

Web UI Reference Guide

Product Model: DGS-3630 Series

Layer 3 Stackable Managed Switch

Release 2.20 (OpenFlow)



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.

© 2018 D-Link Corporation. All rights reserved.

Table of Contents

1.	Introduction	1
	Audience	1
	Other Documentation	1
	Conventions	1
	Notes, Notices, and Cautions	1
2.	Web-based Switch Configuration	3
	Management Options	3
	Areas of the User Interface	5
3.	System	6
	Device Information	6
	System Information Settings	6
	Peripheral Settings	7
	Port Configuration	8
	Port Settings	8
	Port Status	10
	Port GBIC	11
	Port Auto Negotiation	11
	Jumbo Frame	12
	Interface Description	13
	Loopback Test	13
	PoE	14
	PoE System	14
	PoE Status	15
	PoE Configuration	16
	PD Alive	17
	PoE Statistics	18
	PoE Measurement	19
	System Log	19
	System Log Settings	19
	System Log Discriminator Settings	21
	System Log Server Settings	22
	System Log	23
	Time and SNTP	24
	Clock Settings	24
	Time Zone Settings	24
	SNTP Settings	26
	Time Range	27
	USB Console Settings	28
4.	Management	29
	Command Logging	29
	User Accounts Settings	29
	CLI Alias Settings	31
	Password Encryption	32
	Password Recovery	32
	Login Method	33
	SNMP	34
	SNMP Global Settings	35
	SNMP Linkchange Trap Settings	36
	SNMP View Table Settings	37

SNMP Community Table Settings	38
SNMP Group Table Settings	39
SNMP Engine ID Local Settings	40
SNMP User Table Settings	40
SNMP Host Table Settings	42
RMON	43
RMON Global Settings	43
RMON Statistics Settings	43
RMON History Settings	44
RMON Alarm Settings	45
RMON Event Settings	46
Telnet/Web	47
Session Timeout	47
File System	48
Reboot Schedule Settings	50
5. Layer 2 Features	52
FDB	52
Static FDB	52
MAC Address Table Settings	53
MAC Address Table	55
MAC Notification	56
VLAN	57
802.1Q VLAN	57
VLAN Interface	58
L2VLAN Interface Description	61
STP	62
STP Global Settings	63
STP Port Settings	65
MST Configuration Identification	67
STP Instance	68
MSTP Port Information	69
Link Aggregation	69
6. Layer 3 Features	73
ARP	73
ARP Aging Time	73
Static ARP	73
ARP Table	74
IPv6 Neighbor	75
Interface	75
IPv4 Interface	75
IPv6 Interface	77
IPv4 Static/Default Route	78
IPv4 Route Table	79
IPv6 Static/Default Route	79
IPv6 Route Table	80
7. Security	82
AAA	82
AAA Global Settings	82
Application Authentication Settings	82
Application Accounting Settings	83
Authentication Settings	84

Accounting Settings	87
RADIUS	89
RADIUS Global Settings	89
RADIUS Server Settings	90
RADIUS Group Server Settings	90
RADIUS Statistic	91
TACACS+	92
TACACS+ Server Settings	92
TACACS+ Group Server Settings	93
TACACS+ Statistic	94
SSH	95
SSH Global Settings	95
Host Key	96
SSH Server Connection	97
SSH User Settings	97
SSL	98
SSL Global Settings	99
Crypto PKI Trustpoint	99
SSL Service Policy	100
SFTP Server Settings	101
Network Protocol Port Protect Settings	102
8. OAM	103
Cable Diagnostics	103
DDM	104
DDM Settings	104
DDM Temperature Threshold Settings	105
DDM Voltage Threshold Settings	105
DDM Bias Current Threshold Settings	106
DDM TX Power Threshold Settings	107
DDM RX Power Threshold Settings	107
DDM Status Table	108
9. Monitoring	109
Utilization	109
Port Utilization	109
History Utilization	109
Statistics	111
Port	111
Interface Counters	112
Interface History Counters	113
Counters	114
Device Environment	116
External Alarm Settings	117
10. Green	119
Power Saving	119
EEE	120
11. Save and Tools	122
Save Configuration	122
Firmware Upgrade & Backup	122
Firmware Upgrade from HTTP	122
Firmware Upgrade from TFTP	123
Firmware Upgrade from FTP	123

Firmware Upgrade from RCP	124
Firmware Upgrade from SFTP	125
Firmware Backup to HTTP	125
Firmware Backup to TFTP	126
Firmware Backup to FTP	126
Firmware Backup to RCP	127
Firmware Backup to SFTP	128
Configuration Restore & Backup	128
Configuration Restore from HTTP	128
Configuration Restore from TFTP	129
Configuration Restore from FTP	130
Configuration Restore from RCP	131
Configuration Restore from SFTP	131
Configuration Backup to HTTP	132
Configuration Backup to TFTP	133
Configuration Backup to FTP	133
Configuration Backup to RCP	134
Configuration Backup to SFTP	135
Certificate & Key Restore & Backup	136
Certificate & Key Restore from HTTP	136
Certificate & Key Restore from TFTP	136
Certificate & Key Restore from FTP	137
Certificate & Key Restore from RCP	137
Certificate & Key Restore from SFTP	138
Certificate & Key Backup to HTTP	139
Certificate & Key Backup to TFTP	139
Certificate & Key Backup to FTP	140
Certificate & Key Backup to RCP	140
Certificate & Key Backup to SFTP	141
Log Backup	142
Log Backup to HTTP	142
Log Backup to TFTP	142
Log Backup to RCP	143
Log Backup to SFTP	143
Ping	144
Trace Route	146
Reset	148
Reboot System	148
Appendix A - Password Recovery Procedure	149
Appendix B - System Log Entries	150
Appendix C - Trap Entries	166
Appendix D - OpenFlow Object Details	171
Flow Table	171
Policy ACL Flow Table	171
Group Table	173
L2 Interface Group Entry Type	173
L2 Rewrite Group Entry Type	174
L2 Multicast Group Entry Type	174
L3 Unicast Group Entry Type	175
L3 ECMP Group Entry Type	176
Meter Table	176

1. Introduction

This manual's feature descriptions are based on the software release **2.20**, running in the **OpenFlow Hybrid Mode**. The features listed here are the subset of features that are supported by the DGS-3630 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-3630 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-3630 Series Hardware Installation Guide*
- *DGS-3630 Series Command Line Interface (CLI) Guide (OpenFlow)*

Conventions

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

Notes, Notices, and Cautions

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



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



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



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

2. Web-based Switch Configuration

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

Management Options

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

Command Line Interface (CLI)

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

Refer to the *DGS-3630 Series CLI Reference Guide* for more detailed information about the CLI.

SNMP-based Management

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

Web User Interface (Web UI)

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

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



NOTE: The **OpenFlow** feature and all settings related to the feature, can only be enabled and configured through the CLI. Refer to the *DGS-3630 Series Command Line Interface (CLI) Guide (OpenFlow)* for more information.



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

Logging into the Web UI

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



NOTE: The factory default IP address of the Switch is 10.90.90.90 (subnet mask of 255.0.0.0) for normal ports and 192.168.0.1 (subnet mask of 255.255.255.0) is for the management port.

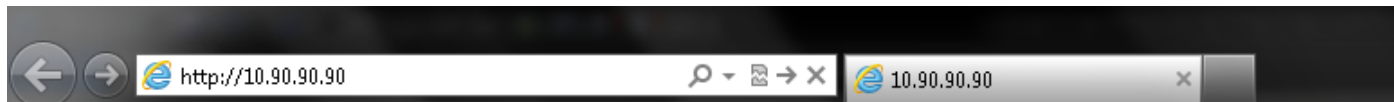


Figure 2-1 Displays entering the IP address in Internet Explorer

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

The screenshot shows a web browser window titled 'Connect to 10.90.90.90'. Inside the window, there is a blue header bar with a key icon. Below the header, there are two input fields: 'User Name' and 'Password'. At the bottom of the window, there are two buttons: 'Login' and 'Reset'.

Figure 2-2 Web UI Login Window

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



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



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

Web User Interface (Web UI)

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

Areas of the User Interface

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

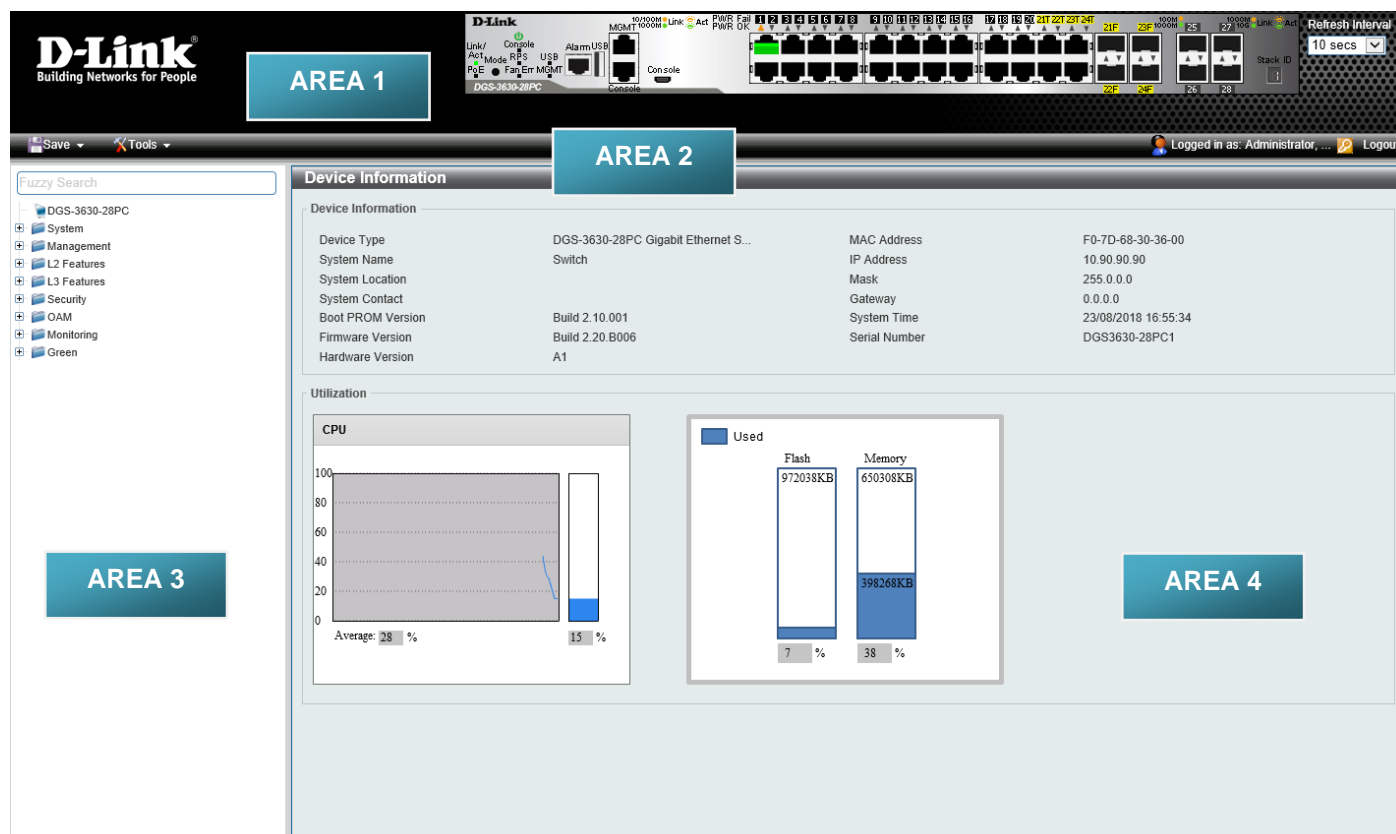


Figure 2-3 Main Web UI Window

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



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

3. System

[Device Information](#)
[System Information Settings](#)
[Peripheral Settings](#)
[Port Configuration](#)
[Interface Description](#)
[Loopback Test](#)
[PoE](#)
[System Log](#)
[Time and SNTP](#)
[Time Range](#)
[USB Console Settings](#)

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-3630-28PC** link.

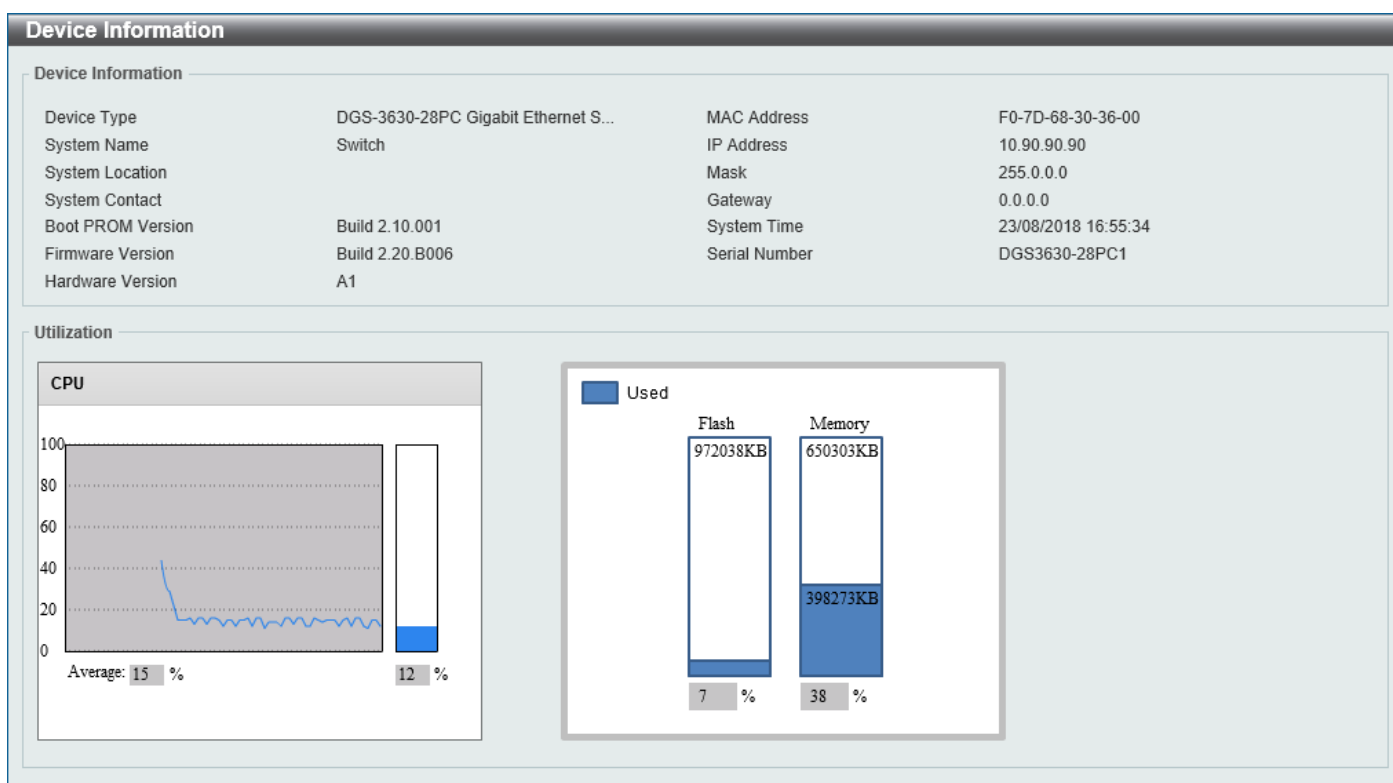


Figure 3-1 Device Information Window

System Information Settings

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

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

System Information Settings

System Information Settings

System Name: Switch

System Location: 255 chars

System Contact: 255 chars

Apply

Management Interface

Interface Name: mgmt_ipif

State: Enabled

IPv4 Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

Description: 64 chars

Link Status: Link Down

Apply

Figure 3-2 System Information Settings Window

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

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

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

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

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

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

Peripheral Settings

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

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

Figure 3-3 Peripheral Settings Window

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

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

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

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

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

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

Port Configuration

Port Settings

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



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

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

Port Settings

Port Settings

From Port: eth1/0/1 To Port: eth1/0/1 Media Type: Auto [Apply]

From Port: eth1/0/1 To Port: eth1/0/1 State: Enabled Flow Control: Off Link Status Log: Enabled Description: 64 chars [Apply]

Media Type: RJ45 Auto Downgrade: Disabled MDIX: Auto Duplex: Auto Speed: Auto Capability Advertised: ☐ 10M ☐ 100M ☐ 1000M ☐ 10G [Apply]

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

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.
Media Type	Select the port media type here. Options to choose from are Auto , RJ45 , and SFP . Selecting the SFP option includes the use of SFP+ transceivers for 10G connectivity.
State	Select to enable or disable the physical port state here.
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. Note: This feature will not work through Switches that are physically stacked.
Link Status Log	Select to enable or disable the link status log function here.
Description	Select the checkbox and enter the description for the corresponding port here. This can be up to 64 characters long.
Auto Downgrade	Select to enable or disable the feature to automatically downgrade the advertised speed in the event that a link cannot be established at the available speed.
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 cross-over cable. Cross - Select this option for cross-over cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another Switch through a straight cable.
Duplex	Select the duplex mode used here. Options to choose from are Auto and Full . The half-duplex mode is not supported on the Switch.
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to connect at the specified speed only.

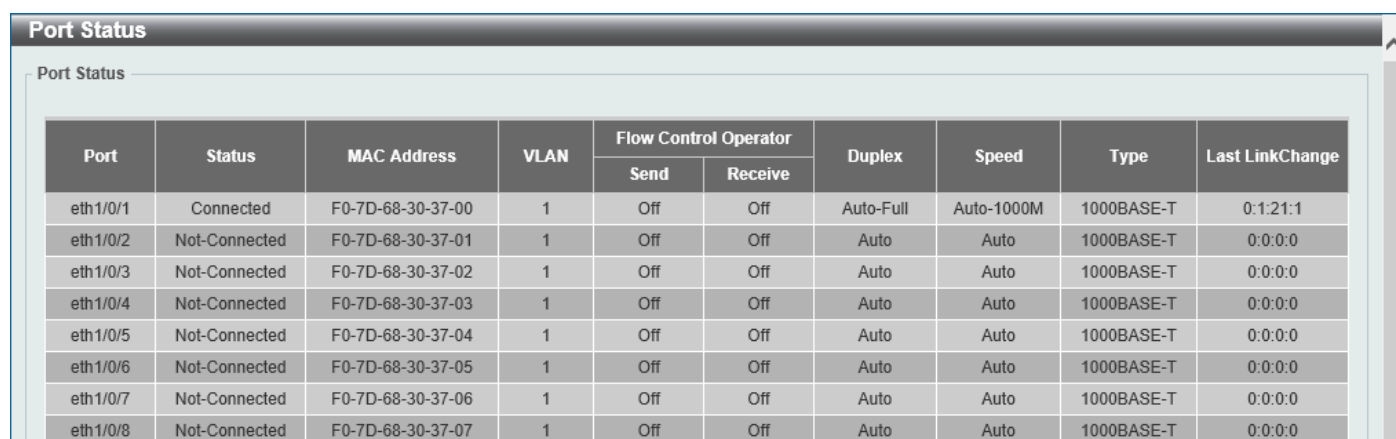
Parameter	Description
	<p>The Master setting will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing 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. This option is only available for 10 Mbps copper connections. • 100M - Specifies to force the port speed to 100 Mbps. This option is only available for 100 Mbps copper connections. • 1000M - Specifies to force the port speed to 1 Gbps. This option is only available for 1 Gbps fiber connections. • 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. This option is only available for 1 Gbps copper connections. • 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. This option is only available for 1 Gbps copper connections. • 10G - Specifies to force the port speed to 10 Gbps. This option is only available for 10 Gbps fiber connections. • 10G Master - Specifies to force the port speed to 10 Gbps and operates as the master, to facilitate the timing of transmit and receive operations. This option is only available for 10 Gbps copper connections. • 10G Slave - Specifies to force the port speed to 10 Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. This option is only available for 10 Gbps copper connections.
Capability Advertised	When the Speed is set to Auto , these capabilities are advertised during auto-negotiation.

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	Last LinkChange
				Send	Receive				
eth1/0/1	Connected	F0-7D-68-30-37-00	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T	0:1:21:1
eth1/0/2	Not-Connected	F0-7D-68-30-37-01	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0
eth1/0/3	Not-Connected	F0-7D-68-30-37-02	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0
eth1/0/4	Not-Connected	F0-7D-68-30-37-03	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0
eth1/0/5	Not-Connected	F0-7D-68-30-37-04	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0
eth1/0/6	Not-Connected	F0-7D-68-30-37-05	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0
eth1/0/7	Not-Connected	F0-7D-68-30-37-06	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0
eth1/0/8	Not-Connected	F0-7D-68-30-37-07	1	Off	Off	Auto	Auto	1000BASE-T	0:0:0:0

Figure 3-5 Port Status Window

Port GBIC

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

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



Port	Interface Type
eth1/0/1	1000BASE-T
eth1/0/2	1000BASE-T
eth1/0/3	1000BASE-T
eth1/0/4	1000BASE-T
eth1/0/5	1000BASE-T
eth1/0/6	1000BASE-T
eth1/0/7	1000BASE-T

Figure 3-6 Port GBIC 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 Auto Negotiation								
Port Auto Negotiation								
Note: AN: Auto Negotiation; RS: Remote Signaling; CS: Config Status; CB: Capability Bits; CAB: Capability Advertised Bits; CRB: Capability Received Bits; RFA: Remote Fault Advertised; RFR: Remote Fault Received								
Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
eth1/0/1	Enabled	Not Detected	Complete	10M_Full, ...	10M_Full, ...	10M_Half, ...	Disabled	NoError
eth1/0/2	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/3	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/4	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/5	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/6	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/7	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/8	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/9	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError
eth1/0/10	Enabled	Not Detected	Configuring	10M_Full, ...	10M_Full, ...	-	Disabled	NoError

Figure 3-7 Port Auto Negotiation Window

Jumbo Frame

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

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

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

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

1/3 < < 1 2 3 > > Go

Figure 3-9 Interface Description Window

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

Loopback Test

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

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

Loopback Test

Loopback Test

From Port

To Port

Loopback Mode

eth1/0/1

eth1/0/1

None

Apply

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

Figure 3-10 Loopback 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.
Loopback Mode	<p>Select the loopback mode here. Options to choose from are:</p> <ul style="list-style-type: none"> • None - Specifies not to enable the loopback mode. • Internal MAC - Specifies the internal loopback mode at the MAC layer. • Internal PHY Default - Specifies the internal loopback mode at the PHY layer to test the default medium. • Internal PHY Copper - Specifies the internal loopback mode at the PHY layer to test the copper medium. • Internal PHY Fiber - Specifies the internal loopback mode at the PHY layer to test the fiber medium. • External MAC - Specifies the external loopback mode at the MAC layer. • External PHY Default - Specifies the external loopback mode at the PHY layer to test the default medium. • External PHY Copper - Specifies the external loopback mode at the PHY layer to test the copper medium. • External PHY Fiber - Specifies the external loopback mode at the PHY layer to test the fiber medium.

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

PoE

The **DGS-3630-28PC** and **DGS-3630-52PC** switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All ports can support PoE up to 30W. 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	16.2 Watts
1	3.84 Watts	4.2 Watts
2	6.49 Watts	7.4 Watts
3	12.95 Watts	16.2 Watts
4	25.5 Watts	31.6 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:

PoE System

PoE System

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

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

Figure 3-11 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) which is power-provisioned with a lower priority in order to release the power to the new connected PD with higher priority under power shortage conditions.
Trap State	Select this option to enable or disable the sending of PoE trap notifications.

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

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

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

PoE System

PoE System

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

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

PoE System Parameters

Unit	Max Ports	Device ID	SW Version
1	0	0	0

Figure 3-12 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:

Port	State	Class	Max (W)	Used (W)	Description	
eth1/0/1		N/A	15.4	0.0		Delete Description
eth1/0/2		N/A	15.4	0.0		Delete Description
eth1/0/3		N/A	15.4	0.0		Delete Description
eth1/0/4		N/A	15.4	0.0		Delete Description
eth1/0/5		N/A	15.4	0.0		Delete Description
eth1/0/6		N/A	15.4	0.0		Delete Description
eth1/0/7		N/A	15.4	0.0		Delete Description
eth1/0/8		N/A	15.4	0.0		Delete Description
eth1/0/9		N/A	15.4	0.0		Delete Description
eth1/0/10		N/A	15.4	0.0		Delete Description

Figure 3-13 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 Powered Device (PD),

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

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

PoE Configuration

PoE Configuration

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

Apply

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

Figure 3-14 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 which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW.
Time Range	When selecting Auto in the Mode drop-down list, this option appears. 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 display and configure the PoE PD alive settings. The PoE alive feature provides the solution when PD devices stop working or are not responding using the ping mechanism.

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

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 3-15 PD Alive Window

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

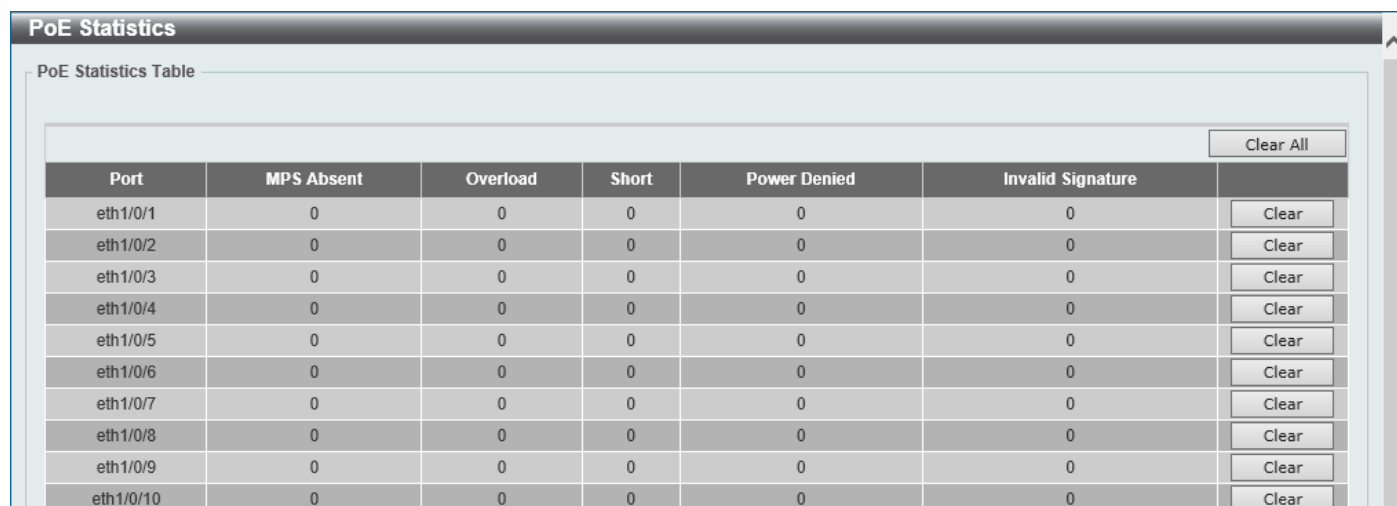
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
PD Alive State	Select to enable or disable the state of the PoE alive function on the specified port(s) here.
PD IP Address	Enter the IPv4 address of the target PD here.
Poll Interval	Enter the poll interval value here. The range is from 10 to 300 seconds. This is the interval at which ping requests will be sent to the target PD to check the status.
Retry Count	Enter the retry count value here. The range is from 0 to 5. This is the amount of times that the ping request will be resend if the target PD does not respond.
Waiting Time	Enter the waiting time value here. The range is from 30 to 300 seconds. This is the time the Switch will wait for the PD to recover from rebooting.
Action	Select the action that will be taken here. Options to choose from are: <ul style="list-style-type: none"> • Reset - Specifies to reset the PoE port state. • Notify - Specifies to send logs and traps to notify the administrator. • Both - Specifies to send logs and traps and then to reset the PoE port state.

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

PoE Statistics

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

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



The screenshot shows the 'PoE Statistics' window with a title bar and a 'PoE Statistics Table' section. The table has 7 columns: Port, MPS Absent, Overload, Short, Power Denied, Invalid Signature, and a 'Clear' button. There are 10 rows of data for ports eth1/0/1 through eth1/0/10, all showing 0 in the statistical columns. A 'Clear All' button is located at the top right of the table area.

Port	MPS Absent	Overload	Short	Power Denied	Invalid Signature	Clear
eth1/0/1	0	0	0	0	0	Clear
eth1/0/2	0	0	0	0	0	Clear
eth1/0/3	0	0	0	0	0	Clear
eth1/0/4	0	0	0	0	0	Clear
eth1/0/5	0	0	0	0	0	Clear
eth1/0/6	0	0	0	0	0	Clear
eth1/0/7	0	0	0	0	0	Clear
eth1/0/8	0	0	0	0	0	Clear
eth1/0/9	0	0	0	0	0	Clear
eth1/0/10	0	0	0	0	0	Clear

Figure 3-16 PoE Statistics Window

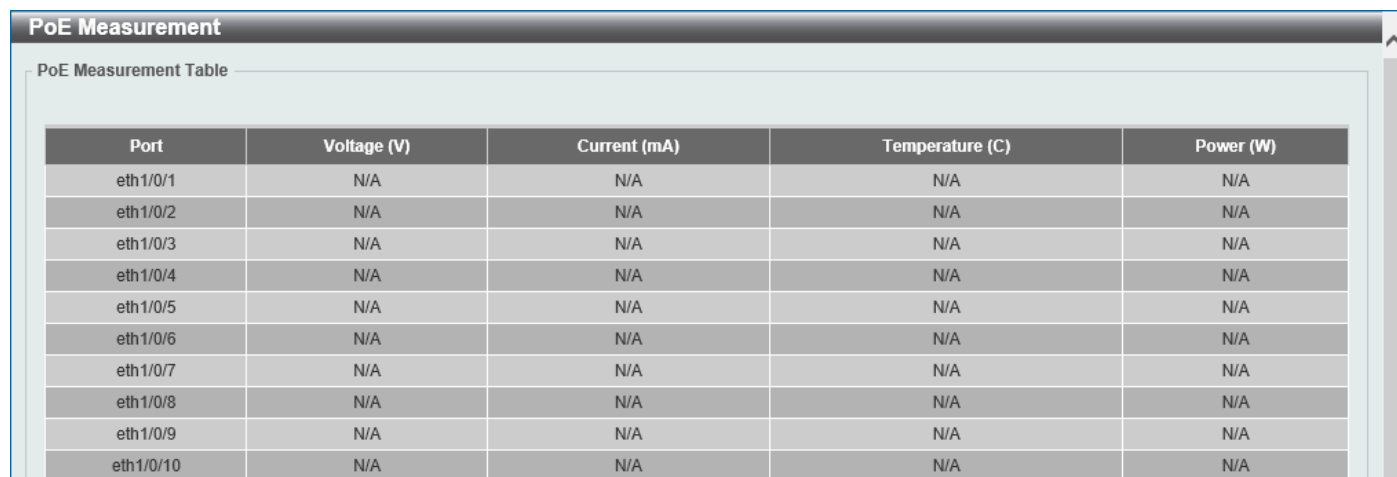
Click the **Clear All** button to clear PoE statistics for all ports.

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 the 'PoE Measurement' window with a title bar and a 'PoE Measurement Table' section. The table has 5 columns: Port, Voltage (V), Current (mA), Temperature (C), and Power (W). There are 10 rows of data for ports eth1/0/1 through eth1/0/10, all showing 'N/A' in the measurement columns.

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 3-17 PoE Measurement 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:

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.

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

Parameter	Description
Console Log State	Select to globally enable or disable the console log state here.

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

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

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

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

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

System Log Discriminator Settings

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

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

System Log Discriminator Settings

Discriminator Log Settings

Discriminator Name: 15 chars

Action: Drops

Severity: Drops

☐ SYS ☐ PORT ☐ STP ☐ LAC ☐ SSH
☐ CLI ☐ WEB ☐ SNMP ☐ ALARM ☐ DDM
☐ AAA ☐ DEVICE ☐ RADIUS ☐ POE ☐ CFG
☐ FIRMWARE ☐ REBOOT_S... ☐ IPV6 ☐ OPENFLOW

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

Apply

Total Entries: 1

Name	Action	Facility List	Severity	Severity List	
Name	Drops	IPV6	Drops	7	Delete

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.

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

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

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

System Log Server Settings

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

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

System Log Server Settings

Log Server

☒ Host IPv4 Address ☐ Host IPv6 Address
 UDP Port (514, 1024-65535) Severity
 Facility Discriminator Name

Apply

Total Entries: 1

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

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

Parameter	Description		
	5	syslog	Messages generated internally by the SYSLOG
	6	lpr	Line printer sub-system
	7	news	Network news sub-system
	8	uucp	UUCP sub-system
	9	clock1	Clock daemon
	10	auth2	Security/authorization messages
	11	ftp	FTP daemon
	12	ntp	NTP subsystem
	13	logaudit	Log audit
	14	logalert	Log alert
	15	clock2	Clock daemon
	16	local0	Local use 0 (local0)
	17	local1	Local use 1 (local1)
	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:

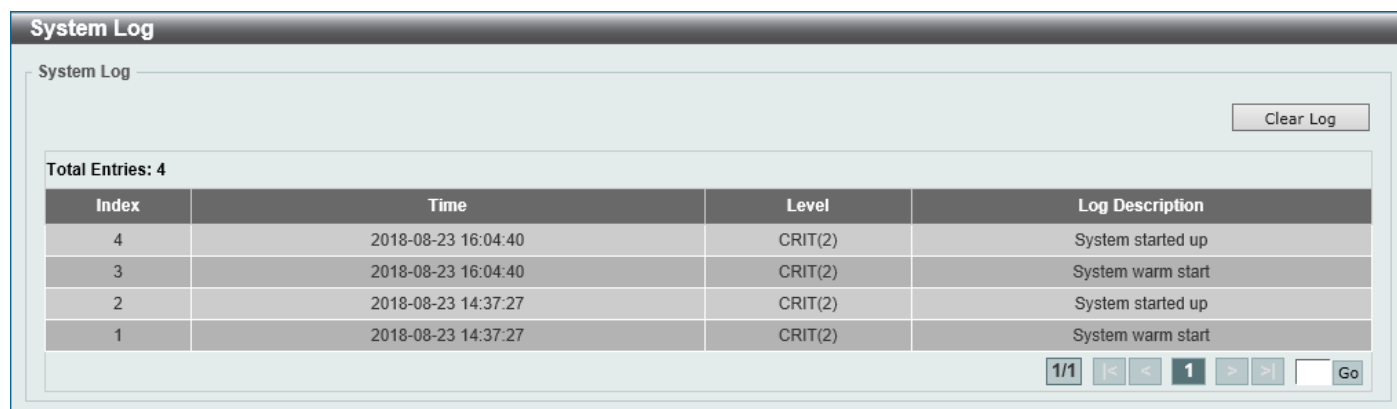


Figure 3-21 System Log Window

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.

Time and SNTP

Clock Settings

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

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

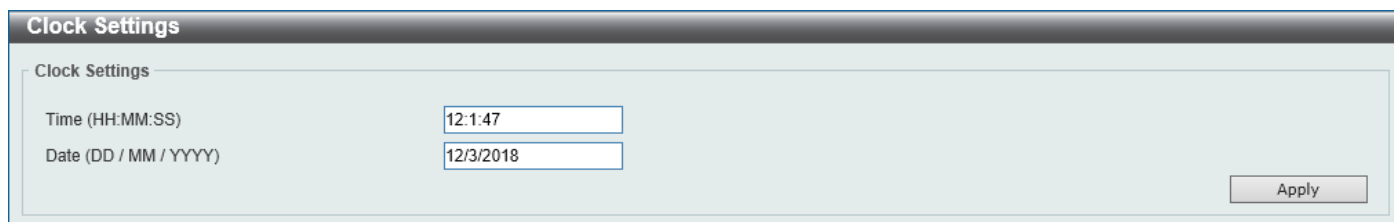


Figure 3-22 Clock Settings Window

The fields that can be configured are described below:

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

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

Time Zone Settings

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

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

Time Zone Settings

Summer Time State: Disabled

Time Zone: + 0 0

Recurring Setting

From: Week of the Month: Last

From: Day of the Week: Sun

From: Month: Jan

From: Time (HH:MM): 00 00

To: Week of the Month: Last

To: Day of the Week: Sun

To: Month: Jan

To: Time (HH:MM): 00 00

Offset: 60

Date Setting

From: Date of the Month: 01

From: Month: Jan

From: Year:

From: Time (HH:MM): 00 00

To: Date of the Month: 01

To: Month: Jan

To: Year:

To: Time (HH:MM): 00 00

Offset: 60

Apply

Figure 3-23 Time Zone Settings Window

The fields that can be configured are described below:

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

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

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

Parameter	Description
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:

SNTP Settings

SNTP Global Settings

Current Time Source: System Clock

SNTP State: Disabled

Poll Interval (30-99999): 720 sec

SNTP Server Setting

☒ IPv4 Address:

☐ IPv6 Address:

Total Entries: 1

SNTP Server	Version	Last Receive	
10.90.90.1	-	-	Delete

Figure 3-24 SNTP Settings Window

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

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

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

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

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

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

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

Time Range

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

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

Figure 3-25 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.

USB Console Settings

This window is used to display and configure the USB console settings.

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

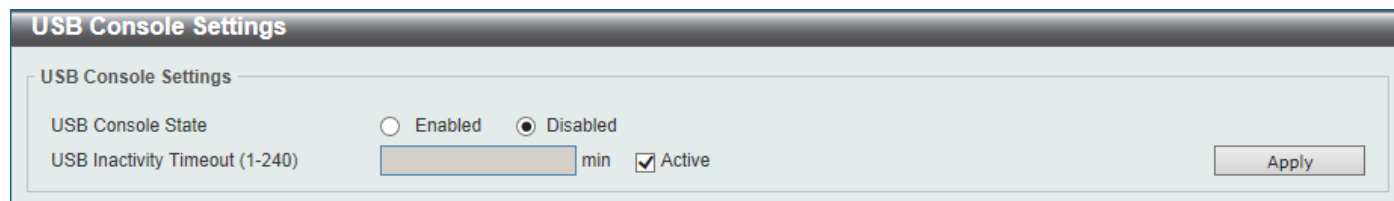


Figure 3-26 USB Console Settings Window

The fields that can be configured are described below:

Parameter	Description
USB Console State	Select to enable or disable the USB console state here.
USB Inactivity Timeout	Enter the USB inactivity timeout value here. The range is from 1 to 240 minutes. Select the Active option to disable the timeout feature.

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



NOTE: When an active console connection is made to both the RJ45 console port and the mini-USB console port at the same time, the mini-USB console port will have higher priority.

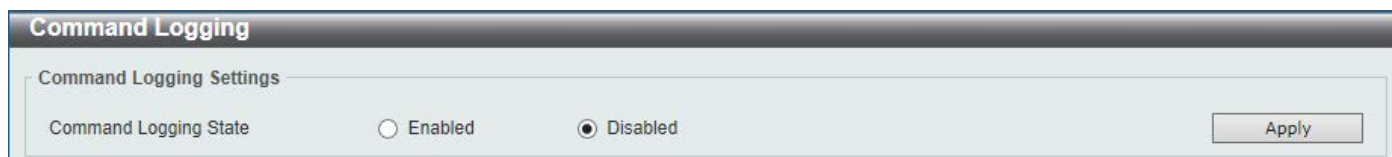
4. Management

[Command Logging](#)
[User Accounts Settings](#)
[CLI Alias Settings](#)
[Password Encryption](#)
[Password Recovery](#)
[Login Method](#)
[SNMP](#)
[RMON](#)
[Telnet/Web](#)
[Session Timeout](#)
[File System](#)
[Reboot Schedule Settings](#)

Command Logging

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

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



The screenshot shows a web interface window titled "Command Logging". Inside, there is a section labeled "Command Logging Settings". Below this, the "Command Logging State" is shown with two radio buttons: "Enabled" and "Disabled". The "Disabled" radio button is selected. An "Apply" button is located on the right side of the settings area.

Figure 4-1 Command Logging Window

The fields that can be configured are described below:

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

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

User Accounts Settings

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

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



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

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

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

User Accounts Settings

User Management Settings | Session Table

User Name: 32 chars | Privilege (1-15): | Password Type: None | Password: | **Apply**

Total Entries: 1

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

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

Figure 4-2 User Accounts Settings Window

The fields that can be configured are described below:

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

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

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

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

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

User Accounts Settings

User Management Settings | **Session Table**

Total Entries: 2

Type	User Name	Privilege	Login Time	IP Address	
console	Anonymous	1	5M10S		
* web	Anonymous	15	4M57S	10.90.90.14	Edit

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

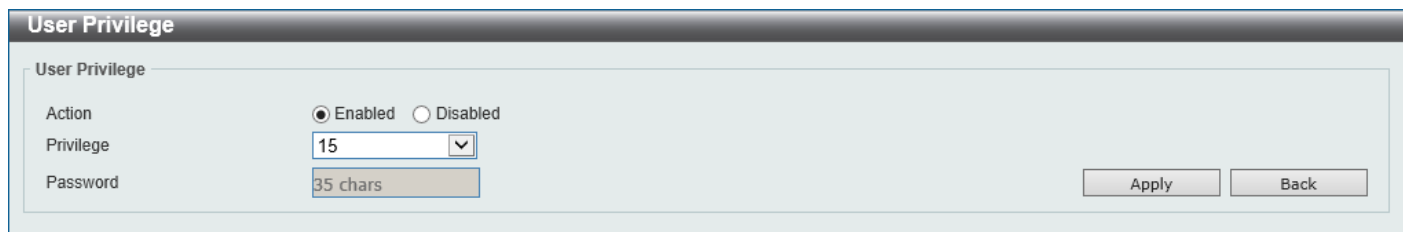
Figure 4-3 Session Table Window

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

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

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

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



The 'User Privilege' window contains the following fields and controls:

- Action:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Privilege:** A dropdown menu showing '15'.
- Password:** A text input field showing '35 chars'.
- Buttons:** 'Apply' and 'Back' buttons on the right side.

Figure 4-4 User Privilege Window

The fields that can be configured are described below:

Parameter	Description
Action	Select to enable or disable user level security.
Privilege	Select the privilege level here. The range is from 1 to 15.
Password	Enter the password here. This can be up to 35 characters long.

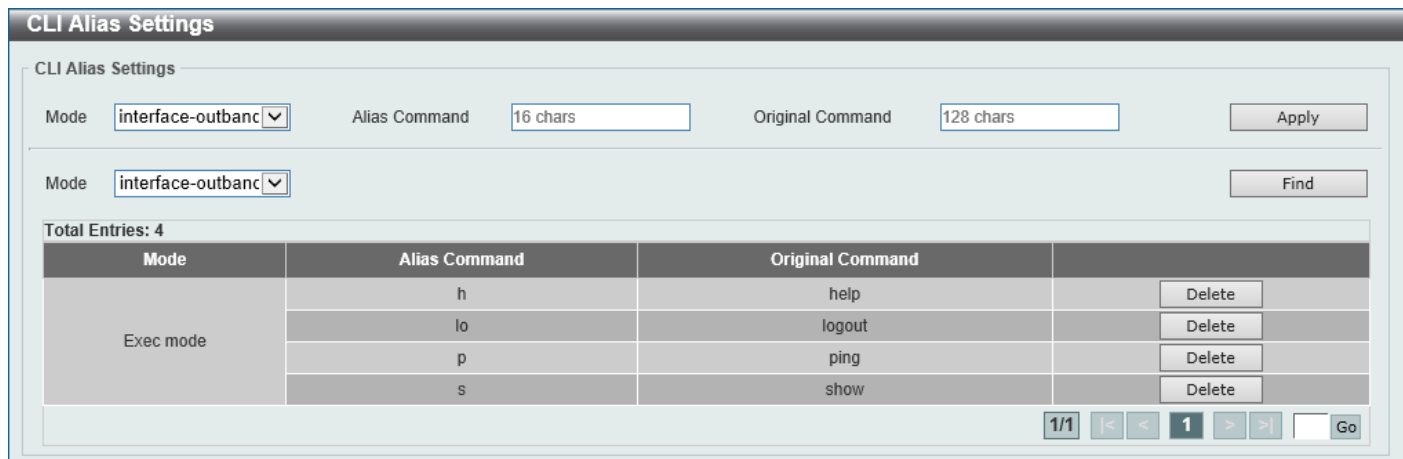
Click the **Apply** button to accept the changes made.

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

CLI Alias Settings

This window is used to display and configure the CLI alias settings. A CLI alias command is a custom string that can be associated with a specific CLI command. This is useful if repeated use of long commands are needed in the CLI.

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



The 'CLI Alias Settings' window contains the following fields and controls:

- Mode:** A dropdown menu showing 'interface-outband'.
- Alias Command:** A text input field showing '16 chars'.
- Original Command:** A text input field showing '128 chars'.
- Buttons:** 'Apply' and 'Find' buttons on the right side.
- Total Entries: 4**
- Table:**

Mode	Alias Command	Original Command	
Exec mode	h	help	Delete
	lo	logout	Delete
	p	ping	Delete
	s	show	Delete
- Page Navigation:** '1/1', '<<', '<', '1', '>', '>>', and 'Go' buttons.

Figure 4-5 CLI Alias Settings Window

The fields that can be configured are described below:

Parameter	Description
Mode	Select the command mode of the original command here.
Alias Command	Enter the alias command here. This can be up to 16 characters long.
Original Command	Enter the original command here. This can be up to 128 characters long.

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

Click the **Find** button to find and displays the CLI alias commands based on the command mode selected.

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.

Password Encryption

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

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

Figure 4-6 Password Encryption Window

The fields that can be configured are described below:

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

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

Password Recovery

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

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

Figure 4-7 Password Recovery Window

The fields that can be configured are described below:

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

Parameter	Description
	can be disabled to allow local authentication. The running configuration can then be saved as the startup configuration. A reboot is required.

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

Login Method

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

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

Login Method

Enable Password

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

Login Method

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

Login Password

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

Application	Password	
SSH	*****	[Delete]

Figure 4-8 Login Method Window

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

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

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

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

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

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

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

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

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

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

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

SNMP

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

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

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

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

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

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

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

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

MIBs

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

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

Traps

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

SNMP Global Settings

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

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

Figure 4-9 SNMP Global Settings Window

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

Parameter	Description
SNMP Global State	Select this option to enable or disable the SNMP feature.
SNMP Response Broadcast Request	Select this option to enable or disable the server to response to broadcast SNMP GetRequest packets.
SNMP UDP Port	Enter the SNMP UDP port number.

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

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

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

SNMP Linkchange Trap Settings

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

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

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

Figure 4-10 SNMP Linkchange Trap Settings Window

The fields that can be configured are described below:

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

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

SNMP View Table Settings

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

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

SNMP View Table Settings

SNMP View Settings

View Name *

Subtree OID *

View Type

* Mandatory Field

Total Entries: 8

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

Figure 4-11 SNMP View Table Settings Window

The fields that can be configured are described below:

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

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

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

SNMP Community Table Settings

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

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

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

Figure 4-12 SNMP Community Table Settings Window

The fields that can be configured are described below:

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

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

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

SNMP Group Table Settings

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

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

SNMP Group Table Settings

SNMP Group Settings

Group Name * Read View Name

User-based Security Model Write View Name

Security Level Notify View Name

* Mandatory Field Add

Total Entries: 5

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

Figure 4-13 SNMP Group Table Settings Window

The fields that can be configured are described below:

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

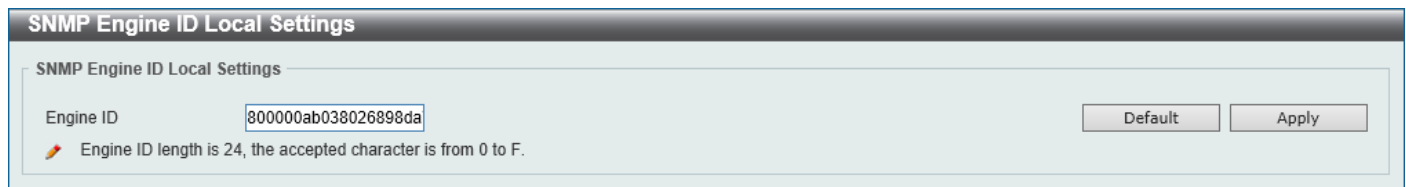
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Engine ID Local Settings

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

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



The screenshot shows the 'SNMP Engine ID Local Settings' window. It has a title bar with the same name. Below the title bar, there's a section titled 'SNMP Engine ID Local Settings'. Inside this section, there is a text input field for 'Engine ID' containing the value '800000ab038026898da'. To the right of the input field are two buttons: 'Default' and 'Apply'. Below the input field, there is a small warning icon and a message: 'Engine ID length is 24, the accepted character is from 0 to F.'

Figure 4-14 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

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

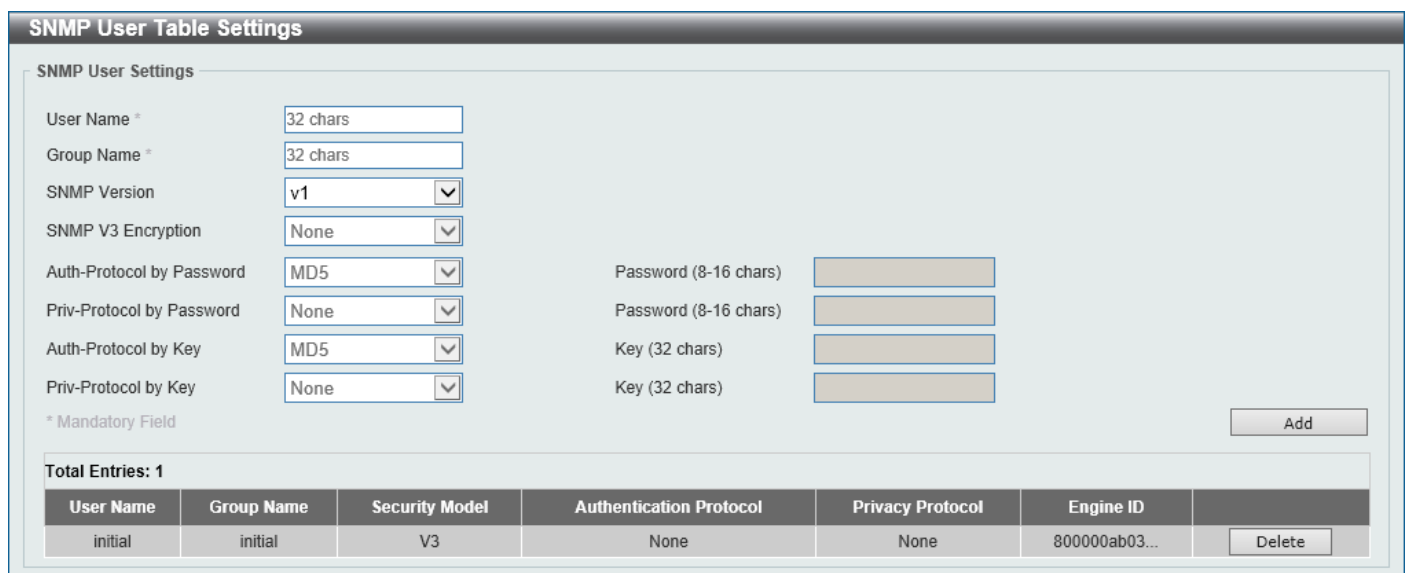
Click the **Default** button to revert the engine ID to the default.

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

SNMP User Table Settings

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

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



The screenshot shows the 'SNMP User Table Settings' window. It has a title bar with the same name. Below the title bar, there's a section titled 'SNMP User Settings'. Inside this section, there are several configuration fields: 'User Name *' (32 chars), 'Group Name *' (32 chars), 'SNMP Version' (v1), 'SNMP V3 Encryption' (None), 'Auth-Protocol by Password' (MD5), 'Priv-Protocol by Password' (None), 'Auth-Protocol by Key' (MD5), and 'Priv-Protocol by Key' (None). To the right of these fields, there are four input fields for 'Password (8-16 chars)' and 'Key (32 chars)'. At the bottom right of the settings section is an 'Add' button. Below the settings section, there is a table showing the current configuration. The table has 7 columns: 'User Name', 'Group Name', 'Security Model', 'Authentication Protocol', 'Privacy Protocol', 'Engine ID', and 'Delete'. There is one entry in the table with the following values: 'initial', 'initial', 'V3', 'None', 'None', '800000ab03...', and a 'Delete' button. Above the table, it says 'Total Entries: 1'. Below the table, there is a note: '* Mandatory Field'.

Figure 4-15 SNMP User Table Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter SNMP user name here. This name can be up to 32 characters long. This is used to identify the SNMP user.

Parameter	Description
Group Name	Enter the SNMP group name to which the user belongs. This name can be up to 32 characters long. Spaces are not allowed.
SNMP Version	Select the SNMP version. Options to choose from are v1 , v2c , and v3 .
SNMP V3 Encryption	When selecting v3 in the SNMP Version drop-down list, this option is available. Options to choose from are None , Password , and Key .
Auth-Protocol by Password	When selecting v3 in the SNMP Version drop-down list, and selecting Password in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are the following: <ul style="list-style-type: none"> • MD5 - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or key. • SHA - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or key.
Password	Enter the Auth-Protocol password here. For MD5 this password must be between 8 and 16 characters long. For SHA this password must be between 8 and 20 characters long.
Priv-Protocol by Password	When selecting v3 in the SNMP Version drop-down list, and selecting Password in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are the following: <ul style="list-style-type: none"> • None - Specify that no authorization protocol is in use. • DES56 - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key. • AES - Specify that Advanced Encryption Standard (AES) encryption is in use. 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 and AES this password must be between 8 and 16 characters long.
Auth-Protocol by Key	When selecting v3 in the SNMP Version drop-down list, and selecting Key in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are the following: <ul style="list-style-type: none"> • MD5 - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. • SHA - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.
Key	Enter the Auth-Protocol key here. For MD5 this key must be 32 characters long. For SHA this key must be 40 characters long.
Priv-Protocol by Key	When selecting v3 in the SNMP Version drop-down list, and selecting Key in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are the following: <ul style="list-style-type: none"> • None - Specify that no authorization protocol is in use. • DES56 - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key. • AES - Specify that AES encryption is in use. 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 and AES this key must be 32 characters long.

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

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

SNMP Host Table Settings

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

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

SNMP Host Table Settings

SNMP Host Settings

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

Add

Total Entries: 1

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

Figure 4-16 SNMP Host Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	Select the security model here. Options to choose from are SNMPv1 , SNMPv2c , and SNMPv3 . <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 manger will be encrypted.
UDP Port	Enter the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string or SNMPv3 user name to be sent with the notification packet.

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

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

RMON

RMON Global Settings

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

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

Figure 4-17 RMON Global Settings Window

The fields that can be configured are described below:

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

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

RMON Statistics Settings

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

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

Figure 4-18 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

RMON Statistics Table

Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
1	eth1/0/1	335205	2348	29	143	0	0	0	0	0	0	148	1835	59	57	201	196	0

Back

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

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

RMON History Settings

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

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

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

Figure 4-20 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.

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

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

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

Figure 4-22 RMON Alarm Settings Window

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 **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:

Figure 4-23 RMON Event Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

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

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

Telnet/Web

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

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

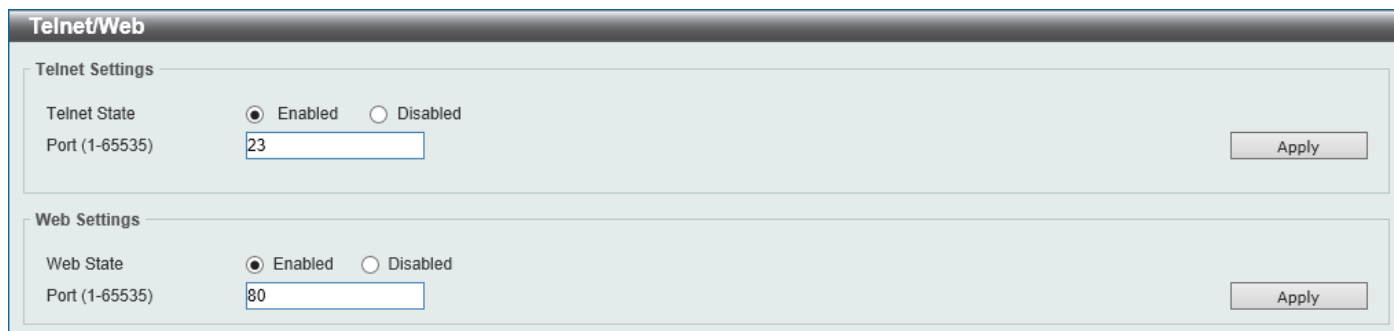


Figure 4-25 Telnet/Web Window

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

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

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

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

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

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

Session Timeout

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

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

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

Apply

Figure 4-26 Session Timeout Window

The fields that can be configured are described below:

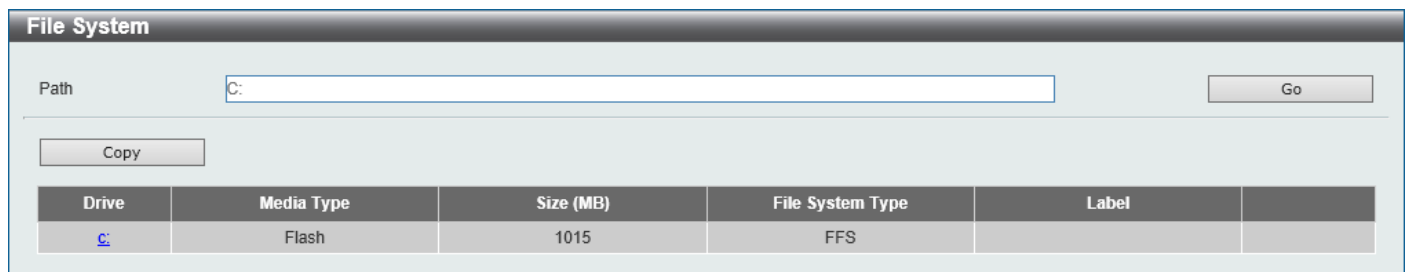
Parameter	Description
Web Session Timeout	Enter the web session timeout value here. The range is from 60 to 36000 seconds. The default value is 180 seconds. Select the Default option to use the default value.
Console Session Timeout	Enter the console session timeout value here. The range is from 0 to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

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

File System

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

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



The File System window shows a 'Path' input field with 'C:' entered and a 'Go' button. Below the input field is a 'Copy' button. A table displays the file system details:

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

Figure 4-27 File System Window

The fields that can be configured are described below:

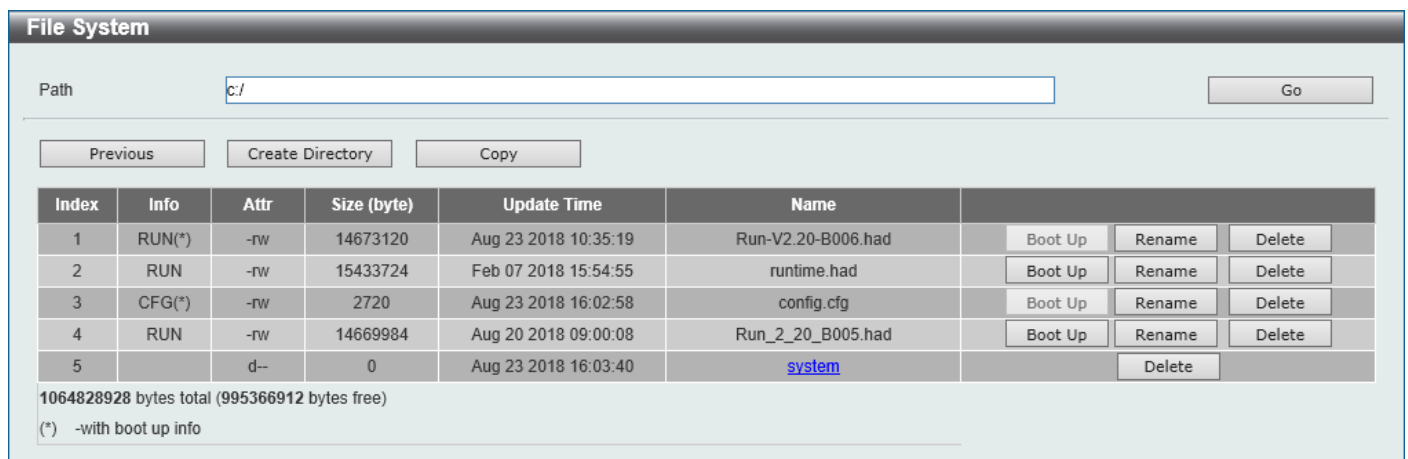
Parameter	Description
Path	Enter the path string.

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

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

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

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



The File System (Drive) window shows the 'Path' input field with 'c:/'. Below the input field are buttons for 'Previous', 'Create Directory', and 'Copy'. A table lists files and directories with columns for Index, Info, Attr, Size (byte), Update Time, and Name. Each row has 'Boot Up', 'Rename', and 'Delete' buttons. At the bottom, it shows '1064828928 bytes total (995366912 bytes free)' and a note: '(*) -with boot up info'.

Index	Info	Attr	Size (byte)	Update Time	Name
1	RUN(*)	-rw	14673120	Aug 23 2018 10:35:19	Run-V2.20-B006.had
2	RUN	-rw	15433724	Feb 07 2018 15:54:55	runtime.had
3	CFG(*)	-rw	2720	Aug 23 2018 16:02:58	config.cfg
4	RUN	-rw	14669984	Aug 20 2018 09:00:08	Run_2_20_B005.had
5		d--	0	Aug 23 2018 16:03:40	system

Figure 4-28 File System (Drive) Window

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

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

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

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

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

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

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



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



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

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

Figure 4-29 File System (Copy) Window

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

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

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

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

Reboot Schedule Settings

This window is used to display and configure the reboot schedule settings. Use this window to configure the reboot schedule of the Switch. The reboot schedule must take effect within 30 days. After the reboot schedule has taken effect and the Switch is restarted, it will generate a log message to identify that the Switch has been restarted using the reboot schedule. After a reboot or a shutdown, the reboot schedule will be deleted automatically. If the Switch was manually rebooted or powered off, before the reboot schedule could take effect, the specified reboot schedule will be cancelled.

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

Figure 4-30 Reboot Schedule Settings Window

The fields that can be configured are described below:

Parameter	Description
Time Interval	Select and enter the reboot schedule time interval value here. The reboot will be initiated after the specified time interval has passed. The range is from 1 to 43200 minutes (30 days).
Time	Select and enter the time at which the reboot should be initiated here. This time uses the 24-hour format, for example, 21:30. If the date was not specified, the reboot will be initiated when the system clock reaches the time specified within the next 24 hours.
Date	Select and enter the date at which the reboot should be initiated here. This date uses the following format: DD/MM/YYYY. For example, 23/12/2015. The reboot schedule can only be initiated within 30 days of configuration.
Save Before Reboot	Select this option to save all configuration changes made before the reboot is initiated.

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

Click the **Delete** button to remove the specified reboot schedule.

5. Layer 2 Features

FDB
VLAN
STP
Link Aggregation

FDB

Static FDB

Unicast Static FDB

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

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

Unicast Static FDB

Unicast Static FDB

Port VID (1-4094) MAC Address

Total Entries: 1

VID	MAC Address	Port
1	00-11-22-33-44-55	eth1/0/6

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.

Multicast Static FDB

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

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

Figure 5-2 Multicast Static FDB Window

The fields that can be configured are described below:

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

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

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

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

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

MAC Address Table Settings

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

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

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

The fields that can be configured are described below:

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

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

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

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

Figure 5-4 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.

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

VID	Status
1	Enabled

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

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used in this configuration or display here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen.

Parameter	Description
Status	Select to enable or disable the MAC address learning function on the VLAN(s) specified here.

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

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

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

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

MAC Address Table

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

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

VID	MAC Address	Type	Port
1	00-11-22-33-44-55	Static	eth1/0/6
1	00-23-7D-BC-08-44	Dynamic	eth1/0/1
1	00-FF-47-77-70-B8	Dynamic	eth1/0/1
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/1
1	D0-AE-EC-D9-9E-5E	Dynamic	eth1/0/1
1	F0-7D-68-30-36-00	Static	CPU
1	01-00-00-00-00-02	Static	eth1/0/7

Figure 5-6 MAC Address Table Window

The fields that can be configured are described below:

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

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

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

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

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

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

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

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

MAC Notification

This window is used to display and configure MAC notification.

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

MAC Notification

MAC Notification Settings | **MAC Notification History**

MAC Notification Global Settings

MAC Address Notification: ☐ Enabled ☒ Disabled

Interval (1-2147483647): sec

History Size (0-500):

MAC Notification Trap State: ☐ Enabled ☒ Disabled

Trap Type:

Apply

From Port: To Port: Added Trap: Removed Trap: **Apply**

Port	Added Trap	Removed Trap
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled

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

The fields that can be configured are described below:

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

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

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

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

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

VLAN

802.1Q VLAN

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

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

Figure 5-9 802.1Q VLAN Window

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

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

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

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

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

Parameter	Description
VID	Enter the VLAN ID that will be displayed here.

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

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

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

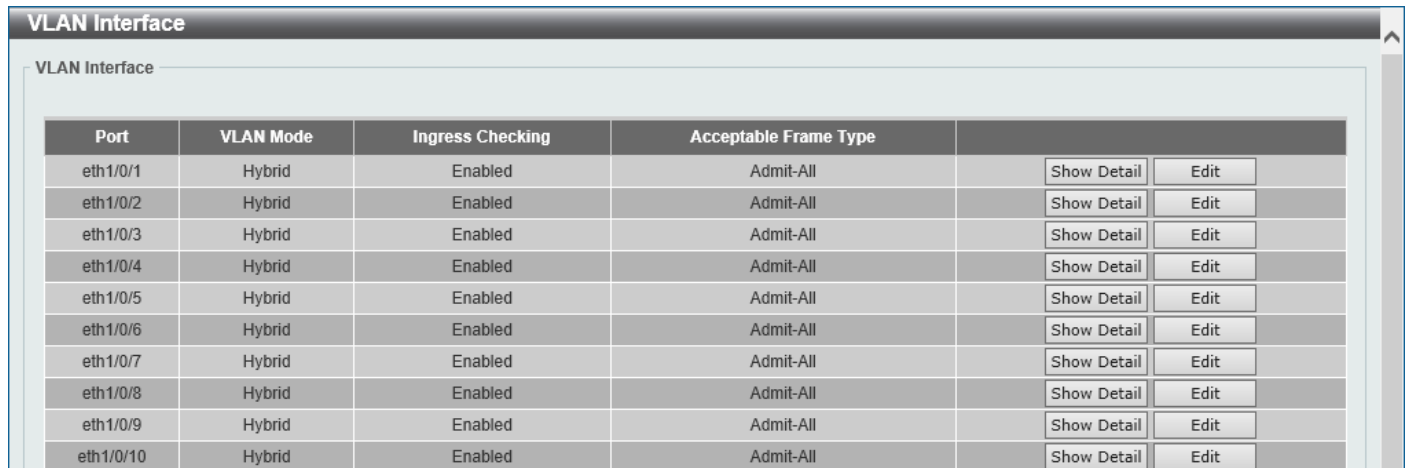
Click the **Delete** button to remove the specific entry.

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

VLAN Interface

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

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



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

Figure 5-10 VLAN Interface Window

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

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

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



VLAN Interface Information	
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

Back

Figure 5-11 VLAN Interface (VLAN Detail) Window

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

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

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

Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/1

VLAN Mode: Access

Acceptable Frame: Admit All

Ingress Checking: ☒ Enabled ☐ Disabled

VID (1-4094): 1

☐ Clone

From Port: eth1/0/1

To Port: eth1/0/1

Back Apply

Figure 5-12 VLAN Interface (Access) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN ID	Enter the VLAN ID used for this configuration here. 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: eth1/0/1

VLAN Mode: Hybrid

Acceptable Frame: Admit All

Ingress Checking: ☒ Enabled ☐ Disabled

VLAN Precedence: Mac-based VLAN

Native VLAN: ☒ Native VLAN

VID (1-4094): 1

Action: Add

Add Mode: ☒ Untagged ☐ Tagged

Allowed VLAN Range:

Current Hybrid untagged VLAN Range: 1

Current Hybrid tagged VLAN Range:

☐ Clone

From Port: eth1/0/1

To Port: eth1/0/1

Back Apply

Figure 5-13 VLAN Interface (Hybrid) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select to enable or disable the ingress checking function.
VLAN Precedence	Select the VLAN precedence option here. Options to choose from are Mac-based VLAN and Subnet-based VLAN .
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. The title bar says 'Configure VLAN Interface'. Inside, there's a sub-header 'Configure VLAN Interface'. The configuration is for port 'eth1/0/1'. The 'VLAN Mode' is set to 'Trunk'. 'Acceptable Frame' is 'Admit All'. 'Ingress Checking' has radio buttons for 'Enabled' (selected) and 'Disabled'. 'Native VLAN' has a checked checkbox and radio buttons for 'Untagged' and 'Tagged'. 'VID (1-4094)' is set to '1'. 'Action' is 'None'. There are 'From Port' and 'To Port' dropdowns, both set to 'eth1/0/1'. A 'Clone' checkbox is unchecked. At the bottom right are 'Back' and 'Apply' buttons.

Figure 5-14 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.

Parameter	Description
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.
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.

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:

Figure 5-15 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.

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:

Figure 5-16 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 1 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out.
NNI BPDU Address	Select the NNI BPDU Address option here. Options to choose from are Dot1d and Dot1ad . By default, this option is Dot1d . This parameter is used to determine the BPDU protocol address for STP in the service provider network. It can use an 802.1d STP address and an 802.1ad service provider STP address.

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

STP Port Settings

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

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

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

Figure 5-17 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 Network, Disabled, and Edge.</p> <ul style="list-style-type: none"> In the Network mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the Disable mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. <p>By default, this option is Network.</p>

Parameter	Description
TCN Filter	Select to enable or disable the TCN Filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is Disabled .
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is Disabled .
Priority	Select the priority value here. Options to choose from are 0 to 240 . By default this option is 0 . A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between 1 and 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.
Loop Guard	<p>Select to enable or disable the Loop Guard feature on the specified port(s) here.</p> <p>The STP Loop Guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the Forwarding state. This usually happens because one of the ports in a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs.</p> <p>When one of the ports in a physically redundant topology no longer receives BPDUs, the STP considers the topology to be loop free. Eventually, an alternate port that was previously a Blocking or Backup port becomes Designated and moves to a Forwarding state. This situation creates a loop.</p>

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

MST Configuration Identification

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

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

MST Configuration Identification

MST Configuration Identification

Configuration Name: F0:7D:68:30:36:00

Revision Level (0-65535): 0

Digest: AC36177F50283CD4B83821D8AB26DE62

Apply

Private VLAN Synchronize

Private VLAN Synchronize

Apply

Instance ID Settings

Instance ID (1-64):

Action: Add VID

VID List: 1 or 3-5

Apply

Total Entries: 1

Instance ID	VID List
CIST	1-4094

Edit Delete

1/1 < < 1 > > Go

Figure 5-18 MST Configuration Identification Window

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

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

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

In the **Private VLAN Synchronize** section, the user can click the **Apply** button to synchronize the private VLANs.

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

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 64.
Action	Select the action that will be taken here. Options to choose from are Add VID and Remove VID .
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

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

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

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

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

STP Instance

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

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

STP Instance

Total Entries: 1

Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	<input type="button" value="Edit"/>

1/1 < < 1 > >

Instance CIST

	CIST Global Info[Mode RSTP]
Bridge Address	F0-7D-68-30-36-00
Designated Root Address / Priority	00-00-00-00-00 / 0
Regional Root Bridge Address / Priority	00-00-00-00-00 / 0
Designated Bridge Address / Priority	00-00-00-00-00 / 0

Figure 5-19 STP Instance Window

The fields that can be configured are described below:

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

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

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

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

MSTP Port Information

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

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

Figure 5-20 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.

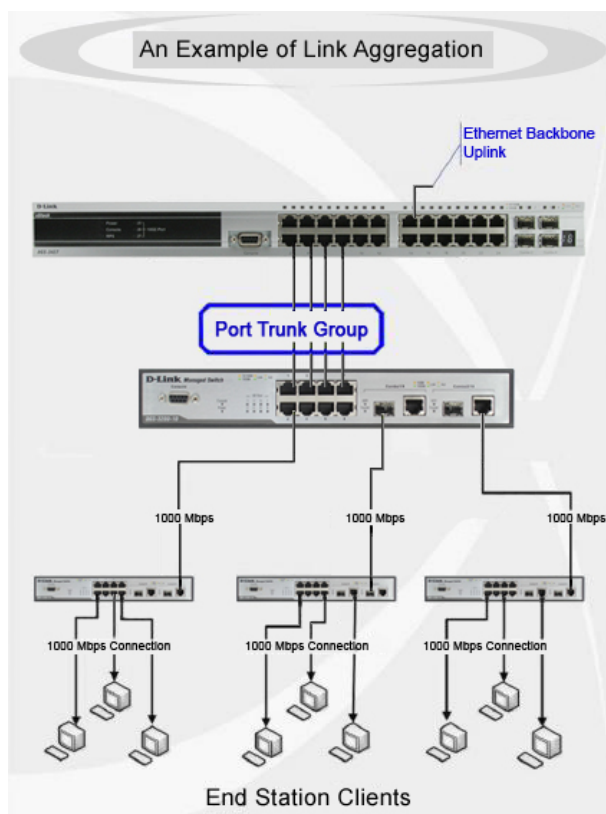
Click the **Edit** button to re-configure the specific entry.

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

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 32 port trunk groups with up to 12 ports in each group.

**Figure 5-21 Example of Port Trunk Group**

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This results in a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link bandwidth intensive network devices, such as servers, to the backbone of a network.

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of up to 12 links (ports). Each port can only belong to a single link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

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



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

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

Link Aggregation

System Priority (1-65535): 32768 Apply

Load Balance Algorithm: Source Destination MAC enhanced MPLS label Apply

System ID: 32768,F0-7D-68-30-36-00

Channel Group Information

From Port: eth1/0/1 To Port: eth1/0/1 Group ID (1-32): Mode: On Add Delete Member Port

Note: Each Channel Group supports up to 12 member ports.

Total Entries: 1

Channel Group	Protocol	Max Ports	Member Number	Member Ports	
Port-channel1	Static	12	4	1/0/20-1/0/23	Delete Channel Show Detail

Figure 5-22 Link Aggregation Window

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

Parameter	Description
System Priority	Enter the system priority value used here. This value must be between 1 and 65535 . By default, this value is 32768 . The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load balancing algorithm that will be used here. Options to choose from are Source MAC , Destination MAC , Source Destination MAC , Source IP , Destination IP , Source Destination IP , Source L4 Port , Destination L4 Port , and Source Destination L4 Port . By default, this option is Source Destination MAC .

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

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

Parameter	Description
From Port - To Port	Select the list of ports that will be associated with this configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 32 . The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are On , Active , and Passive . If the mode On is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

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

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

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

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

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

Port Channel

Port Channel Description Information

Port Channel 1

Description 64 chars

Apply

Port	Status	Administrative	Description
Port-channel1	down	enabled	Delete Description

Port Channel Information

Port Channel 1

Protocol Static

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/20	None	None	down	None	None	Edit
eth1/0/21	None	None	down	None	None	Edit
eth1/0/22	None	None	down	None	None	Edit
eth1/0/23	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
eth1/0/20	None	None	None	None	None
eth1/0/21	None	None	None	None	None
eth1/0/22	None	None	None	None	None
eth1/0/23	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 5-23 Link Aggregation (Channel Detail) Window

The fields that can be configured are described below:

Parameter	Description
Description	Enter the description for the port channel here. This string can be up to 64 characters long.

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

Click the **Delete Description** button to delete the description for the port channel.

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

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

6. Layer 3 Features

[ARP](#)
[IPv6 Neighbor Interface](#)
[IPv4 Static/Default Route](#)
[IPv4 Route Table](#)
[IPv6 Static/Default Route](#)
[IPv6 Route Table](#)

ARP

ARP Aging Time

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

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

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	After click the Edit button, enter the ARP aging timeout value here.

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

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

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

Static ARP

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

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

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:

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

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

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

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

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

IPv6 Neighbor

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

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

Figure 6-4 IPv6 Neighbor Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

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

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

Click the **Clear by Interface** button to clear all the dynamic information for the specific interface.

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

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

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

Interface

IPv4 Interface

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

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

IPv4 Interface

Interface VLAN (1-4094) Apply Find

Total Entries: 1

Interface	State	IP Address	Link Status
vlan1	Enabled	192.168.70.123/255.255.255.0 Manual	Up

Edit Delete

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

Figure 6-5 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.

IPv4 Interface Configure

IPv4 Interface Settings

Interface vlan1 Back

Settings

State Enabled > Apply

Primary IP Settings

Get IP From Static >

IP Address 10 . 90 . 90 . 90

Mask 255 . 0 . 0 . 0 Apply Delete

Figure 6-6 IPv4 Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.
Get IP From	Displays Static which means that the IP address can only be configured manually.
IP Address	Enter the IPv4 address for this interface here.
Mask	Enter the IPv4 subnet mask for this interface here.

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

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

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

IPv6 Interface

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

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

Interface	IPv6 State	Link Status
vlan1	Disabled	Up

Figure 6-7 IPv6 Interface Window

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

Parameter	Description
Interface VLAN	Enter the VLAN interface ID that will be associated with the IPv6 entry.

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

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

Click the **Show Detail** button to view and configure more detailed settings for the IPv6 interface entry.

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

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

Figure 6-8 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.

Parameter	Description
	Select the Default option to specify that if the default router is selected on this interface, a default route will be installed using that default router. This option can only be specified on one interface.

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

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

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here. Select the EUI-64 option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the Link Local option to configure a link-local address for the IPv6 interface.

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

After selecting the **Interface IPv6 Address** tab option, at the top of the page, the following page will be available.

Figure 6-9 IPv6 Interface (Detail, Interface IPv6 Address) Window

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

IPv4 Static/Default Route

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

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

Figure 6-10 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	This field cannot be configured in the OpenFlow mode. Only the Default Route is supported.
Mask	This field cannot be configured in the OpenFlow mode.

Parameter	Description
	Only the Default Route is supported.
Gateway	Enter the gateway address for this route here.

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

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

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

IPv4 Route Table

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

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

IPv4 Route Table

IPv4 Route Table

☒ Show All
☐ Connected

Find

Total Entries: 1

IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
192.168.70.0	255.255.255.0	Directly Connected	vlan1		Connected	-

1/1 < < 1 > > Go

Figure 6-11 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
Show All	Select this option to display all IPv4 routes.
Connected	Select this option to display only connected routes.

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 default IPv6 route settings.

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

Figure 6-12 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	This field cannot be configured in the OpenFlow mode. Only the Default Route is supported.
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.

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

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

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

IPv6 Route Table

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

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

Figure 6-13 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.

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.

7. Security

AAA
RADIUS
TACACS+
SSH
SSL
SFTP Server Settings
Network Protocol Port Protect Settings

AAA

AAA Global Settings

This window is used to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

To view the following window, click **Security > AAA > AAA Global Settings**, as shown below:

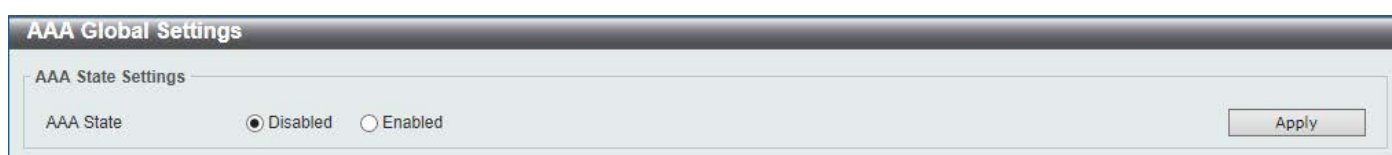


Figure 7-1 AAA Global Settings Window

The fields that can be configured are described below:

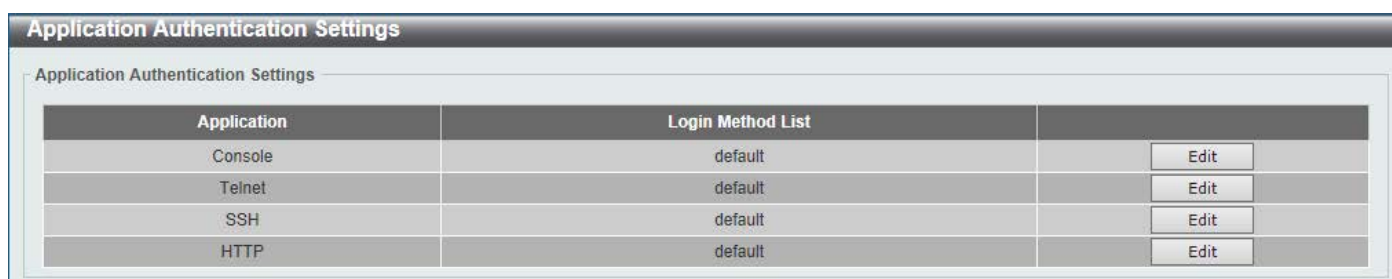
Parameter	Description
AAA State	Select to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

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

Application Authentication Settings

This window is used to display and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:



Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 7-2 Application Authentication Settings Window

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

Application	Login Method List	
Console	<input type="text" value="default"/>	Apply
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 7-3 Application Authentication Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the Edit button for the specific entry, enter the login method list name used here.

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

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

Application Accounting Settings

This window is used to display and configure the application accounting settings.

To view the following window, click **Security > AAA > Application Accounting Settings**, as shown below:

Application	Exec Method List	
Console		Edit
Telnet		Edit
SSH		Edit
HTTP		Edit

Application: Level: Commands Method List:

Total Entries: 1

Application	Level	Commands Method List	
Console	1	method	Delete

1/1 < > 1 > > Go

Figure 7-4 Application Accounting Settings Window

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

Figure 7-5 Application Accounting Settings (Edit) Window

The fields that can be configured in **Application Accounting Exec Method list** are described below:

Parameter	Description
Exec Method List	After clicking the Edit button for the specific entry, enter the EXEC method list name used here.

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

The fields that can be configured in **Application Accounting Commands Method List** are described below:

Parameter	Description
Application	Select the application used here. Options to choose from are Console , Telnet , and SSH .
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
Commands Method List	Enter the commands method list name used here.

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

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

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

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

Authentication Settings

This window is used to display and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:

Figure 7-6 Authentication Settings Window

The fields that can be configured in **AAA Authentication 802.1X** are described below:

Parameter	Description
Status	Select to enable or disable the AAA 802.1X authentication state here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. local - Specifies to use the local database for authentication. group - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. radius - Specifies to use the servers defined by the RADIUS server host command.

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

The fields that can be configured in **AAA Authentication MAC-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA MAC authentication state here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. local - Specifies to use the local database for authentication. group - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. radius - Specifies to use the servers defined by the RADIUS server host command.

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

The fields that can be configured in **AAA Authentication WEB-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA Web authentication state here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. local - Specifies to use the local database for authentication. group - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. radius - Specifies to use the servers defined by the RADIUS server host command.

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

After clicking the **AAA Authentication Exec** tab, the following page will appear.

Figure 7-7 Authentication Settings (AAA Authentication EXEC) Window

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

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> none - Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by previous method authentication. enable - Specifies to use the local enable password for authentication. group - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. radius - Specifies to use the servers defined by the RADIUS server host command. tacacs+ - Specifies to use the servers defined by the TACACS+ server host command.

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

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

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Method 1 ~ Method 4	<p>Select the method lists that will be used for this configuration here. Options to choose from are:</p> <ul style="list-style-type: none"> • none - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method's authentication. • local - Specifies to use the local database for authentication. • group - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • radius - Specifies to use the servers defined by the RADIUS server host command. • tacacs+ - Specifies to use the servers defined by the TACACS+ server host command.

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

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

Accounting Settings

This window is used to display and configure the AAA accounting settings.

To view the following window, click **Security > AAA > Accounting Settings**, as shown below:

Figure 7-8 Accounting Settings Window

The fields that can be configured in **AAA Accounting Network** are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ . The none option is only available for Method 1 .

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

After clicking the **AAA Accounting System** tab, the following page will appear.

Figure 7-9 Accounting Settings (AAA Accounting System) Window

The fields that can be configured in **AAA Accounting System** are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ . The none option is only available for Method 1 .

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

After clicking the **AAA Accounting Exec** tab, the following page will appear.

Figure 7-10 Accounting Settings (AAA Accounting Exec) Window

The fields that can be configured in **AAA Accounting Exec** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA accounting EXEC option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , radius , and tacacs+ . The none option is only available for Method 1 .

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

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

After clicking the **AAA Accounting Commands** tab, the following page will appear.

Figure 7-11 Accounting Settings (AAA Accounting Commands) Window

The fields that can be configured are described below:

Parameter	Description
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
List Name	Enter the method list name that will be used with the AAA accounting commands option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are none , group , and tacacs+ . The none option is only available for Method 1 .

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

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

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

RADIUS

RADIUS Global Settings

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

To view the following window, click **Security > RADIUS > RADIUS Global Settings**, as shown below:

Figure 7-12 RADIUS Global Settings Window

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

Parameter	Description
DeadTime	<p>Enter the dead time value here. This value must be between 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.</p> <p>When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.</p>

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

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

Parameter	Description
RADIUS Server Attribute NAS-IP-Address	Enter the RADIUS server's attribute NAS-IP-Address here.

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

RADIUS Server Settings

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

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:

IPv4/IPv6 Address	Authentication Port	Accounting Port	Timeout	Retransmit	Key	
10.90.90.1	1812	1813	5	2	*****	Delete

Figure 7-13 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.
Accounting Port	Enter the accounting port number used here. This value must be between 0 and 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 3. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 254 characters long.

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

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

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:

RADIUS Group Server Settings

RADIUS Group Server Settings

Group Server Name: 32 chars

☒ IP Address: - . - .

☐ IPv6 Address: 2013::1

Add

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
Group	10.90.90.1...	-	-	-	-	-	-	-	Show Detail
radius	-	-	-	-	-	-	-	-	Delete

Figure 7-14 RADIUS Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IP Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

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

Click the **Show Detail** button to view and configure more detailed settings for the RADIUS group server.

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

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

RADIUS Group Server Settings

Group Server Name: Group

IPv4/IPv6 Address	
10.90.90.16	Delete

Back

Figure 7-15 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

RADIUS Statistic

Group Server Name: Please Select

Total Entries: 1

RADIUS Server Address	Authentication Port	Accounting Port	State
10.90.90.91	1812	1813	Up

1/1

RADIUS Server Address: 10.90.90.91

Parameter	Authentication Port	Accounting Port
Round Trip Time	0	0
Access Requests	0	NA
Access Accepts	0	NA
Access Rejects	0	NA
Access Challenges	0	NA
Acct Request	NA	0
Acct Response	NA	0
Retransmissions	0	0
Malformed Responses	0	0
Bad Authenticators	0	0
Pending Requests	0	0
Timeouts	0	0
Unknown Types	0	0
Packets Dropped	0	0

Figure 7-16 RADIUS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the **Clear** button to clear the information based on the selections made.

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

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

TACACS+

TACACS+ Server Settings

This window is used to display and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Server Settings**, as shown below:

TACACS+ Server Settings

TACACS+ Server Settings

☒ IP Address
☐ IPv6 Address

Port (1-65535)
 Timeout (1-255) sec

Key Type Plain Text
 Key
Apply

Total Entries: 1

IPv4/IPv6 Address	Port	Timeout	Key	
10.90.90.1	49	5	*****	Delete

Figure 7-17 TACACS+ Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server IPv4 address here.
IPv6 Address	Enter the TACACS+ server IPv6 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are Plain Text and Encrypted .
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

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

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

TACACS+ Group Server Settings

This window is used to display and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Group Server Settings**, as shown below:

TACACS+ Group Server Settings

TACACS+ Group Server Settings

Group Server Name
☒ IPv4 Address
☐ IPv6 Address
Add

Total Entries: 2

Group Server Name	IPv4/IPv6 Address	
Group	10.90.90...	Show Detail Delete
tacacs+	-	

Figure 7-18 TACACS+ Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the TACACS+ group server here.
IPv6 Address	Enter the IPv6 address of the TACACS+ group server here.

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

Click the **Show Detail** button to view and configure more detailed settings for the TACACS+ group server.

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

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

Figure 7-19 TACACS+ Group Server Settings (Show Detail) Window

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

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

TACACS+ Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click **Security > TACACS+ > TACACS+ Statistic**, as shown below:

Figure 7-20 TACACS+ Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the information based on the group selected.

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

Click the second **Clear** button to clear all the information for the specific entry.

SSH

Secure Shell (SSH) is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

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

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

Figure 7-21 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' window. It has a title bar 'Host Key'. Below it is a section 'Host Key Management' with two dropdown menus: 'Crypto Key Type' set to 'RSA' and 'Key Modulus' set to '768' with a 'bit' label. To the right are 'Generate' and 'Delete' buttons. Below this is a section 'Host Key' showing the same 'Crypto Key Type' as 'RSA'. It also displays 'Key pair was generated at' as '11:04:36, 2018-03-13', 'Key Size' as '768', and 'Key Data' as a long alphanumeric string starting with 'AAAAB3NzaC1yc2EAAAADAQABAAQQA...'.

Figure 7-22 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. It has a title bar 'Host Key Management'. Below it is a section 'Host Key Management' with a 'Result' field that contains the text 'Generating...'.

Figure 7-23 Host Key (Generating) Window

After the key was successfully generated, the following window will appear.

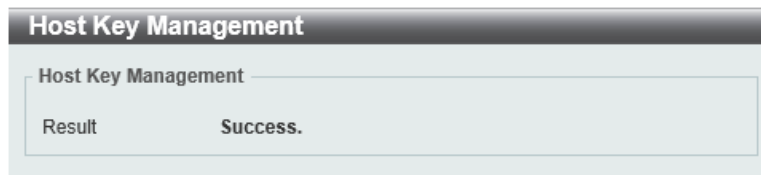


Figure 7-24 Host Key (Generating, Success) Window

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:



Figure 7-25 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:

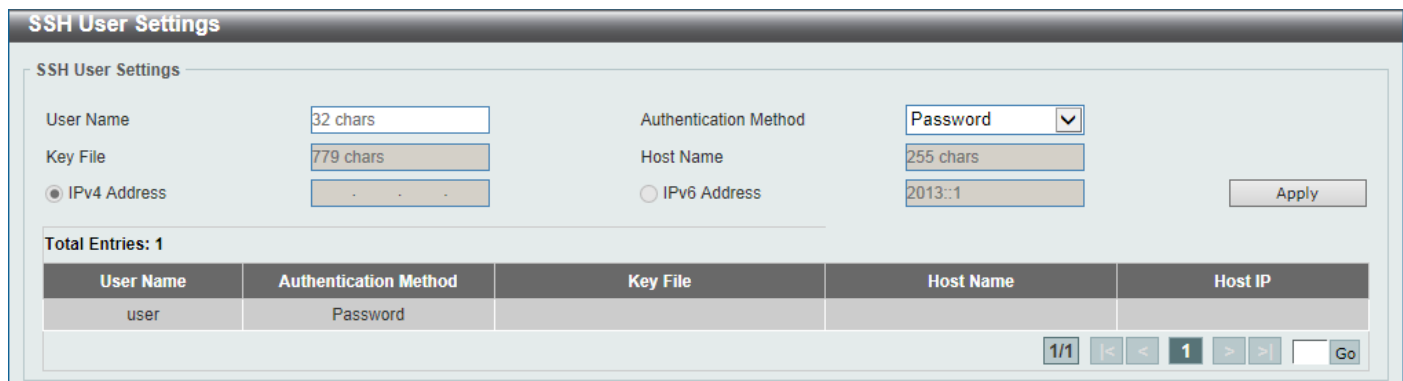


Figure 7-26 SSH User Settings Window

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.

Parameter	Description
Host Name	After selecting the Host-based option as the Authentication Method , enter the host name here.
IPv4 Address	After selecting the Host-based option as the Authentication Method , select and enter the IPv4 address here.
IPv6 Address	After selecting the Host-based option as the Authentication Method , select and enter the IPv6 address here.

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

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

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a server and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and server as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
 - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
 - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) to create the encrypted text.
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA256.

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the client. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server or the Switch file system. The Switch supports TLS 1.0, TLS 1.1, and TLS 1.2. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to server.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https:// (Ex. https://xx.xx.xx.xx). Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

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

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:

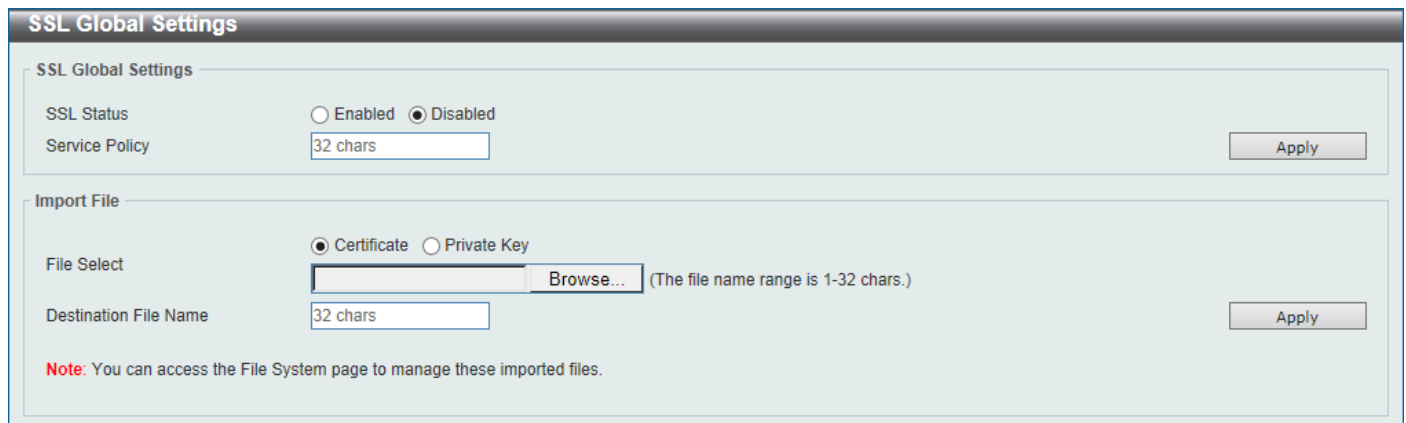


Figure 7-27 SSL Global Settings Window

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

Parameter	Description
SSL Status	Select to enable or disable the global SSL status here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

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

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

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are Certificate and Private Key . After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the Browse button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

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

Crypto PKI Trustpoint

This window is used to display and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:

Figure 7-28 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server path here.
Type	<p>Select the type of certificate that will be imported here. Options to choose from are Both, CA, and Local.</p> <ul style="list-style-type: none"> Selecting Both specifies to import the CA certificate, local certificate and key pairs. Selecting CA specifies to import the CA certificate only. Selecting Local specifies to import local certificate and key pairs only.

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

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

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

SSL Service Policy

This window is used to display and configure the SSL service policy settings.

To view the following window, click **Security > SSL > SSL Service Policy**, as shown below:

Figure 7-29 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.

SFTP Server Settings

This window is used to display and configure the Secure File Transfer Protocol (SFTP) server settings. SFTP is a remotely secure file transfer protocol over a reliable data stream. Because SFTP itself does not provide authentication and security, the SFTP server runs as a sub-system of the SSH server.



NOTE: Only IPv4 SFTP servers are supported.

To view the following window, click **Security > SFTP Server Settings**, as shown below:

Figure 7-30 SFTP Server Settings Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server	Select to globally enable or disable the SFTP server feature here.
Idle Timeout	Enter the idle timeout value here. If the SFTP server detects no operation after the duration of the idle timer for a specific SFTP session, the Switch will close this SFTP session. The range is from 30 to 600 seconds. By default, this value is 120 seconds.

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

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:

Figure 7-31 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.

8. OAM

Cable Diagnostics DDM

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

The screenshot shows the 'Cable Diagnostics' window. At the top, there are two dropdown menus for 'From Port' (set to eth1/0/1) and 'To Port' (set to eth1/0/1). To the right of these is a 'Test' button. Below the dropdowns is a 'Clear All' button. The main part of the window is a table with the following columns: Port, Type, Link Status, Test Result, Cable Length (M), and an action column with 'Clear' buttons. The table contains 10 rows of data for ports eth1/0/1 through eth1/0/10.

Port	Type	Link Status	Test Result	Cable Length (M)	
eth1/0/1	1000BASE-T	Link Up	(OK)	-	Clear
eth1/0/2	1000BASE-T	Link Down	-	-	Clear
eth1/0/3	1000BASE-T	Link Down	-	-	Clear
eth1/0/4	1000BASE-T	Link Down	-	-	Clear
eth1/0/5	1000BASE-T	Link Down	-	-	Clear
eth1/0/6	1000BASE-T	Link Down	-	-	Clear
eth1/0/7	1000BASE-T	Link Down	-	-	Clear
eth1/0/8	1000BASE-T	Link Down	-	-	Clear
eth1/0/9	1000BASE-T	Link Down	-	-	Clear
eth1/0/10	1000BASE-T	Link Down	-	-	Clear

Figure 8-1 Cable Diagnostics Window

The fields that can be configured are described below:

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

Click the **Test** button to test the specific port.

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

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



NOTE: Cable diagnostic function limitations. Cable length detection is only supported on GE ports.



NOTE: The maximum cable diagnosis length is 120 meters.



NOTE: The deviation of cable length detection is about 5 meters for GE ports.

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.

DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP/SFP+ modules inserting to the Switch and to configure alarm settings, warning settings, temperature threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to view and configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:

Port	State	Shutdown
eth1/0/21	Enabled	Alarm
eth1/0/22	Enabled	Alarm
eth1/0/23	Disabled	None
eth1/0/24	Disabled	None
eth1/0/25	Disabled	None
eth1/0/26	Disabled	None
eth1/0/27	Disabled	None
eth1/0/28	Disabled	None

Figure 8-2 DDM Settings Window

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

Parameter	Description
Transceiver Monitoring Traps Alarm	Select to enable or disable the transceiver monitoring traps alarm feature here.
Transceiver Monitoring Traps Warning	Select to enable or disable the transceiver monitoring traps warning feature here.

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

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

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the Alarm or Warning threshold. <ul style="list-style-type: none"> • Alarm - Shutdown the port when the configured alarm threshold range is exceeded. • Warning - Shutdown the port when the configured warning threshold range is exceeded. • None - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

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

DDM Temperature Threshold Settings

This window is used to display and configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:

DDM Temperature Threshold Settings

DDM Temperature Threshold Settings

Port: eth1/0/1 Action: Add Type: Low Alarm Value: (-128-127.996) Celsius [Apply]

Port	Current	High Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)	Low Alarm (Celsius)
eth1/0/21	28.570	78.000	73.000	-8.000	-13.000
eth1/0/22	26.249	78.000	73.000	-8.000	-13.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 8-3 DDM Temperature Threshold Settings Window

The fields that can be configured are described below:

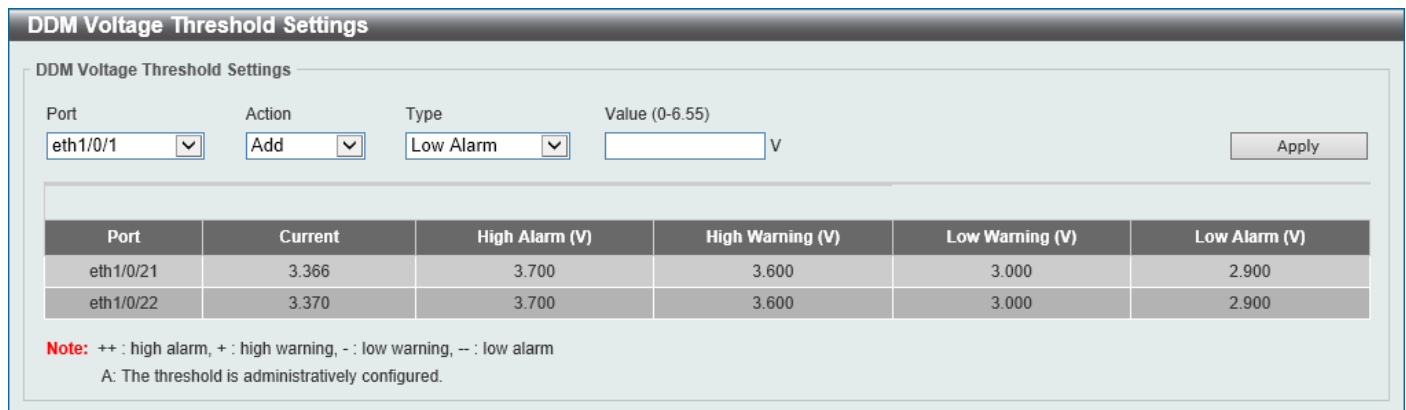
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of temperature threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. This value must be between -128 and 127.996 °C.

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

DDM Voltage Threshold Settings

This window is used to display and configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Voltage Threshold Settings**, as shown below:



Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
eth1/0/21	3.366	3.700	3.600	3.000	2.900
eth1/0/22	3.370	3.700	3.600	3.000	2.900

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 8-4 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

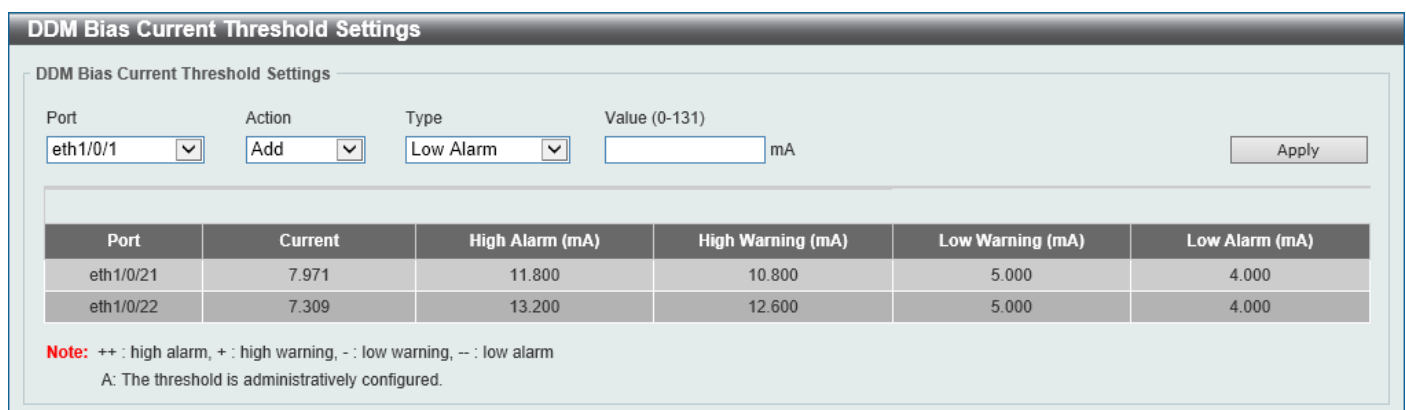
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of voltage threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. This value must be between 0 and 6.55 Volt.

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

DDM Bias Current Threshold Settings

This window is used to display and configure the threshold of the bias current for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Bias Current Threshold Settings**, as shown below:



Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
eth1/0/21	7.971	11.800	10.800	5.000	4.000
eth1/0/22	7.309	13.200	12.600	5.000	4.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 8-5 DDM Bias Current Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port used for the configuration here.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of bias current threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Value	Enter the threshold value. This value must be between 0 and 131 mA.

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

DDM TX Power Threshold Settings

This window is used to display and configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:

DDM TX Power Threshold Settings

DDM TX Power Threshold Settings

Port: eth1/0/1 Action: Add Type: Low Alarm Power Unit: mW Value (0-6.5535): mW Apply

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
eth1/0/21	0.571	-2.432	0.832	-0.800	0.661	-1.800	0.316	-5.000	0.251	-6.000
eth1/0/22	0.621	-2.069	1.000	0.000	0.794	-1.000	0.316	-5.000	0.251	-6.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 8-6 DDM TX Power Threshold Settings Window

The fields that can be configured are described below:

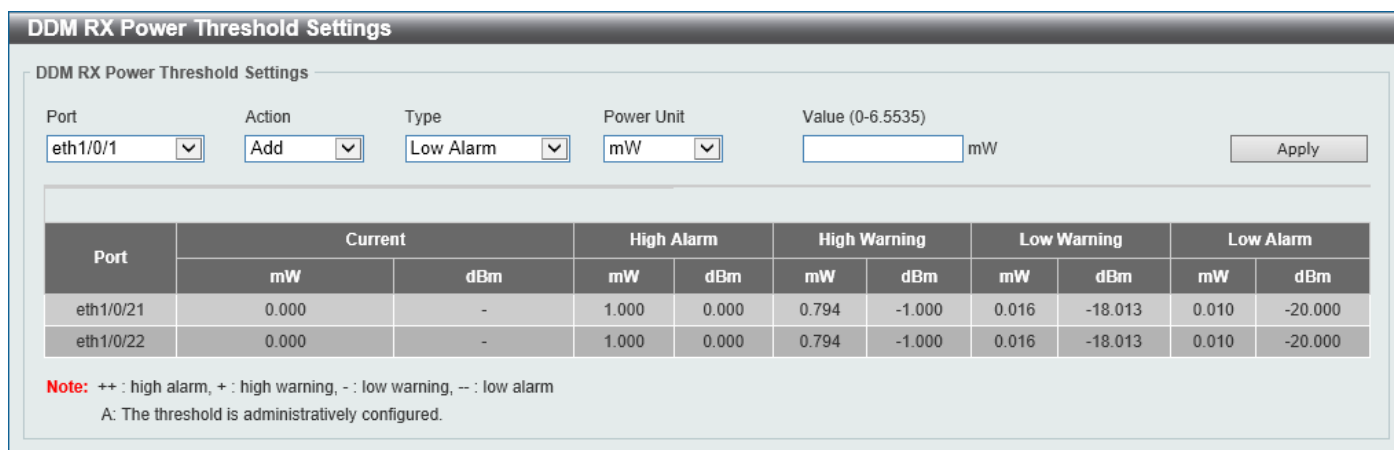
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of TX power threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value either in mW or dBm here. <ul style="list-style-type: none"> When selecting mW in the Power Unit drop-down list, this value must be between 0 and 6.5535. When selecting dBm in the Power Unit drop-down list, this value must be between -40 and 8.1647.

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

DDM RX Power Threshold Settings

This window is used to display and configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:



DDM RX Power Threshold Settings

Port: Action: Type: Power Unit: Value (0-6.5535): mW

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
eth1/0/21	0.000	-	1.000	0.000	0.794	-1.000	0.016	-18.013	0.010	-20.000
eth1/0/22	0.000	-	1.000	0.000	0.794	-1.000	0.016	-18.013	0.010	-20.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 8-7 DDM RX Power Threshold Settings Window

The fields that can be configured are described below:

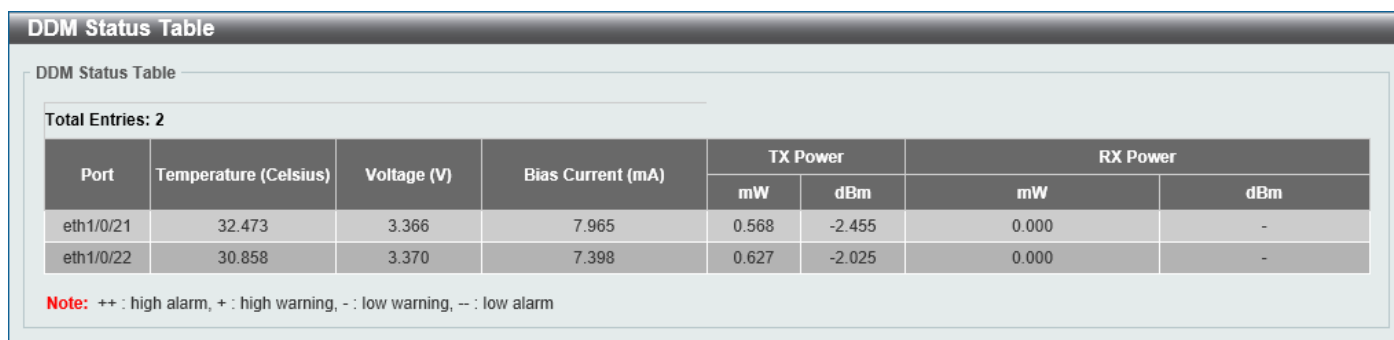
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are Add and Delete .
Type	Select the type of RX power threshold. Options to choose from are Low Alarm , Low Warning , High Alarm , and High Warning .
Power Unit	Select the power unit here. Options to choose from are mW and dBm .
Value	Enter the threshold value either in mW or dBm here. <ul style="list-style-type: none"> When selecting mW in the Power Unit drop-down list, this value must be between 0 and 6.5535. When selecting dBm in the Power Unit drop-down list, this value must be between -40 and 8.1647.

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

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:



DDM Status Table

Total Entries: 2

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
				mW	dBm	mW	dBm
eth1/0/21	32.473	3.366	7.965	0.568	-2.455	0.000	-
eth1/0/22	30.858	3.370	7.398	0.627	-2.025	0.000	-

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm

Figure 8-8 DDM Status Table Window

9. Monitoring

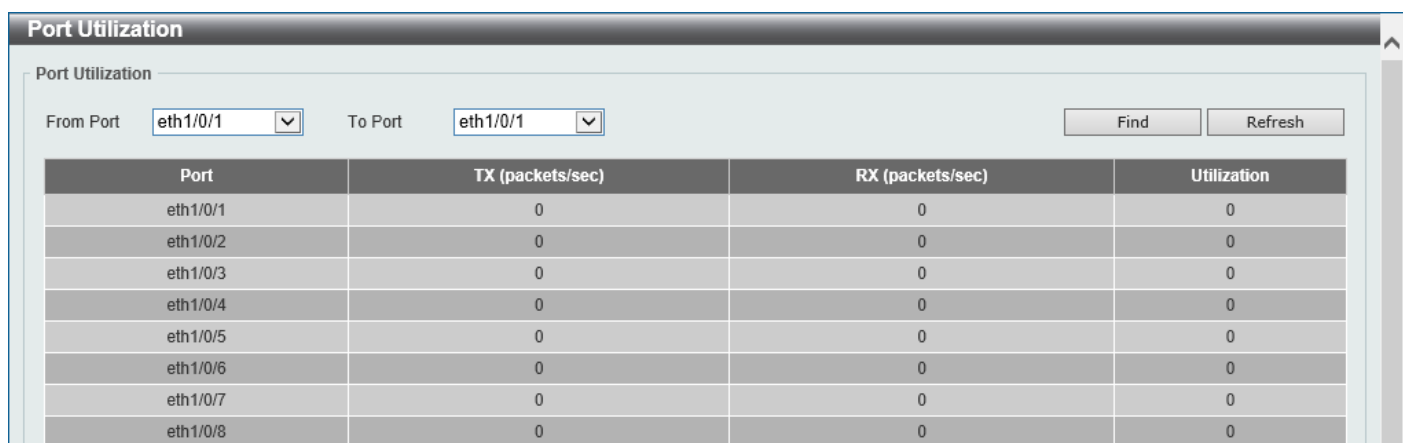
Utilization
Statistics
Device Environment
External Alarm Settings

Utilization

Port Utilization

This window is used to view the port utilization table.

To view the following window, click **Monitoring > Utilization > Port Utilization**, as shown below:



The screenshot shows the 'Port Utilization' window. It has a title bar 'Port Utilization' and a subtitle 'Port Utilization'. Below the subtitle, there are two dropdown menus: 'From Port' and 'To Port', both set to 'eth1/0/1'. To the right of these are two buttons: 'Find' and 'Refresh'. Below these elements is a table with four columns: 'Port', 'TX (packets/sec)', 'RX (packets/sec)', and 'Utilization'. The table contains eight rows of data, all showing zero utilization for the selected ports.

Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	0	0	0
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

Figure 9-1 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.

History Utilization

This window is used to view the memory, CPU and port history utilization.

To view the following window, click **Monitoring > Utilization > History Utilization**, as shown below:

The screenshot shows the 'History Utilization' window with the 'Type' dropdown set to 'Memory'. The 'Time Based' dropdown is set to '15 Minutes' and the 'Slot Index' dropdown is set to 'All'. A 'Find' button is located on the right. Below the filters is a table with the following data:

Type	Start Time	End Time	Utilization
Memory	24 Aug 2018 14:15:56	24 Aug 2018 14: 0:56	37%
Memory	24 Aug 2018 14: 0:56	24 Aug 2018 13:45:56	37%
Memory	24 Aug 2018 13:45:56	24 Aug 2018 13:30:56	37%
Memory	24 Aug 2018 13:30:56	24 Aug 2018 13:15:56	37%
Memory	24 Aug 2018 13:15:56	24 Aug 2018 13: 0:56	37%

Figure 9-2 History Utilization (Memory) Window

After selecting **CPU** as the **Type**, the following window will appear:

The screenshot shows the 'History Utilization' window with the 'Type' dropdown set to 'CPU'. The 'Time Based' dropdown is set to '15 Minutes' and the 'Slot Index' dropdown is set to 'All'. A 'Find' button is located on the right. Below the filters is a table with the following data:

Type	Start Time	End Time	Utilization
CPU	24 Aug 2018 14:16:16	24 Aug 2018 14: 1:16	13%
CPU	24 Aug 2018 14: 1:16	24 Aug 2018 13:46:16	13%
CPU	24 Aug 2018 13:46:16	24 Aug 2018 13:31:16	13%
CPU	24 Aug 2018 13:31:16	24 Aug 2018 13:16:16	13%
CPU	24 Aug 2018 13:16:16	24 Aug 2018 13: 1:16	13%

Figure 9-3 History Utilization (CPU) Window

After selecting **Port** as the **Type**, the following window will appear:

The screenshot shows the 'History Utilization' window with the 'Type' dropdown set to 'Port'. The 'From Port' dropdown is set to 'eth1/0/1' and the 'To Port' dropdown is set to 'eth1/0/1'. The 'Time Based' dropdown is set to '15 Minutes' and the 'Slot Index' dropdown is set to 'All'. A 'Find' button is located on the right. Below the filters is a table with the following data:

Port	Start Time	End Time	Utilization
eth1/0/1	24 Aug 2018 14:16:40	24 Aug 2018 14: 1:40	0%
eth1/0/1	24 Aug 2018 14: 1:40	24 Aug 2018 13:46:40	0%
eth1/0/1	24 Aug 2018 13:46:40	24 Aug 2018 13:31:40	0%
eth1/0/1	24 Aug 2018 13:31:40	24 Aug 2018 13:16:40	0%
eth1/0/1	24 Aug 2018 13:16:40	24 Aug 2018 13: 1:40	0%

Figure 9-4 History Utilization (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the history utilization type to display here. Options to choose from are: <ul style="list-style-type: none"> Memory - Specifies to display the historical memory utilization information. CPU - Specifies to display the historical CPU utilization information. Port - Specifies to display the historical port utilization information.
From Port - To Port	Select the range of ports that will be used here.
Time Based	Select the time-based statistical count value here. Options to choose from are:

Parameter	Description
	<ul style="list-style-type: none"> • 15 Minutes - Specifies to display slots of 15-minute based information. • 1 Day - Specifies to display slots of daily based information. <p>For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.</p>
Slot Index	<p>Select the slot index here.</p> <ul style="list-style-type: none"> • After selecting to use 15 minute slots, the options to choose from are All, and 1 to 5. • After selecting to use 1 day slots, the options to choose from are All, and 1 to 2.

Click the **Find** button to display entries in the table based on the information selected.

Statistics

Port

This window is used to view the port statistics information.

To view the following window, click **Monitoring > Statistics > Port**, as shown below:

The screenshot shows the 'Port' window with a table of statistics. The table has columns for Port, RX Rate (bits/sec, packets/sec), RX Total (bytes, packets), TX Rate (bits/sec, packets/sec), TX Total (bytes, packets), and a 'Show Detail' button for each row. The 'From Port' and 'To Port' are both set to 'eth1/0/1'.

Port	RX				TX				Show Detail
	Rate		Total		Rate		Total		
	bits/sec	packets/sec	bytes	packets	bits/sec	packets/sec	bytes	packets	
eth1/0/1	0	0	5749296	35401	0	0	7083388	9462	Show Detail
eth1/0/2	0	0	0	0	0	0	0	0	Show Detail
eth1/0/3	0	0	0	0	0	0	0	0	Show Detail
eth1/0/4	0	0	0	0	0	0	0	0	Show Detail
eth1/0/5	0	0	0	0	0	0	0	0	Show Detail
eth1/0/6	0	0	0	0	0	0	0	0	Show Detail
eth1/0/7	0	0	0	0	0	0	0	0	Show Detail
eth1/0/8	0	0	0	0	0	0	0	0	Show Detail
eth1/0/9	0	0	0	0	0	0	0	0	Show Detail
eth1/0/10	0	0	0	0	0	0	0	0	Show Detail

Figure 9-5 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:

Port Detail	
Port Detail	
Back Refresh	
eth1/0/1	
RX rate	14680 bits/sec
TX rate	23720 bits/sec
RX rate	9 packets/sec
TX rate	6 packets/sec
RX bytes	13081971
TX bytes	13293331
RX packets	62205
TX packets	26438
RX multicast	16916
RX broadcast	0
RX CRC error	0
RX undersize	0
RX fragment	0
RX dropped Pkts	16684
RX MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0
TX late collision	0
TX collision	0

Figure 9-6 Port (Show Detail) Window

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

Click the **Refresh** button to refresh the information displayed in the table.

Interface Counters

This window is used to view the interface counter information.

To view the following window, click **Monitoring > Statistics > Interface Counters**, as shown below:

Interface Counters

Interface Counters

Type

From Port

To Port

Port

eth1/0/1

eth1/0/1

Find

Refresh

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
eth1/0/1	5816699	33080	2896	6848	9367489	28182	0	2	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

Figure 9-7 Interface Counters (Port) Window

The fields that can be configured are described below:

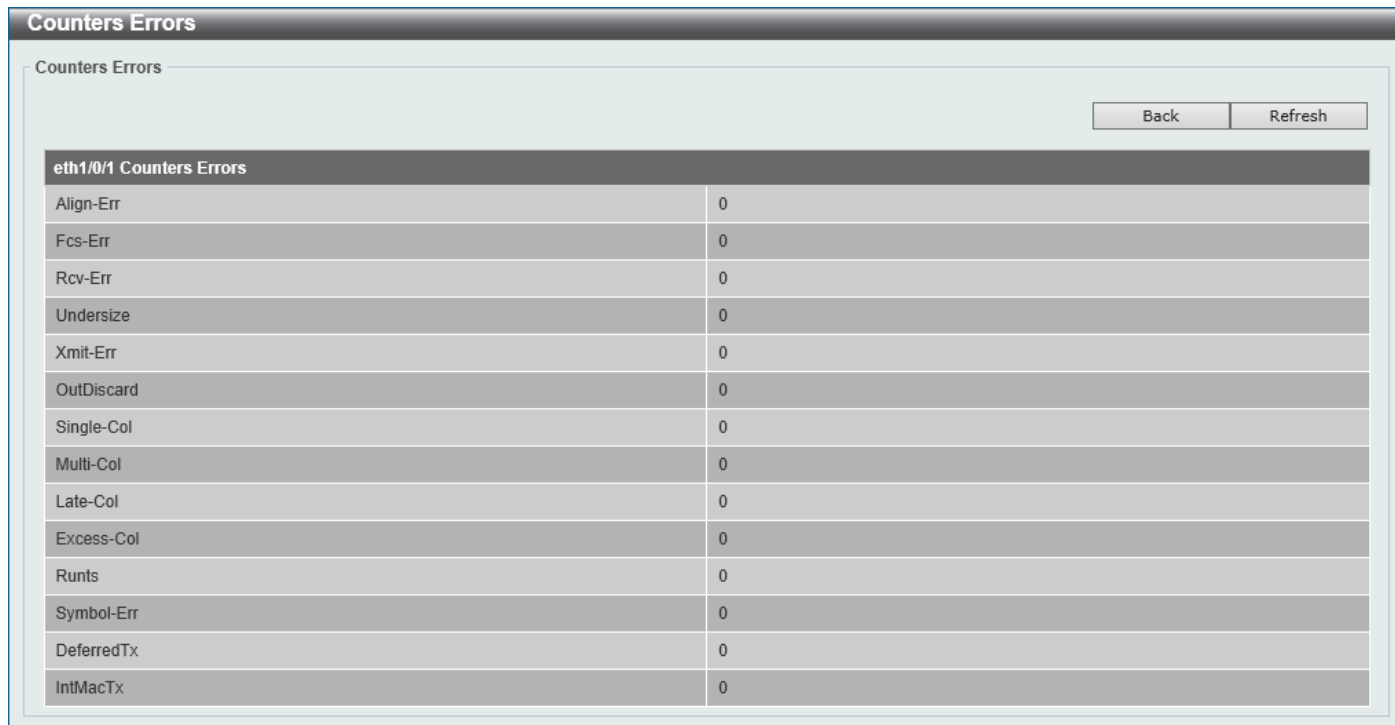
Parameter	Description
Type	Specifies to display port-based counter information.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Errors** button to view more detailed error information on the specified port.

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



Counters Errors	
Counters Errors	
eth1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Undersize	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Multi-Col	0
Late-Col	0
Excess-Col	0
Runts	0
Symbol-Err	0
DeferredTx	0
IntMacTx	0

Figure 9-8 Interface Counters (Show Errors) Window

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

Click the **Refresh** button to refresh the information displayed in the table.

Interface History Counters

This window is used to view the history counter information per interface.

To view the following window, click **Monitoring > Statistics > Interface History Counters**, as shown below:

Frame Size/Type	Frame Count
rxHCTotalPkts	2267
txHCTotalPkts	1172
rxHCUnicastPkts	1680
txHCUnicastPkts	1170
rxHCMulticastPkts	159
txHCMulticastPkts	0
rxHCBroadcastPkts	428
txHCBroadcastPkts	2
rxHCOctets	399337
txHCOctets	613984
rxHCPkt64Octets	1590
rxHCPkt65to127Octets	51
rxHCPkt128to255Octets	59
rxHCPkt256to511Octets	286

Figure 9-9 Interface History Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here.
Port	Select the port that will be used in this display here.
Time Based	<p>Select the time-based statistical count value here. Options to choose from are:</p> <ul style="list-style-type: none"> • 15 Minutes - Specifies to display slots of 15-minute based information. • 1 Day - Specifies to display slots of daily based information. <p>For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.</p>
Slot index	<p>Select the slot index here.</p> <ul style="list-style-type: none"> • After selecting to use 15 minute slots, the options to choose from are All, and 1 to 5. • After selecting to use 1 day slots, the options to choose from are All, and 1 to 2.

Click the **Find** button to display entries in the table based on the information selected/entered.

Counters

This window is used to view and clear counter information.

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:

Port	linkChange	
eth1/0/1	5	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 9-10 Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select to display port-based counter information here.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the counter information displayed in the table.

Click the **Clear** button clear the counter information displayed in the table based on the information selected.

Click the **Clear All** button clear all the counter information displayed in the table.

Click the **Show Detail** button to view more detailed counter information on the specified port.

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

Port Counters Detail	
Port Counters Detail	
<div>Back Refresh</div>	
eth1/0/1 Counters	
rxHCTotalPkts	63777
txHCTotalPkts	37492
rxHCUnicastPkts	50647
txHCUnicastPkts	37094
rxHCMulticastPkts	3534
txHCMulticastPkts	180
rxHCBroadcastPkts	9596
txHCBroadcastPkts	218
txHCOctets	11179584
txHCOctets	12797166
rxHCPkt64Octets	43743
rxHCPkt65to127Octets	2714
rxHCPkt128to255Octets	1155
rxHCPkt256to511Octets	12368
rxHCPkt512to1023Octets	3714
rxHCPkt1024to1518Octets	83
rxHCPkt1519to1522Octets	0
rxHCPkt1519to2047Octets	0
rxHCPkt2048to4095Octets	0
rxHCPkt4096to9216Octets	0
txHCPkt64Octets	2865

Figure 9-11 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.

Device Environment

The device environment feature displays the Switch internal temperature status.

To view the following window, click **Monitoring > Device Environment**, as shown below:

Device Environment

Detail Temperature Status

Unit	Temperature Descr/ID	Current/Threshold Range
1	Central Temperature /1	29C/0~45C

Status code: * temperature is out of threshold range

Detail Fan Status

Items	Status
Right Fan 1	(OK)
Right Fan 2	(OK)
Right Fan 3	(OK)
Right Fan 4	(OK)

Detail Power Status

Unit	Power Module	Power Status
1	Power 1	In-operation
	Power 2	Empty

Figure 9-12 Device Environment Window

External Alarm Settings

This window is used to display and configure the external alarm settings. This is used to enable monitoring the external alarm source status or to configure external alarm message for a channel. The source of alarm is located outside of the Switch and is monitored via pre-defined connecting channels. Each channel represents a specific alarm event. The status of an alarm source can be either in the alarm state or in the normal state. If the source is absent or the source is present and in the normal state, the status will be normal. The status will be abnormal if the source is in the abnormal state. A notification will be sent when the monitoring status is changed.

To view the following window, click **Monitoring > External Alarm Settings**, as shown below:

External Alarm Settings

External Alarm Trap Settings

External Alarm Trap State

☐ Enabled
 ☒ Disabled

Apply

External Alarm Settings

Channel

1

Message

128 chars

Apply

Total Entries: 2

Channel	Status	Message	
1	Normal	External Alarm 1	Default
2	Normal	External Alarm 2	Default

1/1

<<

<

1

>

>>

Go

Figure 9-13 External Alarm Settings Window

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

Parameter	Description
External Alarm Trap State	Select to enable or disable the external alarm trap state here.

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

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

Parameter	Description
Channel	Select the channel to be configured here. The range is from 1 to 2.
Message	Enter the alarm message associated with the channel here. This string can be up to 128 characters long.

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

Click the **Default** button return the entry to the default settings.

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

10. 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 10-1 Power Saving Global Settings Window

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

Parameter	Description
Link Detection Power Saving	Select this option to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Length Detection Power Saving	Select this option to enable or disable the cable length detection power saving feature. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power.
Scheduled Port-shutdown Power Saving	Select this option to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Hibernation Power Saving	Select this option to enable or disable applying the power saving by scheduled hibernation.
Scheduled Dim-LED Power Saving	Select this option to enable or disable applying the power saving by scheduled dimming LEDs.
Administrative Dim-LED	Select this option to enable or disable the port LED function.

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

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

Parameter	Description
Type	Select the type here. Options to choose from are Dim-LED and Hibernation .
Time Range	Enter the name of the time range to associate with the power saving type.

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

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



NOTE: The **hibernation** feature can only be configured when physical stacking is disabled on this Switch.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

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 10-2 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 10-3 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.

11. Save and Tools

Save Configuration
Firmware Upgrade & Backup
Configuration Restore & Backup
Certificate & Key Restore & Backup
Log Backup
Ping
Trace Route
Reset
Reboot System

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

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

Figure 11-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
File Path	Enter the filename and path in the space provided.

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

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

Figure 11-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	In this field the source firmware file's filename and path will be displayed after selection. To navigate to the location of the firmware file located on the local PC, either double click in the text box or click the Browse button.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP**, as shown below:

Figure 11-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from FTP

This window is used to initiate a firmware upgrade from an FTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from FTP**, as shown below:

Figure 11-4 Firmware Upgrade from FTP Window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Enter the FTP server IP address here. When select the IPv4 option, enter the IPv4 address of the FTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the firmware file located on the FTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from RCP

This window is used to initiate a firmware upgrade from an RCP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from RCP**, as shown below:

Figure 11-5 Firmware Upgrade from RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from SFTP

This window is used to initiate a firmware upgrade from an SFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from SFTP**, as shown below:

Figure 11-6 Firmware Upgrade from SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the firmware file located on the SFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

Figure 11-7 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

Figure 11-8 Firmware Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to FTP

This window is used to initiate a firmware backup to an FTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to FTP**, as shown below:

Figure 11-9 Firmware Backup to FTP Window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Enter the FTP server IP address here. When select the IPv4 option, enter the IPv4 address of the FTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the FTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to RCP

This window is used to initiate a firmware backup to an RCP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to RCP**, as shown below:

Figure 11-10 Firmware Backup to RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the RCP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to SFTP

This window is used to initiate a firmware backup to an SFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to SFTP**, as shown below:

Figure 11-11 Firmware Backup to SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the SFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 11-12 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	In this field the source configuration file's filename and path will be displayed after selection. To navigate to the location of the configuration file located on the local PC, either double click in the text box or click the Browse button.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

Figure 11-13 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.

Parameter	Description
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from FTP

This window is used to initiate a configuration restore from an FTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from FTP**, as shown below:

Figure 11-14 Configuration Restore from FTP Window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Enter the FTP server IP address here. When select the IPv4 option, enter the IPv4 address of the FTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the configuration file located on the FTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from RCP

This window is used to initiate a configuration restore from an RCP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from RCP**, as shown below:

Figure 11-15 Configuration Restore from RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> • Select the running-config option to restore and overwrite the running configuration file on the Switch. • Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from SFTP

This window is used to initiate a configuration restore from an SFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from SFTP**, as shown below:

Figure 11-16 Configuration Restore from SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the configuration file located on the SFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to restore and overwrite the running configuration file on the Switch. Select the startup-config option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 11-17 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long.

Parameter	Description
	<ul style="list-style-type: none"> Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

Figure 11-18 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to FTP

This window is used to initiate a configuration file backup to an FTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to FTP**, as shown below:

Figure 11-19 Configuration Backup to FTP Window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Enter the FTP server IP address here. When select the IPv4 option, enter the IPv4 address of the FTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the FTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to RCP

This window is used to initiate a configuration file backup to an RCP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to RCP**, as shown below:

Figure 11-20 Configuration Backup to RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the RCP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to SFTP

This window is used to initiate a configuration file backup to an SFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to SFTP**, as shown below:

Figure 11-21 Configuration Backup to SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. <ul style="list-style-type: none"> Select the running-config option to back up the running configuration file from the Switch. Select the startup-config option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the SFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Certificate & Key Restore & Backup

Certificate & Key Restore from HTTP

This window is used to initiate a certificate and key restore from a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP**, as shown below:

Figure 11-22 Certificate & Key Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	In this field the source certificate and key file's filename and path will be displayed after selection. To navigate to the location of the certificate and key file located on the local PC, either double click in the text box or click the Browse button.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from TFTP

This window is used to initiate a certificate and key restore from a TFTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP**, as shown below:

Figure 11-23 Certificate & Key Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.

Parameter	Description
Source File	Enter the source filename and path of the certificate and key file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from FTP

This window is used to initiate a certificate and key restore from an FTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from FTP**, as shown below:

Figure 11-24 Certificate & Key Restore from FTP Window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Enter the FTP server IP address here. When select the IPv4 option, enter the IPv4 address of the FTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the FTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from RCP

This window is used to initiate a certificate and key restore from an RCP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from RCP**, as shown below:

The screenshot shows a web interface window titled "Certificate & Key Restore from RCP". It contains the following fields:

- RCP Server IP: A text input field.
- User Name: A text input field with a "32 chars" label.
- Source File: A text input field with a "64 chars" label.
- Destination File: A text input field with a "64 chars" label.
- A "Restore" button located at the bottom right of the form area.

Figure 11-25 Certificate & Key Restore from RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from SFTP

This window is used to initiate a certificate and key restore from an SFTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from SFTP**, as shown below:

The screenshot shows a web interface window titled "Certificate & Key Restore from SFTP". It contains the following fields:

- SFTP Server IP: A text input field.
- Authentication Method: A dropdown menu currently set to "Password".
- User Name: A text input field with a "32 chars" label.
- Password: A text input field with a "15 chars" label.
- Source File: A text input field with a "64 chars" label.
- Destination File: A text input field with a "64 chars" label.
- A "Restore" button located at the bottom right of the form area.

Figure 11-26 Certificate & Key Restore from SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the SFTP server here. This field can be up to 64 characters long.

Parameter	Description
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key 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 > Certificate & Key Backup to HTTP**, as shown below:

The screenshot shows a window titled 'Firmware Backup to HTTP'. Inside, there is a 'Source File' label followed by a text input field with a '64 chars' limit. To the right of the input field is a 'Backup' button.

Figure 11-27 Certificate & Key Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Certificate & 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 > Certificate & Key Backup to TFTP**, as shown below:

The screenshot shows a window titled 'Certificate & Key Backup to TFTP'. It contains three input fields: 'TFTP Server IP' with a radio button selection for 'IPv4' (selected) and 'IPv6'; 'Source File' with a '64 chars' limit; and 'Destination File' with a '64 chars' limit. A 'Backup' button is located at the bottom right.

Figure 11-28 Certificate & Key Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.

Parameter	Description
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Certificate & Key Backup to FTP

This window is used to initiate a certificate and key backup to an FTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Certificate & Key Backup to FTP**, as shown below:

Figure 11-29 Certificate & Key Backup to FTP Window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Enter the FTP server IP address here. When select the IPv4 option, enter the IPv4 address of the FTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the FTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Certificate & Key Backup to RCP

This window is used to initiate a certificate and key backup to an RCP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Certificate & Key Backup to RCP**, as shown below:

Figure 11-30 Certificate & Key Backup to RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the RCP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Certificate & Key Backup to SFTP

This window is used to initiate a certificate and key backup to an SFTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Certificate & Key Backup to SFTP**, as shown below:

Figure 11-31 Certificate & Key Backup to SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.

Parameter	Description
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the SFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

Figure 11-32 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. <ul style="list-style-type: none"> When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

Figure 11-33 Log Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the IPv4 option, enter the IPv4 address of the TFTP server in the space provided. When the IPv6 option is selected, enter the IPv6 address of the TFTP server in the space provided.

Parameter	Description
Destination File	Enter the destination path and location where the log file should be stored on the TFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the TFTP server. <ul style="list-style-type: none"> When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Log Backup to RCP

This window is used to initiate a system log backup to an RCP server.

To view the following window, click **Tools > Log Backup > Log Backup to RCP**, as shown below:

Figure 11-34 Log Backup to RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Destination File	Enter the destination path and location where the log file should be stored on the RCP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the RCP server. <ul style="list-style-type: none"> When the System Log option is selected, the system log will be backed up. When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Log Backup to SFTP

This window is used to initiate a system log backup to an SFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to SFTP**, as shown below:

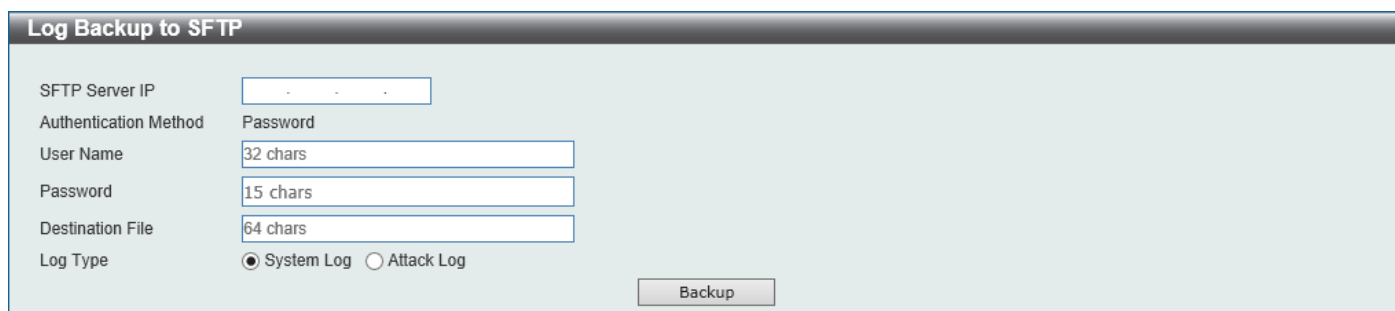


Figure 11-35 Log Backup to SFTP Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server IP	Enter the IPv4 address of the SFTP server here.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 15 characters long.
Destination File	Enter the destination path and location where the log file should be stored on the SFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the SFTP server. <ul style="list-style-type: none">When the System Log option is selected, the system log will be backed up.When the Attack Log is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Ping

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

To view the following window, click **Tools > Ping**, as shown below:

The screenshot shows the 'Ping' configuration window. It is divided into two main sections: 'IPv4 Ping' and 'IPv6 Ping'. Each section contains the following fields:

- Target IP Address:** A text input field.
- Ping Times (1-255):** A numeric input field with a dropdown menu and a checked 'Infinite' checkbox.
- Timeout (1-99):** A numeric input field with a unit of 'sec'.
- Length (1-1420):** A numeric input field with a unit of 'bytes'.
- ToS (0-255):** A numeric input field.
- Stop Time (0-99):** A numeric input field.
- Start:** A button to initiate the ping test.

Figure 11-36 Ping Window

The fields that can be configured in **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Length	Enter the length value here. This specifies the number of data bytes to send. The default value is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. It does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420 bytes.
ToS	Enter the ToS value here. This is used to configure the QoS on ICMP datagrams. The range is from 0 to 255.
Stop Time	Enter the stop time value here. This specifies to stop the ping after the amount of times entered here. If this value is configured as 0, then the ping can only be stopped by clicking the Stop button manually. The range is from 0 to 99.

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.
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.

Parameter	Description
Length	Enter the length value here. This specifies the number of data bytes to send. The default value is 56, which translates into 64 ICMPv6 data bytes when combined with the 8 bytes of ICMPv6 header data. It does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420 bytes.
Stop Time	Enter the stop time value here. This specifies to stop the ping after the amount of times entered here. If this value is configured as 0, then the ping can only be stopped by clicking the Stop button manually. The range is from 0 to 99.

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:

IPv4 Ping Result

```
[1] Reply from 10.90.90.90, time<10ms
[2] Reply from 10.90.90.90, time<10ms
[3] Reply from 10.90.90.90, time<10ms
[4] Reply from 10.90.90.90, time<10ms
Ping Statistics for 10.90.90.90
Packets: Sent = 4, Received = 4, Lost = 0
```

Stop Back

Figure 11-37 Ping (Start) Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Trace Route

The trace route page allows the user to trace a route between the Switch and a given host on the network.

To view the following window, click **Tools > Trace Route**, as shown below:

Trace Route

IPv4 Trace Route

IPv4 Address: . . .

Initial TTL (1-255): 1

Max TTL (1-255): 30

Port (1-65535): 33434

Timeout (1-65535): 5 sec

Length (1-1420): 40 bytes

ToS (0-255): 0

Probe Number (1-1000): 1

Start

IPv6 Trace Route

IPv6 Address: 2233::1

Initial TTL (1-255): 1

Max TTL (1-255): 30

Port (1-65535): 33434

Timeout (1-65535): 5 sec

Length (1-1420): 40 bytes

Probe Number (1-1000): 1

Start

Figure 11-38 Trace Route Window

The fields that can be configured in **IPv4 Trace Route** are described below:

Parameter	Description
IPv4 Address	Select and enter the IPv4 address of the destination here.
Initial TTL	Enter the initial Time-To-Live (TTL) value here. The range is from 1 to 255.
Max TTL	Enter the Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 255 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Length	Enter the length value here. This specifies the number of bytes of the outgoing datagram. The range is from 1 to 1420 bytes.
ToS	Enter the ToS value here. This specifies the ToS to be set in the IP header of the outgoing datagram. The range is from 0 to 255.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

The fields that can be configured in **IPv6 Trace Route** are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address of the destination here.
Initial TTL	Enter the initial Time-To-Live (TTL) value here. The range is from 1 to 255.
Max TTL	Enter the Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 255 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Length	Enter the length value here. This specifies the number of bytes of the outgoing datagram. The range is from 1 to 1420 bytes.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

After clicking the **Start** button in **IPv4 Trace Route** section, the following **IPv4 Trace Route Result** section will appear:

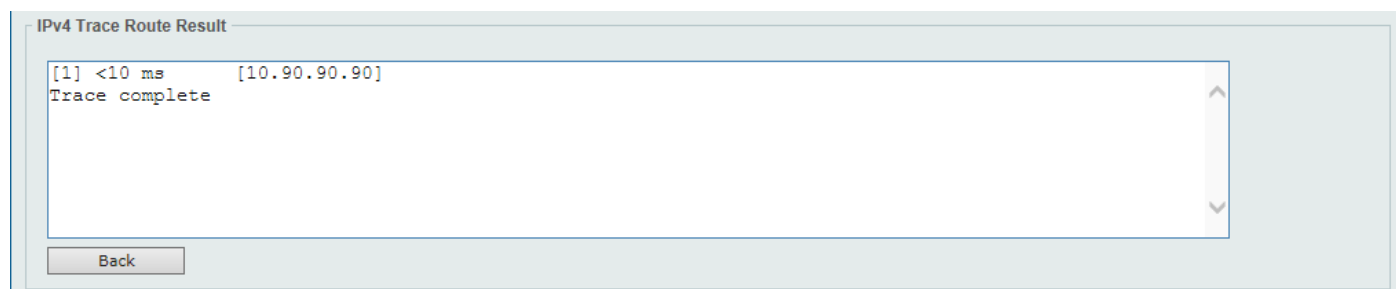


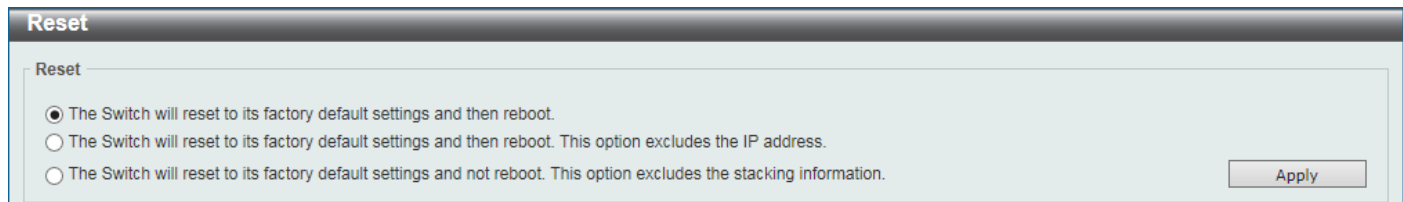
Figure 11-39 Trace Route (Start) Window

Click the **Back** button to stop the trace route and return to the IPv4 Trace Route section.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

The screenshot shows a web UI window titled "Reset". Inside, there is a section labeled "Reset" with three radio button options. The first option is selected: "The Switch will reset to its factory default settings and then reboot." The second option is "The Switch will reset to its factory default settings and then reboot. This option excludes the IP address." The third option is "The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information." An "Apply" button is located on the right side of the window.

Reset

Reset

☒ The Switch will reset to its factory default settings and then reboot.

☐ The Switch will reset to its factory default settings and then reboot. This option excludes the IP address.

☐ The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information.

Apply

Figure 11-40 Reset Window

Select one of the following options:

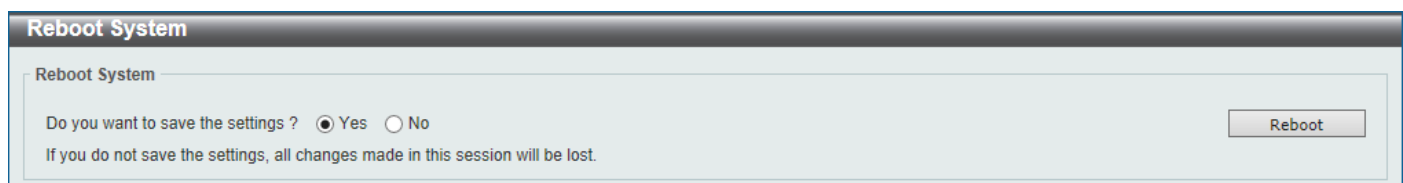
- The Switch will reset to its factory default settings and then reboot.
- The Switch will reset to its factory default settings and then reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot. This option excludes the stacking information.

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

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

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

The screenshot shows a web UI window titled "Reboot System". Inside, there is a section labeled "Reboot System" with a question "Do you want to save the settings ?" and two radio button options: "Yes" (selected) and "No". Below the question, there is a warning: "If you do not save the settings, all changes made in this session will be lost." A "Reboot" button is located on the right side of the window.

Reboot System

Reboot System

Do you want to save the settings ? ☒ Yes ☐ No

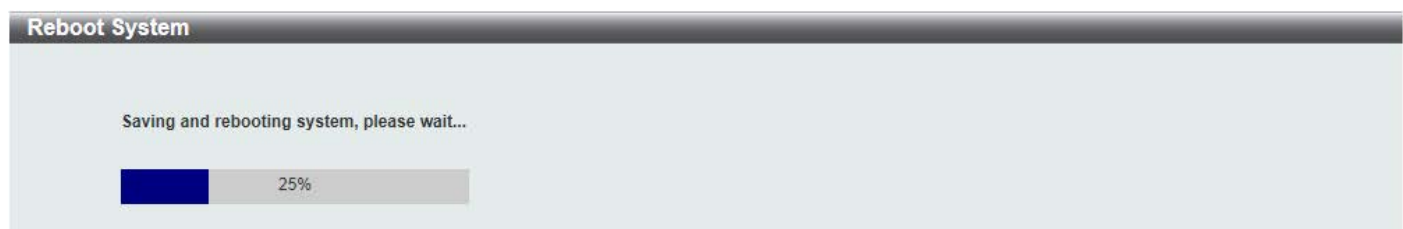
If you do not save the settings, all changes made in this session will be lost.

Reboot

Figure 11-41 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.

The screenshot shows a web UI window titled "Reboot System". Inside, there is a message "Saving and rebooting system, please wait..." and a progress bar. The progress bar is partially filled with a blue bar, and the text "25%" is displayed next to it.

Reboot System

Saving and rebooting system, please wait...

25%

Figure 11-42 Reboot System (Rebooting) Window

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DGS-3630 Series Switch.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords will be forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the **Password Recovery** feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on this Switch to easily recover passwords. Complete these steps to reset the password:

- For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the Switch.
- Power on the Switch. After the **UART init** is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (**Shift+6**) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled.

```

Boot Procedure                                     V2.10.001
-----
Power On Self Test ..... 100 %

MAC Address   : F0-7D-68-30-36-00
H/W Version   : A1

Please Wait, Loading 2.20.B006 Runtime Image ..... 100 %
UART init ..... 100 %

```

```

Password Recovery Mode
Switch(reset-config)#

```

In the "Password Recovery Mode" only the following commands can be used.

Command	Description
<code>no enable password</code>	This command is used to delete all account level passwords.
<code>no login password</code>	This command is used to clear the local login methods.
<code>no username</code>	This command is used to delete all local user accounts.
<code>password-recovery</code>	This command is used to initiate the password recovery procedure.
<code>reload</code>	This command is used to save and reboot the Switch.
<code>reload clear running-config</code>	This command is used to reset the running configuration to the factory default settings and then reboot the Switch.
<code>show running-config</code>	This command is used to display the current running configuration.
<code>show username</code>	This command is used to display local user account information.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

AAA

Log Description	Severity
Event Description: AAA global state is enabled or disabled. Log Message: AAA is <status> Parameters Description: status: The status indicates the AAA enabled or disabled.	Informational
Event Description: Successful login. Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web (SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Informational
Event Description: Login failed. Log Message: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web (SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event Description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web (SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event Description: Enable privilege successfully. Log Message: Successful enable privilege through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web (SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Informational
Event Description: Enable privilege failure. Log Message: Enable privilege failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description:	Warning

Log Description	Severity
<p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web (SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	
<p>Event Description: the remote server does not respond to the enable password authentication request.</p> <p>Log Message: Enable privilege failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>)</p> <p>Parameters Description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web (SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event Description: RADIUS assigned a valid VLAN ID attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Parameters Description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>vid: The assign VLAN ID that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event Description: RADIUS assigned a valid bandwidth attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface -id> (Username: <username>)</p> <p>Parameters Description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>direction: It indicates the direction for bandwidth control, e.g.: ingress or egress.</p> <p>threshold: The assign threshold of bandwidth that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event Description: RADIUS assigned a valid priority attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port <interface -id> (Username: <username>)</p> <p>Parameters Description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>priority: The assign priority that authorized by from RADIUS server.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>username: It indicates the username for authentication.</p>	Informational
<p>Event Description: RADIUS assigned ACL script but fails to apply to the system due to insufficient resource.</p> <p>Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port <interface -id> (<acl-script>)</p> <p>Parameters Description:</p> <p>server-ip: It indicates the RADIUS server IP address.</p> <p>username: It indicates the username for authentication.</p> <p>interface-id: It indicates the port number of the client authenticated.</p> <p>acl-script: The assign ACL script that authorized by from RADIUS server.</p>	Warning

ARP

Log Description	Severity
<p>Event Description: Gratuitous ARP detected duplicate IP.</p> <p>Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>)</p> <p>Parameters Description:</p> <p>ipaddr: The IP address which is duplicated with our device.</p> <p>macaddr: The MAC address of the device that has duplicated IP address as our device.</p> <p>unitID: 1.Interger value;2.Represent the id of the device in the stacking system.</p> <p>portNum: 1.Interger value;2.Represent the logic port number of the device.</p> <p>ipif_name: The name of the interface of the switch which has the conflict IP address.</p>	Warning

Configuration/Firmware

Log Description	Severity
<p>Event Description: Firmware upgraded successfully.</p> <p>Log Message: [Unit <unitID>],Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
<p>Event Description: Firmware upgraded unsuccessfully.</p> <p>Log Message: [Unit <unitID>],Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
<p>Event Description: Firmware uploaded successfully.</p> <p>Log Message: [Unit <unitID>],Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <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>	Informational

Log Description	Severity
pathFile: Path and file name on server.	
<p>Event Description: Firmware uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>],Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
<p>Event Description: Configuration downloaded successfully.</p> <p>Log Message: [Unit <unitID>],Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
<p>Event Description: Configuration downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>],Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning
<p>Event Description: Configuration uploaded successfully.</p> <p>Log Message: [Unit <unitID>],Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Informational
Event Description: Configuration uploaded unsuccessfully.	Warning

Log Description	Severity
<p>Log Message: [Unit <unitID>], Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	
<p>Event description: Configuration saved to flash by console.</p> <p>Log Message: [Unit <unitID>,]Configuration saved to flash by console (Username: <username>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>username: Represent current login user.</p>	Informational
<p>Event description: Configuration saved to flash by remote.</p> <p>Log Message: [Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p>	Informational
<p>Event description: Configuration saved to flash by console.</p> <p>Log Message: [Unit <unitID>,]System log saved to flash by console (Username: <username>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>username: Represent current login user.</p>	Informational
<p>Event description: Configuration saved to flash by remote.</p> <p>Log Message: [Unit <unitID>,]System log saved to flash (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <p>unitID: The unit ID.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p>	Informational
<p>Event Description: Unknown type files downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>], Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>session: The user's session.</p> <p>username: Represent current login user.</p> <p>ipaddr: Represent client IP address.</p> <p>macaddr: Represent client MAC address.</p> <p>serverIP: Server IP address.</p> <p>pathFile: Path and file name on server.</p>	Warning

NOTE:

- The user's session refers to Console, Web, SNMP, Telnet, and SSH sessions.
- If the Switch is in the standalone state, there will be no unit ID in the log message.
- If the configuration or firmware was downloaded or uploaded through the console, there will be no IP address and MAC address information in the log message.

DDM

Log Description	Severity
<p>Event Description: when the any of SFP parameters exceeds from the warning threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded</p> <p>Parameters Description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type.</p> <p>It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p> <p>high-low: High or low threshold.</p>	Warning
<p>Event Description: when the any of SFP parameters exceeds from the alarm threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded</p> <p>Parameters Description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type.</p> <p>It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p> <p>high-low: High or low threshold.</p>	Critical
<p>Event Description: when the any of SFP parameters recovers from the warning threshold.</p> <p>Log Message: Optical transceiver <interface-id> <component> back to normal</p> <p>Parameters Description:</p> <p>interface-id: port interface ID.</p> <p>component: DDM threshold type.</p> <p>It can be one of the following types:</p> <p>temperature</p> <p>supply voltage</p> <p>bias current</p> <p>TX power</p> <p>RX power</p>	Warning

Interface

Log Description	Severity
Event Description: Port link up. Log Message: Port <portNum> link up, <link state> Parameters Description: portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex.	Informational
Event Description: Port link down. Log Message: Port <portNum> link down Parameters Description: portNum: 1.Interger value;2.Represent the logic port number of the device.	Informational

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up. Log Message: Link Aggregation Group <group_id> link up Parameters Description: group_id: The group id of the link up aggregation group.	Informational
Event Description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group_id> link down Parameters Description: group_id: The group id of the link down aggregation group.	Informational
Event Description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id> Parameters Description: ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
Event Description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id> Parameters Description: ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

Login/Logout

Log Description	Severity
Event Description: Login through console successfully. Log Message: [Unit <unitID>.]Successful login through Console (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Login through console unsuccessfully. Log Message: [Unit <unitID>.] Login failed through Console (Username: <username>) Parameters Description: unitID: The unit ID.	Warning

Log Description	Severity
username: Represent current login user.	
Event Description: Console session timed out. Log Message: [Unit <unitID>.] Console session timed out (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Logout through console. Log Message: [Unit <unitID>.] Logout through Console (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Login through Telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through Telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Critical
Event Description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational

Log Description	Severity
Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	

MSTP Debug

Log Description	Severity
Event Description: Topology changed. Log Message: Topology changed [(Instance:<InstanceID>] , <portNum> ,MAC: <macaddr>)] Parameters Description: InstanceID: Instance ID. portNum: Port ID. macaddr: MAC address.	Notification
Event Description: Spanning Tree new Root Bridge. Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected [(Instance: <InstanceID>],MAC: <macaddr>, Priority:<value>) Parameters Description: InstanceID: Instance ID. macaddr: Mac address. value: priority value.	Informational
Event Description: Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
Event Description: Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
Event Description: New root port. Log Message: New root port selected [(Instance:<InstanceID>], <portNum>)] Parameters Description: InstanceID: Instance ID. portNum: Port ID.	Notification
Event Description: Spanning Tree port status changed. Log Message: Spanning Tree port status change [(Instance:<InstanceID>], <portNum>)] <old_status> -> <new_status> Parameters Description: InstanceID: Instance ID. portNum: Port ID. old_status: new_status: The port of STP state. The value may be Disable, Discarding, Learning, Forwarding.	Notification
Event Description: Spanning Tree port role changed. Log Message: Spanning Tree port role change [(Instance:<InstanceID>], <portNum>)] <old_role> -> <new_role> Parameters Description: InstanceID: Instance ID. portNum: Port ID. old_role: new_status: The port role of stp. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	Informational

Log Description	Severity
Event Description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance:<InstanceID>) Parameters Description: InstanceID: Instance ID.	Informational
Event Description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance:<InstanceID>) Parameters Description: InstanceID: Instance ID.	Informational
Event Description: Spanning Tree Version changed. Log Message: Spanning Tree version change.(New version:<new_version>) Parameters Description: new_version: New STP version.	Informational
Event Description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>) Parameters Description: name: New name. revision_level: New revision level.	Informational
Event Description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: InstanceID: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
Event Description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: InstanceID: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
Event Description: Spanning Tree port role change to alternate port due to the guard root. Log Message: Spanning Tree port role change (Instance: <InstanceID>, <portNum>) to alternate port due to the guard root Parameters Description: InstanceID: Instance ID. portNum: Port ID.	Informational
Event Description: Spanning Tree loop guard blocking. Log Message: Spanning Tree loop guard blocking(Instance: <InstanceID>, <portNum>) Parameters Description: InstanceID: Instance ID. portNum: Port ID.	Informational

OpenFlow

Log Description	Severity
<p>Event Description: This log will be generated when OpenFlow TCP/TLS session is successfully connected with the controller.</p> <p>Log Message: <connection-type> session is successfully connected with the controller <ipaddr>:<port></p> <p>Parameters Description:</p> <p>connection-type: It indicates TCP or TLS connection.</p> <p>ipaddr: It indicates the controller's IP address.</p> <p>port: It indicates the L4 port number.</p>	Informational
<p>Event Description: This log will be generated when OpenFlow TCP/TLS session is disconnected from the controller.</p> <p>Log Message: <connection-type> session is disconnected from the controller <ipaddr>:<port></p> <p>Parameters Description:</p> <p>connection-type: It indicates TCP or TLS connection.</p> <p>ipaddr: It indicates the controller's IP address.</p> <p>port: It indicates the L4 port number.</p>	Informational
<p>Event Description: This log will be generated when flow setting from controller is failed.</p> <p>Log Message: Flow entry (cookie is <cookie>) setting <set-type> from the controller is failed.</p> <p>Parameters Description:</p> <p>cookie: The cookie is specified by the controller when the flow is installed.</p> <p>set-type: It indicates the flow entry settings. The types include:</p> <p>OFPPFC_ADD</p> <p>OFPPFC_MODIFY</p> <p>OFPPFC_MODIFY_STRICT</p> <p>OFPPFC_DELETE</p> <p>OFPPFC_DELETE_STRICT</p>	Error
<p>Event Description: This log will be generated when the flow entry is deleted by the controller.</p> <p>Log Message: Flow entry cookie <cookie> is deleted by controller <ipaddr>:<port></p> <p>Parameters Description:</p> <p>cookie: The cookie is specified by the controller when the flow is installed.</p> <p>ipaddr: It indicates the controller's IP address.</p> <p>port: It indicates the L4 port number.</p>	Warning
<p>Event Description: This log will be generated when the flow entry is deleted because of idle time, hard timeout expire, flow-mod request, and overwrite.</p> <p>Log Message: Flow entry cookie <cookie> is deleted because of <delete-reason></p> <p>Parameters Description:</p> <p>cookie: The cookie is specified by the controller when the flow is installed.</p> <p>delete-reason: It indicates the reason to delete the flow entry. It contains:</p> <p>"idle timeout (<duration> seconds)"</p> <p>"hard timeout (<duration> seconds)"</p> <p>"FLOW_MOD request"</p> <p>"overwrite"</p> <p><duration> indicates the value of timeout.</p>	Warning
<p>Event Description: This log will be generated when the flow setting from the controller failed.</p> <p>Log Message: An error <error-type> occurs with the controller <ipaddr></p> <p>Parameters Description:</p>	Error

Log Description	Severity
<p>error-type: It indicates the error type when an error occurs between the Switch and the controller. The error type may be:</p> <p> OFPET_BAD_REQUEST OFPET_FLOW_MOD_FAILED OFPET_GROUP_MOD_FAILED OFPET_ROLE_REQUEST_FAILED OFPET_METER_MOD_FAILED </p> <p>ipaddr: It indicates the controller's IP address.</p>	

Peripheral

Log Description	Severity
<p>Event Description: Fan Recovered.</p> <p>Log Message: Unit <unit-id>, <fan-descr> back to normal</p> <p>Parameters Description:</p> <p>Unit <id>: The unit ID.</p> <p><fan-descr>: For example, right fan, left fan etc.</p>	Critical
<p>Event Description: Fan Fail.</p> <p>Log Message: Unit <unit-id> <fan-descr> failed</p> <p>Parameters Description:</p> <p>Unit <id>: The unit ID.</p> <p><fan-descr>: For example, right fan, left fan etc.</p>	Critical
<p>Event Description: Temperature sensor enters alarm state.</p> <p>Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree></p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>thermal-sensor-descr: Description of the sensor.</p> <p>degree: The current temperature of the sensor.</p>	Warning
<p>Event Description: Temperature recovers to normal.</p> <p>Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal</p> <p>Parameters Description:</p> <p>unitID: The unit ID.</p> <p>thermal-sensor-descr: Description of the sensor.</p> <p>degree: The current temperature of the sensor.</p>	Informational
<p>Event Description: Power failed.</p> <p>Log Message: Unit <unit-id> <power-descr> failed</p> <p>Parameters Description:</p> <p>Unit <id>: The unit ID.</p> <p>power-descr: Describe the power.</p>	Critical
<p>Event Description: Power is recovered.</p> <p>Log Message: Unit <unit-id> <power-descr> back to normal</p> <p>Parameters Description:</p> <p>Unit <id>: The unit ID.</p> <p>power-descr: Describe the power.</p>	Critical
<p>Event Description: External Alarm state to change.</p> <p>Log Message: Unit <unit-id> External Alarm Channel <channelID>:<alarmMsg></p> <p>Parameters Description:</p>	Critical

Log Description	Severity
Unit <id>: The unit ID. channelID: The channel ID. alarmMsg: The alarm Msg.	

PoE

Log Description	Severity
Event Description: Total power usage threshold is exceeded. Log Message: Unit <unit-id> usage threshold <percentage> is exceeded Parameters Description: unit-id: The box ID. percentage: Usage threshold.	Warning
Event Description: Total power usage threshold is recovered. Log Message: Unit <unit-id> usage threshold <percentage> is recovered Parameters Description: unit-id: The box ID. percentage: Usage threshold.	Warning
Event Description: PD doesn't reply the ping request. Log Message: PD alive check failed. (Port: <portNum>, PD: <ipaddr>) portNum: The port number. ipaddr: The IP (IPv4/IPv6) address of PD.	Warning

Port

Log Description	Severity
Event Description: Port linkup. Log Message: Port <port> link up, <nway> Parameters Description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
Event Description: Port link down. Log Message: Port <port> link down Parameters Description: port: Represents the logical port number.	Informational

Reboot Schedule

Log Description	Severity
Event Description: Tips is about will to reboot switch within the specified time. Log Message: Display "Reboot scheduled in 5 minutes" when the countdown equals 5 minutes	Warning
Event Description: Tips is about will to reboot switch within the specified time. Log Message: Display "Reboot scheduled in 1 minute" when the countdown equals 1 minute	Critical
Event Description: after schedule reboot in a specific interval. Log Message: System was restarted by schedule in an interval time	Informational

Log Description	Severity
Event Description: after schedule reboot at specific time. Log Message: System was restarted by schedule at specific time	Informational
Event Description: after schedule reboot happens with save_before_reboot configured. Log Message: Configuration was saved by schedule	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event Description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event Description: SSH server is disabled. Log Message: SSH server is disabled	Informational

System

Log Description	Severity
Event Description: This log will be generated when system warm start. Log Message: [Unit <unitID>,]System warm start Parameters Description: unitID: The unit ID.	Critical
Event Description: This log will be generated when system cold start. Log Message: [Unit <unitID>,]System cold start Parameters Description: unitID: The unit ID.	Critical
Event Description: This log will be generated when system start up. Log Message: [Unit <unitID>,]System started up. Parameters Description: unitID: The unit ID.	Critical

Telnet

Log Description	Severity
Event Description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description:	Informational

Log Description	Severity
ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	
Event Description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Warning
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Informational
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Informational

Web

Log Description	Severity
Event Description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event Description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Successful login through Web (SSL). Log Message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTPS server. ipaddr: The IP address of HTTPS client.	Informational
Event Description: Login failed through Web (SSL).	Warning

Log Description	Severity
<p>Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>)</p> <p>Parameters Description:</p> <p>username: The use name that used to login HTTPS server.</p> <p>ipaddr: The IP address of HTTPS client.</p>	
<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 use name that used to login HTTPS server.</p> <p>ipaddr: The IP address of HTTPS 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 use name that used to login HTTPS server.</p> <p>ipaddr: The IP address of HTTPS client.</p>	Informational

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

Authentication Fail

Trap Name	Description	OID
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

DDM

Trap Name	Description	OID
dDdmAlarmTrap	A notification is generated when an abnormal alarm situation occurs or recovers from an abnormal alarm situation to normal status. Only when the current value > low warning or current value < high warning will send recover trap. Binding objects: (1) dDdmNotifyInfoIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.1 4.72.0.1
dDdmWarningTrap	A notification is generated when an abnormal warning situation occurs or recovers from an abnormal warning situation to normal status. Binding objects: (1) dDdmNotifyInfoIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.1 4.72.0.2

External Alarm

Trap Name	Description	OID
dExternalAlarmStatusChg	The commander switch will send this notification when External alarm state is changed. Binding objects: (1) dExternalAlarmUnitID (2) dExternalAlarmChannel (3) dExternalAlarmStatus	1.3.6.1.4.1.171.1 4.32.0.1

LACP

Trap Name	Description	OID
linkup	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one	1.3.6.1.6.3.1.1.5.4

Trap Name	Description	OID
	<p>of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ifIndex (2) ifAdminStatus (3) ifOperStatus 	
linkDown	<p>A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) ifIndex (2) ifAdminStatus (3) ifOperStatus 	1.3.6.1.6.3.1.1.5.3

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 	1.3.6.1.4.1.171.14.3.0.1
dL2FdbMacNotificationWithVID	<p>This trap indicate the MAC addresses variation in the address table.</p> <p>Binding objects:</p> <ul style="list-style-type: none"> (1) dL2FdbMacChangeNotifyInfoWithVID 	1.3.6.1.4.1.171.14.3.0.2

MSTP

Trap Name	Description	OID
newRoot	<p>The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.</p>	1.3.6.1.2.1.17.0.1
topologyChange	<p>A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.</p>	1.3.6.1.2.1.17.0.2

Peripheral

Trap Name	Description	OID
dEntityExtFanStatusChg	The commander switch will send this notification when a fan fails (dEntityExtEnvFanStatus is 'fault') or recovers (dEntityExtEnvFanStatus is 'ok'). Binding objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171.14.5.0.1
dEntityExtThermalStatusChg	The commander switch will send this notification when a thermal alarms (dEntityExtEnvTempStatus is 'abnormal') or recover(dEntityExtEnvTempStatus is 'ok'). Binding objects: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2
dEntityExtPowerStatusChg	The commander switch will send this notification when a power module fails, recovers or is removed. Binding objects: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.171.14.5.0.3

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 msec 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 msec 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 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1
dPoelfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects:	1.3.6.1.4.1.171.14.24.0.2

Trap Name	Description	OID
	(1) pethPsePortOverLoadCounter	
dPoelfPowerShortCircuitNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortShortCounter	1.3.6.1.4.1.171.14.24.0.3
dPoelfPdAliveFailOccurNotification	This trap indicates if the PD device has the stop working or no response problem. At least 500 msec must elapse between notifications being emitted by the same object instance.	1.3.6.1.4.1.171.14.24.0.4

Port

Trap Name	Description	OID
linkup	A notification is generated when port linkup. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	A notification is generated when port link down. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

Reboot Schedule

Trap Name	Description	OID
agentRebootIn5Min	This trap is sent when the countdown equals 5 minutes.	1.3.6.1.4.1.171.14.170.0.1
agentRebootIn1Min	This trap is sent when the countdown equals 1 minute.	1.3.6.1.4.1.171.14.170.0.2

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

Trap Name	Description	OID
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

Start

Trap Name	Description	OID
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.171.14.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.171.14.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.171.14.14.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.171.14.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.171.14.14.0.5

Upload/Download

Trap Name	Description	OID
agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding objects: (1) swMultiImageVersion	1.3.6.1.4.1.171.12.1.7.2.0.7
agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded. Binding objects: (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.171.12.1.7.2.0.9

Appendix D - OpenFlow Object Details

Application developers can program a set of objects in the Switch using the OpenFlow protocol (version 1.3). The programmable objects include Flow Tables, Group Table entries, and Meter Table entries. This section provides programming descriptions for these objects.

Flow Table

Flow Table Number Assignments

Flow Table Name	Flow Table ID	Default Table Miss Action
Policy ACL Flow Table	0	Drop

Flow Table Counters

Field	Description
Reference Count (Active Entries)	Reference count of number of active entries in the table.
Packet Lookups	Not supported.
Packet Matches	Not supported.

Policy ACL Flow Table

Policy ACL Flow Table Match Fields

Field	Description
IN_PORT	The input port on the Switch.
IN_PHY_PORT	The physical input port on the Switch.
ETH_DST	The Ethernet destination address. Note: IPv6 flow (ETH_TYPE=0x86DD) is not supported.
ETH_SRC	The Ethernet source address. Note: IPv6 flow (ETH_TYPE=0x86DD) is not supported.
ETH_TYPE	The Ethernet frame type. Note: The Policy ACL Flow Table is organized into two mutually exclusive logical sub-tables. The flow entries in the IPv6 logical tables match only IPv6 packets (ETH_TYPE=0x86DD). The non-IPv6 logical table matches any non-IPv6 packets (ETH_TYPE≠0x86DD or when the ETH_TYPE is not specified).
VLAN_VID	The VLAN ID. Note: This must be programmed with 0x1000 (OFPVID_PRESENT).
VLAN_PCP	The VLAN priority.
IP_DSCP	The IP DSCP (6 bits in the ToS field).
IP_PROTO	The IP protocol.
IPV4_SRC	The source IPv4 address.
IPV4_DST	The destination IPv4 address.
TCP_SRC	The source TCP port.
TCP_DST	The destination TCP port.
UDP_SRC	The source UDP port.

Field	Description
UDP_DST	The destination UDP port.
SCTP_SRC	The source SCTP port.
SCTP_DST	The destination SCTP port.
ARP_SPA	The ARP source IPv4 address.
IPV6_SRC	The source IPv6 address.
IPV6_DST	The destination IPv6 address.

Policy ACL Flow Table Instructions

Field	Description
Write-Actions	Only the actions in the Policy ACL Flow Table Action Set table can be specified.
Apply-Actions	Only the actions in Policy ACL Flow Table Action List Actions table can be specified.
Clear-Actions	This is used to clear the action set.
Goto-Table	Not supported.
Write-Metadata	Not supported.
Meter	Specifies to apply the indicated meter. The meter entry must exist before the flow is installed.

Policy ACL Flow Table Action List Actions

Field	Description
Output	This sets the output port. It supports physical ports and the reserved controller port.
Set-Field	This supports VLAN_PCP, IP_ECN and IP_DSCP fields.

Policy ACL Flow Table Action Set

Field	Description
Group	<p>This sets the output group entry for processing the packet after this table. The group must exist, be consistent with the type of rule and packet, and can be any of the following:</p> <ul style="list-style-type: none"> • a Layer 2 interface group entry, • a Layer 2 rewrite group entry, • a Layer 2 multicast group entry, • a Layer 3 unicast group entry, and • a Layer 3 ECMP group entry.

Policy ACL Flow Table Counters

Field	Description
Received Packets	The number of packets that is received by this flow entry.
Received Bytes	The number of bytes that is received by this flow entry.
Duration (Seconds)	The time, in seconds, since this flow entry was installed.

Restrictions:

This Policy ACL Flow Table is organized into two mutually exclusive logical sub-tables. One is used to match IPv6 flows and the other one is used to match non-IPv6 flows. These two tables should be considered as a single table. But there are some restrictions:

- IPv6 packets might match two rules in the Policy ACL Flow table. It is recommended add ETH_TYPE or other Match Fields in the non-IPv6 logical table to avoid this issue.
- The same meter cannot be applied to two rules in different sub-tables. It is recommended to apply different meters for different rules to avoid this issue.

Group Table

L2 Interface Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the L2 Interface Group Entry Naming Conversion table.
Group Type	Indirect.
Counters	Specifies per-group entry counters.
Action Buckets	Supports a single action bucket.

L2 Interface Group Entry Naming Conversion

Field	Bits	Description
Interface ID	0 to 15	The interface ID.
Chain ID	16 to 27	The ID that other group type entries chain to. The range is from 1 to 4094.
Kind	28 to 31	0 (L2 Interface).

L2 Interface Group Entry Bucket Actions

Field	Description
Output	Supported on physical ports only.

L2 Interface Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed.

L2 Rewrite Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the L2 Rewrite Group Entry Naming Conversion table.
Group Type	Indirect.
Counters	Specifies per-group entry counters.
Action Buckets	Supports a single action bucket.

L2 Rewrite Group Entry Naming Conversion

Field	Bits	Description
ID	0 to 27	This is the index to differentiate between group entries of this type.
Kind	28 to 31	1 (L2 Rewrite).

L2 Rewrite Group Entry Bucket Actions

Field	Description
Group	This required field must be chained to a Layer 2 interface group entry.
Set-Field	This optional field sets the ETH_DST, ETH_SRC, and VLAN_VID fields.

L2 Rewrite Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed.

L2 Multicast Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the L2 Multicast Group Entry Naming Conversion table.
Group Type	All.
Counters	Specifies per-group entry counters.
Action Buckets	Supports multiple action buckets.

L2 Multicast Group Entry Naming Conversion

Field	Bits	Description
Index	0 to 15	This is the index to these kind of groups.

Field	Bits	Description
Chain ID	16 to 27	The chain ID is used to reference to Layer 2 interface group entries. The range is from 1 to 4094.
Kind	28 to 31	3 (L2 Multicast).

L2 Multicast Group Entry Bucket Actions

Field	Description
Group	This must chain to a Layer 2 interface group entry whose chain ID name component matches the chain ID component of this group entry's name.

L2 Multicast Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed.

L3 Unicast Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the L3 Unicast Group Entry Naming Conversion table.
Group Type	Indirect.
Counters	Specifies per-group entry counters.
Action Buckets	Supports a single action bucket.

L3 Unicast Group Entry Naming Conversion

Field	Bits	Description
ID	0 to 27	This is the index to differentiate between group entries of this type.
Kind	28 to 31	2 (L3 Unicast).

L3 Unicast Group Entry Bucket Actions

Field	Description
Group	This required field must be chained to a Layer 2 interface group entry.
Decrement TTL	The decremented TTL. Note: The check for invalid TTLs is not supported.
Set-Field	This required field sets the ETH_DST, ETH_SRC, and VLAN_ID fields.

L3 Unicast Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed

L3 ECMP Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the L3 ECMP Group Entry Naming Conversion table.
Group Type	Select.
Counters	Specifies per-group entry counters.
Action Buckets	Supports multiple action buckets.

L3 ECMP Group Entry Naming Conversion

Field	Bits	Description
ID	0 to 27	This is used to differentiate between Layer 3 ECMP group entries.
Kind	28 to 31	7 (L3 ECMP).

L3 ECMP Group Entry Bucket Actions

Field	Description
Group	This is chained to a Layer 3 unicast group entry.

L3 ECMP Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed

Meter Table

Meter Table Entry Parameters

Field	Description
Meter Identifier	The meter instance.
Flags	The bit position: <ul style="list-style-type: none"> 0: Kbps (Kbps and Packets cannot be used at the same time). 1: Packets (Kbps and Packets cannot be used at the same time). 2: Burst (Required).

Field	Description
	<ul style="list-style-type: none">• 3: Stats (Not supported).
Meter Bands	Only one meter band is supported.
Counters	Specifies per-meter entry counters.

Meter Entry Counters

Field	Description
Flow Count	The number of flow entities that are currently referencing to this meter table entry.
Input Packet Count	Not supported.
Input Byte Count	Not supported.
Duration (Seconds)	The time, in seconds, since this meter table entry was installed.

Meter Band Configuration Parameters

Field	Description
Band Type	Only the Drop band type is supported
Rate	This is used by the meter to select the meter band. It defines the lowest rate applied to the band.
Burst	This defines the granularity of the meter band.
Counters	Not supported.