

Web UI Reference Guide

Product Model : DIS-200G Series
Industrial Gigabit Ethernet Switch
Release 1.10

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

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

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

© 2017 D-Link Corporation. All rights reserved.

August 2017

Table of Contents

1. INTRODUCTION	1
AUDIENCE	1
OTHER DOCUMENTATION	1
CONVENTIONS	1
NOTES, NOTICES, AND CAUTIONS	2
2. WEB-BASED SWITCH CONFIGURATION	3
MANAGEMENT OPTIONS	3
CONNECTING USING THE WEB USER INTERFACE	3
LOGGING ONTO THE WEB MANAGER.....	3
SMART WIZARD	5
WEB USER INTERFACE (WEB UI)	9
<i>Areas of the User Interface</i>	9
<i>Surveillance Mode</i>	10
3. SAVE AND TOOLS.....	11
SAVE CONFIGURATION	11
FIRMWARE INFORMATION	11
FIRMWARE UPGRADE & BACKUP	12
<i>Firmware Upgrade from HTTP</i>	12
<i>Firmware Upgrade from TFTP</i>	12
<i>Firmware Backup to HTTP</i>	13
<i>Firmware Backup to TFTP</i>	13
CONFIGURATION RESTORE & BACKUP	14
<i>Configuration Restore from HTTP</i>	14
<i>Configuration Restore from TFTP</i>	14
<i>Configuration Backup to HTTP</i>	15
<i>Configuration Backup to TFTP</i>	15
LOG BACKUP.....	16
<i>Log Backup to HTTP</i>	16
<i>Log Backup to TFTP</i>	16
PING	17
RESET.....	18
REBOOT SYSTEM.....	18
4. SYSTEM	19
DEVICE INFORMATION	19
SYSTEM INFORMATION SETTINGS	19
<i>System Information</i>	19
<i>IPv4 Interface</i>	20

<i>IPv6 Interface</i>	21
PORT CONFIGURATION	21
<i>Port Settings</i>	21
<i>Jumbo Frame</i>	23
POE(DIS-200G-12PS AND DIS-200G-12PSW ONLY)	24
<i>PoE System</i>	24
<i>PoE Status</i>	25
<i>PoE Configuration</i>	25
<i>PD Alive</i>	26
SYSTEM LOG	27
<i>System Log Settings</i>	27
<i>System Log Server Settings</i>	27
<i>System Log</i>	28
TIME AND SNTP	28
<i>Clock Settings</i>	28
<i>Time Zone Settings</i>	29
SNTP SETTINGS	30
TIME PROFILE	31
5. MANAGEMENT.....	32
USER ACCOUNT SETTINGS	32
SNMP	33
<i>SNMP Global Settings</i>	34
<i>SNMP View Table Settings</i>	35
<i>SNMP Community Table Settings</i>	36
<i>SNMP Group Table Settings</i>	37
<i>SNMP Engine ID Local Settings</i>	38
<i>SNMP User Table Settings</i>	38
<i>SNMP Host Table Settings</i>	39
RMON	41
<i>RMON Global Settings</i>	41
<i>RMON Statistics Settings</i>	41
<i>RMON History Settings</i>	42
<i>RMON Alarm Settings</i>	43
<i>RMON Event Settings</i>	44
HTTP/HTTPS.....	45
D-LINK DISCOVERY PROTOCOL	45
6. LAYER 2 FEATURES	46
FDB	46
<i>Static FDB</i>	46
<i>MAC Address Table Settings</i>	47

MAC Address Table	48
VLAN	49
802.1Q VLAN	49
Management VLAN	49
GVRP	50
Asymmetric VLAN	53
VLAN Interface	53
Auto Surveillance VLAN	56
Voice VLAN	60
SPANNING TREE	63
STP Global Settings	65
STP Port Settings	66
MST Configuration Identification	67
STP Instance	68
MSTP Port Information	68
ERPS (G.8032)	69
ERPS	69
ERPS Profile	71
LOOPBACK DETECTION	72
LINK AGGREGATION	74
L2 MULTICAST CONTROL	77
IGMP Snooping	77
MLD Snooping	79
Multicast Filtering	82
LLDP	82
LLDP Global Settings	83
LLDP Neighbor Port Information	83
7. QUALITY OF SERVICE (QOS)	84
802.1P PRIORITY	84
PORT RATE LIMITING	85
PORT TRUST STATE	86
DSCP CoS MAPPING	86
8. SECURITY	87
PORT SECURITY	87
Port Security Global Settings	87
Port Security Port Settings	88
Port Security Address Entries	89
RADIUS	90
RADIUS Global Settings	90
RADIUS Server Settings	90

<i>RADIUS Statistic</i>	91
SAFEGUARD ENGINE.....	92
<i>Safeguard Engine Settings</i>	92
TRAFFIC SEGMENTATION SETTINGS.....	93
STORM CONTROL	93
DoS ATTACK PREVENTION SETTINGS	95
ZONE DEFENSE.....	96
SSL.....	97
<i>SSL Global Settings</i>	98
WEB-BASED ACCESS CONTROL.....	99
<i>Web Authentication</i>	100
<i>WAC Port Settings</i>	101
<i>WAC Customize Page</i>	102
9. OAM.....	103
CABLE DIAGNOSTICS	103
DDM.....	104
<i>DDM Settings</i>	104
<i>DDM Temperature Threshold Settings</i>	105
<i>DDM Voltage Threshold Settings</i>	105
<i>DDM Bias Current Threshold Settings</i>	106
<i>DDM TX Power Threshold Settings</i>	106
<i>DDM RX Power Threshold Settings</i>	109
<i>DDM Status Table</i>	109
10. MONITORING	110
STATISTICS.....	110
<i>Port Counters</i>	110
MIRROR SETTINGS	111
11. GREEN	112
POWER SAVING.....	112
EEE	115
12. SURVEILLANCE MODE.....	116
SURVEILLANCE OVERVIEW	116
<i>Surveillance Topology</i>	116
<i>Device Information</i>	119
PORT INFORMATION.....	120
<i>Group Details</i>	121
IP-CAMERA INFORMATION	122
NVR INFORMATION	123
POE INFORMATION.....	124

POE SCHEDULING	125
TIME	127
<i>Clock Settings</i>	127
<i>SNTP Settings</i>	127
SURVEILLANCE SETTINGS	129
SURVEILLANCE LOG	132
HEALTH DIAGNOSTIC	132
TOOLBAR	134
<i>Wizard</i>	134
<i>Tools</i>	134
<i>Save</i>	138
<i>Help</i>	139
<i>Online Help</i>	140
<i>Standard Mode</i>	140
<i>Logout</i>	140
APPENDIX A - SYSTEM LOG ENTRIES	141
APPENDIX B - TRAP ENTRIES.....	151
APPENDIX C - IETF RADIUS ATTRIBUTES SUPPORT.....	156

1. Introduction

This manual's descriptions are based on the software release 1.10. All software functions of the DIS-200G Series switches can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

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 DIS-200G 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:

- *DIS-200G Series Industrial Gigabit Ethernet Smart Managed Switch Hardware Installation Guide*
- *DIS-200G Series Industrial Gigabit Ethernet Smart Managed Switch CLI Reference Guide*

Conventions

Parameter	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 > System > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.

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

Connecting using the Web User Interface Logging onto the Web Manager

Smart Wizard

Web User Interface (Web UI)

Management Options

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

The Command Line Interface (CLI) through the RJ45 Console port or remote Telnet

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

SNMP-based Management

The Switch can be managed with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Web-based Management Interface

After successfully installing the Switch, the user can configure the Switch and monitor the LED panel using a Web browser, such as Microsoft® Internet Explorer, Mozilla Firefox, Safari, or Google Chrome.

Connecting using the Web User Interface

Most software functions of the DIS-200G Series switches can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard web browser. The web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP or HTTPS protocol.



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

Logging onto the Web Manager

To access the Web User Interface, simply open a standard web browser on the management PC and enter the Switch's default IP address into the address bar of the browser and press the Enter key.



NOTE: The default IP address of this switch is 10.90.90.90, with a subnet mask of 255.0.0.0.



NOTE: The default username and password is admin.

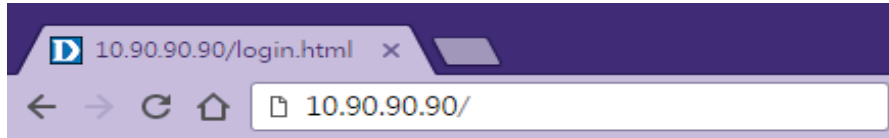


Figure 2-1 Displays entering the IP address in Internet Explorer

This will open the user authentication window, as seen below.

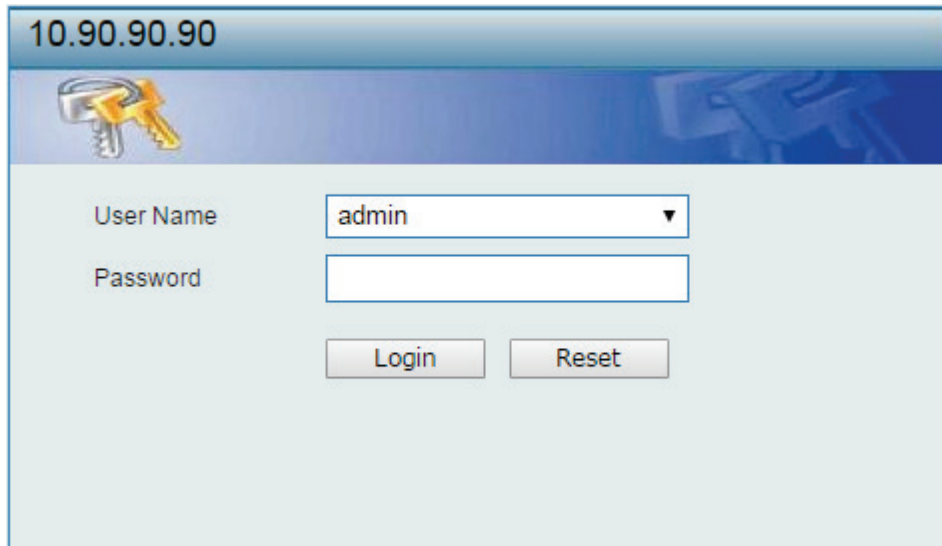


Figure 2-2 User Authentication window

Enter the **User Name** and **Password** in the corresponding fields and click **Login**. The default username is admin and the default password is admin. This will open the Web-based user interface. The Switch's management features available in the web-based manager are explained below.

Smart Wizard

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

Step 1 - Web Mode

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



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

Figure 2-3 Web Mode

The fields that can be configured are described below:

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

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

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

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

Step 2 – System IP Information

In this window, the user can configure the IP address assignment method, the static IP address, Netmask and Gateway address.

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

The screenshot shows a web-based configuration wizard titled "Welcome to Smart Wizard". The current step is "Step 2 of 4: The wizard will help to complete settings for System IP address, Netmask, and Gateway." The main content area is titled "System IP Information" and contains the following elements:

- Two radio buttons for IP assignment: "Static" (selected) and "DHCP".
- An "IP Address" field with the value "10 . 90 . 90 . 90".
- A "Netmask" field with a dropdown menu showing "8 (255.0.0.0)".
- A "Gateway" field with the value "0 . 0 . 0 . 0".
- At the bottom, there is a checkbox labeled "Ignore the wizard next time" which is currently unchecked.
- Three buttons: "Exit", "Back", and "Next".

Figure 2-4 System IP Information window

The fields that can be configured are described below:

Parameter	Description
Static	Select this option to manually configure and use IP address settings on this switch.
DHCP	Select this option to obtain IP address settings from a DHCP server.
IP Address	Enter the IP address of the Switch here.
Netmask	Select the Netmask option here.
Gateway	Enter the default gateway IP address here.

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

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

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

Step 3 – User Accounts Settings

In this window, the user can configure the user password of 'admin' account.

The screenshot shows a web-based configuration window titled "Welcome to Smart Wizard". The main content area is titled "Step 3 of 4: Configure User Account for management." and features a wizard icon. Below the title, there is a "Password" section with two text input fields labeled "Password" and "Confirm Password". At the bottom of the form, there is a checkbox labeled "Ignore the wizard next time" and three buttons: "Exit", "Back", and "Next".

Figure 2-5 Password window

The fields that can be configured are described below:

Parameter	Description
Password	Enter the new password for the user account here.
Confirm Password	Enter the new password again for confirmation here.

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

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

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

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

Step 4 – SNMP Settings

In this window, the user can enable or disable the SNMP function.

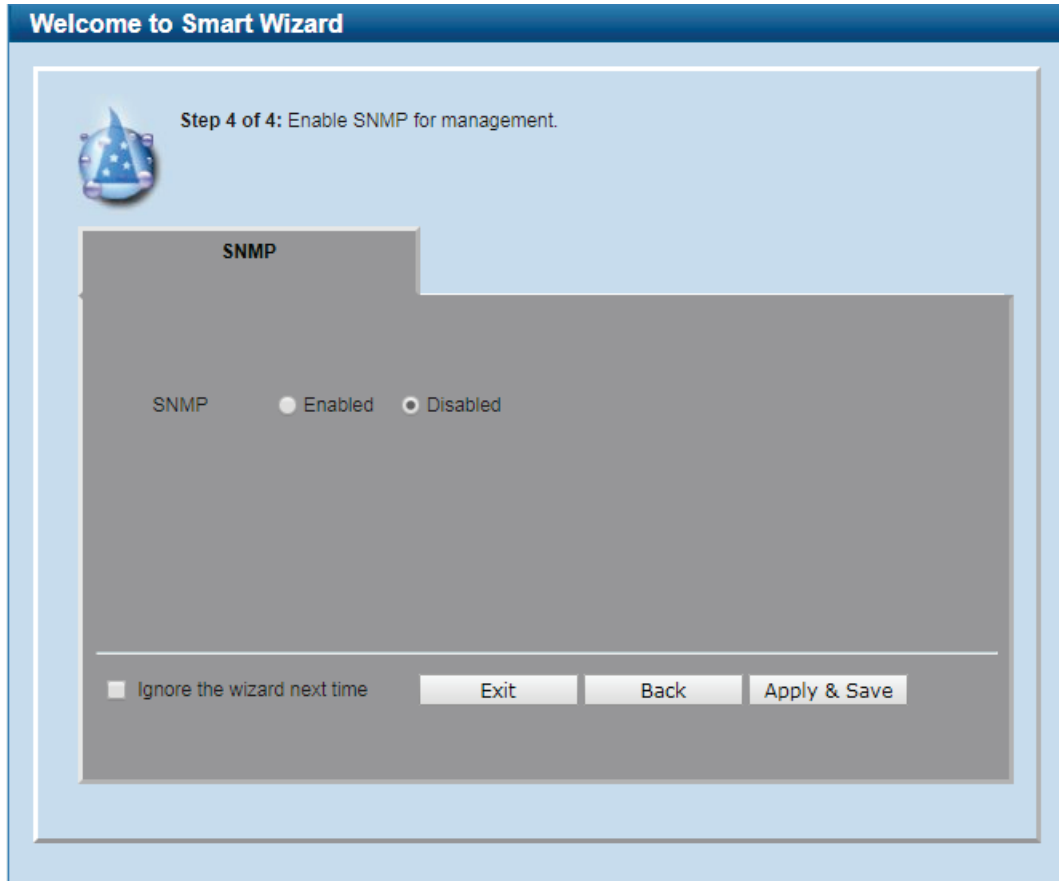


Figure 2-6 SNMP window

The fields that can be configured are described below:

Parameter	Description
SNMP	Select the Enabled option to enable the SNMP function. Select the Disabled option to disable the SNMP function.

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

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

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

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

Web User Interface (Web UI)

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface.

Areas of the User Interface

The figure below shows the Web UI in the **Standard Mode**. Three distinct areas that divide the user interface, as described in the table.

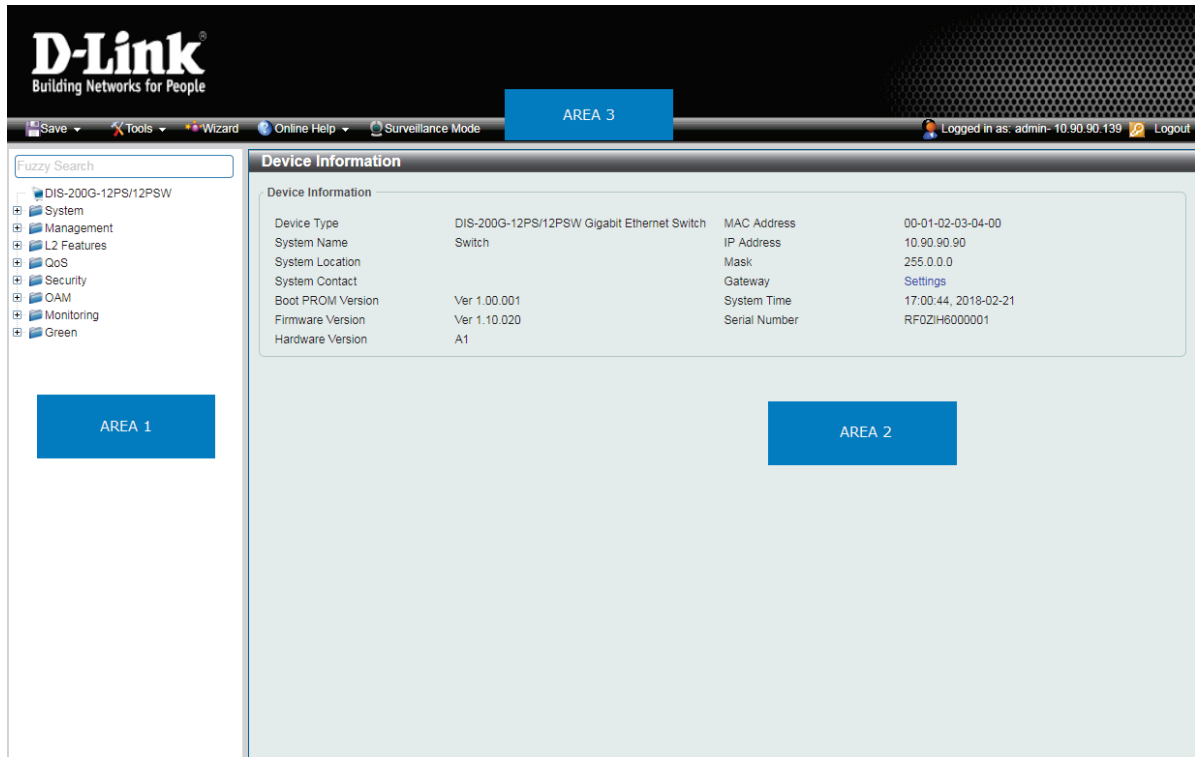


Figure 2-7 Web UI (Standard Mode)

The following **Areas** can be observed in the above window:

Parameter	Description
AREA 1	Select the folder or window to display. Open folders and click the hyperlinked window buttons and subfolders contained within them to display windows.
AREA 2	Presents Switch status based on user selection and the entry of configuration data. In addition, hyperlink of Settings is offered to enable quick Gateway configuration.
AREA 3	Presents a toolbar used to access function like Save, Tools, the Wizard and Online Help, accessing the Web UI in the Surveillance Mode, and a Logout option. Click the Surveillance Mode option to change the switch mode from Standard Mode to Surveillance Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.

Surveillance Mode

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

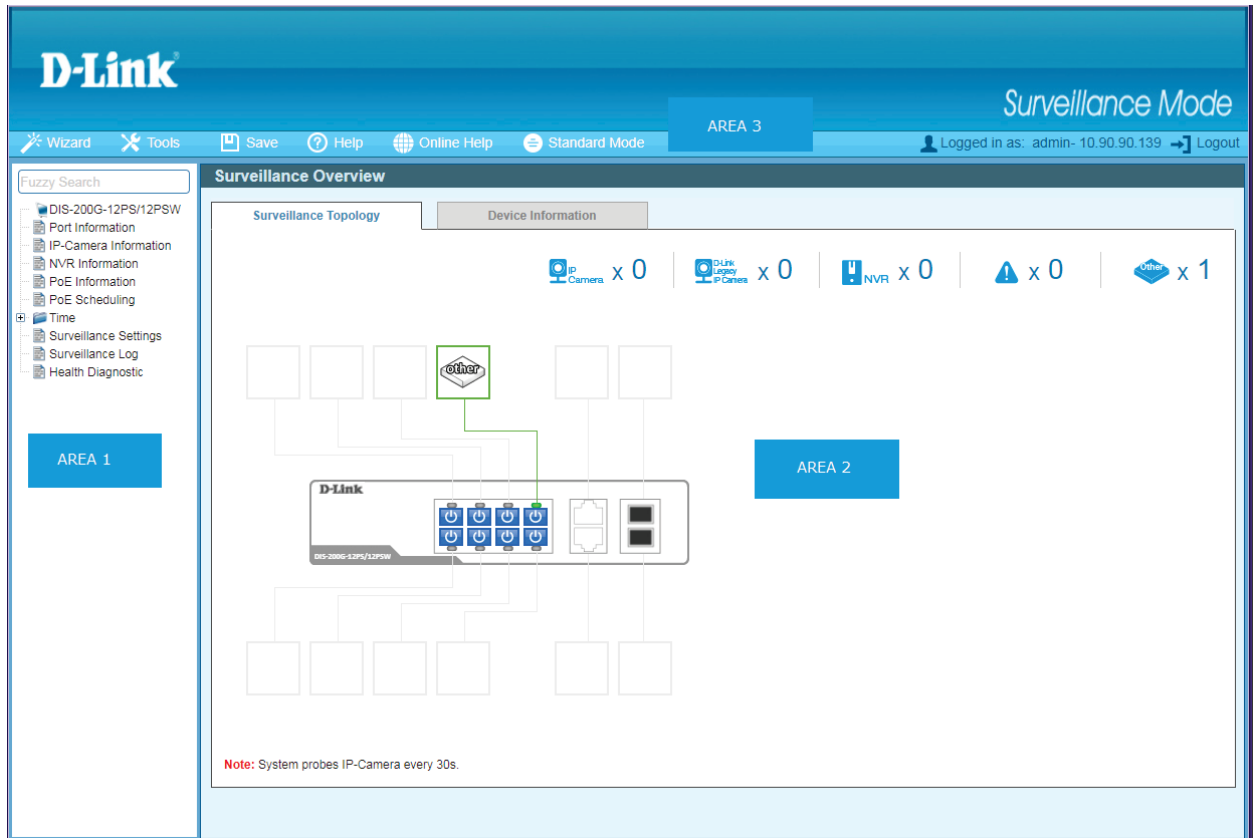


Figure 2-8 Web UI (Surveillance Mode)

The following **Areas** can be observed in the above window:

Parameter	Description
AREA 1	Select the folder or window to display. Open folders and click the hyperlinked window buttons and subfolders contained within them to display windows.
AREA 2	In this area, configuration and monitoring window frames are available based on the selections made in area 1.
AREA 3	Presents a toolbar used to access function like Save , Tools , the Wizard and Online Help , accessing the Web UI in the Surveillance Mode , and a Logout option. Click the Standard Mode option to change the switch mode from Surveillance Mode to Standard Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.

3. Save and Tools

[Save Configuration](#)
[Firmware Information](#)
[Firmware Upgrade & Backup](#)
[Configuration Restore & Backup Log Backup](#)
[Ping](#)
[Reset](#)
[Reboot System](#)

Save Configuration

This window is used to save the running configuration to the start-up configuration or the file system of the Switch. 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:

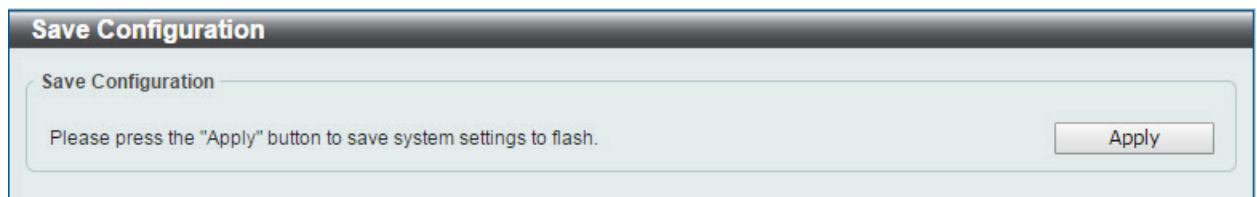


Figure 3-1 Save Configuration window

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

Firmware Information

This window is used to configure the firmware image boot up.

To view the following window, click **Tools > Firmware Information**, as shown below:

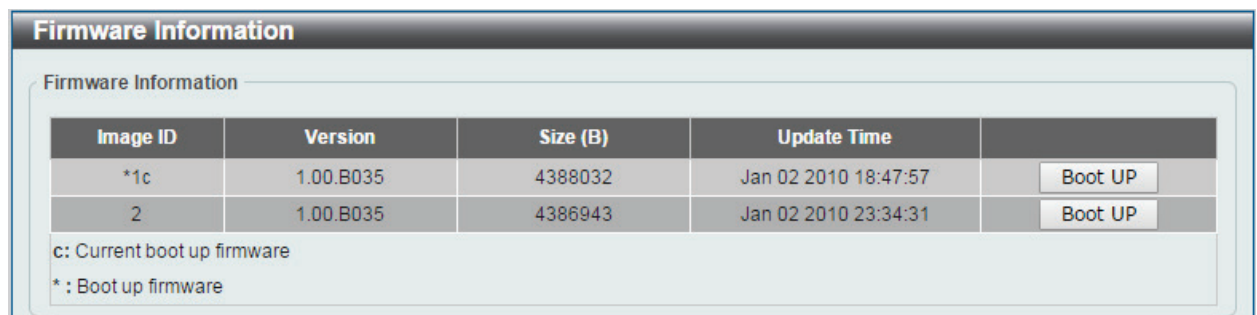


Figure 3-2 Firmware Information window

Click the **Boot UP** button of image 1 or image 2 for boot up.

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 3-3 Firmware Upgrade from HTTP window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button to navigate to the location of the firmware file located on the local PC.
Destination	The destination Image ID is automatically assigned to new upgrade firmware by system.

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 3-4 Firmware Upgrade from TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
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	The destination Image ID is automatically assigned to new upgrade firmware by system.

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 3-5 Firmware Backup to HTTP window

The fields that can be configured are described below:

Parameter	Description
Source	Specify the firmware image ID to be backup.

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 3-6 Firmware Backup to TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path where the firmware should be stored on the TFTP server. 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 3-7 Configuration Restore from HTTP window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the Browse button to navigate to the location of the configuration file located on the local PC.
Effective immediately(running-config)	Specify this radio button to restore and overwrite the running configuration file on the Switch.
Take effect after the next boot (startup-config)	Specify this radio button to restore and overwrite the start-up configuration file on the Switch.

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 3-8 Configuration Restore from TFTP window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IPv4 address here.
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.
Effective immediately (running-config)	Specify this radio button to restore and overwrite the running configuration file on the Switch.

Take effect after the next boot (startup-config)	Specify this radio button to restore and overwrite the start-up configuration file on the Switch.
---	---

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 3-9 Configuration Backup to HTTP window

The fields that can be configured are described below:

Parameter	Description
Include Username Password	Specify this radio button to back up the running configuration file include username password from the Switch.
Exclude Username Password	Specify this radio button to back up the running configuration file exclude username password 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 3-10 Configuration Backup to TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Destination File	Enter the destination filename and path where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

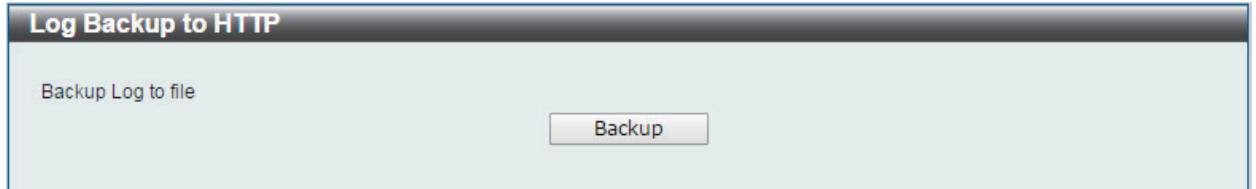


Figure 3-11 Log Backup to HTTP window

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:

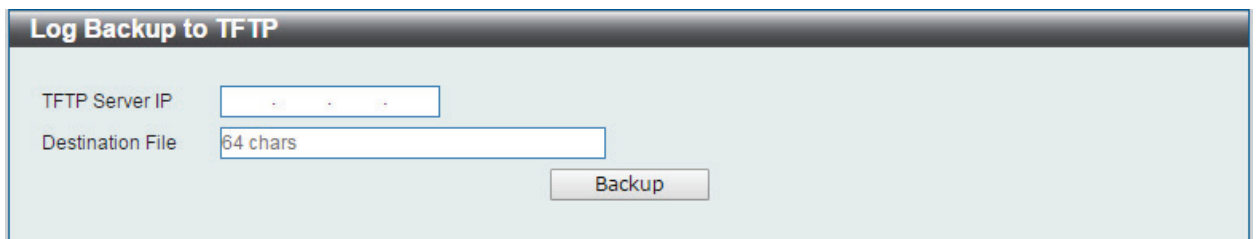


Figure 3-12 Log Backup to TFTP window

T

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IPv4 address here.
Destination File	Enter the destination filename and path where the log file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the system log backup.

Ping

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

To view the following window, click **Tools > Ping**, as shown below:

Figure 3-13 Ping window

The fields that can be configured for 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.

Click the **Start** button to initiate the Ping Test for each individual section.

After clicking the Start button in IPv4 Ping section, the following IPv4 Ping Result section will appear:

Figure 3-14 Ping - IPv4 Ping Result window

Click the **New Ping** button to halt the Ping Test and return to the IPv4 Ping section.

Reset

This window is used to reset the Switch's configuration to the factory default settings. To view the following window, click **Tools > Reset**, as shown below:

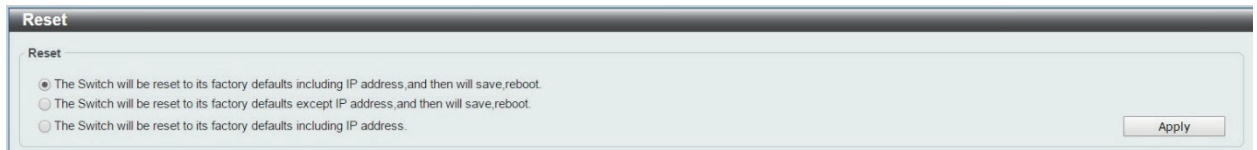


Figure 3-15 Reset window

Select the **The Switch will be reset to its factory defaults including IP address, and then will save, reboot** option to reset the Switch's configuration to its factory default settings.

Select the **The Switch will be reset to its factory default except IP address, and then will save, reboot** option to reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

Select the **The Switch will be reset to its factory defaults including IP address** option to reset the Switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so. To view the following window, click **Tools > Reboot System**, as shown below:

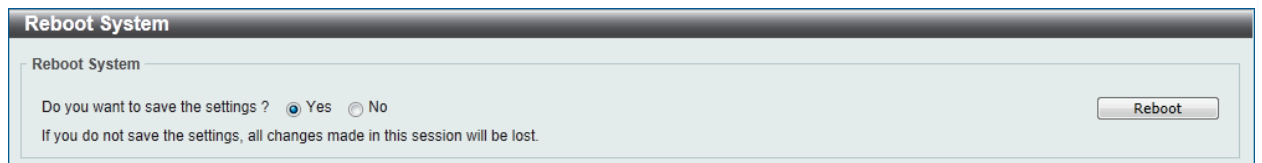


Figure 3-16 Reboot System window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

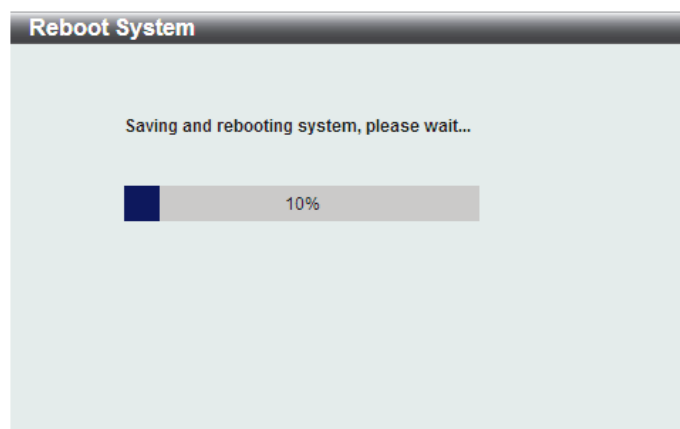


Figure 3-17 Reboot System - Rebooting window

4. System

[Device Information](#)
[System Information Settings](#) [Port Configuration](#)
[PoE](#)
[System Log Time](#)
[Time Profile](#)

Device Information

In this window, the Device Information, CPU, and Used status are displayed. It appears automatically when you log in the Switch. To return to the Device Information window after viewing other windows, click the **DIS-200G-12PS/12PSW** link.

Device Information			
Device Information			
Device Type	DIS-200G-12PS/12PSW PoE GE Switch	MAC Address	00-01-02-03-04-05
System Name	Switch	IP Address	10.90.90.90
System Location		Mask	255.0.0.0
System Contact		Gateway	Settings
Boot PROM Version	Ver 1.00.001	System Time	10:56:17, 2017-06-21
Firmware Version	Ver 1.00.B035	Serial Number	
Hardware Version	A1		

Figure 4-1 Device Information window

System Information Settings

System Information

The user can enter a System Name, System Location, and System Contact to aid in defining the Switch. To view the following window, click **System > System Information Settings**, as shown below:

System Information Settings	
System Information Settings	
System Name	<input type="text" value="Switch"/>
System Location	<input type="text" value="255 chars"/>
System Contact	<input type="text" value="255 chars"/>
<input type="button" value="Apply"/>	

Figure 4-2 System Information Settings window

The fields that can be configured 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. This string can be up to 255 characters long.
System Contact	Enter a contact name for the Switch, if so desired. This string can be up to 255 characters long.

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

IPv4 Interface

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

To view the following window, click **System > System Information Settings > IPv4 Interface**, as shown below:

Figure 4-3 IPv4 Interface window

The fields that can be configured are described below:

Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are Static and DHCP. When the Static option is selected, users can enter the IPv4 address of this interface manually in the fields provided. When the DHCP option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for management interface here.
Mask	Enter the IPv4 subnet mask for management interface here.
Gateway	Enter the IPv4 default gateway here.
DHCP Retry Time	Enter the DHCP retry times when “Get IP From” is selected as DHCP mode. The times are valid from 5 to 120 times. Each time of retry contains 5 seconds.

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

IPv6 Interface

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

To view the following window, click **System > System Information Settings > IPv6 Interface**, as shown below:

Figure 4-4 IPv6 Interface window

The fields that can be configured are described below:

Parameter	Description
IPv6 State	Click to enable or disable the IPv6 feature. When state is enabled, IPv6 link-local address will assigned to management VLAN automatically. If state is disabled and static IPv6 address is not set, the IPv6 feature will be disabled on switch.
Static IPv6 Address / Mask	Enter the IPv6 address and submask for management interface here.

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

Port Configuration

Port Settings

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

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

Port	Link Status	State	MDIX	Flow Control	Duplex	Speed	Description
eth1/0/1	1000M-Full	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/2	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/3	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/4	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/5	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/6	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/7	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/8	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/9	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/10	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/11	Down	Enabled	Auto	Disabled	Auto	Auto	
eth1/0/12	Down	Enabled	Auto	Disabled	Auto	Auto	

Figure 4-5 Port Settings window

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 physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are Auto, Normal, and Cross. 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's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a cross-over cable. Cross - Select this option for cross cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another switch through a straight cable.
Flow Control	Select to either turn flow control On or Off here. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two.
Duplex	Select the duplex mode used here. Options to choose from are Auto, Half, and Full.
Speed	Select the port speed option here. This option will manually force the connected on the selected port to only connect at the speed specified here. Options to choose from are Auto, 10M, 100M, 1000M.
Description	Enter a 64 characters description for the corresponding port here.

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

Jumbo Frame

This window is used to view 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 9600 bytes.

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

Port	Maximum Receive Frame Size (bytes)
eth1/0/1	1518
eth1/0/2	1518
eth1/0/3	1518
eth1/0/4	1518
eth1/0/5	1518
eth1/0/6	1518
eth1/0/7	1518
eth1/0/8	1518
eth1/0/9	1518
eth1/0/10	1518
eth1/0/11	1518
eth1/0/12	1518

Figure 4-6 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 1518 and 9600 bytes. By default, this value is 1518 bytes.

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

PoE(DIS-200G-12PS and DIS-200G-12PSW Only)

This switch 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 follows the standard PSE (Power Sourcing Equipment) 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 (Powered Device) and automatically sends power to it.
- The Auto-disable feature occurs under two conditions: firstly, if the total power consumption exceeds the system power limit; and secondly, 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 802.3af/at PDs receive power according to the following classification:

Class	Maximum power used by PD
0	12.95W
1	3.84W
2	6.49W
3	12.95W
4	25.5W

PSE provides power according to the following classification:

Class	Maximum power used by PD
0	15.4W
1	4.0W
2	7.0W
3	15.4W
4	30W

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:

Delivered (W)	Power Budget (W)	Usage Threshold (%)	Trap State
0.0	240	99	Disabled

Figure 4-7 PoE System window

The fields that can be configured 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.
Trap State	Select this option to enable or disable the sending of PoE notifications.

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

PoE Status

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

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

PoE Status

PoE Status

Port	State	Class	Max (W)	Used (W)
eth1/0/1	Searching	Class-0	0.0	0.0
eth1/0/2	Searching	Class-0	0.0	0.0
eth1/0/3	Searching	Class-0	0.0	0.0
eth1/0/4	Searching	Class-0	0.0	0.0
eth1/0/5	Searching	Class-0	0.0	0.0
eth1/0/6	Searching	Class-0	0.0	0.0
eth1/0/7	Searching	Class-0	0.0	0.0
eth1/0/8	Searching	Class-0	0.0	0.0

Note:
Faulty Code:
 [1] MPS (Maintain Power Signature) Absent
 [2] PD short
 [3] Overload
 [4] Power Denied
 [5] Thermal Shutdown
 [6] Startup Failure
 [7] Classification Failure

Figure 4-8 PoE Status window

PoE Configuration

This window is used to configure the PoE 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 Mode: Auto Time Profile: None Apply

Port	Admin	Priority	Time Profile
eth1/0/1	auto	Low	Delete Time Profile
eth1/0/2	auto	Low	Delete Time Profile
eth1/0/3	auto	Low	Delete Time Profile
eth1/0/4	auto	Low	Delete Time Profile
eth1/0/5	auto	Low	Delete Time Profile
eth1/0/6	auto	Low	Delete Time Profile
eth1/0/7	auto	Low	Delete Time Profile
eth1/0/8	auto	Low	Delete Time Profile

Figure 4-9 PoE Configuration 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.
Priority	Select the priority for provisioning power to the port. Options to choose from are Critical, High and Low.
Mode	Select the power management mode for the PoE ports. Options to

	choose from are Auto and Never.
Time Profile	Select the name of the time range to determine the activation period.

Click the **Delete** Time Profile button to clear the setting in the corresponding Time Range field.

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

PD Alive

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

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

Figure 4-10 PD Alive window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
PD Alive State	Select to enable or disable the PD Alive function on the specified port(s).
PD IP Address	Enter the IP address of the PD here.
Poll Interval	Enter the poll interval here. This is the interval between ping messages from the system to PDs connected to the PoE port(s). The range is from 10 to 300 seconds.
Retry Count	Enter the retry count here. This is the amount of ping messages that will be sent (at each interval) when PDs are not responding. The range is from 0 to 5.
Waiting Time	Enter the waiting time here. This is how long the system will wait before sending ping messages to the PD connected to the PoE port after a 'Reset' action was taken. The range is from 30 to 300 seconds.
Action	Select the action that will be taken here. Options to choose from are Reset, Notify, and Both. Reset - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

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

System Log

System Log Settings

This window is used to view and configure the system's log settings.

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

Figure 4-11 System Log Settings window

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

Parameter	Description
System log	Select this option to enable or disable the global state.

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

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

Parameter	Description
Buffer Log State	Select whether the enable or disable the buffer log's global state.

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

System Log Server Settings

This window is used to view and configure system log's server settings.

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

Figure 4-12 System Log Server Settings window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the system log server's IPv4 address here.
UDP Port	Enter the system log server's UDP port number here. This value must be 514 or between 1024 and 65535. By default, this value is 514.

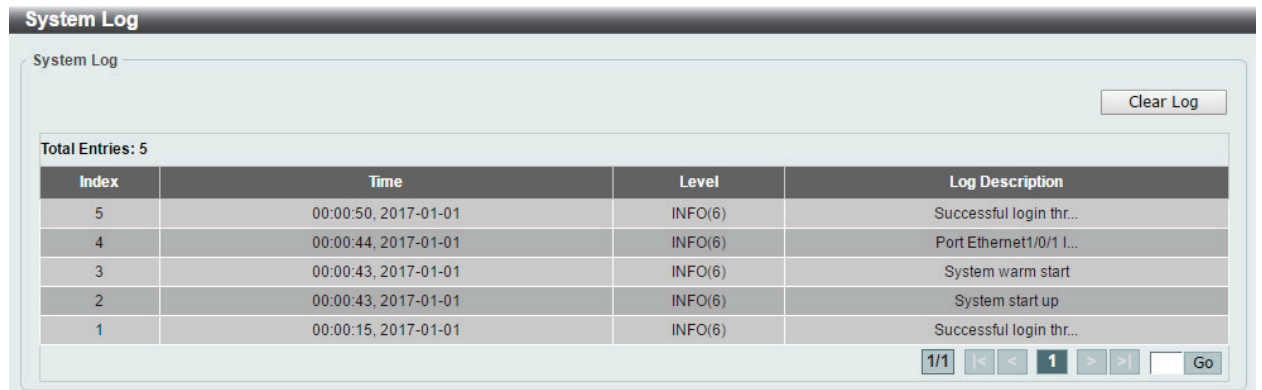
Severity	Select the severity value of the type of information that will be logged. Options to choose from are Errors, Warning, Notice and Informational.
Facility	Select the facility value here. Options to choose from are 0 to 7.

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

System Log

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

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



The screenshot shows the 'System Log' window with a 'Clear Log' button in the top right. Below the title bar, it indicates 'Total Entries: 5'. A table displays the following log entries:

Index	Time	Level	Log Description
5	00:00:50, 2017-01-01	INFO(6)	Successful login thr...
4	00:00:44, 2017-01-01	INFO(6)	Port Ethernet1/0/1 L...
3	00:00:43, 2017-01-01	INFO(6)	System warm start
2	00:00:43, 2017-01-01	INFO(6)	System start up
1	00:00:15, 2017-01-01	INFO(6)	Successful login thr...

At the bottom right of the table, there are navigation controls: '1/1', left and right arrows, a '1' in a box, and a 'Go' button.

Figure 4-13 System Log window

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

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

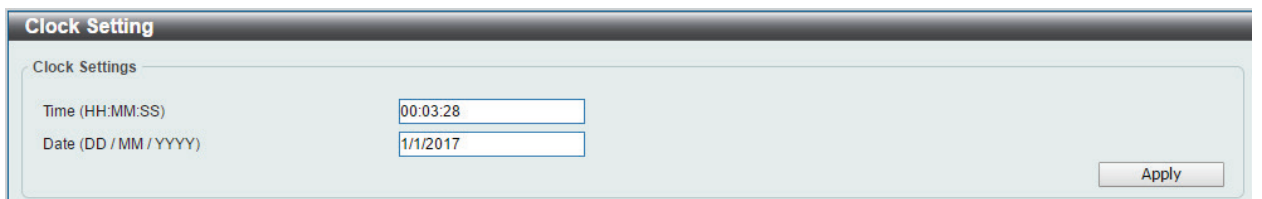
Time and SNTP

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, organize the SNTP subnet of servers and clients, and adjust the system clock in each participant.

Clock Settings

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

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



The screenshot shows the 'Clock Setting' window with an 'Apply' button in the bottom right. The 'Clock Settings' section contains two input fields:

Time (HH:MM:SS)

Date (DD / MM / YYYY)

Figure 4-14 Clock Settings window

The fields that can be configured are described below:

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

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

Time Zone Settings

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

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

Figure 4-15 Time Zone Settings window

The fields that can be configured are described below:

Parameter	Description
Summer Time State	Select the summer time setting. Options to choose from are Disabled, Recurring Setting, and Date Setting. 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's offset from Coordinated Universal Time (UTC).

The fields that can be configured for **Recurring Setting** are described below:

Parameter	Description
From: Week of the Month	Select week of the month that summer time will start.
From: Day of the Week	Select the day of the week that summer time will start.
From: Month	Select the month that summer time will start.
From: Time (HH:MM)	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 (HH:MM)	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 for Date Setting 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 (HH:MM)	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 (HH:MM)	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

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

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

The screenshot shows the SNTP Settings window with the following details:

- SNTP Global Settings:**
 - Current Time Source: System Clock
 - SNTP State: Disabled (dropdown menu)
 - Pool Interval (30-99999): 720 sec
 - Apply button
- SNTP Server Setting:**
 - IPv4 Address: [Empty text box]
 - Apply button
- Table:**

SNTP server	Stratum	Version	Last Receive
0.0.0.0	-	-	-

Figure 4-16 SNTP Settings window

The fields that can be configured for 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 for SNTP Server Setting are described below:

Parameter	Description
IPv4 Address	Enter the IP address of the SNTP server which provides the clock synchronization.

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

Time Profile

This window is used to view and configure the time range settings.

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

Figure 4-17 Time Range window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter the name of the time range. 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 range. Tick the Daily option to use this time range for every day of the week. Tick the End Week Day option to use this time range from the starting day of the week until the end of the week, which is Sunday.
From Time / To Time	Select the starting and ending time of the day that will be used for this time range. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

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

5. Management

User Account Settings

SNMP

RMON

HTTP/HTTPS

D-Link Discovery Protocol

User Account Settings

This window is used to create and configure the user accounts. The active user account sessions can be viewed.

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

- **User - Privilege read-only.** This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- **Administrator - Privilege read-write.** This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this guide.

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

User Name	Privilege	Password	
admin	Read-Write	*****	Delete

Figure 5-1 User Management Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	Choose the user account name here.
Password	The password belongs to the user account. Up to 32 characters.

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

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 for proper operation, monitor performance and detect potential problems in 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 SNMP v.1 and v.2, 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 SNMP v.1 and v.2 management access are:

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

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

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 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

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 OFF 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.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from 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 for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. 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 on the SNMP V3 folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

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

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

Figure 5-2 SNMP Global Settings window

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

Parameter	Description
SNMP Global State	Select this option to enable or disable the SNMP feature.

The fields that can be configured for 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 authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string
Port Link Up	Tick this option to control the sending of port link up notifications. A linkup 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 linkDown trap is generated when the device recognizes a failure in one of the communication links.
Coldstart	Tick this option to control the sending of SNMP coldStart

	notifications.
Warmstart	Tick this option to control the sending of SNMP warmStart notifications.

Click the **Apply** button to 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 Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

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

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

Figure 5-3 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) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select the view type here. Options to choose from are Included, and Excluded. 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.

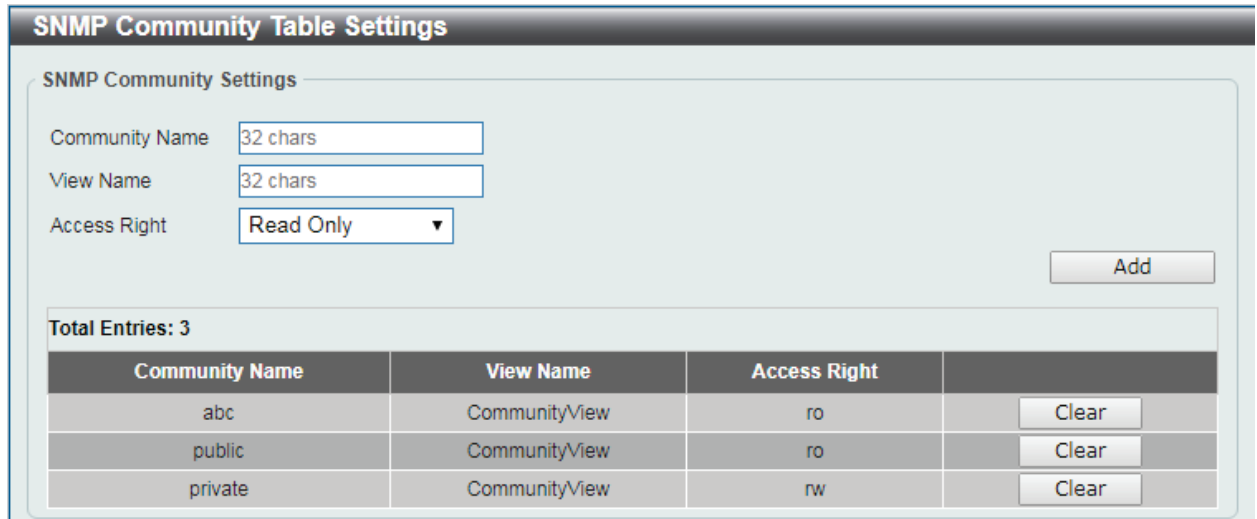
Click the **Delete** button to remove the specified entry.

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. The characteristics can be associated with the community string:

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

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



SNMP Community Table Settings

SNMP Community Settings

Community Name

View Name

Access Right

Total Entries: 3

Community Name	View Name	Access Right	
abc	CommunityView	ro	<input type="button" value="Clear"/>
public	CommunityView	ro	<input type="button" value="Clear"/>
private	CommunityView	rw	<input type="button" value="Clear"/>

Figure 5-4 SNMP Community Table Settings window

The fields that can be configured are described below:

Parameter	Description
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. 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 **Clear** button to remove the specified entry.

SNMP Group Table Settings

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous 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

SNMP Version Write View Name

Security Level Notify View Name

* Mandatory Field

Total Entries: 9

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

Figure 5-5 SNMP Group Table Settings window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the group name of a maximum of 32 characters. The syntax is general string that does not allow space.
User-based Security Model	Select the security model here. Options to choose from are SNMPv1 , SNMPv2c , and SNMPv3 . 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. 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.
Read View Name	Enter the read view name that the group user can access.
Write View Name	Enter the write view name that the group user can access.
Notify View Name	Enter a write view name that the group user 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 SNMP V3 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 features a text input field for 'Engine ID' containing the value '800000ab0300010203040000'. Below the input field is a note: 'Engine ID length is 24, the accepted character is from 0 to F.' To the right of the input field are two buttons: 'Default' and 'Apply'.

Figure 5-6 SNMP Engine ID Local Settings window

The fields that can be configured are described below:

Parameter	Description
Engine ID	Enter the engine ID string with the maximum of 24 characters.

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 configure and display 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 contains several configuration fields: 'User Name *' (32 chars), 'Group Name *' (32 chars), 'SNMP Version' (v1), 'Auth-Protocol by Password' (MD5), and 'Priv-Protocol by Password' (None). There are also two 'Password (8-32 chars)' input fields. An 'Add' button is located at the bottom right. Below the configuration fields, a table displays the current user settings:

Total Entries: 1						
User Name	Group Name	Security Model	Authentication Protocol	Privacy Protocol	Engine ID	
initial	initial	V3	None	None	800000ab03...	Delete

Figure 5-7 SNMP User Table Settings window

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	Enter the SNMP group name to which the user belongs. The syntax is general string that does not allow spaces.
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	When selecting v3 in the SNMP Version drop-down list, and selecting either Password or Key in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are MD5 , and SHA . 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.
Priv-Protocol	When selecting v3 in the SNMP Version drop-down list, and selecting either Password or Key in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are None , and DES56 . 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.

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 configure and display 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:

SNMP Version:

Security Level:

UDP Port (0-65535):

Community String / SNMPv3 User Name:

Total Entries: 2

Host IP Address	SNMP Version	UDP Port	Community String/ SNMPv3 User Name	
10.10.2.3	SNMPv3	162	initial	<input type="button" value="Delete"/>
10.10.2.3	SNMPv2c	162	public	<input type="button" value="Delete"/>

Figure 5-8 SNMP Host Table Settings

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
SNMP Version	Select the security model here. Options to choose from are SNMPv1, SNMPv2c, and SNMPv3. 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. 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 0 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string to be sent with the notification packet.

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

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

RMON

RMON Global Settings

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

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

Figure 5-9 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 configure and display the RMON statistics on the specified port.

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

Figure 5-10 RMON Statistics Settings window

The fields that can be configured are described below:

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

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

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

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

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

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

RMON Statistics Table																		
Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
2	eth1/0/1	4840998	27108	1130	1756	0	0	0	0	0	0	2881	16448	2494	399	7051	716	0

[Back](#)

Figure 5-11 RMON Statistics Table window

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

RMON History Settings

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

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

Figure 5-12 RMON History Settings window

The fields that can be configured are described below:

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

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

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

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

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

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

RMON History Table													
Index	Sample	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Utilization	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event
1	1	356188	1961	69	114	100	0	0	0	0	0	0	183

Figure 5-13 RMON History Table window

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

RMON Alarm Settings

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

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

RMON Alarm Settings											
RMON Alarm Settings											
Index (1-65535) *	<input type="text"/>	Interval (1-2147483647) *	<input type="text"/>	sec							
Variable *	<input type="text" value="N.N.N..N"/>	Type	<input type="text" value="Absolute"/>	▼							
Rising Threshold (0-2147483647) *	<input type="text"/>	Falling Threshold (0-2147483647) *	<input type="text"/>								
Rising Event Number (1-65535)	<input type="text"/>	Falling Event Number (1-65535)	<input type="text"/>								
Owner	<input type="text" value="1-127 chars"/>										
											<input type="button" value="Add"/>
Total Entries: 1											
Index	Interval (sec)	Variable	Type	Last Value	Rising Threshold	Falling Threshold	Rising Event No.	Falling Event No.	Startup Alarm	Owner	
1	30	1.3.6.1.2.1.2.2.1.12.6	Absolute	0	20	10	1	1	Rising or Faling	Name	<input type="button" value="Delete"/>
											1/1 <input type="button" value="←"/> <input type="button" value="1"/> <input type="button" value="→"/> <input type="button" value="Go"/>

Figure 5-14 RMON Alarm Settings window

The fields that can be configured are described below:

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

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

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

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

RMON Event Settings

This window is used to configure and display event entries.

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

Figure 5-15 RMON Event Settings

The fields that can be configured are described below:

Parameter	Description
Index	Enter the index of the alarm entry between 1 and 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 5-16 Event Logs Table window

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

HTTP/HTTPS

This window is used to configure the web server running on HTTP or HTTPS protocol.
To view the following window, click **Management > HTTP/HTTPS**, as shown below:

Figure 5-17 HTTP/HTTPS window

The fields that can be configured for **HTTP/HTTPS** are described below:

Parameter	Description
WEB Session	Select the protocol for web server.
Web Session Timeout	Enter the session timeout value for web session. The range of this value is from 60 to 36000 seconds.

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

D-Link Discovery Protocol

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

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

Figure 5-18 D-Link Discovery Protocol window

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

Parameter	Description
D-Link Discovery Protocol State	Select this option to enable or disable DDP global state.
Report Timer	Select the interval in seconds between two consecutive DDP report messages. Options to choose from are 30, 60, 90, 120, and Never.

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

6. Layer 2 Features

FDB
VLAN
Spanning Tree
Loopback Detection
Link Aggregation
L2 Multicast Control
LLDP

FDB

Static FDB

Unicast Static FDB

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

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

Figure 6-1 Unicast Static FDB window

The fields that can be configured are described below:

Parameter	Description
Port	Allows the selection of the port number on which the MAC address entered resides.
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 or dropped. 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 remove 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 view 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 6-2 Multicast Static FDB window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID 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 view and configure the MAC address table's global settings.

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

Figure 6-3 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's aging time value here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

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

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.

Port	State
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled
eth1/0/10	Enabled
eth1/0/11	Enabled
eth1/0/12	Enabled

Figure 6-4 MAC Address Table Settings (MAC Address Learning) window

The fields that can be configured are described below:

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

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

MAC Address Table

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

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

VID	MAC Address	Type	Port
1	00-01-C1-13-12-02	Static	CPU
1	00-E0-4C-68-03-12	Dynamic	eth1/0/9
1	01-00-00-00-00-02	Static	eth1/0/1

Figure 6-5 MAC Address Table window

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

VLAN

802.1Q VLAN

This window is used to view and configure the VLAN settings on this switch.

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

Figure 6-6 802.1Q VLAN window

The fields that can be configured for 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 accept the changes made.

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

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.

Management VLAN

This window is used to configure the management VLAN function.

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

Figure 6-7 Management VLAN window

The fields that can be configured are described below:

Parameter	Description
VID	Enter the VID to allow user use this VLAN to manage the switch.

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

GVRP

GVRP Global

This window is used to view and configure the GARP VLAN Registration Protocol (GVRP) global settings. To view the following window, click **L2 Features > VLAN > GVRP > GVRP Global**, as shown below:

Figure 6-8 GVRP Global window

The fields that can be configured are described below:

Parameter	Description
Asymmetric VLAN State	Select this option to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select this option to enable or disable the dynamic VLAN creation function here.
Join Time	Enter the Join Time value in centiseconds. This value must be between 1 and 20 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value in centiseconds. This value must be between 60 and 300 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value in centiseconds. This value must be between 1000 and 5000 centiseconds. By default, this value is 1000 centiseconds..

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

GVRP Port

This window is used to view and configure the GVRP port settings.

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

Figure 6-9 GVRP Port window

Guide 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.
GVRP Status	Select this option to enable or disable the GVRP port status. This enables the port to dynamically become a member of a VLAN. By default, this option is disabled.

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

GVRP Advertise VLAN

This window is used to view and configure the GVRP advertised VLAN settings.

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

The screenshot shows the 'GVRP Advertise VLAN' configuration window. At the top, there are four input fields: 'From Port' (dropdown menu showing 'eth1/0/1'), 'To Port' (dropdown menu showing 'eth1/0/1'), 'Action' (dropdown menu showing 'Add'), and 'Advertise VID List' (text input field containing '1,3 or 2-5'). An 'Apply' button is located to the right of these fields. Below the form is a table with two columns: 'Port' and 'Advertise VLAN'. The 'Port' column lists ports from eth1/0/1 to eth1/0/12. The 'Advertise VLAN' column is currently empty.

Figure 6-10 GVRP Advertise VLAN window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Action	Select the advertised VLAN to port mapping action that will be taken here. Options to choose from are All, Add, Remove and Replace. When selecting All, all the advertised VLANs will be used.
Advertise VID List	Enter the advertised VLAN ID list here.

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

GVRP Forbidden VLAN

This window is used to view and configure the GVRP forbidden VLAN settings.

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

Port	Forbidden VLAN
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	
eth1/0/9	
eth1/0/10	
eth1/0/11	
eth1/0/12	

Figure 6-11 GVRP Forbidden VLAN window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are All, Add, Remove and Replace. When selecting All, all the forbidden VLANs will be used.
Forbidden VID List	Enter the forbidden VLAN ID list here.

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

Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

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

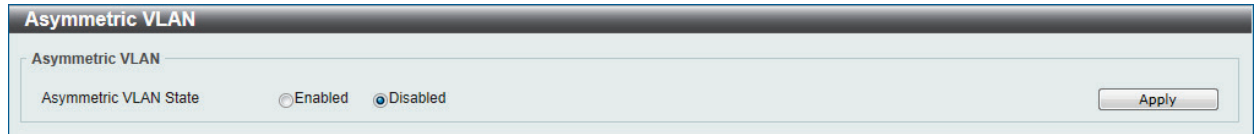


Figure 6-12 Asymmetric VLAN window

The fields that can be configured are described below:

Parameter	Description
Asymmetric VLAN State	Select this option to enable or disable the asymmetric VLAN function

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

VLAN Interface

This window is used to view and configure 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	VLAN Detail	Edit
eth1/0/1	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/2	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/3	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/4	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/5	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/6	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/7	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/8	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/9	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/10	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/11	Hybrid	Enabled	Admit All	VLAN Detail	Edit
eth1/0/12	Hybrid	Enabled	Admit All	VLAN Detail	Edit

Figure 6-13 VLAN Interface window

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

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

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

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

Figure 6-14 VLAN Interface Information window

More detailed information about the VLAN of the specific interface is displayed.

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

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

Figure 6-15 Configure 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 this option to enable or disable the ingress checking function.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

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

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

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

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

- Port: eth1/0/1
- VLAN Mode: Hybrid
- Acceptable Frame: Admit All
- Ingress Checking: Disabled
- Native VLAN: Native VLAN
- VID (1-4094): [Empty text box]
- Action: Add
- Add Mode: Untagged Tagged
- Allowed VLAN Range: [Empty text box]

Figure 6-16 Configure 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 the check box to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the Native VLAN check box, this option 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 information here.

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

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

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

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

- Port: eth1/0/1
- VLAN Mode: Trunk
- Acceptable Frame: Admit All
- Ingress Checking: Disabled
- Native VLAN: Native VLAN
- Action: All
- Add Mode: Untagged Tagged
- Allowed VLAN Range: [Empty text box]

Figure 6-17 Configure VLAN Interface - Trunk window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access, Hybrid, and Trunk.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only, Untagged Only, and Admit All.
Ingress Checking	After selecting Trunk as the VLAN Mode the following parameter will be available. Select to enable or disable the ingress checking function.
Native VLAN	Tick the check box to enable the native VLAN function. Also select if this VLAN supports Untagged or Tagged frames.
VID	After ticking the Native VLAN check box, this option 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, and Except.
Allowed VLAN Range	Enter the allowed VLAN range information here.

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

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

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.

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

Auto Surveillance Properties

Global Settings

Surveillance VLAN State: Enabled Disabled

Surveillance VLAN ID (2-4094):

Surveillance VLAN CoS:

Aging Time (1-65535): min

ONVIF Discover Port (554, 1025-65535):

Log State: Enabled Disabled

Member Ports

Dynamic Member Ports

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

ONVIF Global Status

Surveillance Device Detected (OUI): 0

IP-Camera Detected (ONVIF): 0

NVR Detected (ONVIF): 0

Port Settings

From Port: To Port: State:

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

Figure 6-18 Auto Surveillance Properties window

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

Parameter	Description
Surveillance VLAN State	Select this option to enable or disable the surveillance VLAN state.
Surveillance VLAN ID	Enter the surveillance VLAN ID. The range is from 2 to 4094.
Surveillance VLAN CoS	Select the priority of the surveillance VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stop.
ONVIF Discover Port	Enter the TCP/UDP port number here. The range is either 554, or from 1025 to 65535. This is used to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.
Log State	Set the Surveillance VLAN log state

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

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

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

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

MAC Settings and Surveillance Device

This window is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device**, as shown below:

MAC Settings and Surveillance Device

User-defined MAC Setting Auto Surveillance VLAN Summary

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

Component Type: Video Management Server Description: 8 chars

MAC Address: 00-01-02-03-00-00 Mask: FF-FF-FF-00-00-00 Apply

Total Entries: 4

ID	Component Type	Description	MAC Address	Mask	
1	D-Link Device	IP Surveillance Devi...	28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Delete
2	D-Link Device	IP Surveillance Devi...	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Delete
3	D-Link Device	IP Surveillance Devi...	B0-C5-54-00-00-00	FF-FF-FF-90-00-00	Delete
4	D-Link Device	IP Surveillance Devi...	F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	Delete

Figure 6-19 User -defined MAC Settings window

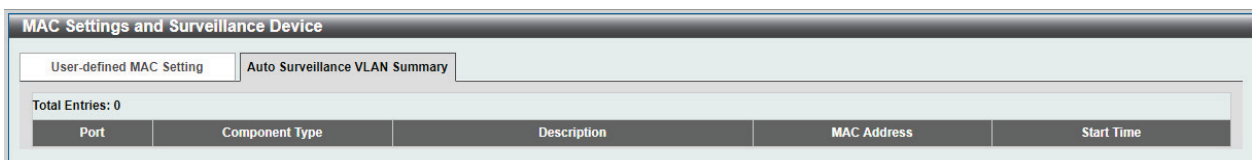
he fields that can be configured are described below:

Parameter	Description
Component Type	Select the surveillance component type. Options to choose from are Video Management Server, VMS Client/Remote Viewer, Video Encoder, Network Storage, and Other IP Surveillance Device.
Description	Enter the description for the user-defined OUI with a maximum of 32 characters.
MAC Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.

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

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

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



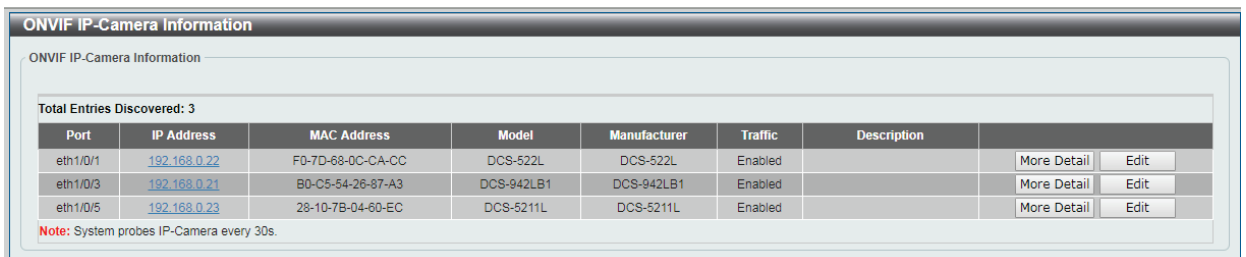
Port	Component Type	Description	MAC Address	Start Time
Total Entries: 0				

Figure 6-20 Auto Surveillance VLAN Summary window

ONVIF IP-Camera Information

This window is used to display ONVIF IP camera information.

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



Port	IP Address	MAC Address	Model	Manufacturer	Traffic	Description	More Detail	Edit
eth1/0/1	192.168.0.22	F0-7D-68-DC-CA-CC	DCS-522L	DCS-522L	Enabled		More Detail	Edit
eth1/0/3	192.168.0.21	B0-C5-54-26-87-A3	DCS-942LB1	DCS-942LB1	Enabled		More Detail	Edit
eth1/0/5	192.168.0.23	28-10-7B-04-60-EC	DCS-5211L	DCS-5211L	Enabled		More Detail	Edit

Note: System probes IP-Camera every 30s.

Figure 6-21 ONVIF IP-Camera Information window

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

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

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

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

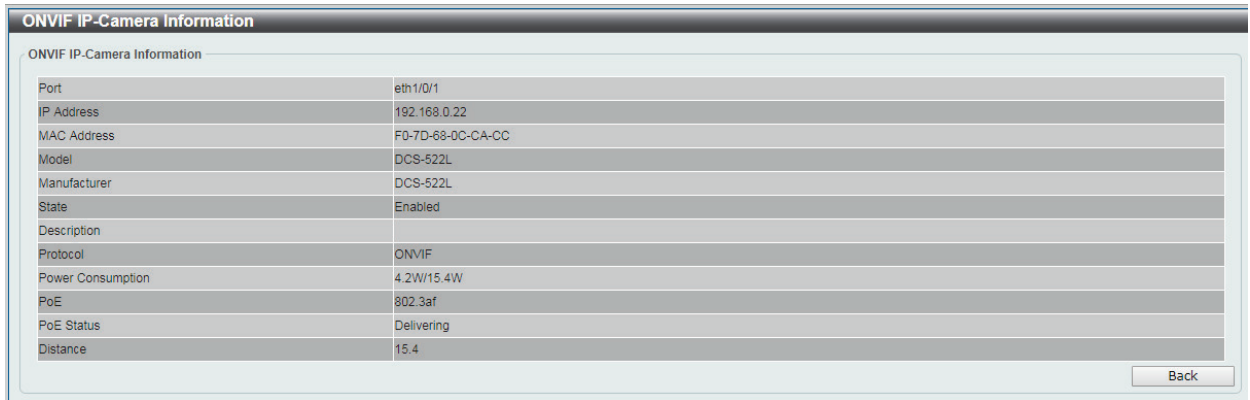


Figure 6-22 ONVIF IP-Camera Information (More Detail) window

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

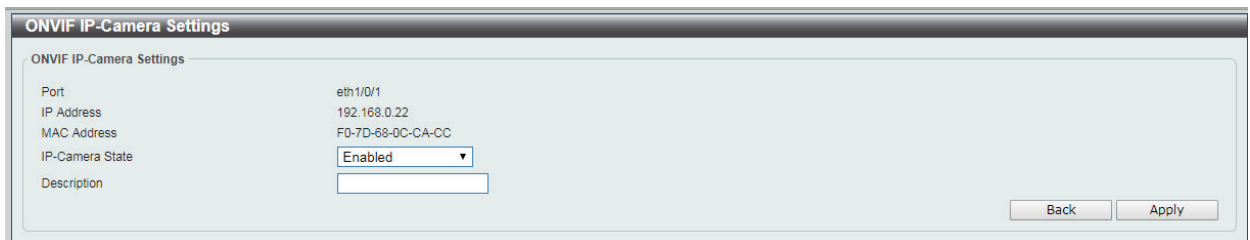


Figure 6-23 ONVIF IP-Camera Information (Edit) window

The fields that can be configured are described below:

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

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

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

ONVIF NVR Information

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

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

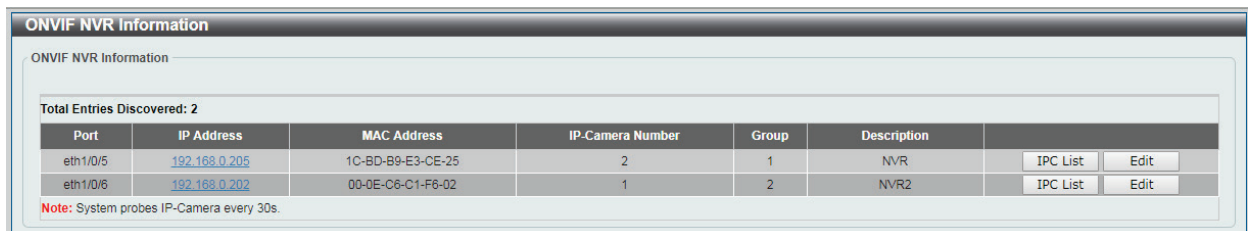


Figure 6-24 ONVIF NVR Information window

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

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

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

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

Port	IP Address	MAC Address	Group	Description
eth1/0/5	192.168.0.22	F0-7D-68-0C-CA-CC	1	
eth1/0/5	192.168.0.21	B0-C6-54-26-87-A3	1	
eth1/0/5	192.168.0.23	28-10-7B-04-60-EC	1	

Figure 6-25 ONVIF NVR Information (IP-Camera List) window

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

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

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

Port	IP Address	MAC Address	IP-Camera Number	Group	Description	IPC List	Apply	Edit
eth1/0/5	192.168.0.205	1C-BD-B9-E3-CE-25	2	1	NVR	IPC List	Apply	
eth1/0/6	192.168.0.202	00-0E-C6-C1-F6-02	1	2	NVR2	IPC List		Edit

Figure 6-26 ONVIF NVR Information (Edit) window

The additional fields that can be configured are described below:

Parameter	Description
Description	Enter the description for this NVR here.

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

Voice VLAN

Voice VLAN Global

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

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

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

Figure 6-27 Voice VLAN Global window

The fields that can be configured are described below:

Parameter	Description
Voice VLAN State	Select this option to enable or disable the voice VLAN.
Voice VLAN ID	Enter the voice VLAN ID. The value is range from 2 to 4094.
Voice VLAN CoS	Select the priority of the voice VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.

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

Voice VLAN Port

This window is used to show the ports voice VLAN information.

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

Port	State	Mode
eth1/0/1	Disabled	Auto Untagged
eth1/0/2	Disabled	Auto Untagged
eth1/0/3	Disabled	Auto Untagged
eth1/0/4	Disabled	Auto Untagged
eth1/0/5	Disabled	Auto Untagged
eth1/0/6	Disabled	Auto Untagged
eth1/0/7	Disabled	Auto Untagged
eth1/0/8	Disabled	Auto Untagged
eth1/0/9	Disabled	Auto Untagged
eth1/0/10	Disabled	Auto Untagged
eth1/0/11	Disabled	Auto Untagged
eth1/0/12	Disabled	Auto Untagged

Figure 6-28 Voice VLAN Port window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.
Mode	Select the mode of the port. Options to choose from are Auto Untagged, Auto Tagged, and Manual.

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

Voice VLAN OUI

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

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

Voice VLAN OUI

Voice VLAN OUI

OUI Address: 00-01-E3-00-00-00 Mask: FF-FF-FF-00-00-00 Description: 8 chars

Total Entries: 8

OUI Address	Mask	Description	
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	<input type="button" value="Delete"/>
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	<input type="button" value="Delete"/>
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	<input type="button" value="Delete"/>
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei3COM	<input type="button" value="Delete"/>
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC/Philips	<input type="button" value="Delete"/>
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	<input type="button" value="Delete"/>
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	<input type="button" value="Delete"/>
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	<input type="button" value="Delete"/>

Figure 6-8 Voice VLAN OUI window

The fields that can be configured are described below:

Parameter	Description
OUI Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.
Description	Enter the description for the user-defined OUI with a maximum of 32 characters.

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

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

Voice VLAN Device

This window is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

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

Voice VLAN Device

Voice VLAN Device Table

Total Entries: 0

Port	Voice Device Address	Start Time
------	----------------------	------------

Figure 6-30 Voice VLAN Device window

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 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 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or 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).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An 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. Consequentially, 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 have 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) and;
- 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 Bridge Global Settings window in the STP Version field)
- The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the MSTI Config 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 the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by

Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

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 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 thus faster topology adjustment. A drawback of 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
Discarding	Discarding	Blocking	No	No
Discarding	Discarding	Listening	No	No
Learning	Learning	Learning	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - 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 a new variable: the edge port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single work- station. 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, immediately becoming a normal spanning tree port.

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

MSTP or RSTP can interoperate with legacy equipment and is 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 provides for 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:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per-user-defined group of ports basis.

STP Global Settings

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

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

Figure 6-31 STP Global Settings window

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

Parameter	Description
Spanning Tree State	Select this option to enable or disable the STP global state 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 Traps are described below:

Parameter	Description
STP New Root Trap	Select this option to enable or disable the STP new root trap option here.
STP Topology Change Trap	Select this option 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 **Spanning Tree 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 **BPDU Forward** are described below:

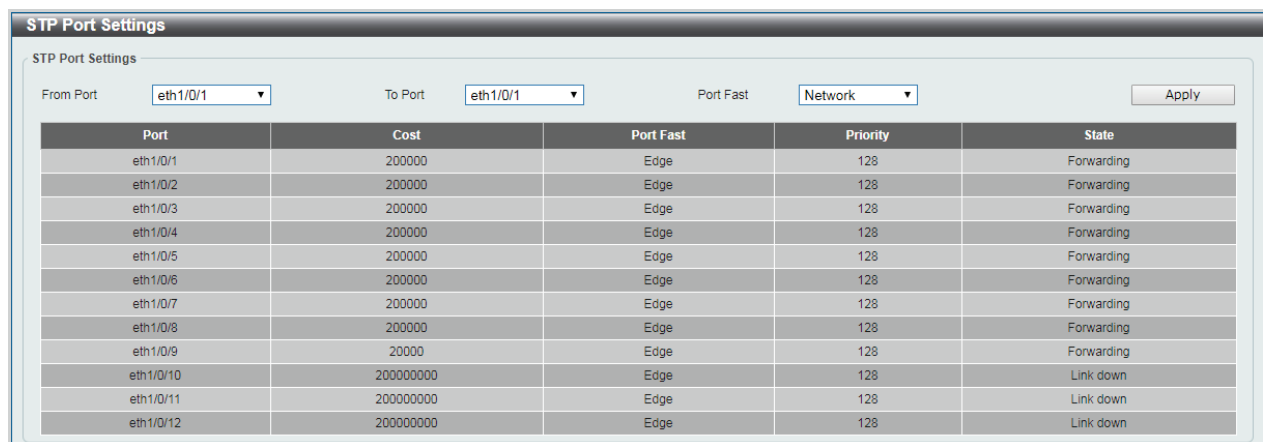
Parameter	Description
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is Disabled.

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

STP Port Settings

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

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



The screenshot shows the 'STP Port Settings' window with the following configuration:

From Port: eth1/0/1, To Port: eth1/0/1, Port Fast: Network, Apply button.

Port	Cost	Port Fast	Priority	State
eth1/0/1	200000	Edge	128	Forwarding
eth1/0/2	200000	Edge	128	Forwarding
eth1/0/3	200000	Edge	128	Forwarding
eth1/0/4	200000	Edge	128	Forwarding
eth1/0/5	200000	Edge	128	Forwarding
eth1/0/6	200000	Edge	128	Forwarding
eth1/0/7	200000	Edge	128	Forwarding
eth1/0/8	200000	Edge	128	Forwarding
eth1/0/9	20000	Edge	128	Forwarding
eth1/0/10	200000000	Edge	128	Link down
eth1/0/11	200000000	Edge	128	Link down
eth1/0/12	200000000	Edge	128	Link down

Figure 6-32 STP 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.
Port Fast	Select the port fast option here. Options to choose from are Network , Disabled , and Edge . 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 Disabled 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. By default, this option is Network .

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

MST Configuration Identification

This window is used to view and configure the MST configuration identification settings. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one CIST, or Common Internal Spanning Tree, of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

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

Figure 6-33 MST Configuration Identification window

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

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

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

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

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 16.
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 view and configure the STP instance settings.

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

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

1/1

CIST Global Info[Mode RSTP]	
Bridge Address	00-01-C1-13-14-10
Designated Root Address / Priority	00-01-C1-13-14-10 / 32768
Regional Root Bridge Address / Priority	00-01-C1-13-14-10 / 32768
Designated Bridge Address / Priority	00-01-C1-13-14-10 / 32768

Figure 6-34 STP Instance window

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.

MSTP Port Information

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

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

Instance ID	Cost	Priority	Status	Role
CIST	200000	128	forwarding	designated

1/1

Figure 6-35 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.

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.

ERPS (G.8032)

ERPS

This window is used to view and configure Ethernet Ring Protection Switching (ERPS) settings.

To view the following window, click **L2 Features > ERPS (G.8032) > ERPS**, as shown below:

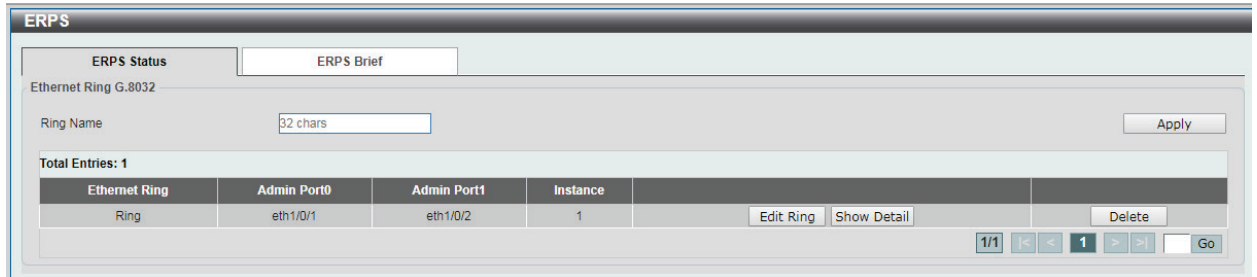


Figure 6-36 ERPS window

The fields that can be configured are described below:

Parameter	Description
Ring Name	Enter the Ethernet Ring Protection (ERP) instance's name here. This name can be up to 32 characters long.

Click the **Apply** button to create an ITU-T G.8032 ERP physical ring.

Click the **Edit Ring** button to modify an ITU-T G.8032 ERP physical ring.

Click the **Show Detail** button to view the ITU-T G.8032 ERP physical ring's status information.

Click the **Delete** button to delete the specified ITU-T G.8032 ERP physical ring.

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

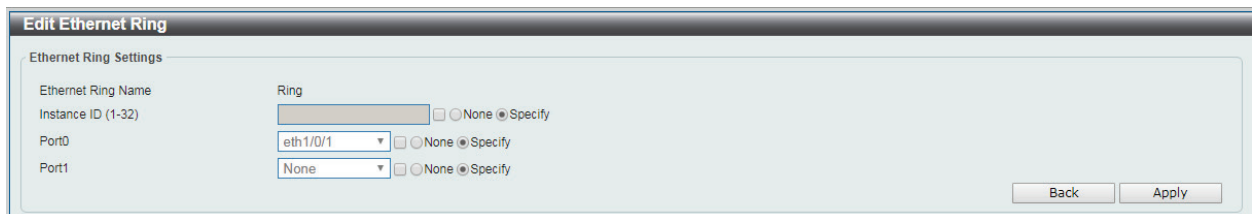


Figure 6-37 ERPS (Edit Ring) window

The fields that can be configured are described below:

Parameter	Description
Instance ID	Select the checkbox and enter the ERP instance number here. This value must be between 1 and 32. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Port0	Select the checkbox and then select the switch's unit ID and the port number that will be the first ring port of the physical ring. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Port1	Select the checkbox and then select the switch's unit ID and the port number that will be the second ring port of the physical ring. Select the None option, from the drop-down menu, specifies that the interconnected node is a local node endpoint of an open ring. Select the

	Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
--	---

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

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

After clicking the **ERPS Brief** tab, the following page will appear.

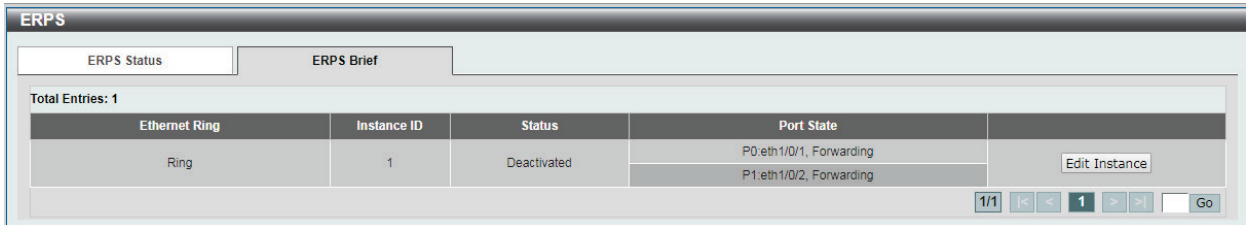


Figure 6-38 ERPS Brief window

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

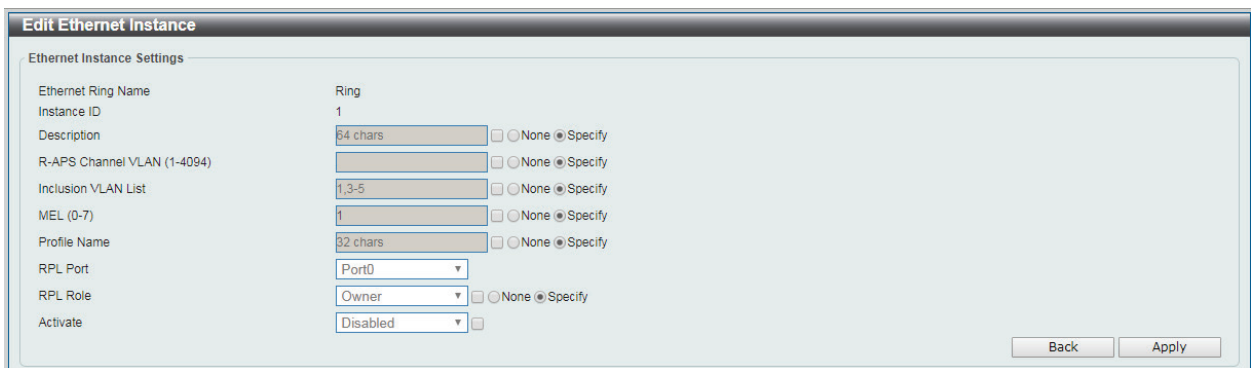


Figure 6-39 ERPS (Edit Instance) window

The fields that can be configured are described below:

Parameter	Description
Description	Select the checkbox and enter the ERP instance's description here. This description can be up to 64 characters long. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
R-APS Channel VLAN	Select the checkbox and enter the R-APS channel VLAN's ID for the ERP instance here. The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring. This value must be between 1 and 4094. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Inclusion VLAN List	Select the checkbox and then select the switch's unit ID and the port number that will be the second ring port of the physical ring. Select the None option, from the drop-down menu, specifies that the inter-connected node is a local node endpoint of an open ring. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
MEL	Select the checkbox and enter the ring MEL value of the ERP instance here. This value must be between 0 and 7. The configured MEL value of all ring nodes that participate in the same ERP

	instance should be identical. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
Profile Name	Select the checkbox and enter the G.8032 profile's name here that will be associated with this ERP instance. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance. This name can be up to 32 characters long. Select the Specify radio button to configure this parameter as per normal. Select the None radio button to revert this parameter to the default setting.
RPL Port	Select the checkbox and then select the RPL port option here. Options to choose from are Port0 and Port1. The option selected will be configured as the RPL port.
RPL Role	Select the checkbox and then select whether this node is the RPL owner or neighbor. Options to choose from are Owner and Neighbor. Enabling this option will specify this RPL as an owner.
Activate	Select the checkbox and then select whether or not to activate this ERP instance. Options to choose from are Enabled and Disabled. Enabling this option will activate this ERP instance.

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

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

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

The screenshot shows the 'ERPS Status' window with the following information:

ERPS Status Information	
Ethernet Ring	Ring
Admin Port0	eth1/0/1
Admin Port1	eth1/0/2
Instance ID	1
Instance Status	Deactivated
R-APS Channel	invalid r-aps vlan
Protected VLANs	
Port0	eth1/1, Forwarding
Port1	eth1/0/2, Forwarding
Profile	
Description	
Guard Timer	500 ms
Hold-Off Timer	0 ms
WTR Timer	5 min
Revertive	Enabled
MEL	1
RPL Role	None
RPL Port	-

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

Figure 6-40 ERPS (View Status) window

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

ERPS Profile

This window is used to view and configure the Ethernet Ring G.8032 profile settings.

To view the following window, click **L2 Features > ERPS (G.8032) > ERPS Profile**, as shown below:

The screenshot shows the 'ERPS Profile' window with the following configuration options and table:

Ethernet Ring G.8032 Profile

Profile Name: Apply

Total Entries: 1

Profile	Guard Timer (ms)	Hold-Off Timer (ms)	WTR Timer (min)	
q	500	0	5	Edit Delete

1/1 | < > 1 > > | Go

Figure 6-41 ERPS Profile window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the G.8032 profile's name here. This name can be up to 32 characters long. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance.

Click the **Apply** button to associate the G.8032 profile with the ERP instance created.

Click the **Delete** button to disassociate the G.8032 profile based on the **Profile Name** entered.

Click the **Edit** button to modify the specified G.8032 profile.

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

Figure 6-42 ERPS Profile (Edit) window

The fields that can be configured are described below:

Parameter	Description
Revertive	Select the checkbox and then select the revertive state. Options to choose from are Enable and Disabled. This function is used to revert back to the working transport entity, for example, when the RPL was blocked.
Guard Timer	Select the checkbox and enter the guard timer value here. This value must be between 10 and 2000 milliseconds. By default, this value is 500 milliseconds.
Hold-Off Timer	Select the checkbox and enter hold-off timer value here. This value must be between 0 and 10 seconds. By default, this value is 0 seconds
WTR Timer	Select the checkbox and enter the WTR timer value here. This value must be between 1 and 12 minutes. By default, this value is 5 minutes.

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

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

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port, this signifies a loop on the network. The Switch will automatically block the port and send an alert to the administrator. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

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

Loopback Detection

Loopback Detection Global Settings

Loopback Detection Enabled Disabled

Time Interval (1-32767) sec

Recover Time (0, 60-1000000) sec

Loopback Detection Trap Enabled Disabled

Apply

Loopback Detection Port Settings

From Port To Port State

Apply

Port	Loopback Detection State	Result
eth1/0/1	Disabled	Normal
eth1/0/2	Disabled	Normal
eth1/0/3	Disabled	Normal
eth1/0/4	Disabled	Normal
eth1/0/5	Disabled	Normal
eth1/0/6	Disabled	Normal
eth1/0/7	Disabled	Normal
eth1/0/8	Disabled	Normal
eth1/0/9	Disabled	Normal
eth1/0/10	Disabled	Normal
eth1/0/11	Disabled	Normal
eth1/0/12	Disabled	Normal

Figure 6-43 Loopback Detection window

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

Parameter	Description
Loopback Detection	Select to enable or disable loopback detection. The default is Disabled.
Time Interval	Enter the interval in seconds that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.
Recover Time	Enter the interval in seconds that the port will re-open if the port is in loop state. The valid range is from 60 to 1000000 seconds. The value 0 will block port forever until the switch next boot up. The default setting is 60 seconds.
Loopback Detection Trap	Select to enable or disable the loopback detection trap state.

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

The fields that can be configured for **Loopback Detection Port Settings** are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

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

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 6 port trunk groups with 1 to 8 ports in each group.

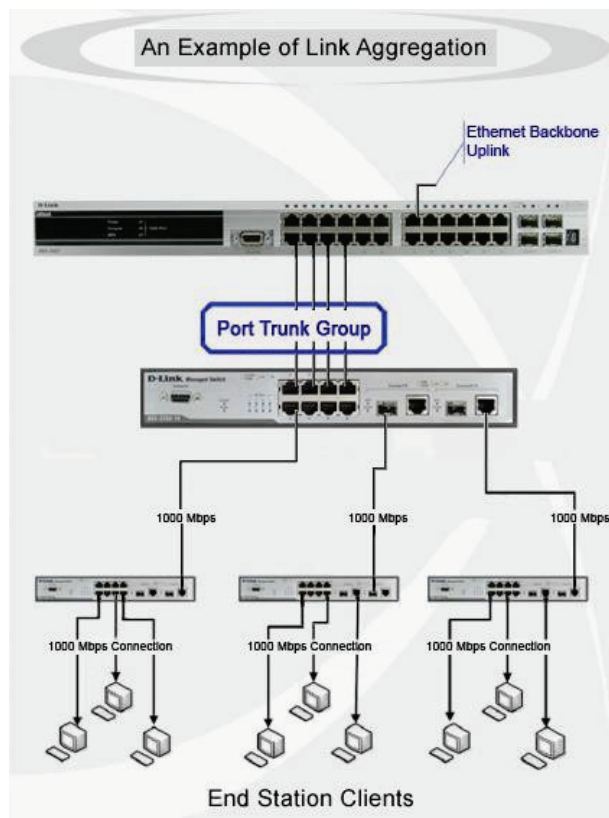


Figure 6-44 Example of Port Trunk Group

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 gives a bandwidth that is a multiple of a single link's bandwidth.

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

The Switch allows the creation of up to 6 link aggregation groups, each group consisting of 1 to 8 links (ports). Each port can only belong to a single link aggregation group.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

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, on the switch level. On the port level, the STP will use the port parameters calculation of port cost and in determining the state of the link aggregation group. 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 view and configure the link aggregation settings.

To view the following window, click **L2 Features > Link Aggregation**, as shown below:

Channel Group	Protocol	Max Ports	Member Number	Member Ports
Port-channel 1	LACP	8	3	eth1/0/3-5

Figure 6-45 Link Aggregation window

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

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 6. 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 entry based on the information entered.

Click the **Delete** Member Port button to remove the specific member port.

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

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

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

Port Channel

Port Channel Information

Port Channel 1
Protocol LACP

Port Channel Detail Information

Port	Working Mode	LACP State	Port Priority	Port Number
eth1/0/3	Active	down	32768	3
eth1/0/4	Active	down	32768	4
eth1/0/5	Active	down	32768	5

Port Channel Neighbor Information

Port	Partner System ID	Partner PortNo	Partner Port Priority
eth1/0/3	0,00-00-00-00-00-00	0	0
eth1/0/4	0,00-00-00-00-00-00	0	0
eth1/0/5	0,00-00-00-00-00-00	0	0

Note:

LACP State:

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

Figure 6-46 Port Channel window

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

L2 Multicast Control

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under IGMP Global Settings at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

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

Figure 6-47 IGMP Snooping Settings window

The field that can be configured for **Global Settings** is described below:

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

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

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

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

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

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

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

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

The fields that can be configured for **VLAN Fast Leave Settings** are described below:

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

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

IGMP Snooping Groups Settings

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

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

Figure 6-48 IGMP Snooping Groups Settings

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

Parameter	Description
VID	Enter a VLAN ID of the multicast group.
Group Address	Enter an IP multicast group address.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports

that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

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

MLD Control Messages

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

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

MLD Snooping Settings

This window is used to configure the MLD snooping settings.

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

Figure 6-49 MLD Snooping Settings window

The field that can be configured for **Global Settings** is described below:

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

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

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

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

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

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

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

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

The fields that can be configured for **VLAN Fast Leave Settings** are described below:

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

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.

MLD Snooping Groups Settings

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

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

Figure 6-50 MLD Snooping Group Settings window

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

Parameter	Description
VID	Enter a VLAN ID of the multicast group.
Group Address	Enter an IPv6 multicast group address.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

Multicast Filtering

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

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

Figure 6-51 Multicast Filtering window

The fields that can be configured are described below:

Parameter	Description
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are Forward Unregistered and Filter Unregistered. When selecting the Forward Unregistered option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the Filter Unregistered option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

LLDP

LLDP Global Settings

This window is used to configure the LLDP global settings.

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

Figure 6-52 LLDP Global Settings window

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

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Trap State	Select this option to enable or disable the LLDP trap state.

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

LLDP Neighbor Port Information

This window is used to display the information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

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

Figure 6-53 LLDP Neighbor Port Information window

7. Quality of Service (QoS)

802.1p Priority
Port Rate Limiting
Port Trust State

802.1p Priority

This window is used to view and configure the port's scheduler method and default CoS settings.

To view the following window, click **QoS > 802.1p Priority**, as shown below:

802.1p Priority Settings

Port Scheduler Method

From Port: eth1/0/1 To Port: eth1/0/1 Scheduler Method: WRR WRR: Low:Medium:High:Highest=1:2:4:8

Port Default CoS

From Port: eth1/0/1 To Port: eth1/0/1 Default CoS: Low

802.1p Priority Table

Class	Class 0 (Low queue)	Class 1 (Middle queue)	Class 2 (High queue)	Class 3 (Highest queue)
802.1p priority	1,2	0,3	4,5	6,7

Port	Scheduler Method	Default
eth1/0/1	WRR	Middle
eth1/0/2	WRR	Middle
eth1/0/3	WRR	Middle
eth1/0/4	WRR	Middle
eth1/0/5	WRR	Middle
eth1/0/6	WRR	Middle
eth1/0/7	WRR	Middle
eth1/0/8	WRR	Middle
eth1/0/9	WRR	Middle
eth1/0/10	WRR	Middle
eth1/0/11	WRR	Middle
eth1/0/12	WRR	Middle

Figure 7-1 802.1p Priority window

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

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Scheduler Method	<p>Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (SP) and Weighted Round-Robin (WRR). By default, the output queue scheduling algorithm is WRR.</p> <p>To set a CoS queue in the SP mode, any higher priority CoS queue must also be in the strict priority mode.</p> <p>WRR operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.</p>

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

The fields that can be configured in Port Default CoS are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are Low , Medium , High , and Highest .

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

Port Rate Limiting

This window is used to view and configure the port scheduler method settings.

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

Port Rate Limiting

Port Rate Limiting

From Port: eth1/0/1 To Port: eth1/0/1 Direction: Input Rate Limit (Granularity is 100 Kbps): 0,100-1048576 Kbps

Note: The input value of rate limit will auto round up to next possible value base on 100 Kbps.

Port	Input (Rate)
eth1/0/1	No Limit
eth1/0/2	No Limit
eth1/0/3	No Limit
eth1/0/4	No Limit
eth1/0/5	No Limit
eth1/0/6	No Limit
eth1/0/7	No Limit
eth1/0/8	No Limit
eth1/0/9	No Limit
eth1/0/10	No Limit
eth1/0/11	No Limit
eth1/0/12	No Limit

Figure 7-2 Port Rate Limiting window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction option here. Only support Input. When Input is selected, the rate limit for ingress packets is configured.
Rate Limit	Enter the input bandwidth value used in the space provided. This value must be between 100 and 1048576 kbps.

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

Port Trust State

This window is used to view and configure port trust state settings

To view the following window, click **QoS > Port Trust State**, as shown below:

Port	Trust State
eth1/0/1	Trust CoS
eth1/0/2	Trust CoS
eth1/0/3	Trust CoS
eth1/0/4	Trust CoS
eth1/0/5	Trust CoS
eth1/0/6	Trust CoS
eth1/0/7	Trust CoS
eth1/0/8	Trust CoS
eth1/0/9	Trust CoS
eth1/0/10	Trust CoS
eth1/0/11	Trust CoS
eth1/0/12	Trust CoS

Figure 7-3 Port Trust State 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.
Trust State	Select the port trust state option here. Options to choose from are CoS and DSCP.

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

DSCP CoS Mapping

This window is used to view and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > DSCP CoS Mapping**, as shown below:

CoS	DSCP List
0	0-7
1	8-16,18
2	17,19-23
3	24-31
4	32-39
5	40-47
6	48-55
7	56-63

Figure 7-4 DSCP CoS Mapping window

The fields that can be configured are described below:

Parameter	Description
CoS	Select the CoS value. Options to choose from are 0 to 7.
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63.

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

8. Security

[Port Security](#)
[RADIUS](#)
[Safeguard Engine](#)
[Traffic Segmentation](#)
[Storm Control](#)
[DoS Attack Prevention](#)
[Zone Defense](#)
[SSL](#)
[Web-based Access Control](#)

Port Security

Port Security Global Settings

This window is used to view and configure the port security global settings. Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

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

Figure 8-1 Port Security Global Settings window

The fields that can be configured for Port Security Trap Settings are described below:

Parameter	Description
Trap State	Click to enable or disable port security traps on the Switch.

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

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 0 indicates an SNMP trap to be generated for every security violation.

Port Security Port Settings

This window is used to view and configure the port security port settings.

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

The screenshot shows the 'Port Security Port Settings' window. At the top, there are configuration fields: 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'State' (Disabled), 'Maximum (1-64)' (32), 'Violation Action' (Protect), and 'Aging Time (0-1440)' (empty). An 'Apply' button is located to the right of these fields. Below the configuration fields is a table with the following data:

Port	Maximum	Current No.	Violation Action	Violation Count	Admin State	Current State	Aging Time
eth1/0/1	32	0	Protect	-	Disabled	-	0
eth1/0/2	32	0	Protect	-	Disabled	-	0
eth1/0/3	32	0	Protect	-	Disabled	-	0
eth1/0/4	32	0	Protect	-	Disabled	-	0
eth1/0/5	32	0	Protect	-	Disabled	-	0
eth1/0/6	32	0	Protect	-	Disabled	-	0
eth1/0/7	32	0	Protect	-	Disabled	-	0
eth1/0/8	32	0	Protect	-	Disabled	-	0

Figure 8-2 Port Security Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 1 and 64. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are Protect , Restrict , and Shutdown . Selecting Protect specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. Selecting Restrict specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. Selecting Shutdown specifies to shut down the port if there is a security violation and record the system log.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.

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

Port Security Address Entries

This window is used to view, clear and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:

Port	VID	MAC Address	Address Type	Remaining Time (mins)
eth1/0/1	1	00-11-22-33-44-55	Delete-on-Timeout	-

Figure 8-3 Port Security Address Entries window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port used for the configuration here.
MAC Address	Enter the MAC address here.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

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

RADIUS

RADIUS Global Settings

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

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

Figure 8-4 RADIUS Global Settings window

The fields that can be configured are described below:

Parameter	Description
Dead Time	Enter the dead time value here. This value must be between 1 and 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries. When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

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

RADIUS Server Settings

This window is used to view 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	
10.10.1.101	1812	1813	5	3	*****	Delete

Figure 8-5 RADIUS Server Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server's IPv4 address here.
IPv6 Address	Enter the RADIUS server's 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	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

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

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

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

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

The screenshot shows the 'RADIUS Statistic' window. It has a title bar 'RADIUS Statistic' and a sub-header 'RADIUS Statistic'. Below the sub-header is the text 'RADIUS Server Statistic' and a 'Clear All' button. A summary line reads 'Total Entries: 1'. Below this is a table with four columns: 'RADIUS Server Address', 'Authentication Port', 'Accounting Port', and 'State'. The data row shows '10.10.1.101', '1812', '1813', and 'Up'. Below the table is the text 'RADIUS Server Address: 10.10.1.101' and a 'Clear' button. At the bottom is another table with three columns: 'Parameter', 'Authentication Port', and 'Accounting Port'. The data rows are: 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), and Acct Response (NA, 0).

RADIUS Server Address	Authentication Port	Accounting Port	State
10.10.1.101	1812	1813	Up

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

Figure 8-6 RADIUS Statistic window

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.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

Safeguard Engine Settings

This window is used to view and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine Settings**, as shown below:

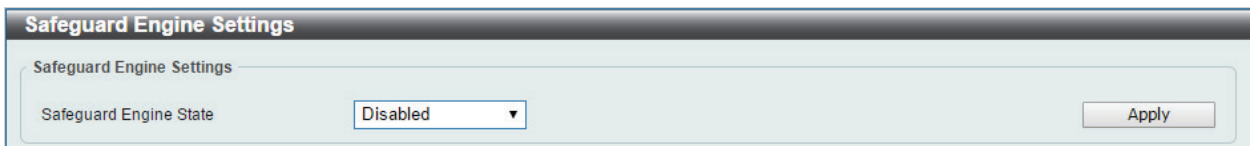


Figure 8-7 Safeguard Engine Settings window

The fields that can be configured for **Safeguard Engine Settings** are described below:

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.

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

Traffic Segmentation Settings

This window is used to view and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

To view the following window, click **Security > Traffic Segmentation Settings**, as shown below:

Port	Forwarding Domain
eth1/0/1	eth1/0/1

Figure 8-8 Traffic Segmentation Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the receiving port range used for the configuration here.
From Forward Port / To Forward Port	Select the forward port range used for the configuration here.

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

Click the **Delete** button to remove an entry based on the information entered.

Storm Control

This window is used to view and configure the storm control settings.

To view the following window, click **Security > Storm Control**, as shown below:

Storm	Status	Threshold
Unicast	Disabled	1
Multicast	Disabled	1
Broadcast	Disabled	1

Figure 8-9 Storm Control Settings window

The fields that can be configured for **Storm Control Settings** are described below:

Parameter	Description
Type	Select the type of storm attack that will be controlled here. Options to choose from are Broadcast, Multicast, and Unicast. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Status	Select to enable or disable the storm control feature for selected type.
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 1 and 1024000 packets per second.

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

DoS Attack Prevention Settings

This window is used to view and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types which can be detected by most switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack:** This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets which contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets which contain source port 0 to 1023 and SYN flag.
- **Ping Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size) which is 65535 bytes. The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

DoS Type	State	Action
Land Attack	Disabled	Drop
Blat Attack	Disabled	Drop
TCP Null Scan	Disabled	Drop
TCP Xmascan	Disabled	Drop
TCP SYN-FIN	Disabled	Drop
TCP SYN Src Port Less 1024	Disabled	Drop
Ping Death Attack	Disabled	Drop

Figure 8-10 DoS Attack Prevention Settings window

The fields that can be configured for **DoS Attack Prevention Settings** are described below:

Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
State	Select to enable or disable the DoS attack prevention feature's global state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is Drop.

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

Zone Defense

This window is used to view and configure the zone defense settings.

To view the following window, click **Security > Zone Defense Settings**, as shown below:

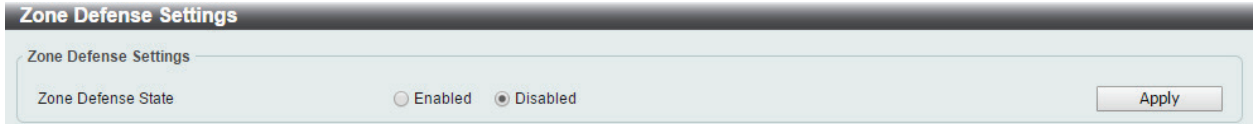


Figure 8-11 Zone Defense Settings window

The fields that can be configured for **Zone Defense Settings** are described below:

Parameter	Description
Zone Defense Status	Select to enable or disable the Zone Defense feature's global status here.

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

SSL

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

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

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support

SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. 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 view and configure the SSL feature's global settings.

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

Figure 8-12 SSL Global Settings window

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

Parameter	Description
SSL State	Select to enable or disable the SSL feature's global status here.

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

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

Parameter	Description
Key	Select the Key file that will be upgraded to switch. To browse to the appropriate file, located on the local computer, by pressing the Choose File button.
Certificate	Select the Certificate file that will be upgraded to switch. To browse to the appropriate file, located on the local computer, by pressing the Choose File button.

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

Web-based Access Control

Web-based Access Control (WAC) is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages (e.g., <http://www.dlink.com>) through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is unauthenticated, the Switch will launch a pop-up user name and password window to query users. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

D-Link's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration.

By default, the authentication web page is running on HTTP but not HTTPS protocol. To do authentication with HTTPS, please change the web server configuration to HTTPS.

Conditions and Limitations

- Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
- If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

Web Authentication

This window is used to view and configure the Web authentication settings.

To view the following window, click **Security > Web-based Access Control > Web Authentication**, as shown below:

Figure 8-13 Port Security Global Settings window

The fields that can be configured are described below:

Parameter	Description
Web Authentication State	Select to enable or disable the Web authentication feature's global state.
Trap State	Select to enable or disable the Web authentication feature's trap state.
Virtual IPv4	Enter the virtual IPv4 address used here. The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. So it's not allowed to configure virtual IP in the same subnet as the Switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly. If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication.
Virtual IPv6	Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.
Redirection Path	Enter the redirection path here. This path can be up to 128 characters long.

WAC Port Settings

This window is used to view and configure the WAC port settings.

To view the following window, click **Security > Web-based Access Control > WAC Port Settings**, as shown below:

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

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled
eth1/0/9	Disabled
eth1/0/10	Disabled
eth1/0/11	Disabled
eth1/0/12	Disabled

Figure 8-14 WAC Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the WAC feature on the port(s) specified.

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

WAC Customize Page

This window is used to view and configure the WAC customized login page.

To view the following window, click **Security > Web-based Access Control > WAC Customize Page**, as shown below:

Figure 8-15 WAC Customize Page window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There are 5 lines available for additional information.

Click the **Set to Default** button to replace the information with the default information.

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

9. 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' and 'To Port', both set to 'eth1/0/1'. To the right of these is a 'Test' button. Below the dropdowns is a table with columns: Port, Type, Link Status, Test Result, Cable Length (M), and a 'Clear' button for each row. A 'Clear All' button is located at the top right of the table area.

Port	Type	Link Status	Test Result	Cable Length (M)	Clear
eth1/0/1	1000BaseT	Link Down	-	-	Clear
eth1/0/2	1000BaseT	Link Down	-	-	Clear
eth1/0/3	1000BaseT	Link Up	OK	<7	Clear
eth1/0/4	1000BaseT	Link Down	-	-	Clear
eth1/0/5	1000BaseT	Link Down	-	-	Clear
eth1/0/6	1000BaseT	Link Down	-	-	Clear
eth1/0/7	1000BaseT	Link Down	-	-	Clear
eth1/0/8	1000BaseT	Link Down	-	-	Clear
eth1/0/9	1000BaseT	Link Down	-	-	Clear
eth1/0/10	1000BaseT	Link Down	-	-	Clear
eth1/0/11	None	Link Down	-	-	Clear
eth1/0/12	None	Link Down	-	-	Clear

Figure 9-1 Cable Diagnostics window

e 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.

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 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 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 show below:

Figure 9-2 DDM Settings window

The fields that can be configured are described below:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select this option to enable or disable sending alarm level trap.
Transceiver Monitoring Traps Warning	Select this option to enable or disable sending warning level trap.
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. 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 for each individual section.

DDM Temperature Threshold Settings

This window is used to 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 show 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)
eth1/0/11	-	-	-	-	-
eth1/0/12	-	-	-	-	-

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

Figure 9-3 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 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 show below:

DDM Voltage Threshold Settings

DDM Voltage Threshold Settings

Port: eth1/0/1 Action: Add Type: Low Alarm Value (0-6.55) V Apply

Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
eth1/0/11	-	-	-	-	-
eth1/0/12	-	-	-	-	-

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

Figure 9-4 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 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 show below:

DDM Bias Current Threshold Settings

DDM Bias Current Threshold Settings

Port: eth1/0/1 Action: Add Type: Low Alarm Value (0-131) mA: mA

Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
eth1/0/11	-	-	-	-	-
eth1/0/12	-	-	-	-	-

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

Figure 9-5 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.
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 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 show below:

DDM TX Power Threshold Settings

DDM TX Power Threshold Settings

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

Port	Current	High Alarm (mW)	High Warning (mW)	Low Warning (mW)	Low Alarm (mW)
eth1/0/11	-	-	-	-	-
eth1/0/12	-	-	-	-	-

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

Figure 9-6 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. 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 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 show below:

DDM RX Power Threshold Settings

DDM RX 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 (mW)	High Warning (mW)	Low Warning (mW)	Low Alarm (mW)
eth1/0/11	-	-	-	-	-
eth1/0/12	-	-	-	-	-

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

Figure 9-7 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 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. 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 show below:

DDM Status Table

DDM Status Table

Total Entries: 2

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power (mW)	RX Power (mW)
eth1/0/11	-	-	-	-	-
eth1/0/12	-	-	-	-	-

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

Figure 9-8 DDM Status Table window

10. Monitoring

Statistics

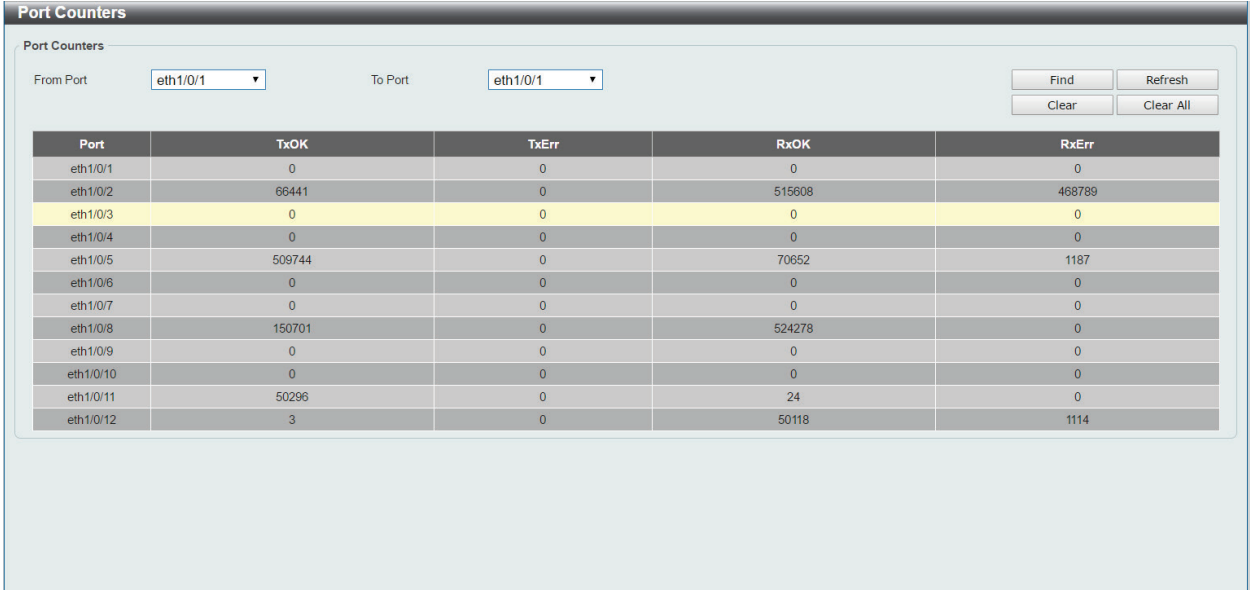
Mirror Settings

Statistics

Port Counters

This window is used to display port counter statistics.

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



The screenshot shows the 'Port Counters' window with a table of statistics. The table has five columns: Port, TxOK, TxErr, RxOK, and RxErr. The 'From Port' and 'To Port' dropdowns are both set to 'eth1/0/1'. The table contains 13 rows of data for ports eth1/0/1 through eth1/0/12. The 'eth1/0/3' row is highlighted in yellow.

Port	TxOK	TxErr	RxOK	RxErr
eth1/0/1	0	0	0	0
eth1/0/2	66441	0	515608	468789
eth1/0/3	0	0	0	0
eth1/0/4	0	0	0	0
eth1/0/5	509744	0	70652	1187
eth1/0/6	0	0	0	0
eth1/0/7	0	0	0	0
eth1/0/8	150701	0	524278	0
eth1/0/9	0	0	0	0
eth1/0/10	0	0	0	0
eth1/0/11	50296	0	24	0
eth1/0/12	3	0	50118	1114

Figure 10-1 Port Counters 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 **Find** button to locate a specific entry based on the information entered.

Click the **Refresh** button to refresh the display table.

Click the **Clear** button to clear all error counters of the specific port.

Click the **Clear All** button to clear all error counters of all ports.

Mirror Settings

This window is used to view and configure the mirror feature's settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

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

The screenshot shows the 'Mirror Settings' window. At the top, there's a title bar 'Mirror Settings'. Below it, the 'Mirror Settings' section contains four dropdown menus: 'Destination' (set to eth1/0/1), 'From Port' (set to eth1/0/1), 'To Port' (set to eth1/0/1), and 'Frame Type' (set to RX). There are 'Apply' and 'Delete' buttons. Below this is the 'Mirror Session Table' which has a table with columns for 'Source Ports' and 'Destination port'. The 'Source Ports' column is divided into 'Both', 'RX', and 'TX'. The 'Destination port' column is set to eth1/0/1.

Source Ports			Destination port
Both	RX	TX	
eth1/0/11			eth1/0/1

Figure 10-2 Mirror Settings window

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

Parameter	Description
Destination	Select the destination switch's port number.
Source	From the From Port drop-down menu, select the starting port number and from the To Port drop-down menu, select the ending port number. Lastly select the Frame Type option from the third drop-down menu. Options to choose from as the Frame Type are Both , RX , and TX . When selecting Both , traffic in both the incoming and outgoing directions will be mirrored. When selecting RX , traffic in only the incoming direction will be mirrored. When selecting TX , traffic in only the outgoing direction will be mirrored.

Click the **Apply** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

11. Green

Power Saving

EEE

Power Saving

This window is used to configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:

Figure 11-1 Power Saving window

The fields that can be configured 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.
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.
Type	Select the type of power saving. Options to choose from are Dim-LED and Hibernation.
Time Range	Select a time range profile.

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 Profile	
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
eth1/0/11		Delete
eth1/0/12		Delete

Figure 11-2 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 associated 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
eth1/0/11	Disabled
eth1/0/12	Disabled

Figure 11-3 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.

12. Surveillance Mode

Surveillance Overview

Port Information

IP-Camera Information

NVR Information

PoE Information

PoE Scheduling

Management

Time

Surveillance Settings

Surveillance Log

Health Diagnostic

Toolbar

Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device (such as the number of devices, device type, IP address, power consumption, link speed, and errors). Click on the **'more'** link to get more information about the devices connected to the port.

To return to the Surveillance Overview window after viewing other windows, click the **DIS-200G-12PS/12PSW** link.

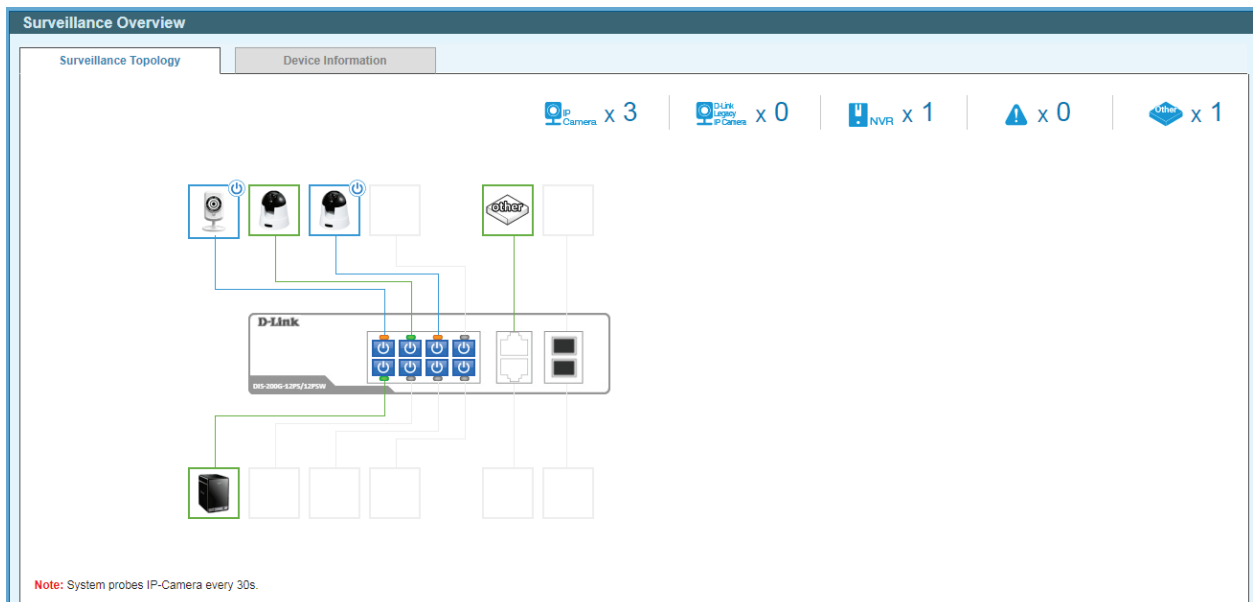












Figure 12-1 Surveillance Overview window

The following icons are available in this window and are described below:

Parameter	Description
 x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
 x 0	This displays the total amount of D-Link legacy IP cameras (detected by ASV 1.0) connected to the Ethernet ports on the Switch.
 x 1	This displays the total amount of Network Video Recorders (NVRs) connected to the Ethernet ports on the Switch.
 x 0	This displays the amount of surveillance warnings generated on the Switch.
 x 1	This displays the amount of other devices connected to the Ethernet ports on the Switch.
	This displays the device connected to the Ethernet port on the Switch. The green border around the image indicates that the device is a non-PoE device. The PD Alive function cannot be used on this device.
	This displays the device connected to the Ethernet port on the Switch. The blue border around the image indicates that the device is a PoE device and is receiving power from the Switch using PoE. The PD Alive function can be used on this device.
	Click this icon to disable PoE on the port.
	Click this icon to enable PoE on the port.

After clicking the  icon, the following window will appear:

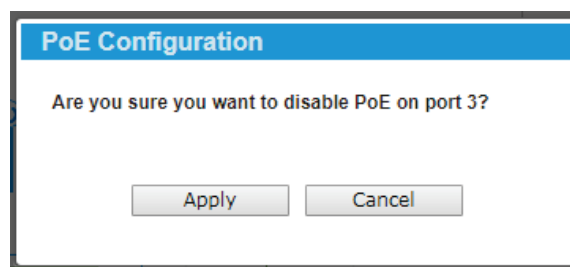


Figure 12-2 PoE Configuration window

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

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

After hovering (with the mouse pointer) over the **network device** icon, the following additional information will be displayed:

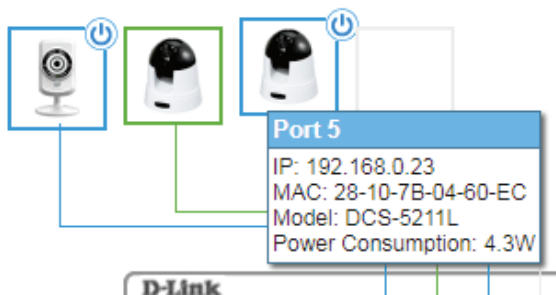


Figure 12-3 Additional Device Information

After clicking (left-click) the **network device** icon, the following window will appear.

Figure 12-4 PD Alive Configuration window

The fields that can be configured are described below:

Parameter	Description
PD Alive State	Select to enable or disable the PD Alive function here.
PD IP Address	Enter the IP address of the PD here.
Action	Select the action that will be taken here. Options to choose from are Reset , Notify , and Both . Reset - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

Click the **Ping Test** button to initiate the ping test to check if the PD is active or not.

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

Click the **Set to Default** button to return the settings to the default settings for this PD.

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

After clicking **Ping Test** button, the following window will appear.

PD Alive Configuration

PD Alive State: Disabled

PD IP Address: 192 - 168 - 0 - 23

Action: Both

Buttons: Ping Test, Apply, Set to Default, Cancel

Ping Result

[1] Request timed out.
 [2] Request timed out.
 [3] Request timed out.
 Ping Statistics for 192.168.0.23
 Packets: Sent = 3, Received = 0, Lost = 3

Figure 12-5 PD Alive Configuration window (Ping Result)

The **Ping Result** will be displayed.



NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.



NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.

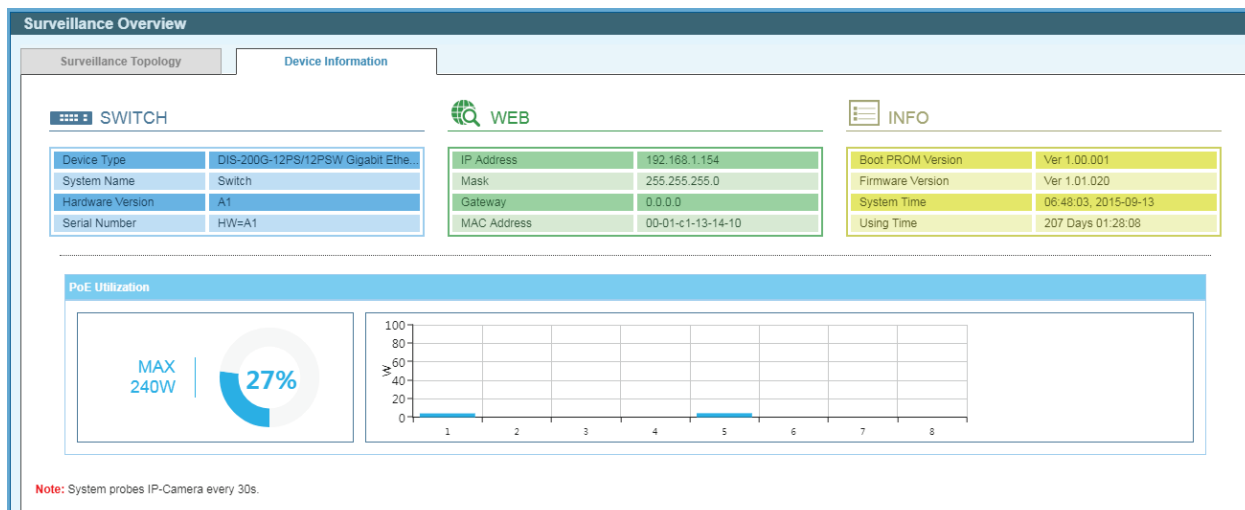


Figure 12-6 Device Information window

Port Information

This window is used to display port information like distance of the network cable, PoE provisioning status, power consumption, Loopback Detection status, group, and how many IP cameras, NVRs, and other devices are connected to the ports.

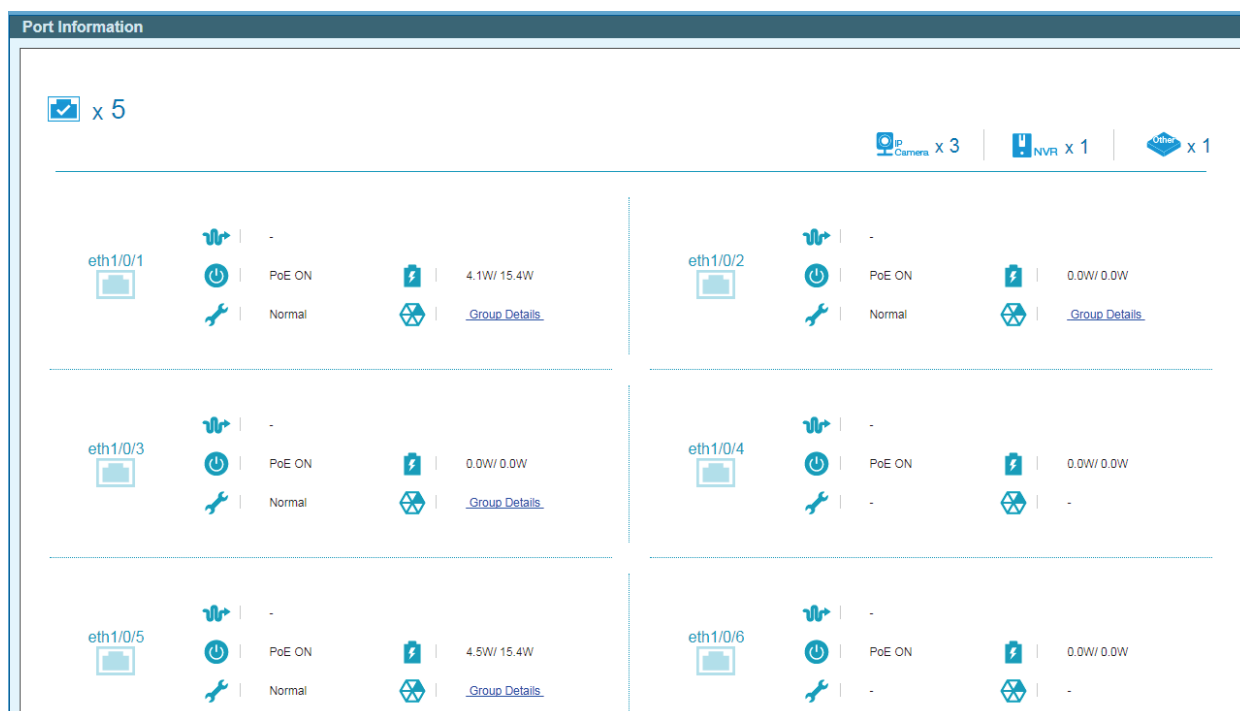






Figure 12-7 Port Information window

The following icons are available in this window and are described below:

Parameter	Description
	This displays the total amount of Ethernet devices connected to the Ethernet ports on the Switch.
	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
	This displays the total amount of other Ethernet devices connected to the Ethernet ports on the Switch.
	This displays the Ethernet port number on the Switch.
	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.
	This displays the PoE status on the port.
	This displays the power consumption and power class of the PD connected to the Ethernet port.

 Normal  <u>Loop</u>	<p>This displays the Loopback Detection status on the Ethernet port.</p> <p>Normal - Specifies that there are no loops in the network.</p> <p>Loop - Specifies that there is a loop in the network. Click the Loop link to navigate to the Health Diagnostic window.</p>
 <u>Group Details</u>	<p>If an ONVIF IP camera or NVR is connected to the port, the Group Details link will be available. Select the Group Details link to access the Group Details window.</p>
 Video Management Server ▾	<p>If a network device is connected to the port that is neither an ONVIF IP camera nor NVR, the device type can be selected. Options to choose from are Video Management Server, VMS Client/Remote Viewer, Video Encoder, Network Storage, and Other IP Surveillance Device.</p>







Group Details

After clicking **Group Details** link, the following window will appear.



Figure 12-8 Port Information / Group Details window

The following icons are available in this window and are described below:

Parameter	Description
 Port eth1/0/5	<p>This displays the Ethernet port number on the Switch.</p>
 0	<p>This displays the group ID of the IP camera or NVR on the port.</p>
 IP-Camera	<p>This displays the type of device connected to the port. The can be either IP-Camera or NVR.</p>
 DCS-5211L / DCS-5211L	<p>This displays the model name of the IP camera.</p>
 192.168.0.23(28-10-7B-04-60-EC)	<p>This displays the IP Address and MAC Address of the IP camera or NVR.</p>
 DCS-942LB1	<p>This displays the description of the device connected to the port.</p>

Guide Click the < **Back** option to return to the previous window.

IP-Camera Information







This window is used to display IP camera information.







To view the following window, click **IP-Camera Information**, as shown below:



Figure 12-9 IP-Camera Information window

The following icons are available in this window and are described below:

Parameter	Description
 x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
 8.5w / 30.8w	The displays the total power consumption and power class (of PDs) used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
 eth1/0/1	This displays the Ethernet port number on the Switch.
 D-Link DCS-942LB1	This displays a photo, the manufacturer and model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
 4.1 W / 15.4 W	This displays the power consumption and power class of the IP camera.
 192.168.0.21 (28-10-7B-04-60-EA)	This displays the IP address and MAC address of the IP camera.

 DCS-942LB1 	This displays the description for the IP camera. Click the  icon to modify the description
 <input type="text" value=""/> 	Enter the description for the IP camera here. Click the  icon to apply the modified description.

NVR Information







This window is used to display NVR information.






To view the following window, click **NVR Information**, as shown below:



Figure 12-10 NVR Information window

Guide The following icons are available in this window and are described below:

Parameter	Description
	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
	This displays the Ethernet port number on the Switch.
	This displays a generic photo of the NVR connected to the port.
 192.168.0.202 (B8-70-F4-B0-42-A1)	This displays the IP address and MAC address of the NVR.
	This displays the description for the NVR. Click the  icon to modify the description

 <input type="text"/>	Enter the description for the NVR here. Click the  icon to apply the modified description.
 Group 1	This displays the group ID of the NVR.
 x 3	This displays the number of ONVIF IP cameras managed by this NVR.
 Port 1 (192.168.0.21) ((28-10-7B-04-60-EA))	This displays information about the ONVIF IP camera that is managed by this NVR.

PoE Information

This window is used to display Power-over-Ethernet (PoE) information.

Guide To view the following window, click **PoE Information**, as shown below:

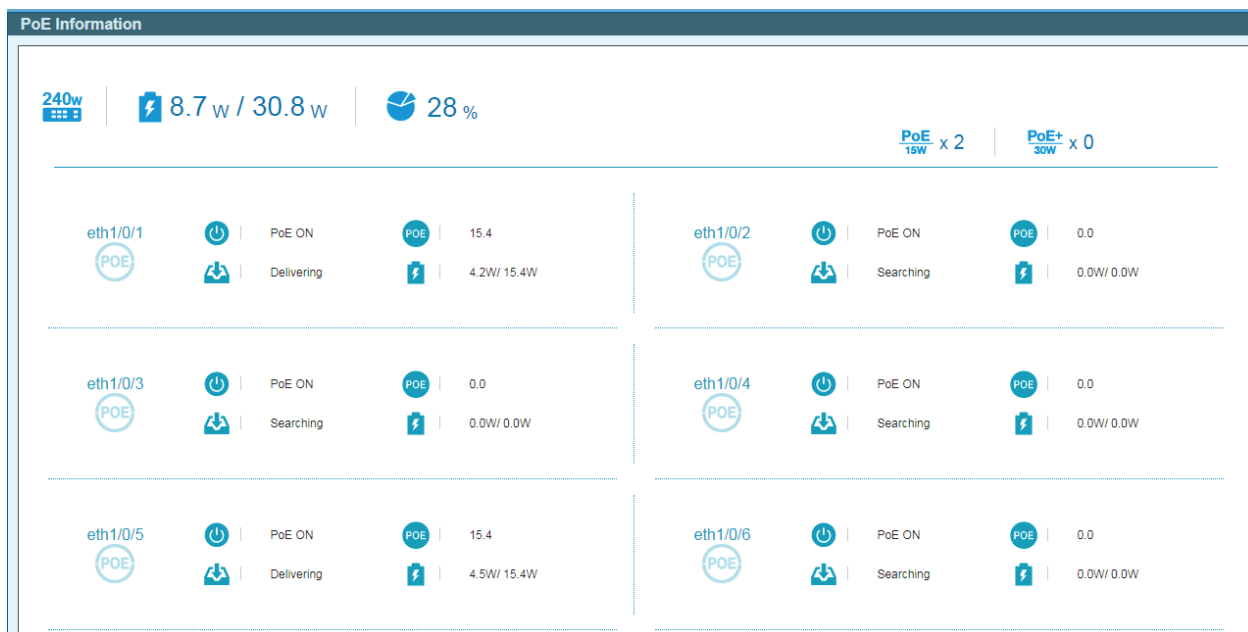






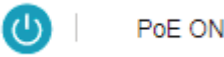


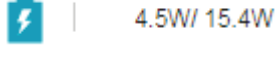


Figure 12-11 PoE Information window

The following icons are available in this window and are described below:

Parameter	Description
	This displays the maximum PoE budget that can be provided by the Switch.
	This displays the total PoE consumption and power class of PDs connected to the Switch.
	This displays the current PoE utilization (in percentage).
	This displays the number of PoE devices connected to the Switch that is using 15 Watts of power per port.

	This displays the number of PoE devices connected to the Switch that is using 30 Watts of power per port.
	This displays the Ethernet port number on the Switch.
	This displays the PoE state on the port. This can be either PoE ON or PoE OFF .
	This displays the maximum PoE budget available on this port.
	This displays the current PoE status on the port. This status can be one of the following: -, Searching , Delivering , or Power Denied . When the Power Denied message is displayed, click on the link to redirect the Health Diagnostic window for more information.
	This displays the PoE consumption and power class of the PD connected to the port.

PoE Scheduling

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

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

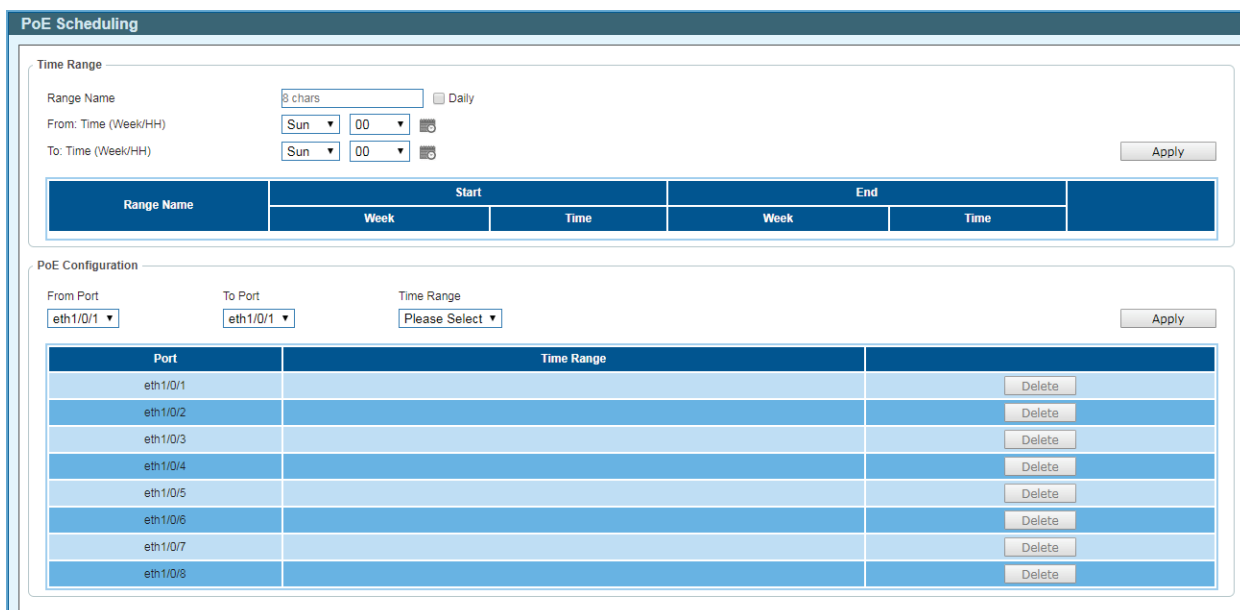




Figure 12-12 PoE Scheduling window

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

Parameter	Description
-----------	-------------

Range Name	Enter the name of the time range schedule here.
From: Time (Week/HH)	Select the starting day and hour in the time range schedule here. Alternatively, click the  icon to open a calendar for easy day and hour selection.
To: Time (Week/HH)	Select the ending day and hour in the time range schedule here. The schedule will end at the end of the selected hour. Alternatively, click the  icon to open a calendar for easy day and hour selection.

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

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

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

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

Parameter	Description
From Port / To Port	Select the port range that will be used here.
Time Range	Select the time range schedule that will be applied to the selected port(s) here.

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

Click the **Delete** button to remove the time range schedule from the specified port.


After clicking the  icon, the following window will appear:



Figure 12-13 Day and Hour window

Click the **OK** button to use the Day and Hour selected.

Time

Clock Settings

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

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

Figure 12-14 Clock Settings window

The fields that can be configured are described below:

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

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

SNTP Settings

This window is used to display and configure the Simple Network Time Protocol (SNTP) settings.

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

Figure 12-15 SNTP Settings window

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

Parameter	Description
SNTP State	Select to enable or disable the SNTP feature here.
Poll Interval	Enter the poll interval value here. The range is from 30 to 99999 seconds. By default, this value is 720 seconds.

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

The fields that can be configured in the **SNTP Server Setting** section are described below:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server here.

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

Click the **Delete** button to remove the SNTP server from the configuration.

Surveillance Settings

This window is used to display and configure the surveillance settings. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

To view the following window, click **Surveillance Settings**, as shown below:

The screenshot shows the 'Surveillance Settings' window with the following sections:

- Surveillance VLAN Settings:** VLAN ID (2-4094) is set to 4094. An 'Apply' button is present.
- IP Settings:** Get IP From is set to 'Static'. IP Address is 172.18.65.210, Mask is 255.255.248.0, and Gateway is 172.18.71.254. An 'Apply' button is present.
- SNMP Host Settings:** Host IPv4 Address is empty. An 'Apply' button is present.
- SNMP Hosts Table:**

Host IP Address	SNMP Version	UDP Port	Community String / SNMPv3 User Name	
172.18.65.10	v2c	162	public	Delete
- Log Server:** Host IPv4 Address is empty. An 'Apply' button is present.
- Log Servers Table:**

Server IP	Severity	Facility	Discriminator Name	UDP Port	
172.18.65.11	Emergencies	0		514	Delete
- Uplink Port Settings:** Unit is 1, From Port is eth1/0/1, and To Port is eth1/0/1. An 'Add' button is present.
- Unit 1 Settings Table:**

Port	
eth1/0/16	Delete

Figure 12-16 Surveillance Settings window

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

Parameter	Description
VLAN ID	Enter the ID of the surveillance VLAN here. The range is from 2 to 4094.

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

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

Parameter	Description
Get IP From	Select the method used to configure the IP address settings on the Switch here. Options to choose from are: Static - Specifies that the IP address settings will be manually configured. DHCP - Specifies that the IP address settings will be automatically obtained from a DHCP server on the network.
IP Address	Enter the IPv4 address of the Switch here.
Mask	Enter the IPv4 subnet mask of the Switch here.
Gateway	Enter the IPv4 address of the default gateway here.

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

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

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP host here.

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

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

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

Parameter	Description
Server IP	Enter the IPv4 address of the log server here.

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

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

The uplink ports join all surveillance VLANs since they forward surveillance traffic to other switches. It is recommended to connect uplink ports to the other switches because the discovery process is disabled on these ports.

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

Parameter	Description
From Port / To Port	Select the uplink port range that will be used here.

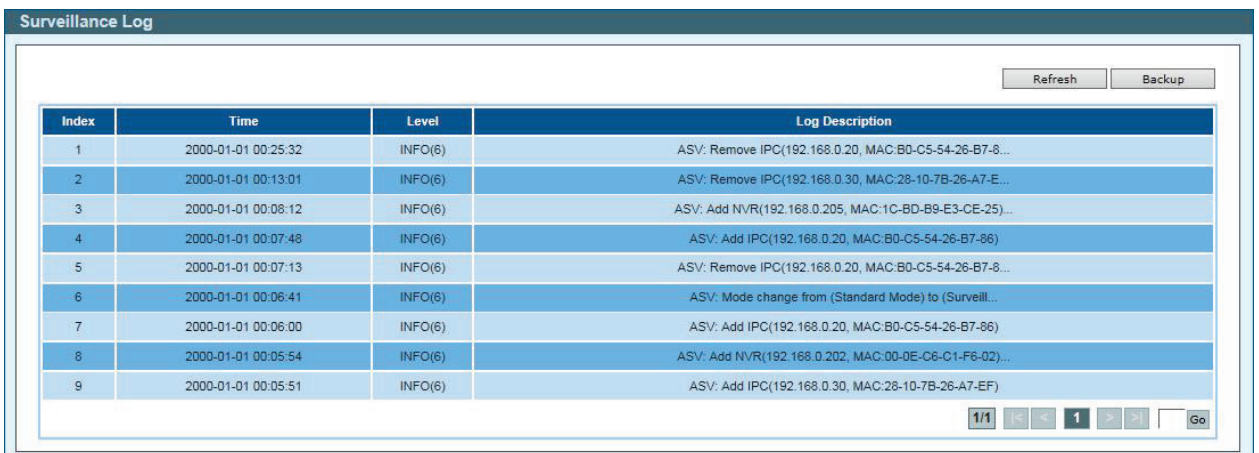
Click the **Apply** button to accept the changes made.

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

Surveillance Log

This window is used to display the surveillance log.

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



Index	Time	Level	Log Description
1	2000-01-01 00:25:32	INFO(6)	ASV: Remove IPC(192.168.0.20, MAC:B0-C5-54-26-B7-8...
2	2000-01-01 00:13:01	INFO(6)	ASV: Remove IPC(192.168.0.30, MAC:28-10-7B-26-A7-E...
3	2000-01-01 00:08:12	INFO(6)	ASV: Add NVR(192.168.0.205, MAC:1C-BD-B9-E3-CE-25)...
4	2000-01-01 00:07:48	INFO(6)	ASV: Add IPC(192.168.0.20, MAC:B0-C5-54-26-B7-86)
5	2000-01-01 00:07:13	INFO(6)	ASV: Remove IPC(192.168.0.20, MAC:B0-C5-54-26-B7-8...
6	2000-01-01 00:06:41	INFO(6)	ASV: Mode change from (Standard Mode) to (Surveill...
7	2000-01-01 00:06:00	INFO(6)	ASV: Add IPC(192.168.0.20, MAC:B0-C5-54-26-B7-86)
8	2000-01-01 00:05:54	INFO(6)	ASV: Add NVR(192.168.0.202, MAC:00-0E-C6-C1-F6-02)...
9	2000-01-01 00:05:51	INFO(6)	ASV: Add IPC(192.168.0.30, MAC:28-10-7B-26-A7-EF)

Figure 12-17 Surveillance Log window

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

Click the **Backup** button to upload the surveillance log to the PC using HTTP.

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

Health Diagnostic

This window is used to display Health Diagnostics information, Discovered Surveillance Devices information, and initiate a cable distance test on all or selected ports on the Switch. For each link-up port, the system will check the link status, PoE status and error counters periodically. This page will refresh every 30s.

To view the following window, click **Health Diagnostic**, as shown below:

Health Diagnostic						
Health Diagnostic						
Port	Loopback Detection Status	Cable Link	PoE Status	Tx/Rx CRC Counter	Discovered Surveillance Devices	Detect Distance
eth1/0/1	Normal	Pass	Pass	0/0	1	<input type="button" value="Detect"/>
eth1/0/2	Normal	Pass	-	0/2	1	<input type="button" value="Detect"/>
eth1/0/3	Normal	Pass	-	0/0	1	<input type="button" value="Detect"/>
eth1/0/4	Normal	-	-	0/0	-	<input type="button" value="Detect"/>
eth1/0/5	Normal	Pass	Pass	0/0	1	<input type="button" value="Detect"/>
eth1/0/6	Normal	-	-	0/0	-	<input type="button" value="Detect"/>
eth1/0/7	Normal	-	-	0/0	-	<input type="button" value="Detect"/>
eth1/0/8	Normal	-	-	0/0	-	<input type="button" value="Detect"/>
eth1/0/9	Normal	Pass	-	0/0	-	<input type="button" value="Detect"/>
eth1/0/10	Normal	-	-	0/0	-	<input type="button" value="Detect"/>
eth1/0/11	Normal	-	-	0/0	-	-
eth1/0/12	Normal	-	-	0/0	-	-

Note: System probes IP-Camera every 30s.

Figure 12-18 Health Diagnostic window

Guide The fields that are displayed in the table are described below:

Parameter	Description
Port	This field displays the Ethernet port number.
Loopback Detection Status	This field displays the Loopback Detection status on the Ethernet port. It can be one of the following: Normal - No loop is detected on the port. Loop - A loop is detected on the port.
Cable Link	This field displays the cable link status. It can be one of the following: PASS - The port link is up and operating in the full-duplex mode. 10M Half - The port link is up and operating at 10 Mbps speed and in the half-duplex mode. 100M Half - The port link is up and operating at 100 Mbps speed and in the half-duplex mode.
PoE Status	This field displays the PoE status. It can be one of the following: PASS , PD Short , Overload , Power Denied , Thermal Shutdown , or Classification Failure .
Tx/Rx CRC Counter	This field displays the TX/RX CRC counter.
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (1) to view the group details associated with IP camera or NVR connected to the port. For more information, refer to Group Details on page 360..

Detect Distance

Click the **Detect** button to initiate a cable distance test on the specified port.

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 4.

Tools

Firmware Information

This window is used to configure the firmware image boot up.

To view the following window, click **Tools > Firmware Information**, as shown below:

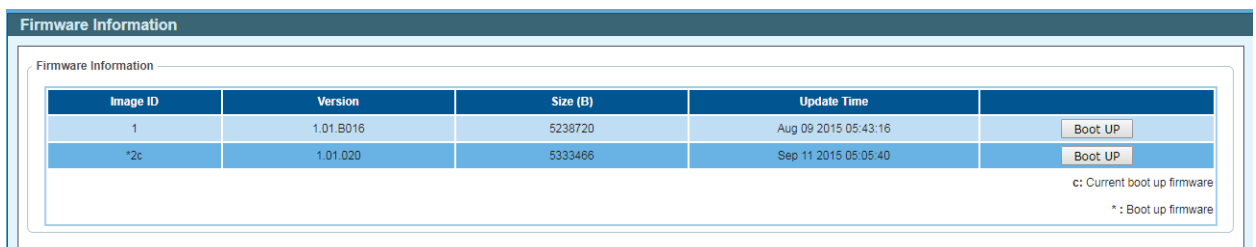


Image ID	Version	Size (B)	Update Time	
1	1.01.B016	5238720	Aug 09 2015 05:43:16	Boot UP
*2c	1.01.020	5333466	Sep 11 2015 05:05:40	Boot UP

c: Current boot up firmware
*: Boot up firmware

Figure 12-19 Firmware Information window

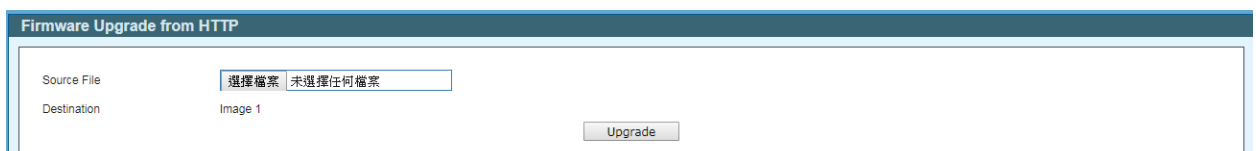
Click the **Boot UP** button of image 1 or image 2 for boot up

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:



Source File:

Destination:

Upgrade

Figure 12-20 Firmware Upgrade from 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 local PC. This field can be up to 64 characters long. Alternatively click the Browse button to navigate to the location of the firmware file located on the local PC.
--	--

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:

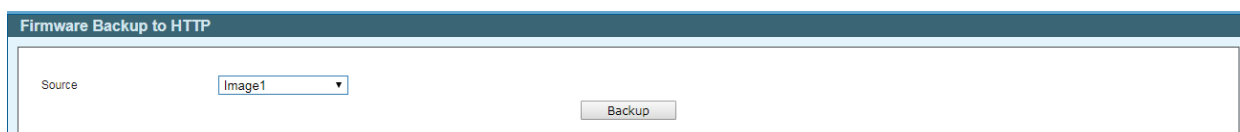


Figure 12-21 Firmware Backup to HTTP window

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. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:



Figure 12-22 Configuration Restore from HTTP window

The fields that can be configured are described below:

Parameter	Description
-----------	-------------

Source File	Click the Browse button to navigate to the location of the configuration file located on the local PC.
Effective immediately (running-config)	Specify this radio button to restore and overwrite the running configuration file on the Switch.
Take effect after the next boot (startup-config)	Specify this radio button to restore and overwrite the start-up configuration file on the Switch.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from 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:

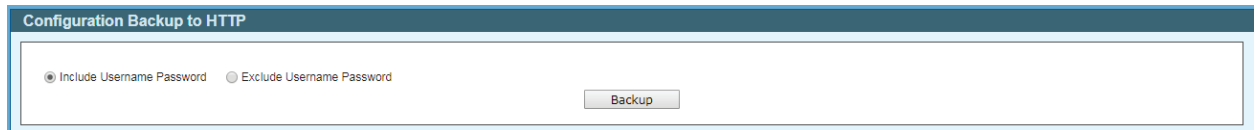


Figure 12-23 Configuration Backup to HTTP window

The fields that can be configured are described below:

Parameter	Description
Include Username Password	Specify this radio button to back up the running configuration file include username password from the Switch.
Exclude Username Password	Specify this radio button to back up the running configuration file exclude username password from the Switch.

Click the **Backup** button to initiate the configuration file backup.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

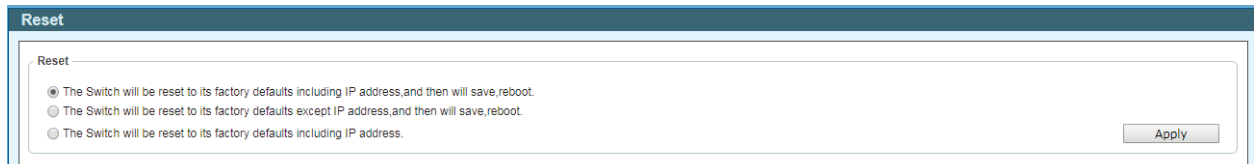


Figure 12-24 Reset window

Select the **The Switch will be reset to its factory defaults including IP address, and then will save, reboot** option to reset the Switch's configuration to its factory default settings.

Select the **The Switch will be reset to its factory default except IP address, and then will save, reboot** option to reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

Select the **The Switch will be reset to its factory defaults including IP address** option to reset the Switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

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

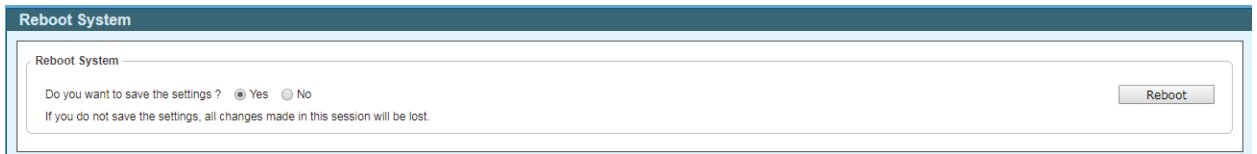


Figure 12-25 Reboot System window

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.

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration or the file system of the Switch. 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:

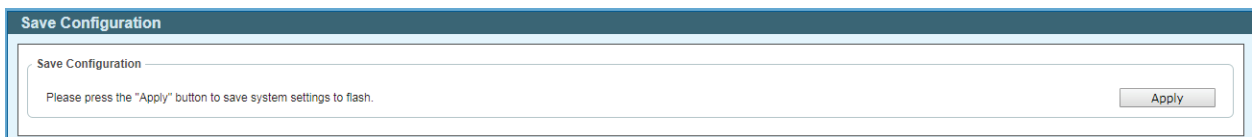


Figure 12-26 Save Configuration window

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

Help

Click this option to access the built-in Surveillance Help window.

Guide After clicking the **Help** option, the following window will appear.

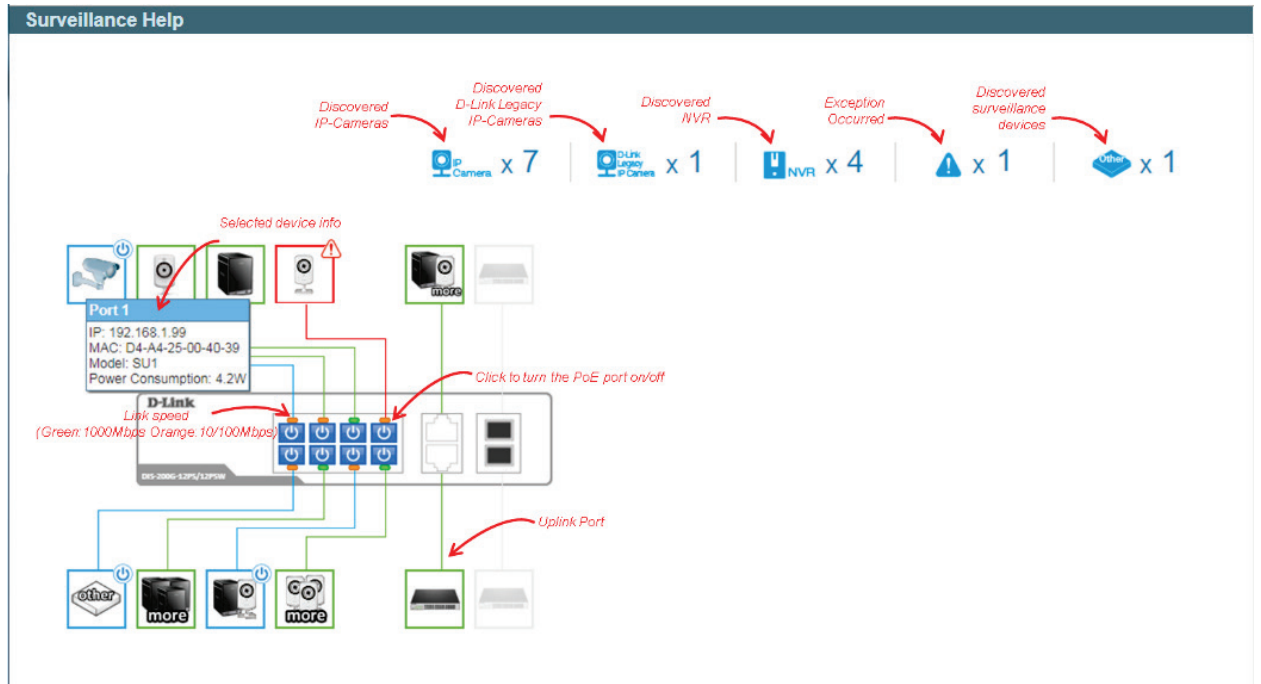


Figure 12-27 Help (Diagram) window

Device Status					
Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.
	This icon indicates that the designated device is operational and is powered by PoE. It also indicates that the PD Alive function is enabled.		The device was rebooted successfully. Please click the icon to recover to its operational state.		The device has malfunctioned. A problem has been detected on this port or device. PD Alive function may have malfunctioned.

IP-Camera/NVR Status					
Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.		Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.		Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
	Multiple ONVIF IP-Cameras and one NVR discovered on this port.		One ONVIF IP-Camera and multiple NVRs discovered on this port.		Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

Figure 12-28 Help (Table) window

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Standard Mode

Click the **Standard Mode** button in the toolbar to change the Web UI mode and style from Surveillance Mode to Standard Mode.



NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

Logout

Click this option to log out of the Web UI of the Switch.

Appendix A - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this switch.

Auto Surveillance VLAN

Log Description	Severity
<p>Event description: When a new surveillance device is detected on an interface.</p> <p>Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <p> interface-id: Interface name.</p> <p> mac-address: Surveillance device MAC address.</p>	Informational
<p>Event description: When an interface which is enabled surveillance VLAN joins the surveillance VLAN automatically.</p> <p>Log Message: <interface-id> add into surveillance VLAN <vid></p> <p>Parameters description:</p> <p> interface-id: Interface name.</p> <p> vid:VLAN ID.</p>	Informational
<p>Event description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent.</p> <p>Log Message: <interface-id> remove from surveillance VLAN <vid></p> <p>Parameters description:</p> <p> interface-id: Interface name.</p> <p> vid:VLAN ID.</p>	Informational
<p>Event description: When an IPC is added in the surveillance VLAN, the log message will be sent.</p> <p>Log Message: ASV: Add IPC (IP:<ipaddr> MAC:< mac-address >)</p> <p>Parameters description:</p> <p> ipaddr: Represent the IP address of the IPC</p> <p> mac-address: Represent the MAC address of the IPC</p>	Informational
<p>Event description: When an IPC is removed from the surveillance VLAN, the log message will be sent.</p> <p>Log Message: ASV: Remove IPC (IP:<ipaddr> MAC:< mac-address >)</p> <p>Parameters description:</p> <p> ipaddr: Represent the IP address of the IPC</p> <p> mac-address: Represent the MAC address of the IPC</p>	Informational

Event description: When an NVR is added in the surveillance VLAN, the log message will be sent. Informational

Log Message: ASV: Add NVR (IP:<ipaddr> MAC:< mac-address >)

Parameters description:

ipaddr: Represent the IP address of the NVR

mac-address: Represent the MAC address of the NVR

Event description: When an NVR is removed from the surveillance VLAN, the log message will be sent. Informational

Log Message: ASV: Remove NVR (IP:<ipaddr> MAC:< mac-address >)

Parameters description:

ipaddr: Represent the IP address of the NVR

mac-address: Represent the MAC address of the NVR

Event description: When the mode of ASV 2.0 is changed by Web GUI, the log message will be sent. Informational

Log Message: ASV: Mode change from <mode> to <mode>

Parameters description:

mode: Represent the mode of ASV 2.0. And the mode can be standard or surveillance.

DDM

Log Description	Severity
-----------------	----------

Event description: when the any of SFP parameters exceeds from the warning threshold. Warning

Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power

high-low: High or low threshold.

Event description: when the any of SFP parameters exceeds from the alarm Warning

threshold.

Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power

high-low: High or low threshold.

Event description: when the any of SFP parameters recovers from the warning threshold. Warning

Log Message: Optical transceiver <interface-id> <component> back to normal

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power

Interface

Log Description	Severity
Event description: When port is down Log Message: Port < interface-id> link down Parameters description: interface-id: Interface name	Informational
Event description: When port is up Log Message: Port < interface-id> link up, <link-speed> Parameters description: interface-id: Interface name link-speed: port link speed.	Informational

LBD

Log Description	Severity
Event description: Record the event when an interface detect loop. Log Message: <interface-id> LBD loop occurred. Parameters description: interface-id: Interface on which loop is detected.	Critical
Event description: Record the event when an interface loop recovered Log Message: <interface-id> LBD loop recovered. Parameters description: interface-id: Interface on which loop is detected.	Critical

Login/Logout CLI

Log Description	Severity
Event description: Login through console successfully. Log Message: Successful login through Console (Username: <username>) Parameters description: username: Represent current login user.	Informational
Event description: Login through console unsuccessfully. Log Message: Login failed through Console (Username: <username>) Parameters description: username: Represent current login user.	Warning
Event description: Console session timed out. Log Message: Console session timed out (Username: <username>) Parameters description: username: Represent current login user.	Informational
Event description: Logout through console. Log Message: Logout through Console (Username: <username>) Parameters description: username: Represent current login user.	Informational
Event description: Login through telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user.	Informational

ipaddr: Represent client IP address.

Event description: Login through telnet unsuccessfully. Warning

Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)

Parameters description:

username: Represent current login user.

ipaddr: Represent client IP address.

Event description: Telnet session timed out. Informational

Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)

Parameters description:

username: Represent current login user.

ipaddr: Represent client IP address.

Event description: Logout through telnet. Informational

Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)

Parameters description:

username: Represent current login user.

ipaddr: Represent client IP address.

PoE

Log Description	Severity
-----------------	----------

Event description: Total power usage threshold is exceeded Warning

Log Message: Unit <unit-id> usage threshold <percentage> is exceeded

Parameters description:

unit-id : box id

percentage : usage threshold

Event description: Total power usage threshold is recovered. Warning

Log Message: Unit <unit-id> usage threshold <percentage> is recovered

Parameters description:

unit-id : box id

percentage : usage threshold

Event description: PD alive check fail. Warning

Log Message: ASV: PD alive check failed. (Port: <interface-id>, PD: <ipaddr>)

Parameters description:

interface-id : Interface name
 ipaddr: Represent PD IP address

Port Security

Log Description	Severity
Event description: Address full on a port. Log Message: MAC address <macaddr> causes port security violation on <interface-id> Parameters description: macaddr: The violation MAC address. interface-id: The interface name.	Warning
Event description: Address full on system. Log Message: Limit on system entry number has been exceeded	Warning

Safeguard

Log Description	Severity
Event description: the host enters the mode of exhausted. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Parameters description: unit-id: The Unit ID	Warning
Event description: the host enters the mode of normal. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Parameters description: unit-id: The Unit ID	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational

Telnet

Log Description	Severity
<p>Event description: Successful login through Telnet.</p> <p>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <p>ipaddr: The IP address of telnet client.</p> <p>username: the user name that used to login telnet server.</p>	Informational
<p>Event description: Login failed through Telnet.</p> <p>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <p>ipaddr: The IP address of telnet client.</p> <p>username: the user name that used to login telnet server.</p>	Warning
<p>Event description: Logout through Telnet.</p> <p>Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <p>ipaddr: The IP address of telnet client.</p> <p>username: the user name that used to login telnet server.</p>	Informational
<p>Event description: Telnet session timed out.</p> <p>Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>ipaddr: The IP address of telnet client.</p> <p>username: the user name that used to login telnet server.</p>	Informational

Voice-VLAN

Log Description	Severity
<p>Event description: When a new voice device is detected on an interface.</p> <p>Log Message: New voice device detected (<interface-id>, MAC: < mac-address >)</p> <p>Parameters description:</p> <p>interface-id: Interface name.</p> <p>mac-address: Voice device MAC address</p>	Informational
<p>Event description: When an interface which is in auto voice VLAN mode joins the voice VLAN</p>	Informational

Log Message: < interface-id > add into voice VLAN <vid >

Parameters description:

interface-id: Interface name.

vid:VLAN ID

Event description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent. Informational

Log Message: < interface-id > remove from voice VLAN <vid >

Parameters description:

interface-id: Interface name.

vid:VLAN ID

Web

Log Description	Severity
<p>Event description: Successful login through Web.</p> <p>Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event description: Login failed through Web.</p> <p>Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Warning
<p>Event description: Web session timed out.</p> <p>Log Message: Web session timed out (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event description: Logout through Web.</p> <p>Log Message: Logout through Web (Username: %S, IP: %S).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational

Web-Authentication

Log Description	Severity
<p>Event description: When a host has passed the authentication.</p> <p>Log Message: Web-Authentication host login success (Username: <string>, IP: <ipaddr ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)</p> <p>Parameters description:</p> <p>Username: The host username.</p> <p>IP: The host IP address</p> <p>mac-address: The host MAC addresses.</p> <p>interface-id: The interface on which the host is authenticated.</p> <p>vlan-id: The VLAN ID on which the host exists.</p>	Informational

Event description: When a host fail to pass the authentication. Error

Message: Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)

Parameters description:

Username: The host username.

IP: The host IP address

mac-address: The host MAC addresses.

interface-id: The interface on which the host is authenticated.

vlan-id: The VLAN ID on which the host exists.

Appendix B - 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	1.3.6.1.4.1.171.11.155.1000.72.0.1
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	1.3.6.1.4.1.171.11.155.1000.72.0.2

LBD

Trap Name	Description	OID
isLbdLoopOccurred	his trap is sent when an interface loop occurs. Binding objects: (1) isLbdNotifyInfolIndex	1.3.6.1.4.1.171. 11.155.1000.46. 0.1
isLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding objects: (1) isLbdNotifyInfolIndex	1.3.6.1.4.1.171. 11.155.1000.46. 0.2

LLDP

Trap Name	Description	OID
lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2. 0.0.1

STP

Trap Name	Description	OID
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0. 1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot	1.3.6.1.2.1.17.0. 2

trap is sent for the same transition. Implementation of this trap is optional

PoE

Trap Name	Description	OID
pethMainPowerUsageOn Notification	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
pethMainPowerUsageOff Notification	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
isPoelfPdAliveFailOccurNotification	This Notification indicates if the PD device has the stop working or no response problem.	1.3.6.1.4.1.171.11.155.1000.24.0.4

Port

Trap Name	Description	OID
linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

Port Security

Trap Name	Description	OID
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security 1.14.8.0.1 configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171.11.155.1000.8.0.1

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

Web-Authentication

Trap Name	Description	OID
isWebAuthLoggedSuccess	The trap is sent when a host has successfully logged in (passed Web-Authentication). Binding objects: (1) ifIndex (2) isSessionAuthVlan (3) isnaSessionClientMacAddress (4) isnaSessionClientAddrType (5) isnaSessionClientAddress (6) isnaSessionAuthUserName	1.3.6.1.4.1.171.11.155.1000.154.0.1

isWebAuthLoggedFail	The trap is sent when a host has failed to pass Web-Authentication (login failed). Binding objects: (1) ifIndex (2) isnaSessionAuthVlan (3) isnaSessionClientMacAddress (4) isnaSessionClientAddrType (5) isnaSessionClientAddress (6) isnaSessionAuthUserName	1.3.6.1.4.1.17.1 1.155.1000.154. 0.2
---------------------	---	--

Appendix C - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link switch.

RADIUS Authentication Attributes:

Trap Name	Description
1	User-Name
2	User-Password