping Binding Entry' configuration window. At the top, there's a section for 'DHCP Snooping Manual Binding' with fields for MAC Address (00-84-57-00-00-00), VID (1-4094), IP Address, Port (eth1/0/1), and Expiry (60-4294967295 sec). Below this is a table titled 'Total Entries: 1' with one row showing a binding entry for MAC Address 00-11-22-33-44-55, VID 1, IP Address 10.90.90.123, Port eth1/0/10, Expiry 3598, Type dhcp-snooping, and a Delete button. Navigation buttons at the bottom include 1/1, <, <, 1, >, >, and Go.

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. This value must be between 1 and 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

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 a web-based configuration interface for an ARP Access List. At the top, there's a header bar with the title 'ARP Access List'. Below it, a sub-header says 'ARP Access List'. A text input field for 'ARP Access List Name' is set to '32 chars', with an 'Add' button to its right. A message 'Total Entries: 1' is displayed above a table. The table has two columns: 'ARP Access List Name' (containing 'ARP-ACL') and actions ('Edit' and 'Delete').

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 'Edit' configuration window for the ARP Access List. It includes dropdown menus for 'Action' (Permit), 'IP' (Any), and 'MAC' (Any). There are also fields for 'Sender IP' and 'Sender MAC'. On the right, there are 'Sender IP Mask' and 'Sender MAC Mask' fields with their respective 'Back' and 'Apply' buttons. Below these, the 'ARP Access List Name' is set to 'ARP-ACL'. A message 'Total Entries: 1' is shown above a table. The table has columns for Action, IP Type, Sender IP, Sender IP Mask, MAC Type, Sender MAC, Sender MAC Mask, and a 'Delete' button. The first row contains the values: Action=Permit, IP Type=Any, Sender IP=-, Sender IP Mask=-, MAC Type=Any, Sender MAC=-, Sender MAC Mask=-, and Delete=button.

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:

The screenshot shows the 'ARP Inspection Settings' window with three main sections:

- ARP Inspection Validation:** Contains fields for Src-MAC, Dst-MAC, and IP, each with Enabled and Disabled radio buttons. An 'Apply' button is located to the right.
- ARP Inspection VLAN Logging:** A table titled 'Total Entries: 1' with columns VID, ACL Logging, and DHCP Logging. The first row shows VID 2, ACL Logging 'None', and DHCP Logging 'None'. Below the table are navigation buttons (1/1, <, >, 1, Go).
- ARP Inspection Filter:** Contains fields for ARP Access List Name (32 chars), VID List (1, 4-6), and Static ACL (No). Buttons for Add and Delete are present. Below is another table titled 'Total Entries: 1' with columns VID, ARP Access List Name, and Static ACL. The first row shows VID 1, ARP Access List Name 'ARP-ACL', and Static ACL 'No'. Navigation buttons (1/1, <, >, 1, Go) are at the bottom.

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 and 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 ARP inspection VLAN logging settings.

After clicking the **Edit** button the following fields can be configured:

Parameter	Description
ACL Logging	Select the ACL logging action here. This specifies the logging criteria for packets that are dropped or permitted based on ACL matches. Options to choose from are: <ul style="list-style-type: none"> • Deny - Specifies logging when denied by the configured ACL. • Permit - Specifies logging when permitted by the configured ACL. • All - Specifies logging when permitted or denied by the configured ACL. • None - Specifies that ACL-matched packets are not logged.
DHCP Logging	Select the DHCP logging action here. This specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings. Options to choose from are: <ul style="list-style-type: none"> • Deny - Specifies logging when denied by DHCP bindings. • Permit - Specifies logging when permitted by DHCP bindings. • All - Specifies logging when permitted or denied by DHCP bindings. • None - Specifies to prevent the logging of all packets permitted or denied by DHCP bindings.

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

The fields that can be configured in **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting Yes or No .

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

Click the **Delete** button to remove an entry based on the information entered.

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

ARP Inspection Port Settings

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

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:

The screenshot shows the 'ARP Inspection Port Settings' window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1') and 'To Port' (set to 'eth1/0/1'). Below these are input fields for 'Rate Limit (1-150)' (set to '15 pps') and 'Burst Interval (1-15)' (set to 'None'). A dropdown menu for 'Trust State' is set to 'Disabled'. On the right side of the window are 'Apply' and 'Set to Default' buttons. Below these buttons is a table with columns: Port, Trust State, Rate Limit (pps), and Burst Interval. The table lists ports eth1/0/1 through eth1/0/10, all of which are set to 'Untrusted' with a rate limit of 15 pps and a burst interval of 1.

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. This value must be between 1 and 150 packets per seconds.
Burst Interval	Enter the burst interval value here. This value must be between 1 and 15. Tick the None option to disable the option.
Trust State	Select to enable or disable the trust state here.

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

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

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

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:

The screenshot shows the 'ARP Inspection VLAN' window. It has fields for 'VID List' (set to '1, 4-6'), 'State' (set to 'Enabled'), and an 'Apply' button. Below these fields is a note: 'ARP Inspection Enabled VID :'. The entire window is enclosed in a light gray border.

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:

ARP Inspection Statistics									
VID List		Total Entries: 1							
VLAN	Forwarded	Dropped	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Source MAC Failures	Dest MAC Failure	IP Validation Failure
1	0	0	0	0	0	0	0	0	0
1/1		<	<	1	>	>	<input type="checkbox"/>	Go	Go

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:

ARP Inspection Log						
ARP Inspection Log						
Log Buffer (1-1024)		32				
Total Entries: 0						
Port						
VLAN		Sender IP		Sender MAC		
Occurrence						

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. This value must be between 1 and 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to display and configure the IP Source Guard (IPSG) port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:

IP Source Guard Port Settings							
From Port	eth1/0/1	To Port	eth1/0/1				
State	Enabled	Validation	IP				
<table border="1"> <thead> <tr> <th>Port</th> <th>Validation Type</th> </tr> </thead> <tbody> <tr> <td>eth1/0/1</td> <td>ip</td> </tr> </tbody> </table>		Port	Validation Type	eth1/0/1	ip	<input type="button" value="Apply"/>	
Port	Validation Type						
eth1/0/1	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 IP and IP-MAC . Selecting IP means that the IP address of the received packets will be checked. Selecting IP-MAC means that the IP address and the MAC address of the received packets will be checked.

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

IP Source Guard Binding

This window is used to display and configure the IPSG binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:

The screenshot shows the 'IP Source Guard Binding' configuration window. It includes sections for 'IP Source Binding Settings' (with fields for MAC Address, VID, IP Address, and port ranges), 'IP Source Binding Entry' (with search fields for From Port, IP Address, VID, To Port, MAC Address, and Type), and a table of 'Total Entries: 1'. The table lists a single entry with columns for MAC Address, IP Address, Lease (sec), Type, VLAN, and Port, along with a Delete button. Navigation buttons at the bottom include 1/1, <, <, 1, >, >, and Go.

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:

IP Source Guard HW Entry					
From Port	eth1/0/1	To Port	eth1/0/1	Find	
Total Entries: 1					
Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
eth1/0/1	ip	Active	deny-all	-	1

1/1 < < 1 > > Go

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:

IP-MAC-Port Binding Trap Settings				
Trap State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled			
IP-MAC-Port Binding Port Settings				
From Port	eth1/0/1	To Port	eth1/0/1	Apply
Mode	Disabled	Apply		
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			
eth1/0/9	Disabled			
eth1/0/10	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.

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

The fields that can be configured in **IP-MAC-Port Binding Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are Disabled , Strict , and Loose . When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry.

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

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.
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:

IPv6 Snooping														
Station Move Setting Station Move Permit <input type="button" value="▼"/> <input type="button" value="Apply"/>														
IPv6 Snooping Policy Settings Policy Name <input type="text" value="32 chars"/> Limit Address Count (0-511) <input type="text" value=""/> <input checked="" type="checkbox"/> No Limit Protocol <input type="button" value="Enabled"/> <input type="checkbox"/> DHCP <input type="checkbox"/> NDP VID List <input type="text" value="1, 4-6"/> <input type="button" value="Apply"/>														
Total Entries: 1 <table border="1"> <thead> <tr> <th>Snooping Policy</th> <th>Protocol</th> <th>Limit Address Count</th> <th>Target VLAN</th> <th></th> </tr> </thead> <tbody> <tr> <td>Policy</td> <td>Enabled</td> <td>511</td> <td>1</td> <td><input type="button" value="Edit"/> <input type="button" value="Delete"/></td> </tr> </tbody> </table>					Snooping Policy	Protocol	Limit Address Count	Target VLAN		Policy	Enabled	511	1	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Snooping Policy	Protocol	Limit Address Count	Target VLAN											
Policy	Enabled	511	1	<input type="button" value="Edit"/> <input type="button" value="Delete"/>										

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 .

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

The fields that can be configured in **IPv6 Snooping Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 511. Tick the No Limit option to disable this option.
Protocol	Select the protocol state here. Options to choose from are Enabled and Disabled . <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 detects DAD messages (DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA)) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.
VID List	Enter the VLAN ID list used here.

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

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

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

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:

The screenshot shows the 'IPv6 ND Inspection' configuration window. At the top, there are fields for 'Policy Name' (32 chars), 'Device Role' (Host), 'Validate Source-MAC' (Disabled), and a checked 'Target Port' option with 'From Port' set to 'eth1/0/1' and 'To Port' set to 'eth1/0/1'. Below these are buttons for 'Apply' and 'Edit'. A table titled 'Total Entries: 1' displays one row with columns for Policy Name, Device Role, Validate Source-MAC, Target Port, Edit, and Delete. The row data is: Policy Name (Policy), Device Role (Host), Validate Source-MAC (Disabled), Target Port (eth1/0/8), Edit, and Delete.

Total Entries: 1					
Policy Name	Device Role	Validate Source-MAC	Target Port	Edit	Delete
Policy	Host	Disabled	eth1/0/8	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

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:

Policy Name	Device Role	Match IPv6 Access List	Target Port	
S-IP6	Host	S-IP6	eth1/0/10	Edit Delete

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:

ID	ACL Name	ACL Type
11000	S-IP6	Standard IPv6 ACL
13000	E-IP6	Extended IPv6 ACL

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:

Total Entries: 1				
Policy Name	Device Role	Match IPv6 Access List	Target Port	
Policy	Client	S-IP6	eth1/0/11	Edit Delete

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:

Total Entries: 2			
	ID	ACL Name	ACL Type
<input type="radio"/>	11000	S-IP6	Standard IPv6 ACL
<input type="radio"/>	13000	E-IP6	Extended IPv6 ACL

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:

The screenshot shows the 'IPv6 Source Guard Settings' window. It includes sections for 'IPv6 Source Guard Policy Settings' and 'IPv6 Source Guard Attach Policy Settings'. In the policy settings section, fields include 'Policy Name' (32 chars), 'Global Auto-Configure Address' (Permit/Deny dropdown), and 'Link Local Traffic' (Deny). The attach policy settings section includes 'Policy Name', 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), and an 'Apply' button. A table lists entries with columns for Policy Name, Global Auto-Configure Address, Link Local Traffic, Target Port, Edit, and Delete buttons. The target port for all listed entries is eth1/0/12.

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 wants to block hosts with self-configured addresses from sending traffic. By default, Permit is used.
Link Local Traffic	Select to Permit or Deny hardware permitted data traffic send by the link-local address. By default, Deny is used.

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

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

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

The fields that can be configured in **IPv6 Source Guard Attach Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Target Port	Select this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

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

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:

The screenshot shows the 'IPv6 Neighbor Binding' configuration window. It includes sections for 'IPv6 Neighbor Binding Settings' (with fields for MAC Address, VID, IPv6 Address, and port ranges) and 'IPv6 Neighbor Binding Entry' (with search fields for From Port, To Port, IPv6 Address, MAC Address, and VID). Below these are sections for 'Total Entries: 1' and a table of one entry. The table columns are IPv6 Address, MAC Address, Port, VLAN, Owner, and Time left. The entry shown is 2019::1, 00-11-22-33-44-55, eth1/0/13, 1, Static, and N/A. Buttons at the bottom include Apply, Find, Delete, and navigation links (1/1, <, >, 1, Go).

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. This value must be between 1 and 4094.
IPv6 Address	Enter the IPv6 address used here.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IPv6 Neighbor Binding Entry** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

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

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

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:

Total Entries: 1			
Profile Name	Client MAC	Bind Client MAC	
Profile	-	Binding	<input type="button" value="Delete"/> <input type="button" value="Delete Profile"/>

Log Information			
Log Buffer Entries (10-1024)		Occurrence	
32		<input type="button" value="Apply"/> <input type="button" value="Clear Log"/>	

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.

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.

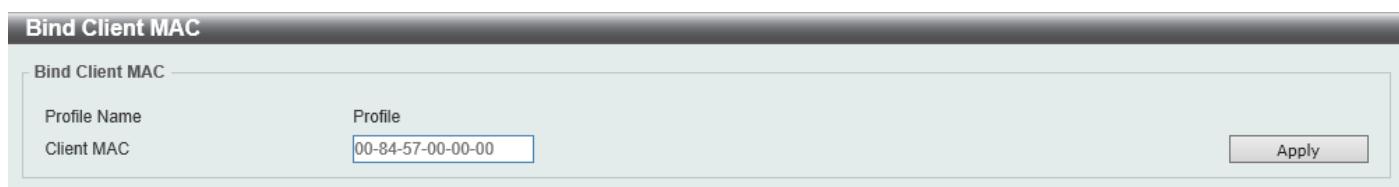
The fields that can be configured in **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. This value must be between 10 and 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

After clicking the **Binding** button, the following window will appear:



The screenshot shows a configuration window titled "Bind Client MAC". It has a sub-section titled "Bind Client MAC". There are two input fields: "Profile Name" (set to "Profile") and "Client MAC" (set to "00-84-57-00-00-00"). A "Apply" button is located on the right side of the window.

Figure 9-51 Bind Client MAC 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:



The screenshot shows a configuration window titled "DHCP Server Screening Port Settings". At the top, there are dropdown menus for "From Port" (set to "eth1/0/1") and "To Port" (set to "eth1/0/1"), a "State" dropdown set to "Disabled", and a "Server IP" field. To the right of these is a "Profile Name" field with a "32 chars" placeholder and an "Apply" button. Below this is a table with columns "Port", "State", "Server IP", and "Profile Name". The table lists ports eth1/0/1 through eth1/0/10, all of which are currently disabled. Each row has a "Delete" button on the far right.

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.
State	Select to enable or disable the DHCP server screening function on the port(s) specified.

Parameter	Description
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:

Total Entries: 1			
Gateway IP	Gateway MAC	Port	
10.90.90.1	00-11-22-33-44-55	eth1/0/10	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:

The screenshot shows the 'Guest VLAN' configuration window. At the top, there are dropdown menus for 'From Port' (set to 'eth1/0/1') and 'To Port' (set to 'eth1/0/1'), and a text input field for 'VID (1-4094)' (set to '1'). An 'Apply' button is located to the right. Below this, a table displays 'Total Entries: 1'. The table has columns for 'Port' (containing 'eth1/0/10') and 'VID' (containing '1'). A 'Delete' button is in the top right of the table area. At the bottom, there are navigation buttons for pages 1/1, and a 'Go' button.

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. This value must be between 1 and 4094.

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

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

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

Network Access Authentication Global Settings

This window is used to display and configure the global Network Access Authentication settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:

The screenshot shows the 'Network Access Authentication Global Settings' configuration window. Under 'General Settings', there are fields for 'Max Users (1-1000)' (set to '1000') and 'Authorization State' (set to 'Enabled'). An 'Apply' button is to the right. Under 'User Information', there are fields for 'User Name' (with a '32 chars' input field), 'Password Type' (set to 'Plain Text'), 'Password' (with a '32 chars' input field), and another 'Apply' button. Below these, a table displays 'Total Entries: 1'. The table has columns for 'User Name' (containing 'User'), 'Password' (containing '*****'), 'Password Type' (containing 'Plaintext'), and 'VID' (containing '1'). A 'Delete' button is in the top right of the table area.

Figure 9-55 Network Access Authentication Global Settings Window

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

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. This value must be between 1 and 1000. The default 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 type is Plain Text .
Password	Enter the password used here. This can be up to 32 characters long.

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

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

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:

The screenshot shows the 'Network Access Authentication Port Settings' window. At the top, there are dropdown menus for 'From Port' (eth1/0/1) and 'To Port' (eth1/0/1), and a 'Host Mode' dropdown set to 'Multi Host'. Below these are input fields for 'Max Users (1-1000)' (1000), 'Periodic' (Disabled), 'ReAuth Timer (1-65535)' (3600 sec), and 'Restart (1-65535)' (60 sec). An 'Apply' button is located to the right of the timer field. Below the configuration area is a table listing port settings for ports eth1/0/1 through eth1/0/21. The table columns are: Port, Host Mode, Max Users, Periodic, ReAuth, and Restart. All ports are configured with Multi Host mode, 1000 users, and a 3600-second re-authentication timer.

Port	Host Mode	Max Users	Periodic	ReAuth	Restart
eth1/0/1	Multi Host	1000	Disabled	3600	60
eth1/0/2	Multi Host	1000	Disabled	3600	60
eth1/0/3	Multi Host	1000	Disabled	3600	60
eth1/0/4	Multi Host	1000	Disabled	3600	60
eth1/0/5	Multi Host	1000	Disabled	3600	60
eth1/0/6	Multi Host	1000	Disabled	3600	60
eth1/0/7	Multi Host	1000	Disabled	3600	60
eth1/0/8	Multi Host	1000	Disabled	3600	60
eth1/0/9	Multi Host	1000	Disabled	3600	60
eth1/0/10	Multi Host	1000	Disabled	3600	60
eth1/0/11	Multi Host	1000	Disabled	3600	60
eth1/0/12	Multi Host	1000	Disabled	3600	60
eth1/0/13	Multi Host	1000	Disabled	3600	60
eth1/0/14	Multi Host	1000	Disabled	3600	60
eth1/0/15	Multi Host	1000	Disabled	3600	60
eth1/0/16	Multi Host	1000	Disabled	3600	60
eth1/0/17	Multi Host	1000	Disabled	3600	60
eth1/0/18	Multi Host	1000	Disabled	3600	60
eth1/0/19	Multi Host	1000	Disabled	3600	60
eth1/0/20	Multi Host	1000	Disabled	3600	60
eth1/0/21	Multi Host	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 port(s) for the configuration here.
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are Multi Host and Multi Auth . If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. If the port is operated in the Multi Auth mode, 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.
Max Users	Enter the maximum users value used here. This value must be between 1 and 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol.
ReAuth Timer	Enter the re-authentication timer value here. The range is from 1 to 65535 seconds. By default, this value is 3600 seconds.

Parameter	Description
Restart	Enter the restart time value used here. The range is from 1 to 65535 seconds. By default, this value is 60 seconds.

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

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:

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	Specifies that the protocol is DOT1X (IEEE 802.1X).

Click the **Clear by Port** button to the clear the information based on the port selected.

Click the **Clear by MAC** button to the clear the information based on the MAC address entered.

Click the **Clear by Protocol** button to the clear the information based on the protocol selected.

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

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

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

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the Switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Packets that are destined to the CPU can be classified into three groups. These groups, otherwise known as sub-interfaces, are logical interfaces that the CPU will use to identify certain types of traffic. The three groups are **Protocol**, **Manage**, and **Route**.

Generally, the **Protocol** group should receive the highest priority when the Switch's CPU processes received packets and the **Route** group should receive the lowest priority as the Switch's CPU usually does get involved in the processing of routing packets. In the **Protocol** group, packets are protocol control packets identified by the router. In the **Manage** group, packets are destined to any router or system network management interface by means of interactive access protocols, like Telnet and SSH. In the **Route** group, packets are identified as traversing routing packets that is generally processed by the router CPU.

In the following table a list of supported protocols are displayed with their respective sub-interfaces (groups):

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
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
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:

The screenshot shows the 'Safeguard Engine Settings' window. It includes sections for 'Safeguard Engine Settings' (with dropdowns for 'Safeguard Engine State' and 'Trap State', both set to 'Disabled'), 'CPU Utilization Settings' (with input fields for 'Rising Threshold (20% ~ 100%)' at 50% and 'Falling Threshold (20% ~ 100%)' at 20%), and an 'Apply' button.

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. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

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

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:

The screenshot shows the 'CPU Protect Counters' window. It includes a section for 'Clear CPU Protect Counters' with dropdowns for 'Sub Interface' (set to 'Manage') and 'Protocol Name' (set to 'dhcp'), and buttons for 'Clear' and 'Clear All'.

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. This value must be between 0 and 1024 packets per second. Tick the No Limit option to disable the rate limit.

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

The fields that can be configured in **Sub-Interface Information** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are Manage , Protocol , and Route .

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

CPU Protect Type

This window is used to display and configure the CPU protection type settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Type**, as shown below:

The screenshot shows the 'CPU Protect Type' configuration window. In the 'Protocol Name' dropdown, 'dhcp' is selected. The 'Rate Limit (0-1024)' field contains '1 pps'. A checkbox for 'No Limit' is unchecked. An 'Apply' button is visible. Below this, the 'Protect Type Information' section shows the same 'Protocol Name' and 'Rate Limit' settings. It includes a 'Find' button and a table with two rows: 'Total' and 'Drop', both showing a value of '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. This value must be between 0 and 1024 packets per second. Tick the No Limit option to disable the rate limit.

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

The fields that can be configured in **Protect Type Information** are described below:

Parameter	Description
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:

The screenshot shows the 'Trusted Host' configuration window. In the 'Type' dropdown, 'Telnet' is selected. The 'ACL Name' field contains 'ACL'. A note states: 'Note: The first character of ACL name must be a letter.' Below this, a table titled 'Total Entries: 1' shows one entry: 'Type' is 'Telnet' and 'ACL Name' is 'ACL'. An 'Delete' button is visible.

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:

The screenshot shows the 'Traffic Segmentation Settings' window. At the top, there are four dropdown menus for 'From Port' (set to 'eth1/0/1'), 'To Port' (set to 'eth1/0/1'), 'From Forward Port' (set to 'eth1/0/1'), and 'To Forward Port' (set to 'eth1/0/1'). Below these are two buttons: 'Add' and 'Delete'. A table below the controls lists a single entry: 'Port' (eth1/0/5) and 'Forwarding Domain' (eth1/0/6-1/0/8).

Port	Forwarding Domain
eth1/0/5	eth1/0/6-1/0/8

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:

The screenshot shows the 'Storm Control Settings' configuration page. It includes sections for 'Storm Control Trap Settings' (Trap State set to 'None'), 'Storm Control Polling Settings' (Polling Interval at 5 seconds, Shutdown Retries at 3 times, Infinite option unchecked), and 'Storm Control Port Settings' (From Port eth1/0/1, To Port eth1/0/1, Type Broadcast, Action None, Level Type PPS, PPS Rise and PPS Low both set to 0). Below these are tables for total entries and specific port configurations.

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 - Specifies that no traps will be sent. Storm Occur - Specifies that a trap notification is sent when a storm event is detected. Storm Clear - Specifies that a trap notification is sent when a storm event is cleared. Both - Specifies that a trap notification is sent when a storm event is detected and/or cleared.

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

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Polling Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the Infinite option to disable this feature.

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

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

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

Parameter	Description
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. This value must be between 0 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 0 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

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

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.

Storm Control Port Settings						
From Port	To Port	Type	Action	Level Type	KBPS Rise (0-2147483647)	KBPS Low (0-2147483647)
eth1/0/1	eth1/0/1	Broadcast	None	Kbps	*16Kbps	*16Kbps
Apply						

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. This value must be between 0 and 2147483647 Kbps.
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

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

After selecting the **Level** option as the **Level Type**, the following parameters are available.

Storm Control Port Settings						
From Port	To Port	Type	Action	Level Type	Level Rise (0-100)	Level Low (0-100)
eth1/0/1	eth1/0/1	Broadcast	None	Level	%	%
Apply						

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. This value must be between 0% and 100%.
Level Low	Enter the low level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%. If the low level is not specified, the default value is 80% of the specified risen level.

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

DoS Attack Prevention Settings

This window is used to display and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types that can be detected by most Switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack:** This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets that contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets that contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets that contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets that contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size which is 65535 bytes). The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **Smurf Attack:** Smurf is a Distributed Denial of Service (DDoS) attack that enables and executes the DDoS.Smurf malware. Smurf attacks are in a way similar to ping floods, as both are carried out by sending a lot of ICMP Echo request packets. Smurf, however, is an amplification attack vector that boosts its damage potential by exploiting the characteristics of broadcast networks.
- **TCP Flag SYN RST** - The TCP SYN/RESET flood is a DDoS attack that exploits part of the normal TCP three-way handshake to consume more resources on targeted nodes to render them unresponsive. TCP connection requests are sent faster than the targeted machine can process, resulting in network traffic saturation.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

The screenshot displays the 'DoS Attack Prevention Settings' configuration page. At the top, under 'SNMP Server Enable Traps DoS Settings', the 'Trap State' is set to 'Disabled'. An 'Apply' button is located at the bottom right. Below this, the 'DoS Attack Prevention Settings' section includes 'DoS Type Selection' with checkboxes for Land Attack, TCP SYN-FIN, Smurf Attack, Blat Attack, TCP SYN SrcPort Less 1024, TCP Null, Ping of Death Attack, TCP Flag SYNrst, TCP Xmas, and TCP Tiny Fragment Attack. Under 'DoS Settings', the 'State' is set to 'Disabled' and the 'Action' is set to 'Drop'. A large table lists specific DoS types, their current state (all are 'Disabled'), and the action taken ('Drop') if detected.

DoS Type	State	Action
Land Attack	Disabled	Drop
Blat Attack	Disabled	Drop
Smurf 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 Flag SYNrst	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. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

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

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

SSH Global Settings	
IP SSH Server State	Disabled
IP SSH Service Port (1-65535)	22
SSH Server Mode	V2
Authentication Timeout (30-600)	120 sec
Authentication Retries (1-32)	3 times
Apply	

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. This value must be between 1 and 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

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

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:

The screenshot shows the 'Host Key' configuration page. Under 'Host Key Management', 'Crypto Key Type' is set to 'RSA' and 'Key Modulus' is set to '768 bit'. There are 'Generate' and 'Delete' buttons. Under 'Host Key', it shows 'Crypto Key Type' as 'RSA', 'Key pair was generated at' as '02:03:01, 2000-01-01', 'Key Size' as '768', and 'Key Data' as a long string of characters.

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 Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.
Key Modulus	Select the key modulus value here. Options to choose from are 360, 512, 768, 1024, and 2048 bit.

Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

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

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (RSA) key type and the Digital Signature Algorithm (DSA) key type.

After clicking the **Generate** button, the following window will appear:

The screenshot shows the 'Host Key Management' window with a progress bar indicating 'Generating...'. Below the progress bar, there are 'Result' and 'Generating...' buttons.

Figure 9-70 Host Key (Generating) Window

After the key was successfully generated, the following window will appear.

The screenshot shows the 'Host Key Management' window with a message 'Success.' displayed below the progress bar.

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:

SSH Server Connection					
SSH Table					
Total Entries: 1					
SID	Version	Cipher	User ID	Client IP Address	
0	V2	aes256-cbc/hmac-sha1...	user	10.90.90.14	

Figure 9-72 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:

SSH User Settings					
SSH User Settings					
User Name	32 chars	Authentication Method	Password		
Key File	779 chars	Host Name	255 chars		
<input checked="" type="radio"/> IPv4 Address	.	<input type="radio"/> IPv6 Address	2013::1		<input type="button" value="Apply"/>
Total Entries: 1					
User Name	Authentication Method	Key File	Host Name	Host IP	
user	Password				
<input type="button" value="1/1"/> <input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">"/> <input type="button" value="Go"/>					

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 that 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:

The screenshot shows the 'SSL Global Settings' window with the following sections:

- SSL Global Settings:** Contains 'SSL Status' (radio buttons for Enabled or Disabled, currently Disabled) and 'Service Policy' (text input field set to '32 chars'). An 'Apply' button is located to the right.
- Import File:** Contains 'File Select' (radio buttons for Certificate or Private Key, currently Certificate selected), a 'Browse...' button, and a note '(The file name range is 1-32 chars.)'. Below it is 'Destination File Name' (text input field set to '32 chars') and another 'Apply' button.
- SSL Self-signed Certificate:** Contains 'Self-signed Certificate' and a 'Generate' button.

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:

The screenshot shows the 'Crypto PKI Trustpoint' configuration window. At the top, there are input fields for 'Trustpoint' (32 chars) and buttons for 'Apply' and 'Find'. Below this, there are fields for 'File System Path' (e.g.:c:/cacert) and 'TFTP Server Path' (e.g.:ip/name), along with 'Password' (64 chars) and 'Type' (Local). A table titled 'Total Entries: 1' lists one entry: 'trustpoint' under 'Trustpoint Name', with 'Primary' checked. There are buttons for 'Delete' and 'Apply' at the bottom right of the table.

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.
Primary	Select the Primary checkbox to specify which entry is the primary trustpoint (when multiple entries exist). After the checkbox is selected, a 'Success' confirmation window will appear.

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

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

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

SSL Service Policy

This window is used to display and configure the SSL service policy settings.

To view the following window, click **Security > SSL > SSL Service Policy**, as shown below:

SSL Service Policy					
SSL Service Policy					
Policy Name	<input type="text" value="32 chars"/> <input type="button" value="Apply"/> <input type="button" value="Find"/>				
Policy Name	<input type="text" value="32 chars"/> <ul style="list-style-type: none"> <input type="checkbox"/> TLS 1.0 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.2 				
Version	<input type="text" value="600 sec"/>				
Session Cache Timeout (60-86400)	<input type="text" value="600 sec"/>				
Secure Trustpoint	<input type="text" value="32 chars"/> <ul style="list-style-type: none"> <input type="checkbox"/> DHE_DSS_WITH_3DES_EDE_CBC_SHA <input type="checkbox"/> RSA_WITH_3DES_EDE_CBC_SHA <input type="checkbox"/> RSA_WITH_RC4_128_SHA <input type="checkbox"/> RSA_EXPORT_WITH_RC4_40_MD5 <input type="checkbox"/> RSA_WITH_RC4_128_MD5 <input type="checkbox"/> RSA_WITH_AES_128_CBC_SHA <input type="checkbox"/> RSA_WITH_AES_256_CBC_SHA <input type="checkbox"/> RSA_WITH_AES_128_CBC_SHA256 <input type="checkbox"/> RSA_WITH_AES_256_CBC_SHA256 <input type="checkbox"/> DHE_DSS_WITH_AES_256_CBC_SHA <input type="checkbox"/> DHE_RSA_WITH_AES_256_CBC_SHA 				
Cipher Suites	<input type="button" value="Apply"/>				
Total Entries: 1					
Policy Name	Version	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint	
Policy	TLS 1.2	DHE_RSA_WITH_AES_256...	600		<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. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust point name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

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

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

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

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

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-based configuration interface for 'Network Protocol Port Protect Settings'. At the top left, it says 'Network Protocol Port Protect Settings'. Below that, there are two main sections: 'TCP Port Protect State' and 'UDP Port Protect State'. Each section has two radio buttons: 'Enabled' (selected) and 'Disabled'. At the bottom right of the window is a small 'Apply' button.

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

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

Cable Diagnostics						
Cable Diagnostics						
From Port	To Port					
eth1/0/1	eth1/0/1					<input type="button" value="Test"/>
<input type="button" value="Clear All"/>						
Port	Type	Link Status	Test Result	Cable Length (M)		
eth1/0/1	1000BASE-T	Link Up	(OK)	4	<input type="button" value="Clear"/>	
eth1/0/2	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/3	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/4	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/5	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/6	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/7	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/8	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/9	1000BASE-T	Link Down	-	-	<input type="button" value="Clear"/>	
eth1/0/10	1000BASE-T	Link Down	-	-	<input type="button" value="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: For this test, the supported cable length is from 10 to 130 meters and wire speed is at 100/1000 Mbps. Testing at 10 Mbps is not supported.



NOTE: The distance deviation of cable length detection on 100/1000 Mbps ports are:

- ± 25 meters on cables that are 40 meters and shorter.
- ± 20 meters on cables that are between 40 and 100 meters.



NOTE: The distance deviation on a link-down detection is:

- ± 15 meters on cables that are 30 meters and shorter.
- ± 7 meters on cables that are between 30 and 110 meters.
- ± 15 meters on cables that are between 110 and 130 meters.



NOTE: For more accurate test results, use the TIA/EIA-568B pin assignment on the RJ45 connectors.

Fault messages:

- **Open** - This pair is left open.
- **Short** - Two lines of this pair is shorted.
- **CrossTalk** - Lines of this pair is short with lines in other pairs.
- **Unknown** - The diagnosis does not obtain the cable status, please try again.
- **NA** - No cable was found, maybe it's because cable is out of diagnosis specification or the quality is too bad.

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:

Port Utilization				
Port Utilization				
From Port	eth1/0/1	To Port	eth1/0/1	
eth1/0/1	1		1	1
eth1/0/2	0		0	0
eth1/0/3	0		0	0
eth1/0/4	0		0	0
eth1/0/5	0		0	0
eth1/0/6	0		0	0
eth1/0/7	0		0	0
eth1/0/8	0		0	0
eth1/0/9	0		0	0
eth1/0/10	0		0	0

Figure 11-1 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								
Port		RX		TX				
Port	Rate		Total		Rate		Total	
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets
eth1/0/1	1116	7	3136527	19435	1619	4	5061348	11292
eth1/0/2	0	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0	0	0
eth1/0/9	0	0	0	0	0	0	0	0
eth1/0/10	0	0	0	0	0	0	0	0

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 more detailed statistics information on the specified port.

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

The screenshot shows a table with the following data:

eth1/0/1	
RX rate	142 bytes/sec
TX rate	78 bytes/sec
RX bytes	3169560
TX bytes	5108854
RX rate	2 packets/sec
TX rate	1 packets/sec
RX packets	19684
TX packets	11466
RX multicast	1106
RX broadcast	3726
RX CRC error	0
RX underrun	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 table with the following data:

Interface Counters									
Type	From Port		To Port						
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	Show Errors
eth1/0/1	3188991	14972	1107	3740	5137990	11291	0	268	Show Errors
eth1/0/2	0	0	0	0	0	0	0	0	Show Errors
eth1/0/3	0	0	0	0	0	0	0	0	Show Errors
eth1/0/4	0	0	0	0	0	0	0	0	Show Errors
eth1/0/5	0	0	0	0	0	0	0	0	Show Errors
eth1/0/6	0	0	0	0	0	0	0	0	Show Errors
eth1/0/7	0	0	0	0	0	0	0	0	Show Errors
eth1/0/8	0	0	0	0	0	0	0	0	Show Errors
eth1/0/9	0	0	0	0	0	0	0	0	Show Errors
eth1/0/10	0	0	0	0	0	0	0	0	Show Errors

Figure 11-4 Interface Counters (Port) Window

The fields that can be configured are described below:

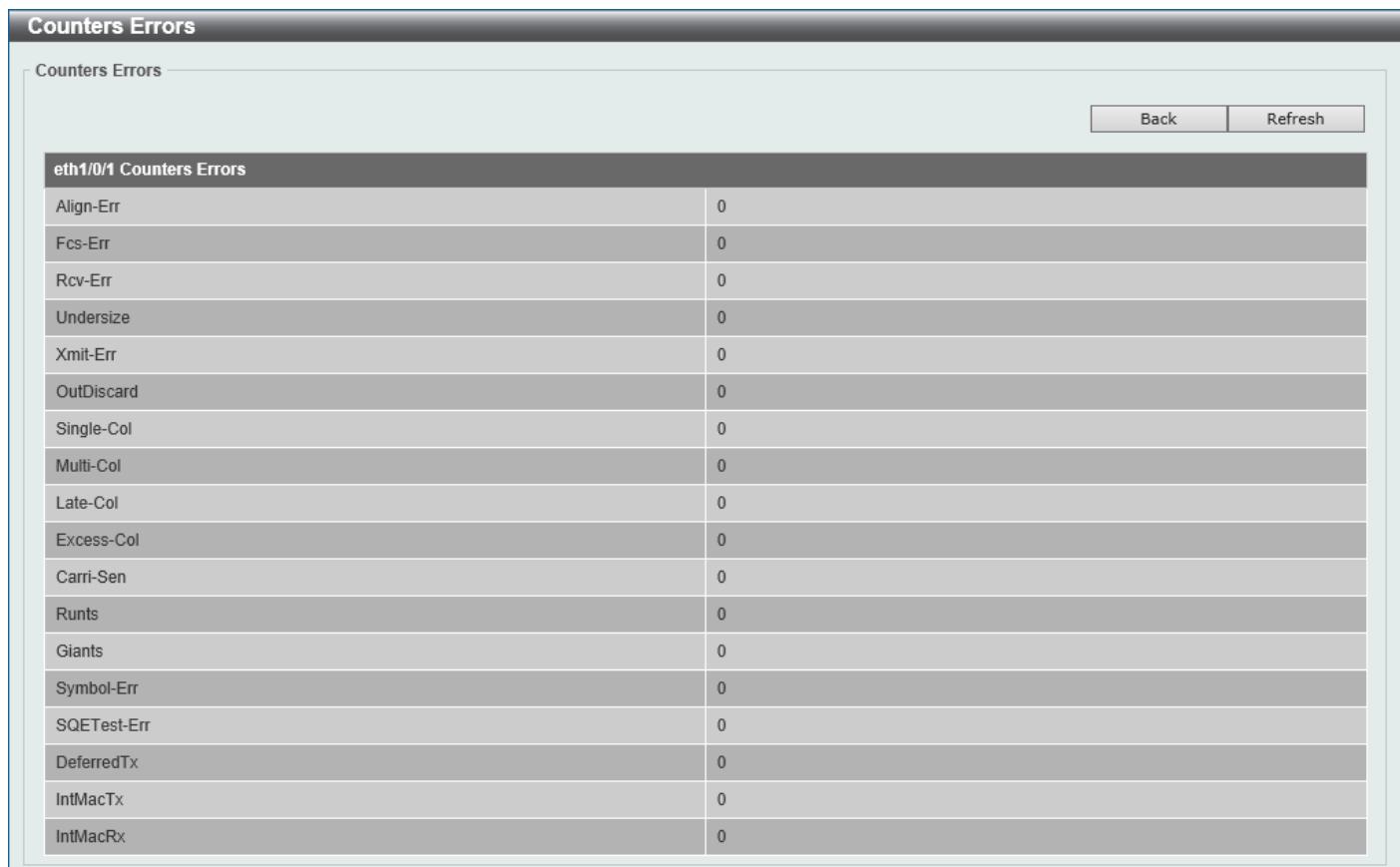
Parameter	Description
Type	Specifies that the type is Port .
From Port - To Port	Select the range of ports that will be used in this display here.

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 more detailed error information on the specified port.

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



The screenshot shows a web-based management interface titled "Counters Errors". On the left, there is a navigation tree with "Counters Errors" selected. At the top right are "Back" and "Refresh" buttons. The main area displays a table for "eth1/0/1 Counters Errors" with 17 rows, each containing an error type and its count (all 0). The table has a dark header row.

eth1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Underrun	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Multi-Col	0
Late-Col	0
Excess-Col	0
Carri-Sen	0
Runts	0
Giants	0
Symbol-Err	0
SQETest-Err	0
DeferredTx	0
IntMacTx	0
IntMacRx	0

Figure 11-5 Interface Counters (Show Errors) Window

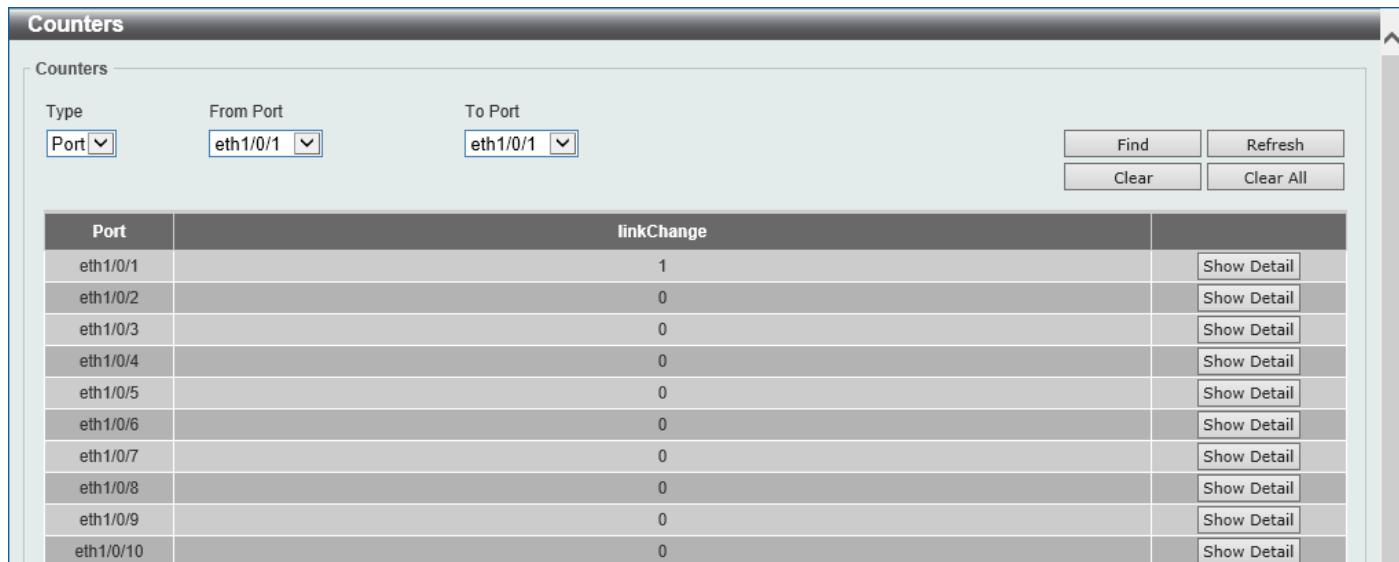
Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Counters

This window is used to view and clear counter information.

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:



The screenshot shows a table titled 'Counters' with the following data:

Port	linkChange	
eth1/0/1	1	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	0	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	Specifies that the type 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:

The screenshot shows a web-based management interface for a DGS-1250 Series Gigabit Ethernet Smart Managed Switch. The main title is "Port Counters Detail". Below it, a sub-section title is "Port Counters Detail". At the top right are two buttons: "Back" and "Refresh". The main content is a table titled "eth1/0/1 Counters" containing 24 rows of network statistics. The table has alternating row colors. The columns represent various packet types and their counts.

eth1/0/1 Counters	
rxHCTotalPkts	20351
txHCTotalPkts	11899
rxHCUnicastPkts	15386
txHCUnicastPkts	11626
rxHCMulticastPkts	1156
txHCMulticastPkts	0
rxHCBroadcastPkts	3809
txHCBroadcastPkts	273
rxHOctets	3272911
txHOctets	5240483
rxHCPkt64Octets	13408
rxHCPkt65to127Octets	2400
rxHCPkt128to255Octets	282
rxHCPkt256to511Octets	2278
rxHCPkt512to1023Octets	1983
rxHCPkt1024to1518Octets	0
rxHCPkt1519toMAXOctets	0
txHCPkt64Octets	370
txHCPkt65to127Octets	2778
txHCPkt128to255Octets	1845
txHCPkt256to511Octets	4499

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:

The screenshot shows the 'Mirror Settings' window. At the top left is a tree menu with 'Mirror Settings' selected. Below it is a table for configuring a mirror session. The 'Session Number' dropdown is set to '1'. Under 'Destination', the 'Port' checkbox is checked, and the dropdown shows 'eth1/0/1'. Under 'Source', the 'Port' checkbox is checked, and the dropdown shows 'eth1/0/1'. To the right of these dropdowns are 'From Port' and 'To Port' dropdowns both set to 'eth1/0/1', and a 'Frame Type' dropdown set to 'Both'. At the bottom right of the configuration area are 'Add' and 'Delete' buttons. Below the configuration area is a table titled 'Mirror Session Table' with one row. The row contains 'Session Number' (1), 'Session Type' (Local Session), and a 'Show Detail' button.

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.
Destination	Tick the checkbox and select the destination port number here.
Source	Tick the checkbox and select the source for this port mirror entry. In the first drop-down menu, select the source type option. Options to choose from are: <ul style="list-style-type: none"> Port - After selecting this option, select the From Port and To Port numbers from the drop-down menus. Lastly select the Frame Type option from the last drop-down menu. Options to choose from are: <ul style="list-style-type: none"> Both - Specifies that traffic in both the incoming and outgoing directions will be mirrored. RX - Specifies that traffic in only the incoming direction will be mirrored. TX - Specifies that traffic in only the outgoing direction will be mirrored.

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

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	eth1/0/11-eth1/0/20
RX Port	
TX Port	
Flow Based Source	
Destination Port	Ethernet1/0/10
Back	

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 Descr/ID	Current/Threshold Range
Central Temperature /1	35C/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**, 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 power saving function here. When enabled, a port that has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Length Detection Power Saving	Select to enable or disable the cable length detection power saving function here. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power.
Scheduled Port-shutdown Power Saving	Select to enable or disable the scheduled port-shutdown power saving function here.
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 the scheduled dimming of LEDs to save power function here.
Administrative Dim-LED	Select this option to enable or disable the port LED function.

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

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

Parameter	Description
Type	Select the power saving type here. Options to choose from are: <ul style="list-style-type: none"> • Dim-LED - Specifies to add or delete a time range profile for the dim LED schedule. When the schedule is up, all the port LEDs are turned off.

Parameter	Description
	<ul style="list-style-type: none"> Hibernation - Specifies to add or delete a time range profile for the system hibernation schedule. When the system enters the hibernation mode, the Switch goes into a low powered state and idle. It shuts down all the ports and LEDs, all network functions is disabled, and only the console connection works through the RS232 port. If the Switch is an endpoint PSE, power is not provided through the ports.
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.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

The screenshot shows the 'Power Saving' configuration interface. At the top, there are two tabs: 'Power Saving Global Settings' (disabled) and 'Power Saving Shutdown Settings' (selected). Below the tabs are three dropdown menus: 'From Port' (set to 'eth1/0/1'), 'To Port' (set to 'eth1/0/1'), and 'Time Range' (set to '32 chars'). To the right of these is an 'Apply' button. Below these controls is a table with two columns: 'Port' and 'Time Range'. The table lists ten ports from 'eth1/0/1' to 'eth1/0/10'. Each row has a 'Delete' button in the last column. The entire window has a dark header bar and a vertical scroll bar on the right side.

Port	Time Range	
eth1/0/1		Delete
eth1/0/2		Delete
eth1/0/3		Delete
eth1/0/4		Delete
eth1/0/5		Delete
eth1/0/6		Delete
eth1/0/7		Delete
eth1/0/8		Delete
eth1/0/9		Delete
eth1/0/10		Delete

Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Time Range	Enter the name of the time range to associate with the ports.

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

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

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:

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

Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
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 window titled "Save Configuration". Inside, there is a single input field labeled "File Path" containing the value "startup-config". To the right of this field is a dropdown menu icon. In the bottom right corner of the window is a button labeled "Apply".

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.

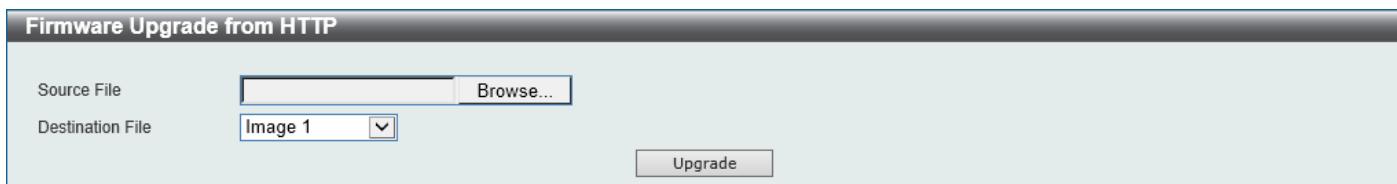
Tools

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 window titled "Firmware Upgrade from HTTP". It contains two main input fields: "Source File" with a "Browse..." button to its right, and "Destination File" with a dropdown menu showing "Image 1". Below these fields is a large "Upgrade" button.

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:

Firmware Upgrade from TFTP	
TFTP Server IP	<input type="text"/> <input checked="" type="radio"/> IPv4 <input type="text"/> <input type="radio"/> IPv6
Source File	<input type="text"/> 64 chars
Destination File	<input type="text"/> Image 1
Upgrade	

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:

Firmware Backup to HTTP	
Source File	<input type="text"/> Image 1
Backup	

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:

The screenshot shows the 'Firmware Backup to TFTP' configuration window. It includes fields for 'TFTP Server IP' (with IPv4 selected), 'Source File' (set to 'Image 1'), and 'Destination File' (set to '64 chars'). A 'Backup' button is at the bottom right.

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:

The screenshot shows the 'Configuration Restore from HTTP' configuration window. It includes fields for 'Source File' (with a 'Browse...' button), 'Destination File' (set to 'Configuration 1'), and 'Replace' (unchecked). A 'Restore' button is at the bottom right.

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:

Configuration Restore from TFTP	
TFTP Server IP	<input type="text"/> . . . <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source File	<input type="text"/> 64 chars
Destination File	<input type="button" value="Configuration 1"/> <input type="checkbox"/> running-config <input type="checkbox"/> startup-config
Replace	<input type="checkbox"/>
<input type="button" value="Restore"/>	

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:

Certificate & Key Restore from HTTP	
Source File	<input type="text"/> Browse...
Destination File	64 chars
Restore	

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:

Certificate & Key Restore from TFTP	
TFTP Server IP	<input type="text"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source File	64 chars
Destination File	64 chars
Restore	

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 contains two main sections: 'IPv4 Ping' and 'IPv6 Ping'. Both sections have the following fields:

- Target IP/Domain Name:** A text input field. In the IPv4 section, it is set to '192.168.1.1'. In the IPv6 section, it is set to '2233::1'.
- 255 chars:** A text input field for specifying the number of characters for the ping message, with a default value of '255 chars'.
- Ping Times (1-255):** A numeric input field for the number of times to ping. In both sections, it is set to '1'.
- Infinite:** A checked checkbox that, when selected, keeps sending ICMP Echo packets until the program is stopped.
- Timeout (1-99):** A numeric input field for the timeout period in seconds. In both sections, it is set to '1 sec'.
- Source IP Address:** A text input field for the source IP address, which is left empty in both sections.
- Start:** A large blue 'Start' button 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. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
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. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMPv6 Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
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:

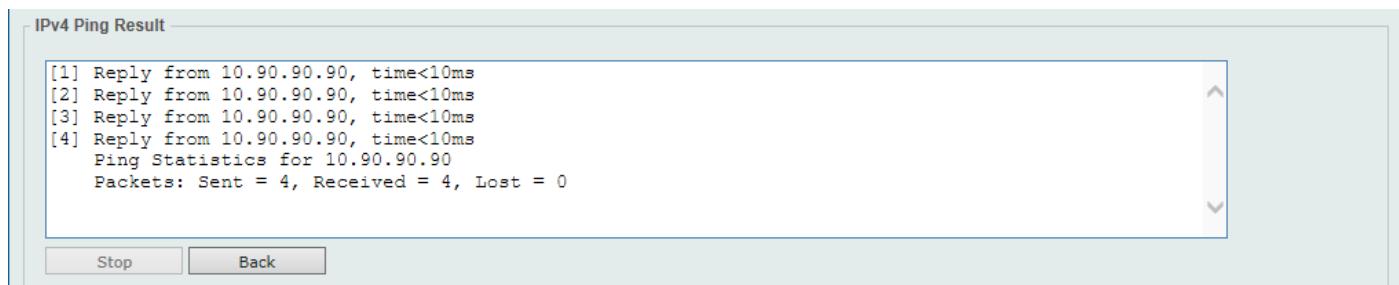


Figure 13-17 Ping (Start) Window

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:

Language Management		
Language File	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Apply"/>		

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:

Reset

Reset

- The Switch will reset to its factory default settings and then save, reboot.
- The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot.

Apply

Figure 13-19 Reset Window

Select one of the following options:

- The Switch will reset to its factory default settings and then save, reboot.
- The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot.

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

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

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

Reboot System

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 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.

Reboot System

Saving and rebooting system, please wait...

25%

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 5.

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.

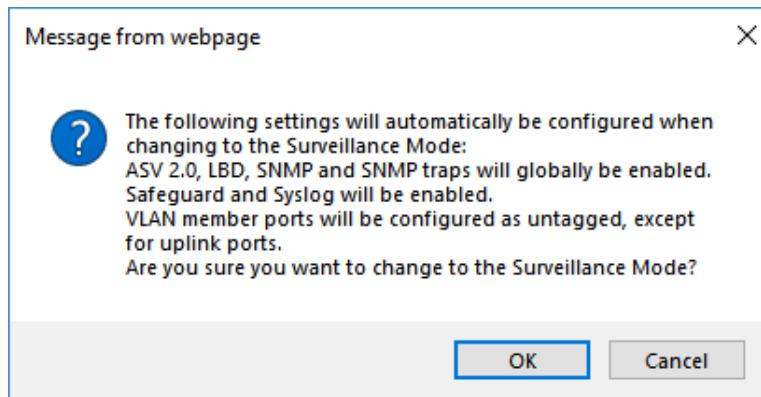


Figure 13-22 Surveillance Mode Confirmation Message

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.

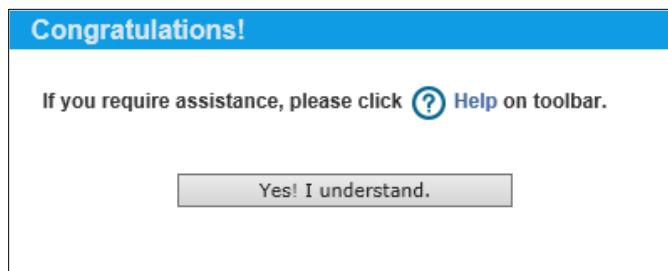


Figure 13-23 Surveillance Mode 'Congratulations' Message

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

PoE Information

PoE Scheduling

Management

Time

Surveillance Settings

Surveillance Log

Health Diagnostic

Toolbar

Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device (such as the number of devices, device type, IP address, power consumption, link speed, and errors).

To return to the Surveillance Overview window after viewing other windows, click the **DGS-1250-28XMP** link.

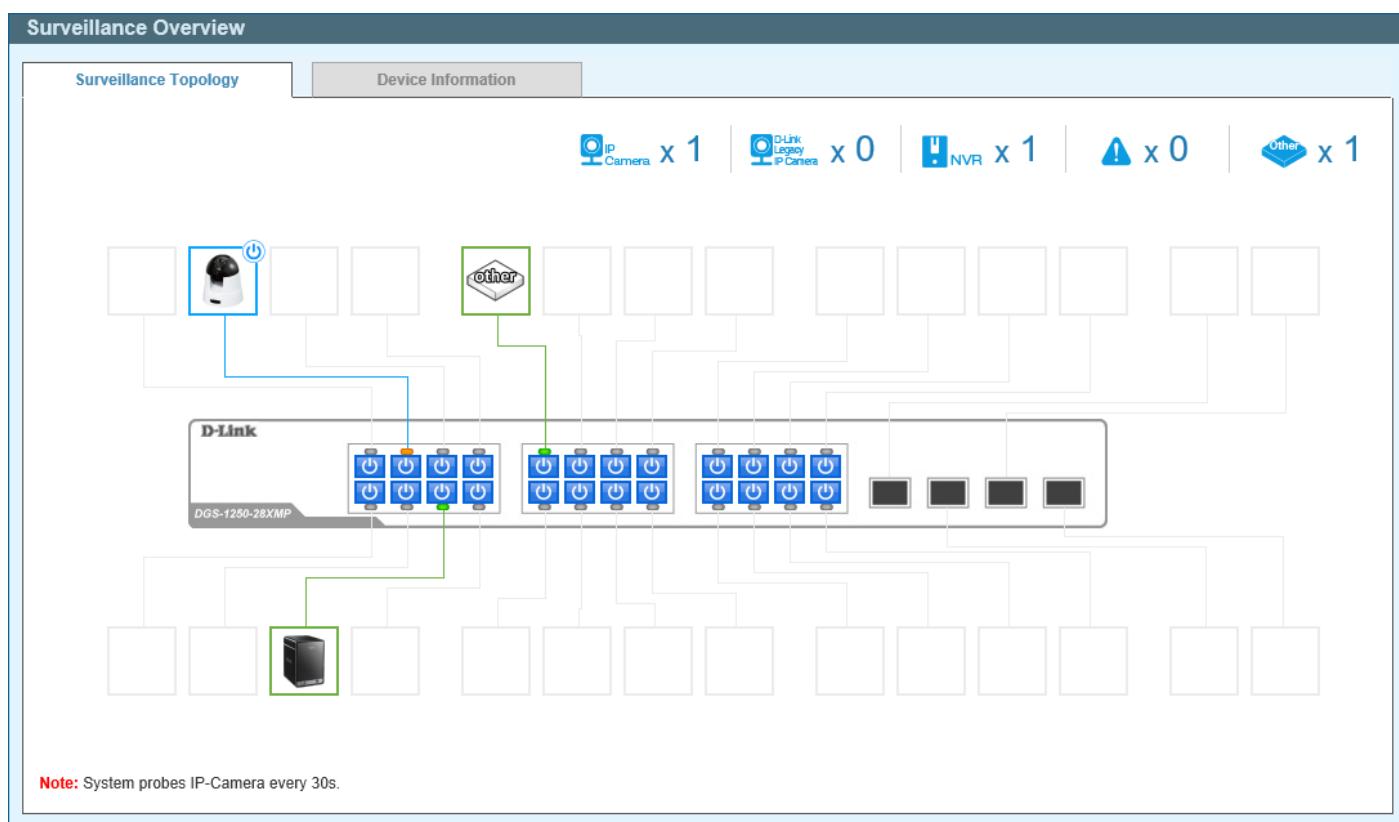


Figure 14-1 Surveillance Overview Window

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.
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.
	This displays the device connected to the Ethernet port on the Switch. The blue border around the image indicates that the device is a PoE device and is receiving power from the Switch using PoE. The PD Alive function can be used on this device.
	Click this icon to disable PoE on the port.
	Click this icon to enable PoE on the port.

After clicking the icon, the following window will appear:

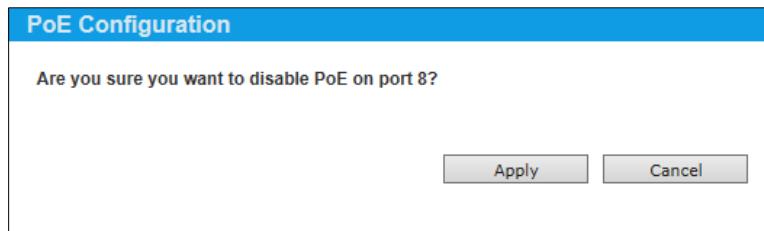


Figure 14-2 PoE Configuration (To Disable) Window

After clicking the , the following window will appear:

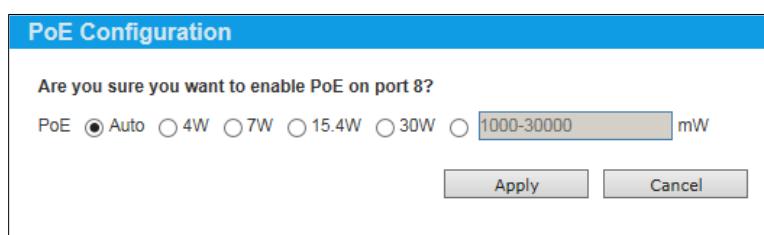


Figure 14-2 PoE Configuration (To Enable) Window

The fields that can be configured are described below:

Parameter	Description
PoE	Select the maximum power that will be supplied on the PoE port. Options to choose from are Auto , 4W , 7W , 15.4W , 30W , and a configurable value from 1000 mW to 30000 mW. The unit is either in watt or milliwatt.

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

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

After hovering (with the mouse pointer) over the network device icon, the following additional information will be displayed:

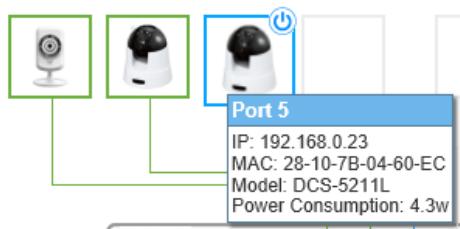


Figure 14-2 Additional Device Information

After clicking (left-click) the network device icon, the following window will

appear.

Figure 14-2 PD Alive Configuration Window

The fields that can be configured are described below:

Parameter	Description
PD Alive State	Select to enable or disable the PD Alive function here.
PD IP Address	Enter the IP address of the PD here.
Action	Select the action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> Reset - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

After clicking **Ping Test** button, the following window will appear.

Figure 14-2 PD Alive Configuration Window (Ping Result)

The **Ping Result** will be displayed.



NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.



NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.

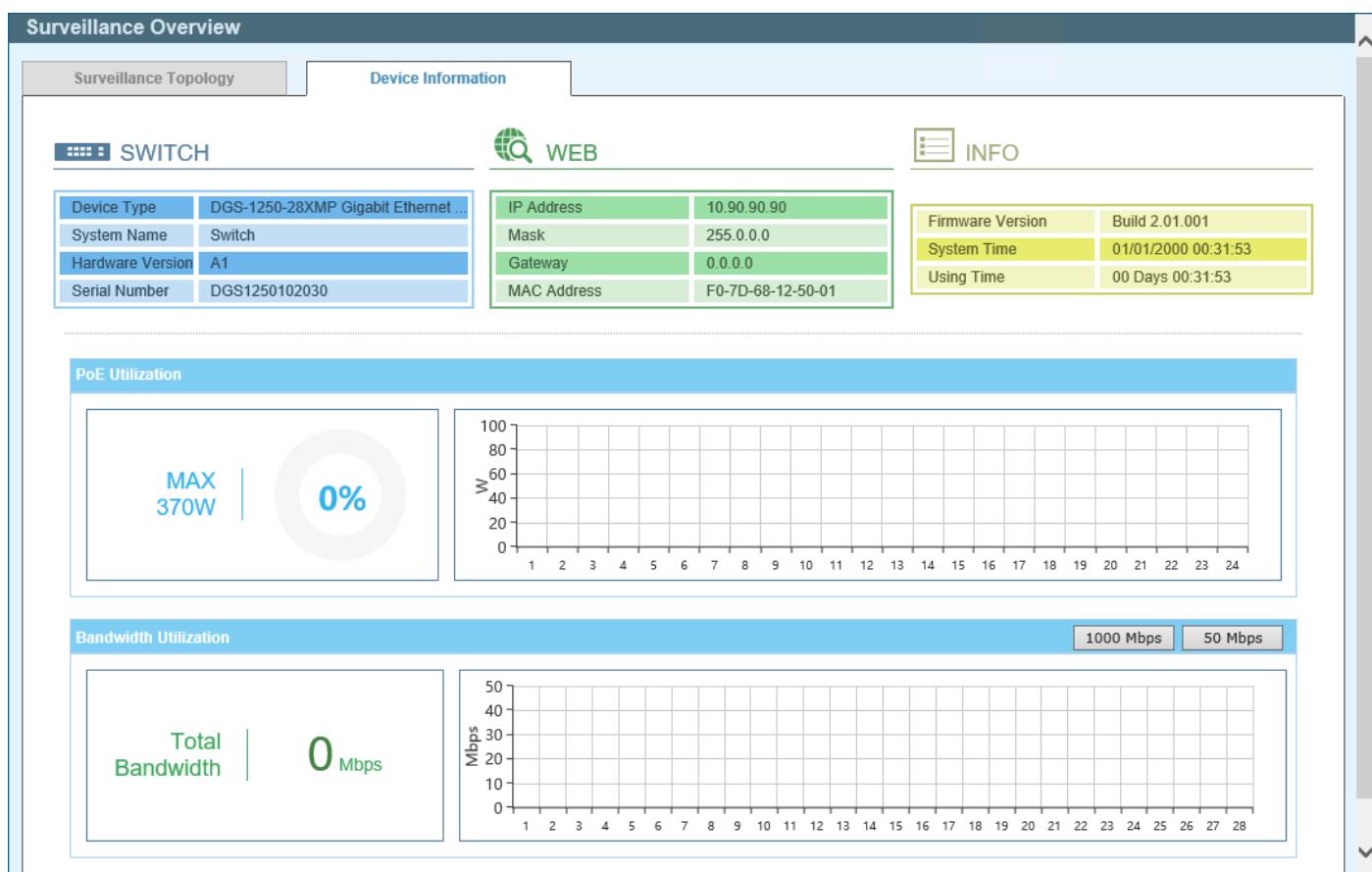


Figure 14-6 Device Information Window

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:

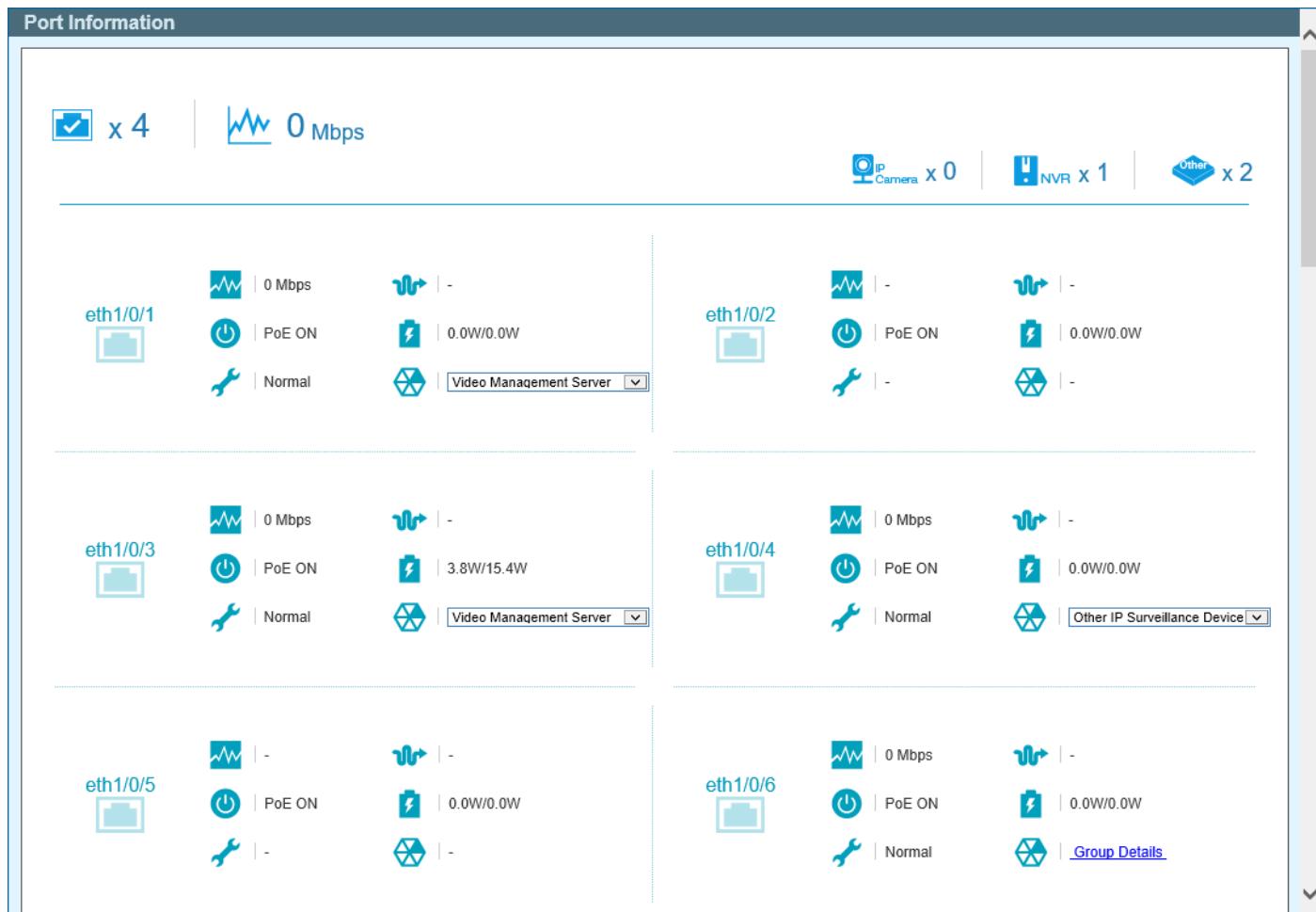


Figure 14-7 Port Information Window

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.

Icon	Description
	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.
	This displays the PoE status on the port.
	This displays the power consumption and power class of the PD connected to the Ethernet port.
Normal	This displays the Loopback Detection status on the Ethernet port.
Loop	<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.
	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.
	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.

The screenshot shows a web-based interface for managing a network port. At the top, a dark header bar displays "Port Information / Group Details". Below this, the main content area has a light blue header " / Group Details". On the left, there's a small blue folder icon followed by "Port eth1/0/1". To the right of the port number is a "Back" button with a left arrow icon. Below the port number, there are several status indicators: a hexagonal icon with "0", an IP-camera icon with "IP-Camera", a speech bubble icon with "DCS-942LB1 / DCS-942LB1", and a magnifying glass icon with "192.168.0.21(B0-C5-54-26-B7-A3)". To the far right, there's another speech bubble icon with "-".

Figure 14-8 Port Information / Group Details Window

The following icons are available in this window and are described below:

Icon	Description
	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
x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
0Mbps	The displays the total amount of inbound bandwidth that is being used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
4.4w / 15.4W	The displays the total power consumption and power class (of PDs) used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
DCS-942LB1 DCS-942LB1	This displays a photo, manufacturer, and model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the IP camera.
4.4W /15.4W	This displays the power consumption and power class of the IP camera.
192.168.0.21 (B0-C5-54-26-B7-A3)	This displays the IP address and MAC address of the IP camera.
DCS-942LB1	This displays the description for the IP camera. Click the icon to modify the description.

Icon	Description
<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
x 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
0 Mbps	The displays the total amount of inbound bandwidth that is being used by the NVRs connected to the Ethernet ports on the Switch.
eth1/0/2	This displays the Ethernet port number on the Switch.
	This displays a generic photo of the NVR connected to the port.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the NVR.
192.168.0.202 (B8-70-F4-B0-42-A1)	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.
<input type="text"/>	Enter the description for the NVR here. Click the icon to apply the modified description.

Icon	Description
Group 1	This displays the group ID of the NVR.
x 3	This displays the number of ONVIF IP cameras managed by this NVR.
eth1/0/5 (192.168.0.23) (28-10-7B-04-60-EC)	This displays information about the ONVIF IP camera that is managed by this NVR.

PoE Information

This window is used to display Power-over-Ethernet (PoE) information.

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

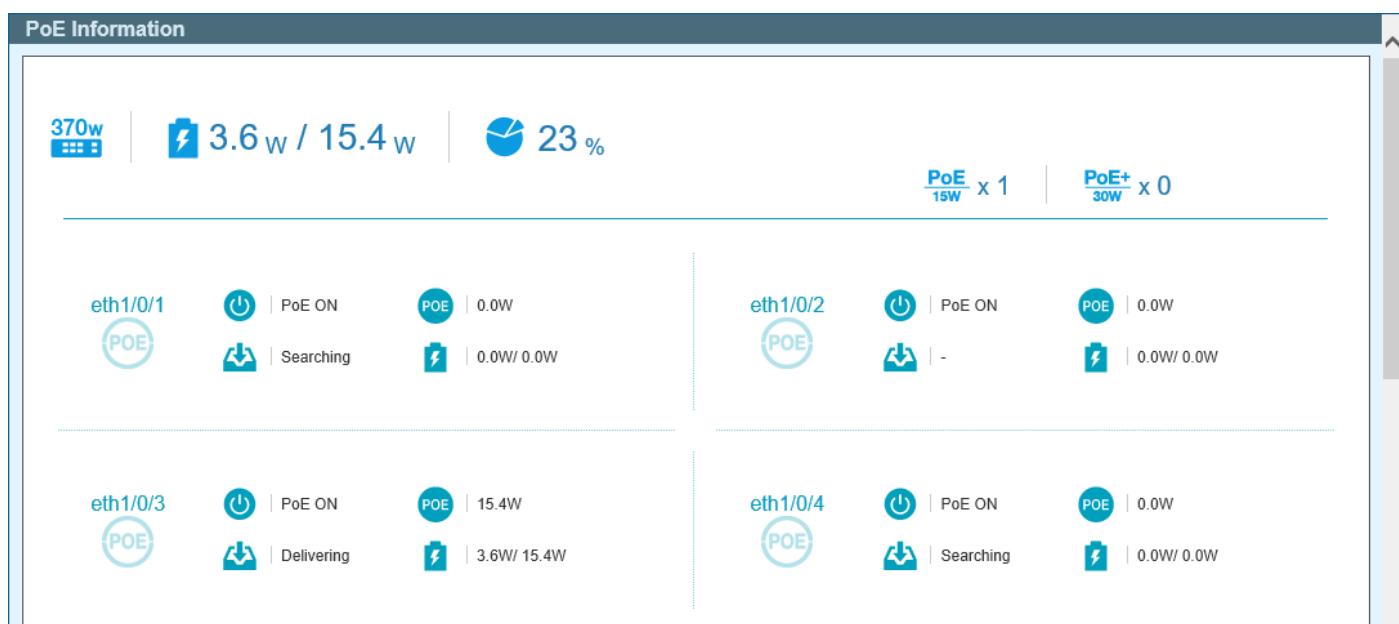


Figure 14-11 PoE Information Window

The following icons are available in this window and are described below:

Icon	Description
	This displays the maximum PoE budget that can be provided by the Switch.
	This displays the total PoE consumption and power class of PDs connected to the Switch.
	This displays the current PoE utilization (in percentage).
	This displays the number of PoE devices connected to the Switch that is using 15 Watts of power per port.
	This displays the number of PoE devices connected to the Switch that is using 30 Watts of power per port.
	This displays the Ethernet port number on the Switch.
	This displays the PoE state on the port. This can be either PoE ON or PoE OFF .

Icon	Description
15.4W	This displays the maximum PoE budget available on this port.
Delivering Power Denied	This displays the current PoE status on the port. This status can be one of the following: -, Searching , Delivering , or Power Denied . When the Power Denied message is displayed, click on the link to redirect the Health Diagnostic window for more information.
3.5W/ 15.4W	This displays the PoE consumption and power class of the PD connected to the port.

PoE Scheduling

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

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

The screenshot shows the PoE Scheduling configuration interface. It includes two main sections: "Time Range" and "PoE Configuration".

Time Range: This section allows you to define a time range schedule. It includes fields for "Range Name" (with a 8 chars input field and a "Daily" checkbox), "From: Time (Week/HH)" (with dropdowns for day and hour), "To: Time (Week/HH)" (with dropdowns for day and hour), and an "Apply" button. Below these are two tables:

Range Name	Start		End	
	Week	Time	Week	Time

Range Name	Start	End

PoE Configuration: This section lists ports and their corresponding time ranges. It includes fields for "From Port" (eth1/0/1) and "To Port" (eth1/0/1), and a "Time Range" dropdown set to "Please Select". An "Apply" button is also present. A table lists the port assignments:

Port	Time Range
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	

Figure 14-12 PoE Scheduling Window

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

Parameter	Description
Range Name	Enter the name of the time range schedule here. Tick the Daily option to use this schedule for every day of the week.
From: Time (Week/HH)	Select the starting day and hour in the time range schedule here. Alternatively, click the icon to open a calendar for easy day and hour selection.
To: Time (Week/HH)	Select the ending day and hour in the time range schedule here. The schedule will end at the end of the selected hour. Alternatively, click the icon to open a calendar for easy day and hour selection.

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.

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

Parameter	Description
From Port / To Port	Select the port range that will be used here.
Time Range	Select the time range schedule that will be applied to the selected port(s) here.

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

Click the **Delete** button to remove the time range schedule from the specified port.

After clicking the  icon, the following window will appear:



Figure 14-13 Day and Hour Window

Click the **OK** button to use the Day and Hour selected.

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:

File System					
Path: C: <input type="text" value="C:"/> <input type="button" value="Go"/> <input type="button" value="Copy"/> <input type="button" value="Boot File"/>					
Drive	Media Type	Size (MB)	File System Type	Label	
C:	Flash	44	swfs		

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.

The screenshot shows a 'File System' interface with the path 'C:/'. The table lists the following files:

Index	Attr	Size (byte)	Update Time	Name	
1	-rw	122858	Jan 01 2000 00:45:43	tech-support.log	Delete
2	-rw	8488464	Jan 01 2000 17:50:00	Image1	Delete
3	-rw	8486640	Jan 01 2000 01:08:30	Image2	Delete
4	-rw	1585	Jan 01 2000 00:01:30	Config1	Delete
5	-rw	29076	Jan 01 2000 00:04:25	Config2	Delete
6	d-	1360	Jan 01 2000 00:00:10	system	Delete

46305280 bytes total (20783104 bytes free)

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.

The screenshot shows a 'File System' interface with the path 'C:/'. Under 'Copy File', the 'Source' dropdown is set to 'startup-config' and the 'Destination' dropdown is set to 'running-config'. There is a checked 'Replace' checkbox and 'Apply' and 'Cancel' buttons.

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.

Parameter	Description
	<ul style="list-style-type: none"> • 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 the 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:

The screenshot shows a web-based configuration interface for 'Clock Settings'. At the top, there's a header bar with the title 'Clock Settings'. Below it is a navigation menu with a single item: 'Clock Settings'. The main area contains two input fields: 'Time (HH:MM:SS)' with the value '07:18:06' and 'Date (DD / MM / YYYY)' with the value '01/01/2000'. In the bottom right corner of this area, there is a grey rectangular button labeled 'Apply'.

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:

The screenshot shows the 'SNTP Settings' window with two main sections: 'SNTP Global Settings' and 'SNTP Server Setting'.

SNTP Global Settings:

- Current Time Source: System Clock
- SNTP State: Disabled (selected from a dropdown menu)
- Poll Interval (30-99999): 720 sec
- An 'Apply' button is located to the right of the poll interval field.

SNTP Server Setting:

- IPv4 Address input field with an 'Add' button to its right.
- Total Entries: 1
- A table showing one entry:

SNTP Server	Version	Last Receive
10.90.90.254	-	-

 An 'Delete' button is located to the right of the last column.

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.

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:

The screenshot shows the Surveillance Settings window with the following sections:

- Surveillance VLAN Settings:** VLAN ID (2-4094) set to 2, Apply button.
- IP Settings:** Get IP From (Static selected), IP Address (10 . 90 . 90 . 90), Mask (255 . 0 . 0 . 0), Gateway (0 . 0 . 0 . 0), Apply button.
- SNMP Host Settings:** Host IPv4 Address, Apply button.
- Total Entries: 1** table:

Host IP Address	SNMP Version	UDP Port	Community String / SNMPv3 User Name	
10.90.90.10	V2c	162	public	Delete
- Log Server:** Host IPv4 Address, Apply button.
- Total Entries: 1** table:

Server IP	Severity	Facility	Discriminator Name	UDP Port	
10.90.90.11	Emergencies	0		514	Delete
- Uplink Port Settings:** From Port (eth1/0/1), To Port (eth1/0/1), Add button.
- Port:** eth1/0/10, Delete button.

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:

Surveillance Log			
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:

Health Diagnostic						
Health Diagnostic						
Port	Loopback Detection Status	Cable Link	PoE Status	Tx/Rx CRC Counter	Discovered Surveillance Devices	Detect Distance
eth1/0/1	-	-	-	-	-	<button>Detect</button>
eth1/0/2	-	-	-	-	-	<button>Detect</button>
eth1/0/3	Normal	Pass	Delivering	0/0	<u>1</u>	<button>Detect</button>
eth1/0/4	-	-	-	-	-	<button>Detect</button>
eth1/0/5	-	-	-	-	-	<button>Detect</button>
eth1/0/6	Normal	Pass	Searching	0/0	<u>1</u>	<button>Detect</button>
eth1/0/7	-	-	-	-	-	<button>Detect</button>
eth1/0/8	-	-	-	-	-	<button>Detect</button>
eth1/0/9	Normal	Pass	Searching	0/0	<u>0</u>	<button>Detect</button>
eth1/0/10	-	-	-	-	-	<button>Detect</button>

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 one of the following: <ul style="list-style-type: none"> Pass - The port link is up and operating in the full-duplex mode. 10M Half - The port link is up and operating at 10 Mbps speed and in the half-duplex mode. 100M Half - The port link is up and operating at 100 Mbps speed and in the half-duplex mode.
PoE Status	This field displays the PoE status. It can be one of the following: Delivering , Searching , Pass , MPS (Maintain Power Signature) Absent , PD Short , Overload , Power Denied , Thermal Shutdown , Startup Failure , or Classification Failure .
Tx/Rx CRC Counter	This field displays the TX/RX CRC counter.

Parameter	Description
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (1) to view the group details associated with IP camera or NVR connected to the port.
Detect Distance	Click the Detect button to initiate a cable distance test on the specified port.

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 5.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

The screenshot shows a web-based configuration interface for upgrading firmware via HTTP. At the top, a header bar reads "Firmware Upgrade from HTTP". Below this, there are two input fields: "Source File" with a "Browse..." button and "Destination File" set to "Image 1". At the bottom right is a large, prominent "Upgrade" button.

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:

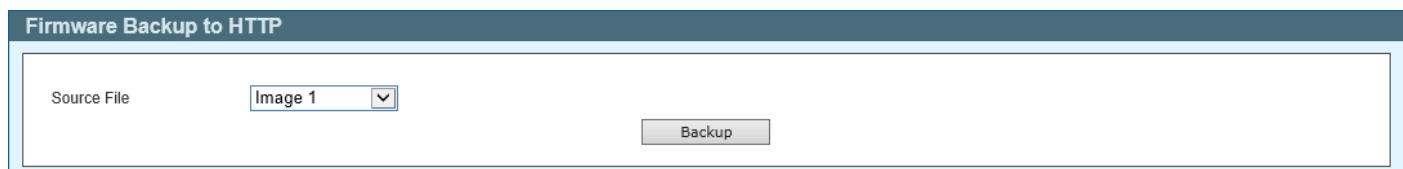


Figure 14-23 Firmware Backup to HTTP Window

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:

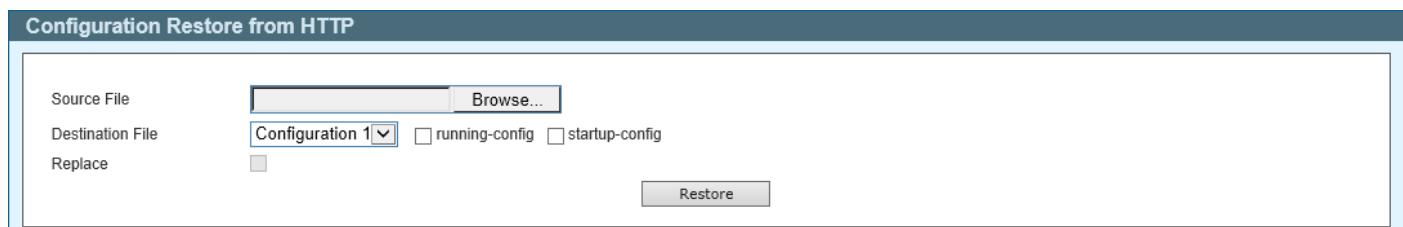


Figure 14-24 Configuration Restore from HTTP Window

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.

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 14-25 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. 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	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:

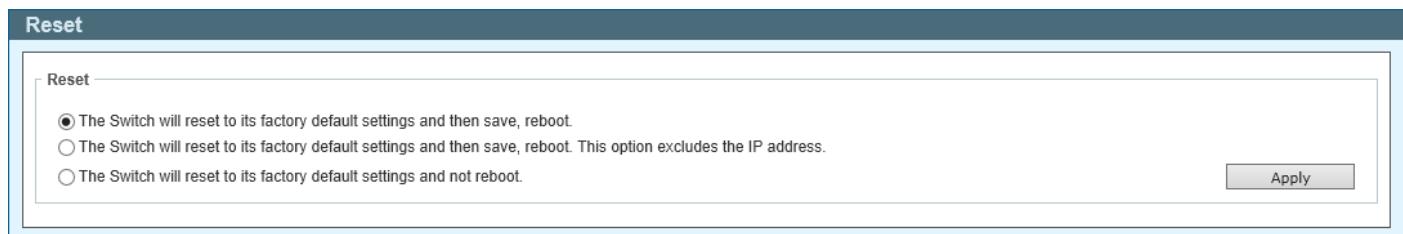


Figure 14-27 Reset Window

Select one of the following options:

- The Switch will reset to its factory default settings and then save, reboot.
- The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot.

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

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

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



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:



The screenshot shows a web-based configuration interface titled "Save Configuration". A dropdown menu labeled "File Path" is open, showing the option "startup-config" which is selected. There is also an "Apply" button in the bottom right corner.

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.

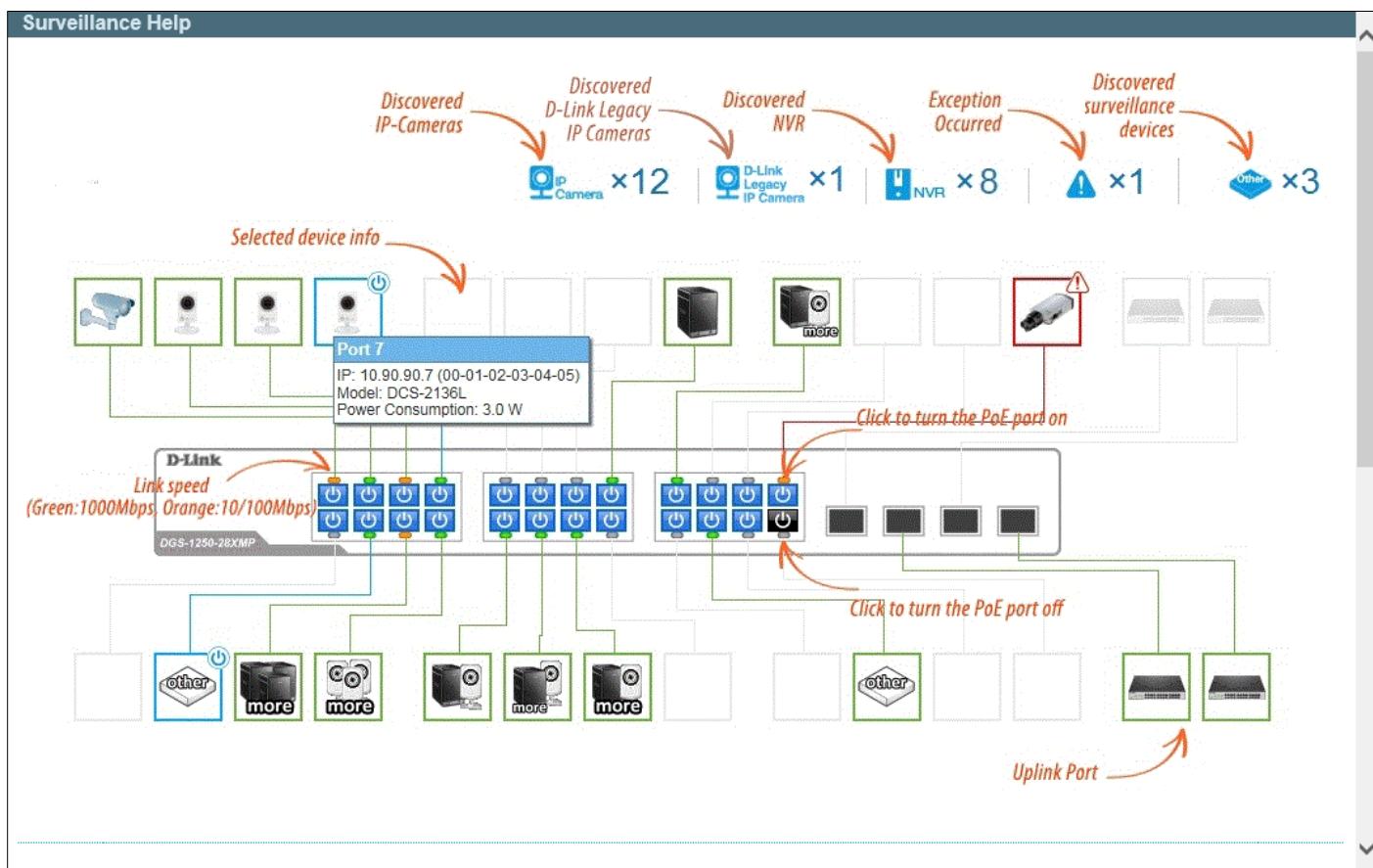


Figure 14-30 Help (Diagram) Window

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.
	This icon indicates that the designated device is operational and is powered by PoE. It also indicates that the PD Alive function is enabled.		The device was rebooted successfully. Please click the icon to recover to its operational state.		The device has malfunctioned. A problem has been detected on this port or device. PD Alive function may have malfunctioned.

IP-Camera/NVR Status

Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.		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 following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

802.1X

Log Description	Severity
<p>Event Description: 802.1X Authentication failure. Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: reason: The reason for the failed authentication. The possible reason may be: (1) user authentication failure (2) no server(s) responding (3) no servers configured (4) no resources (5) user timeout expired username: The user that is being authenticated. interface-id: The switch interface number. mac-address: The MAC address of the authenticated device.</p>	Critical
<p>Event Description: 802.1X Authentication successful. Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: username: The user that is being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.</p>	Informational

AAA

Log Description	Severity
<p>Event Description: This log will be generated when AAA global state is enabled or disabled. Log Message: AAA is <status> Parameters Description: status: The status indicates the AAA enabled or disabled.</p>	Informational
<p>Event Description: This log will be generated when login successfully. Log Message: Successful login through <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types. For example, Console, Telnet, SSH, Web, and Web (SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method. For example, none and local. Username: It indicates the username for authentication. Note: For console, there will be no client IP information for logging.</p>	Informational
<p>Event Description: This log will be generated when login failure. Log Message: Login failed through <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> (Username: <username>)</p>	Warning

Log Description	Severity
<p>Parameters Description:</p> <p>exec-type: It indicates the EXEC types. For example, Console, Telnet, SSH, Web, and Web (SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method. For example, local.</p> <p>username: It indicates the username for authentication.</p> <p>Note: For console, there will be no client IP information for logging.</p>	

Auto Surveillance VLAN

Log Description	Severity
<p>Event Description: 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 interface name.</p> <p>mac-address: Surveillance device MAC address.</p>	Informational
<p>Event Description: When an interface that is enabled surveillance, VLAN joins the surveillance VLAN automatically.</p> <p>Log Message: <interface-id> add into surveillance VLAN <vid></p> <p>Parameters Description:</p> <p>interface-id: The interface name.</p> <p>vid: The VLAN ID.</p>	Informational
<p>Event Description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent.</p> <p>Log Message: <interface-id> remove from surveillance VLAN <vid></p> <p>Parameters Description:</p> <p>interface-id: The interface name.</p> <p>vid: The VLAN ID.</p>	Informational
<p>Event Description: When an IPC is added in the surveillance VLAN, the log message will be sent.</p> <p>Log Message: ASV: Add IPC(<ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: Represent the IP address of the IPC.</p>	Informational
<p>Event Description: When an IPC is removed from the surveillance VLAN, the log message will be sent.</p> <p>Log Message: ASV: Remove IPC(<ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: Represent the IP address of the IPC.</p>	Informational
<p>Event Description: When an NVR is added in the surveillance VLAN, the log message will be sent.</p> <p>Log Message: ASV: Add NVR(<ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: Represent the IP address of the NVR.</p>	Informational
<p>Event Description: When an NVR is removed from the surveillance VLAN, the log message will be sent.</p> <p>Log Message: ASV: Remove NVR(<ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: Represent the IP address of the NVR.</p>	Informational

Log Description	Severity
<p>Event Description: When the mode of ASV 2.0 is changed by Web GUI, the log message will be sent.</p> <p>Log Message: ASV: Mode change from <mode> to <mode></p> <p>Parameters Description:</p> <p>mode: Represent the mode of ASV 2.0. The mode can be standard or surveillance.</p>	Informational

Configuration/Firmware

Log Description	Severity
<p>Event Description: Firmware upgraded successfully.</p> <p>Log Message: Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p> <p>Note: For console, there will be no IP and MAC information for logging.</p>	Informational
<p>Event Description: Firmware upgraded unsuccessfully.</p> <p>Log Message: Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p> <p>Note: For console, there will be no IP and MAC information for logging.</p>	Warning
<p>Event Description: Firmware uploaded successfully.</p> <p>Log Message: Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p> <p>Note: For console, there will be no IP and MAC information for logging.</p>	Informational
<p>Event Description: Firmware uploaded unsuccessfully.</p> <p>Log Message: Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p>	Warning

Log Description	Severity
<p>serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.</p>	
<p>Event Description: Configuration downloaded successfully. Log Message: Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.</p>	Informational
<p>Event Description: Configuration downloaded unsuccessfully. Log Message: Configuration downloaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.</p>	Warning
<p>Event Description: Configuration uploaded successfully. Log Message: Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.</p>	Informational
<p>Event Description: Configuration uploaded unsuccessfully. Log Message: Configuration uploaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.</p>	Warning

Log Description	Severity
<p>Event Description: Configuration saved to flash by console. Log Message: Configuration saved to flash by console (Username: <username> Parameters Description: username: Represent current login user.</p>	Informational
<p>Event Description: Configuration saved to flash by remote. Log Message: Configuration saved to flash (Username: <username>, IP: <ipaddr> Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Informational
<p>Event Description: Log message uploaded successfully. Log Message: Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. Note: For console, there will be no IP and MAC information for logging.</p>	Informational
<p>Event Description: Log message uploaded unsuccessfully. Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. Note: For console, there will be no IP and MAC information for logging.</p>	Warning
<p>Event Description: Unknown type files downloaded unsuccessfully. Log Message: Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.</p>	Warning

NOTE:

1. The user's session indicates Console, Web, SNMP, Telnet, or SSH.
2. If update configuration/firmware through Console, there will be no IP and MAC information for logging.

DAI

Log Description	Severity
<p>Event Description: This log will be generated when DAI detect invalid ARP packet.</p> <p>Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Parameters Description:</p> <p>type: The type of ARP packet, it indicates that ARP packet is request or ARP response.</p>	Warning
<p>Event Description: This log will be generated when DAI detect valid ARP packet.</p> <p>Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)</p> <p>Parameters Description:</p> <p>type: The type of ARP packet, it indicates that ARP packet is request or ARP response.</p>	Informational

DHCPv6 Client

Log Description	Severity
<p>Event Description: DHCPv6 client interface administrator state changed.</p> <p>Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled]</p> <p>Parameters Description:</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event Description: DHCPv6 client obtains an IPv6 address from a DHCPv6 server.</p> <p>Log Message: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name></p> <p>Parameters Description:</p> <p>ipv6address: The IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event Description: The IPv6 address obtained from a DHCPv6 server starts renewing.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing</p> <p>Parameters Description:</p> <p>ipv6address: The IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event Description: The IPv6 address obtained from a DHCPv6 server renews success.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success</p> <p>Parameters Description:</p> <p>ipv6address: The IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event Description: The IPv6 address obtained from a DHCPv6 server starts rebinding.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding</p> <p>Parameters Description:</p> <p>ipv6address: The IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event Description: The IPv6 address obtained from a DHCPv6 server rebinds success.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success</p> <p>Parameters Description:</p> <p>ipv6address: The IPv6 address obtained from a DHCPv6 server.</p> <p>ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event Description: The IPv6 address from a DHCPv6 server was deleted.</p> <p>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted</p>	Informational

Log Description	Severity
Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	

DHCPv6 Relay

Log Description	Severity
Event Description: DHCPv6 relay on a specify interface's administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] Parameters Description: ipif-name: Name of the DHCPv6 relay agent interface.	Informational

DoS Prevention

Log Description	Severity
Event Description: Detect DOS attack. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>) Parameters Description: dos-type: DOS attack type. ip-address: IP address. interface-id: Interface name.	Notice

DNS Resolver

Log Description	Severity
Event Description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted. Log Message: [DNS-RESOLVER(1):]Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domain-name: The domain name string. ipaddr: The IP address.	Informational

Interface

Log Description	Severity
Event Description: When port is down. Log Message: Port <port-type><interface-id> link down Parameters Description: port-type: The port type. interface-id: Interface name.	Informational
Event Description: When port is up. Log Message: Port <port-type><interface-id> link up, <link-speed> Parameters Description: port-type: The port type.	Informational

Log Description	Severity
interface-id: The interface name. link-speed: The port link speed.	
Event Description: Port is linked on half-duplex mode. Log Message: ASV: Port <interface-id> Half duplex detected Parameters Description: interface-id: Interface name.	Warning

IPv6 Duplicate Address

Log Description	Severity
Event Description: This log will be generated when DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages Parameters Description: ipv6address: ipv6 address in Neighbor Solicitation Messages interface-id: Interface name	Warning
Event Description: This log will be generated when DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages Parameters Description: ipv6address: ipv6 address in Neighbor Advertisement Messages interface-id: Interface name	Warning

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up. Log Message: Link Aggregation Group <group-id> link up Parameters Description: group-id: The group ID of the link down aggregation group.	Informational
Event Description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group-id> link down Parameters Description: group-id: The group ID of the link down aggregation group.	Informational
Event Description: Member port attach to Link Aggregation Group. Log Message: <filename> attach to Link Aggregation Group <group-id> Parameters Description: filename: The interface name of the port that attach to aggregation group. group-id: The group ID of the aggregation group that port attach to.	Informational
Event Description: Member port detach from Link Aggregation Group. Log Message: <filename> detach from Link Aggregation Group <group-id> Parameters Description: filename: The interface name of the port that detach from aggregation group. group-id: The group ID of the aggregation group that port detach from.	Informational

LBD

Log Description	Severity
<p>Event Description: Record the event when an interface detect loop.</p> <p>Log Message: <interface-id> LBD loop occurred</p> <p>Parameters Description:</p> <p>interface-id: Interface on which loop is detected.</p>	Critical
<p>Event Description: Record the event when an interface detect loop.</p> <p>Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred</p> <p>Parameters Description:</p> <p>interface-id: Interface on which loop is detected.</p> <p>vlan-id: VLAN on which loop is detected.</p>	Critical
<p>Event Description: Record the event when an interface loop recovered.</p> <p>Log Message: <interface-id> LBD loop recovered</p> <p>Parameters Description:</p> <p>interface-id: Interface on which loop is detected.</p>	Critical
<p>Event Description: Record the event when an interface loop recovered.</p> <p>Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered</p> <p>Parameters Description:</p> <p>interface-id: Interface on which loop is detected.</p> <p>vlan-id: VLAN on which loop is detected.</p>	Critical
<p>Event Description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number.</p> <p>Log Message: Loop VLAN numbers overflow</p>	Critical

LLDP/LLDP-MED

Log Description	Severity
<p>Event Description: LLDP-MED topology change detected</p> <p>Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>Parameters Description:</p> <p>portNum: The port number.</p> <p>chassisType: The chassis ID subtype.</p> <p>Value list:</p> <ul style="list-style-type: none"> 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) <p>chassisID: The chassis ID.</p> <p>portType: The port ID subtype.</p> <p>Value list:</p> <ul style="list-style-type: none"> 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 	Notice

Log Description	Severity
<p>6. agentCircuitId(6) 7. local(7) portID: The port ID. deviceClass: The LLDP-MED device type.</p>	
<p>Event Description: Conflict LLDP-MED device type detected. Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: The chassis ID. portType: The port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: The port ID. deviceClass: The LLDP-MED device type.</p>	Notice
<p>Event Description: Incompatible LLDP-MED TLV set detected. Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: The chassis ID. portType: The port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4)</p>	Notice

Log Description	Severity
5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: The port ID. deviceClass: The LLDP-MED device type.	

Login/Logout

Log Description	Severity
Event Description: Login through console successfully. Log Message: Successful login through Console (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Login through console unsuccessfully. Log Message: Login failed through Console (Username: <username>) Parameters Description: username: Represent current login user.	Warning
Event Description: Console session timed out. Log Message: Console session timed out (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Logout through console. Log Message: Logout through Console (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Login through Telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through Telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description:	Informational

Log Description	Severity
<p>username: Represent current login user. ipaddr: Represent client IP address.</p>	
<p>Event Description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Critical
<p>Event Description: The SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Informational
<p>Event Description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.</p>	Informational

MSTP Debug Enhancement

Log Description	Severity
<p>Event Description: Used to record the event that Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled</p>	Informational
<p>Event Description: Used to record the event that Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled</p>	Informational
<p>Event Description: Used to record MSTP instance topology change event. Log Message: Topology changed (Instance: <Instance-id>,<interface-id>, MAC:<macaddr>) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. interface-id: The port number that detect or receive topology change information. macaddr: The system of bridge MAC address.</p>	Notice
<p>Event Description: Used to record MSTP instance new root bridge 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 for default instance, CIST. macaddr: The system of bridge MAC address. priority: The bridge priority value must be divisible by 4096.</p>	Informational
<p>Event Description: Used to record MSTP instance new root port selected. Log Message: New root port selected (Instance:<Instance-id>, <interface-id>) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. interface-id: The port number that detect or receive topology change information.</p>	Notice
<p>Event Description: Used to record MSTP instance port state change event. Log Message: Spanning Tree port status change (Instance:<Instance-id>, <interface-id> <old-status> -> <new-status>) Parameters Description:</p>	Notice

Log Description	Severity
<p>Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST.</p> <p>interface-id: The port number that detect or receive topology change information.</p> <p>old-status: The old status.</p> <p>new-status: The new status.</p> <p>The port of STP state. The value may be Disable, Discarding, Learning, or Forwarding.</p>	
<p>Event Description: Used to record MSTP instance port role change event.</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 for default instance, CIST.</p> <p>Interface-id: The port number that detect or receive topology change information.</p> <p>old-role: The old role.</p> <p>new-role: The new role.</p> <p>The port role of STP. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, or MasterPort.</p>	Informational
<p>Event Description: Use to record action to create an MST instance.</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 for default instance, CIST.</p>	Informational
<p>Event Description: Use to record action to delete an MST instance.</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 for default instance, CIST.</p>	Informational
<p>Event Description: Use to record action to change the STP version.</p> <p>Log Message: Spanning Tree version change (new version:<new-version>)</p> <p>Parameters Description:</p> <p>new-version: Running under which version of STP.</p>	Informational
<p>Event Description: Used to record 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 a specified MST region.</p> <p>revision-level: Switches using the same given name but with a different revision level are considered members of different MST regions.</p>	Informational
<p>Event Description: Use to record action to maps a VLAN(s) 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 for default instance, CIST.</p> <p>startvlanid: The start VID of add VLAN range.</p> <p>endvlanid: The end VID of add VLAN range.</p>	Informational
<p>Event Description: Use to record action to delete a VLAN(s) 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 for default instance, CIST.</p> <p>startvlanid: The start VID of delete VLAN range.</p> <p>endvlanid: The end VID of delete VLAN range.</p>	Informational

Log Description	Severity
<p>Event Description: Used to record the event that port role change 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 for default instance, CIST.</p> <p>Interface-id: The port number that detect the event.</p>	Informational

Peripheral

Log Description	Severity
<p>Event Description: Fan 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
<p>Event Description: Fan Failed.</p> <p>Log Message: <fan-descr> failed</p> <p>Parameters Description:</p> <p>fan-descr: The FAN ID and position.</p>	Critical
<p>Event Description: Temperature sensor enters 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
<p>Event Description: 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
<p>Event Description: Power failed.</p> <p>Log Message: <power-descr> failed</p> <p>Parameters Description:</p> <p>power-descr: The power position and ID.</p>	Critical
<p>Event Description: Power is recovered.</p> <p>Log Message: <power-descr> back to normal</p> <p>Parameters Description:</p> <p>power-descr: The power position and ID.</p>	Critical
<p>Event Description: Press the factory reset button.</p> <p>Log Message: Factory reset button pressed</p>	Critical

PoE

Log Description	Severity
<p>Event Description: Total power usage threshold is exceeded.</p> <p>Log Message: Usage threshold <percentage> is exceeded</p> <p>Parameters Description:</p> <p>percentage: The usage threshold.</p>	Warning
<p>Event Description: Total power usage threshold is recovered.</p>	Warning

Log Description	Severity
<p>Log Message: Usage threshold <percentage> is recovered</p> <p>Parameters Description:</p> <p>percentage: The usage threshold.</p>	
<p>Event Description: PD doesn't reply the ping request.</p> <p>Log Message: ASV: PD alive check failed. (Port: <portNum>, PD: <ipaddr>)</p> <p>Parameters Description:</p> <p>portNum: The port number.</p> <p>ipaddr: The IP address of PD.</p>	Warning

Port Security

Log Description	Severity
<p>Event Description: Address full on a port.</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 ID.</p>	Warning
<p>Event Description: Address full on system.</p> <p>Log Message: Limit on system entry number has been exceeded</p>	Warning

Safeguard

Log Description	Severity
<p>Event Description: The host enters the exhausted mode.</p> <p>Log Message: Safeguard Engine enters EXHAUSTED mode</p>	Warning
<p>Event Description: The host enters the normal mode.</p> <p>Log Message: Safeguard Engine enters NORMAL mode</p>	Informational

SNMP

Log Description	Severity
<p>Event Description: SNMP request received with 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
<p>Event Description: The SSH server is enabled.</p> <p>Log Message: SSH server is enabled</p>	Informational
<p>Event Description: The SSH server is disabled.</p> <p>Log Message: SSH server is disabled</p>	Informational

Storm Control

Log Description	Severity
<p>Event Description: Storm occurrence.</p> <p>Log Message: <Broadcast Multicast Unicast> storm is occurring on <interface-id></p> <p>Parameters Description:</p> <p>Broadcast: Storm is resulted by broadcast packets (DA = FF:FF:FF:FF:FF:FF).</p> <p>Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast, and known IP multicast.</p> <p>Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets.</p> <p>interface-id: The interface ID on which a storm is occurring.</p>	Warning
<p>Event Description: Storm cleared.</p> <p>Log Message: <Broadcast Multicast Unicast> storm is cleared on <interface-id></p> <p>Parameters Description:</p> <p>Broadcast: Broadcast storm is cleared.</p> <p>Multicast: Multicast storm is cleared.</p> <p>Unicast: Unicast storm (including both known and unknown unicast packets) is cleared.</p> <p>interface-id: The interface ID on which a storm is cleared.</p>	Informational
<p>Event Description: Port 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 on which is error-disabled by storm.</p> <p>Broadcast: The interface is disabled by broadcast storm.</p> <p>Multicast: The interface is disabled by multicast storm.</p> <p>Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).</p>	Warning

System

Log Description	Severity
<p>Event Description: This log will be generated when system warm start.</p> <p>Log Message: System warm start</p>	Critical
<p>Event Description: This log will be generated when system cold start.</p> <p>Log Message: System cold start</p>	Critical
<p>Event Description: This log will be generated when system start up.</p> <p>Log Message: System started up</p>	Critical

Telnet

Log Description	Severity
<p>Event Description: Successful login through Telnet.</p> <p>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: The IP address of Telnet client.</p> <p>username: The username that used to login Telnet server.</p>	Informational
<p>Event Description: Login failed through Telnet.</p> <p>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</p>	Warning

Log Description	Severity
<p>Parameters Description:</p> <p>ipaddr: The IP address of Telnet client.</p> <p>username: The username that used to login Telnet server.</p>	
<p>Event Description: Logout through Telnet.</p> <p>Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: The IP address of Telnet client.</p> <p>username: The username that used to login Telnet server.</p>	Informational
<p>Event Description: Telnet session timed out.</p> <p>Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>ipaddr: The IP address of Telnet client.</p> <p>username: The username that used to login Telnet server.</p>	Informational

Voice VLAN

Log Description	Severity
<p>Event Description: When a new voice device is detected on an interface.</p> <p>Log Message: New voice device detected (<interface-id>, MAC: <mac-address>)</p> <p>Parameters Description:</p> <p>interface-id: Interface name.</p> <p>mac-address: Voice device MAC address.</p>	Informational
<p>Event Description: When an interface that is in auto voice VLAN mode joins the voice VLAN.</p> <p>Log Message: <interface-id> add into voice VLAN <vid></p> <p>Parameters Description:</p> <p>interface-id: The interface name.</p> <p>vid: The VLAN ID.</p>	Informational
<p>Event Description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent.</p> <p>Log Message: <interface-id> remove from voice VLAN <vid></p> <p>Parameters Description:</p> <p>interface-id: The interface name.</p> <p>vid: The VLAN ID.</p>	Informational

Web

Log Description	Severity
<p>Event Description: Successful login through Web.</p> <p>Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event Description: Login failed through Web.</p> <p>Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login HTTP server.</p>	Warning

Log Description	Severity
<p>ipaddr: The IP address of HTTP client.</p> <p>Event Description: Web session timed out.</p> <p>Log Message: Web session timed out (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event Description: Logout through Web.</p> <p>Log Message: Logout through Web (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event Description: Successful login through Web (SSL).</p> <p>Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login SSL server.</p> <p>ipaddr: The IP address of SSL client.</p>	Informational
<p>Event Description: Login failed through Web (SSL).</p> <p>Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login SSL server.</p> <p>ipaddr: The IP address of SSL client.</p>	Warning
<p>Event Description: Web (SSL) session timed out.</p> <p>Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login SSL server.</p> <p>ipaddr: The IP address of SSL client.</p>	Informational
<p>Event Description: Logout through Web (SSL).</p> <p>Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The username that used to login SSL server.</p> <p>ipaddr: The IP address of SSL client.</p>	Informational

Appendix B - Trap Entries

The following table lists the trap log entries and their corresponding meanings that will appear in the Switch.

802.1X

Trap Name	Description	OID
dDot1xExtLoggedSuccess	<p>This trap is sent when a host has successfully logged in (passed 802.1X authentication).</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName 	1.3.6.1.4.1.171 .11.165.1000.3 0.0.1
dDot1xExtLoggedFail	<p>This trap is sent when a host failed to pass IEEE 802.1X authentication (login failed).</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason 	1.3.6.1.4.1.171 .11.165.1000.3 0.0.2

Authentication Fail

Trap Name	Description	OID
authenticationFailure	<p>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 the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.</p>	1.3.6.1.6.3.1.1. 5.5

DHCP Server Screen Prevention

Trap Name	Description	OID
dDhcpFilterAttackDetected	<p>When DHCP Server Screen is enabled, if the switch received the forge DHCP Server packet, the switch will trap the event if any attacking packet is received.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime 	1.3.6.1.4.1.171 .11.165.1000.1 33.0.1

DoS Prevention

Trap Name	Description	OID
dDosPreveAttackDetected Packet	This trap is sent when detect DOS attack. Binding objects: (1) dDoSPrevCtrlAttackType (2) dDoSPrevNotiInfoDropIpAddr (3) dDoSPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171 .11.165.1000.5 9.0.2

ErrDisable

Trap Name	Description	OID
dErrDisNotifyPortDisabled Assert	This trap is sent when a port enters into error-disabled state. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171 .11.165.1000.4 5.0.1
dErrDisNotifyPortDisabled Clear	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171 .11.165.1000.4 5.0.2

General Management

Trap Name	Description	OID
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 .11.165.1000.1 65.0.1

Gratuitous ARP

Trap Name	Description	OID
agentGratuitousARPTrap	This trap is sent when IP address conflicted. Binding objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPIfaceName	1.3.6.1.4.1.171 .11.165.1000.7 5.0.1

IMPB

Trap Name	Description	OID
dlmpbViolationTrap	This notification is generated when IP-MAC-Port binding address violation is detected. Binding objects: (1) ifIndex (2) dlmpbViolationIpAddrType	1.3.6.1.4.1.171 .11.165.1000.2 2.0.1

Trap Name	Description	OID
	(3) dlmpbViolationIpAddress (4) dlmpbViolationMacAddress	

LACP

Trap Name	Description	OID
linkUp	This trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	This trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

LBD

Trap Name	Description	OID
dLbdLoopOccurred	This trap is sent when an interface loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171 .11.165.1000.4 6.0.1
dLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171 .11.165.1000.4 6.0.2
dLbdVlanLoopOccurred	This trap is sent when an interface with a VID loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .11.165.1000.4 6.0.3
dLbdVlanLoopRestart	This trap is sent when an interface loop with a VID restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .11.165.1000.4 6.0.4

LLDP

Trap Name	Description	OID
lldpRemTablesChange	<p>This notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts 	1.0.8802.1.1.2. 0.0.1
lldpXMedTopologyChangeDetected	<p>A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass 	1.0.8802.1.1.2. 1.5.4795.0.1

MAC Notification

Trap Name	Description	OID
dL2FdbMacNotification	<p>This trap indicate the MAC addresses variation in the address table.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) dL2FdbMacChangeNotifyInfo 	1.3.6.1.4.1.171 .11.165.1000.3 .0.1

MSTP

Trap Name	Description	OID
newRoot	<p>This trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root. For example, upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.</p>	1.3.6.1.2.1.17. 0.1
topologyChange	<p>This trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.</p>	1.3.6.1.2.1.17. 0.2

PD Alive

Trap Name	Description	OID
dPoelfPdAliveFailOccurNotification	<p>This trap indicates if the PD reply the ping request. At least 500 ms must elapse between notifications being emitted by the same object instance.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) pethMainPseGroupIndex (2) pethPsePortIndex 	1.3.6.1.4.1.171 .14.24.0.4

Trap Name	Description	OID
	(3) dPoelfPdAliveCfgPdlpType (4) dPoelfPdAliveCfgPdlpAddr	

Peripheral

Trap Name	Description	OID
dEntityExtFanStatusChg	Fan status change notification. Binding objects: (1) dEntityExtEnvFanIndex (2) dEntityExtEnvFanStatus	1.3.6.1.4.1.171 .11.165.1000.5 .0.1
dEntityExtThermalStatusChg	Temperature status change notification. Binding objects: (1) dEntityExtEnvTempIndex (2) dEntityExtEnvTempStatus	1.3.6.1.4.1.171 .11.165.1000.5 .0.2
dEntityExtFactoryResetButton	Press the factory reset button.	1.3.6.1.4.1.171 .11.165.1000.5 .0.5

PoE

Trap Name	Description	OID
pethMainPowerUsageOnNotification	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105 .0.2
pethMainPowerUsageOffNotification	This trap indicates PSE Threshold usage indication is off; the usage power is below the threshold. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105 .0.3
dPoelfPowerDeniedNotification	This notification indicates if PSE state diagram enters the state POWER_DENIED. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171 .11.165.1000.2 4.0.1
dPoelfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171 .11.165.1000.2 4.0.2
dPoelfPowerShortCircuitNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortShortCounter	1.3.6.1.4.1.171 .11.165.1000.2 4.0.3

Port

Trap Name	Description	OID
linkUp	This notification is generated when the port link is up. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	This notification is generated when the port link is 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
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfLastMacAddress	1.3.6.1.4.1.171.11.165.1000.8.0.1

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Trap Name	Description	OID
dSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhausted. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171 .11.165.1000.1 9.1.1.0.1
dSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171 .11.165.1000.1 9.1.1.0.2

Start

Trap Name	Description	OID
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
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
dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .11.165.1000.2 5.0.1
dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .11.165.1000.2 5.0.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.4

Trap Name	Description	OID
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.171 .11.165.1000.1 4.0.5

Appendix C - RADIUS Attributes Assignment

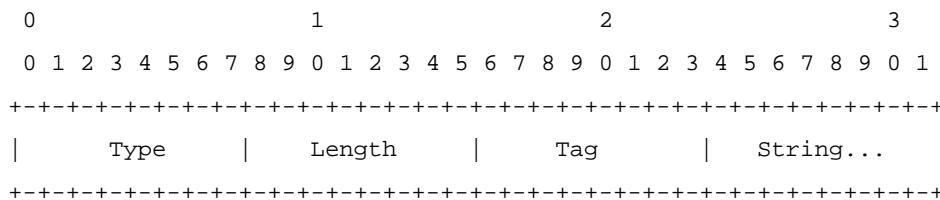
The RADIUS Attributes Assignment on the Switch is used in the 802.1X module. The descriptions that follow explain the VLAN RADIUS Attributes Assignment type.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.



The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
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 **Appendix C - RADIUS Attributes Assignment**.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, and RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF **RADIUS Authentication Attributes** supported by the D-Link Switch.

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