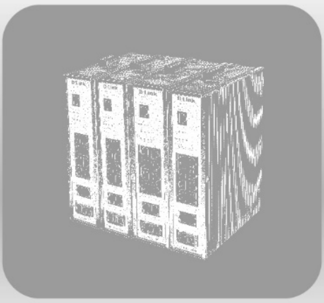
D-Link®
Building Networks for People



Web UI Reference Guide

Product Model : DIS-200G Series
Industrial Gigabit Ethernet Switch
Release 1.00

August 2017

Table of Contents

1. Introduction

This manual's descriptions are based on the software release R1.00. 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.
Blue Courier Font	This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes, Notices, and Cautions

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

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

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

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

2. Web-based Switch Configuration

Management Options

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.

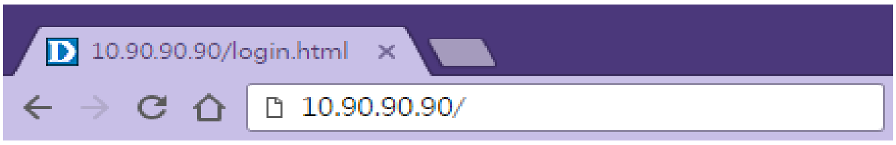
NOTE: The Command Line Interface (CLI) provides the functionality of managing, configuring, and monitoring all of the software features that are available on the Switch.

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.

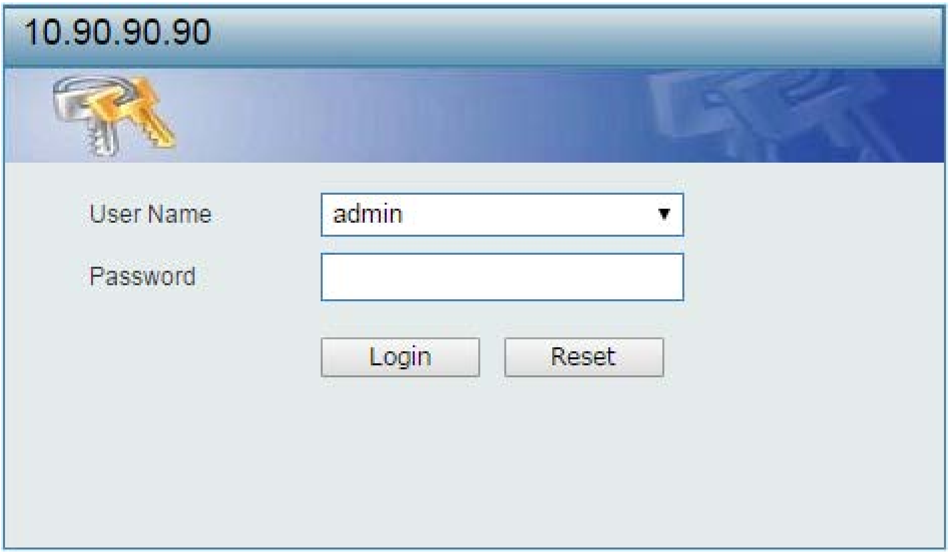


10.90.90.90/login.html

10.90.90.90/

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

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



10.90.90.90

User Name: admin

Password:

Figure 2-2 User Authentication window

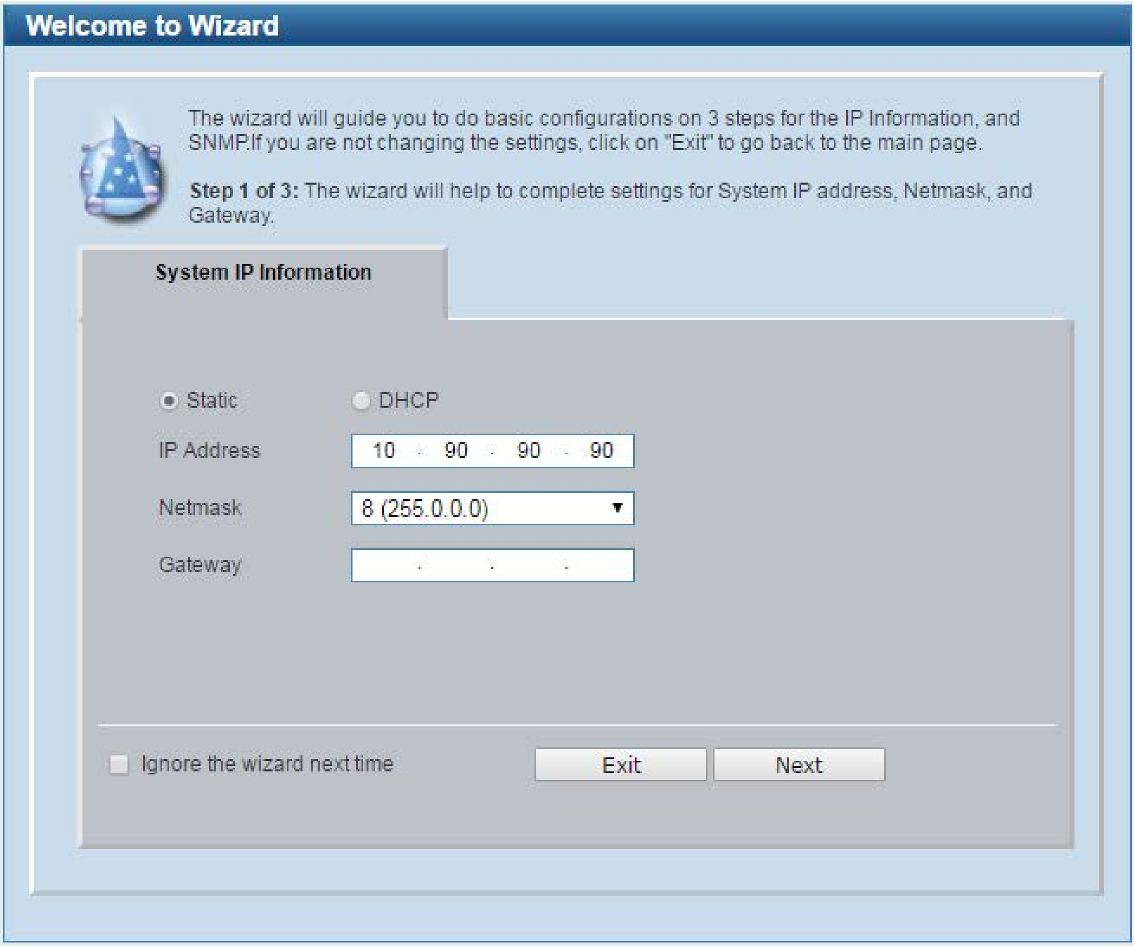
Enter the **User Name** and **Password** in the corresponding fields and click **Login**. The default username is admin and the default password is admin. This will open the Web-based user interface. The Switch's management features available in the web-based manager are explained below.

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 – System IP Information

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



Welcome to Wizard

The wizard will guide you to do basic configurations on 3 steps for the IP Information, and SNMP.If you are not changing the settings, click on "Exit" to go back to the main page.

Step 1 of 3: The wizard will help to complete settings for System IP address, Netmask, and Gateway.

System IP Information

● Static ○ DHCP

IP Address: 10 . 90 . 90 . 90

Netmask: 8 (255.0.0.0)

Gateway: . . .

□ Ignore the wizard next time

Figure 2-3 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.

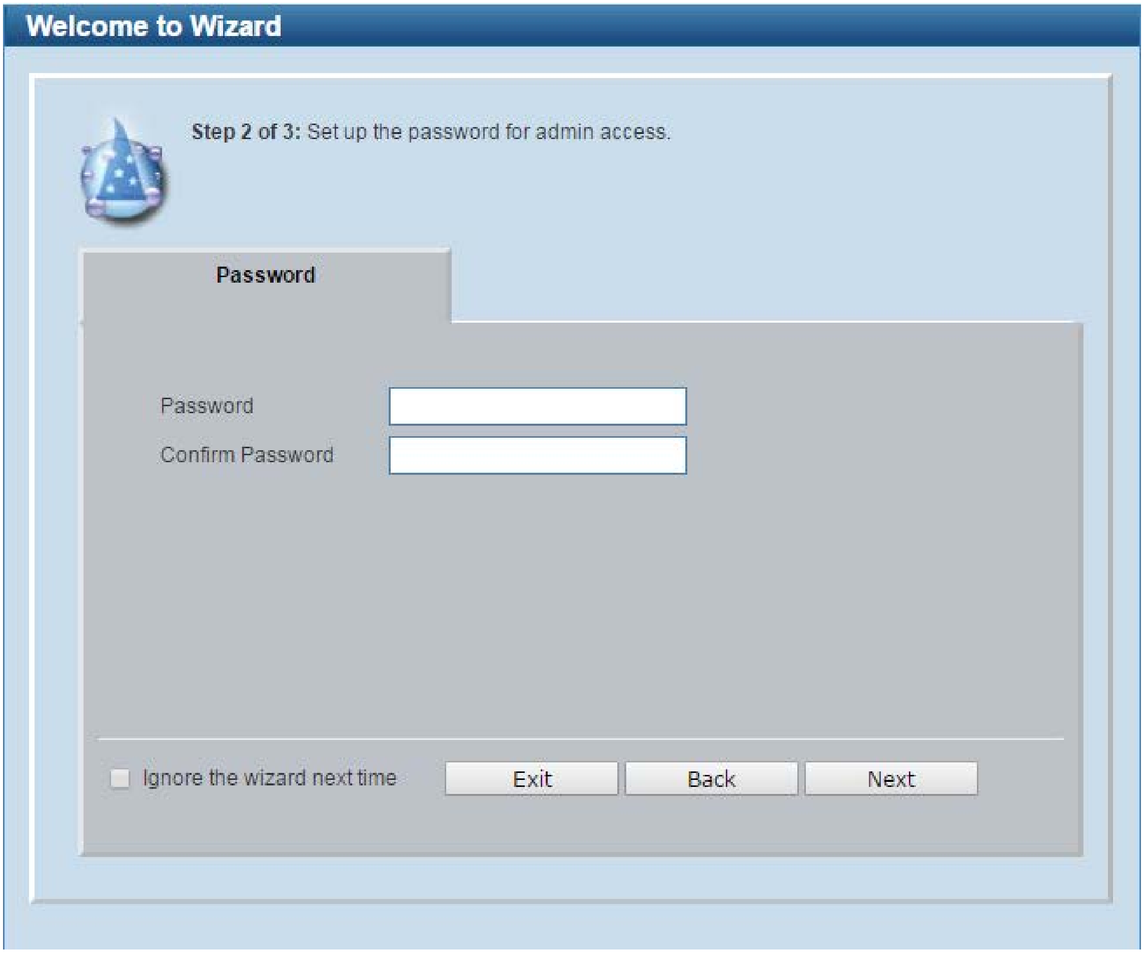
Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

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 2 – User Accounts Settings

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



Welcome to Wizard

Step 2 of 3: Set up the password for admin access.

Password

Password

Confirm Password

Figure 2-4 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.

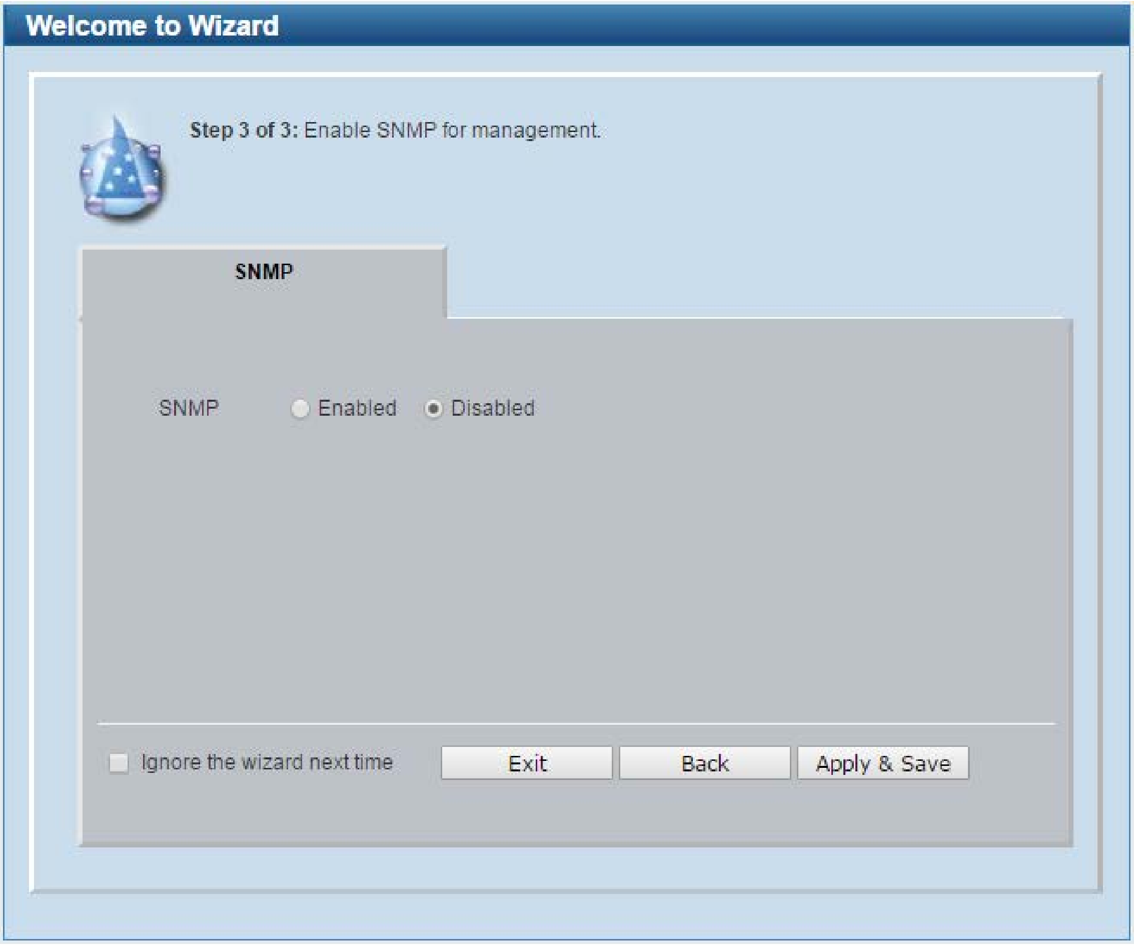
Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

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 3 – SNMP Settings

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



Welcome to Wizard

Step 3 of 3: Enable SNMP for management.

SNMP

SNMP ○ Enabled ● Disabled

☐ Ignore the wizard next time

Figure 2-5 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.

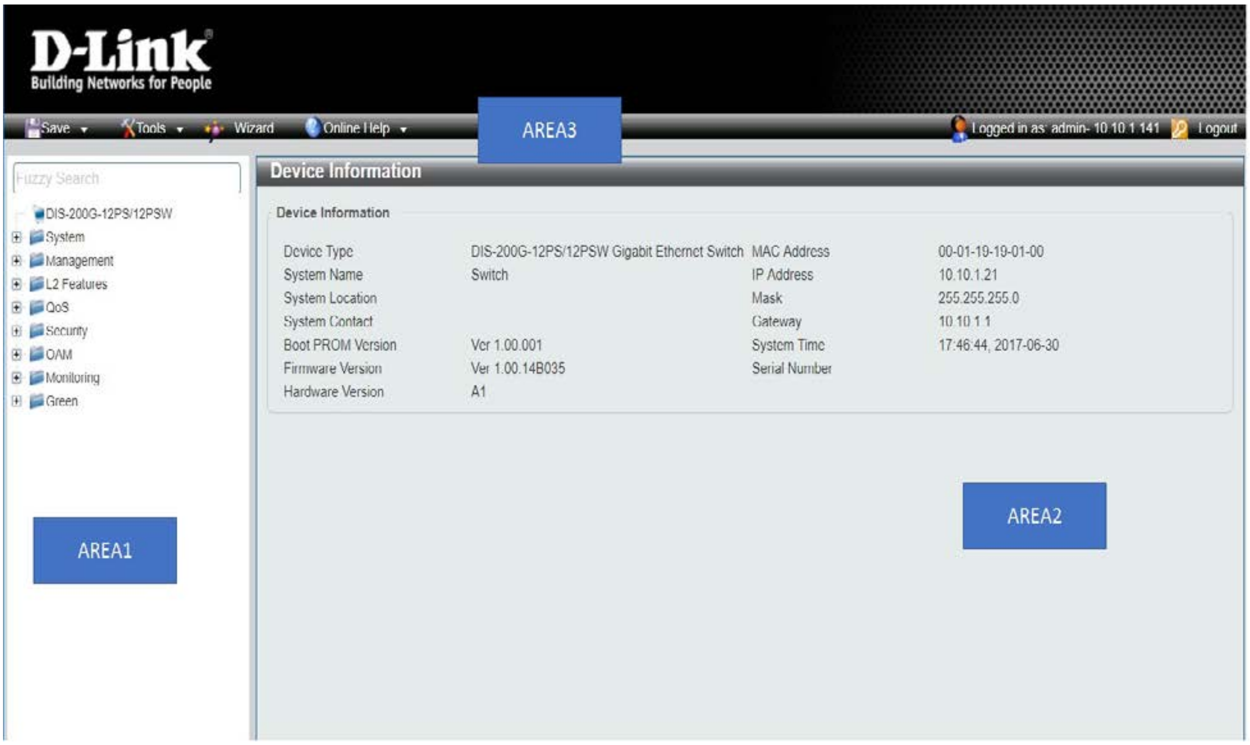
Click the **Apply & Save** button to accept the changes made and continue to the Web UI.

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 user interface. Three distinct areas that divide the user interface, as described in the table.



Device Information

Device Information

Device Type	DIS-200G-12PS/12PSW Gigabit Ethernet Switch	MAC Address	00-01-19-19-01-00
System Name	Switch	IP Address	10.10.1.21
System Location		Mask	255.255.255.0
System Contact		Gateway	10.10.1.1
Boot PROM Version	Ver 1.00.001	System Time	17:46:44, 2017-06-30
Firmware Version	Ver 1.00.14B035	Serial Number	
Hardware Version	A1		

Figure 2-6 Main Web UI 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**.

3. Save and Tools

Save Configuration

Firmware Information

Firmware Upgrade & Backup

Configuration Restore & Backup Log Backup

Ping

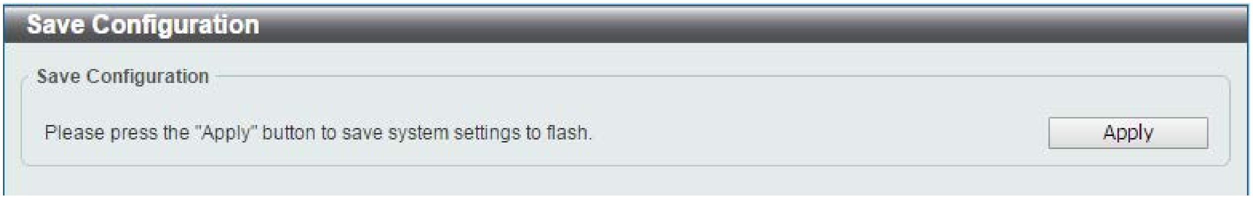
Reset

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:



Save Configuration

Save Configuration

Please press the "Apply" button to save system settings to flash.

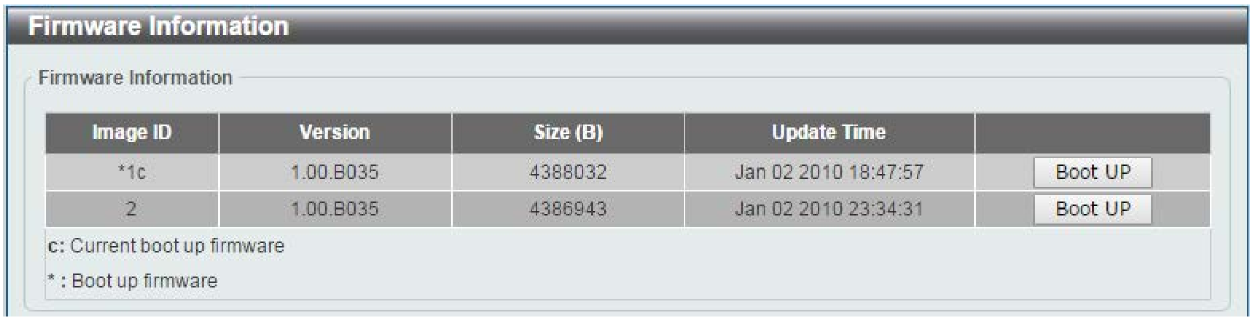
Figure 3-1 Save Configuration window

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:



Firmware Information

Firmware Information

Image ID	Version	Size (B)	Update Time	
*1c	1.00.B035	4388032	Jan 02 2010 18:47:57	Boot UP
2	1.00.B035	4386943	Jan 02 2010 23:34:31	Boot UP

c: Current boot up firmware

***** : Boot up firmware

Figure 3-2 Firmware Information window

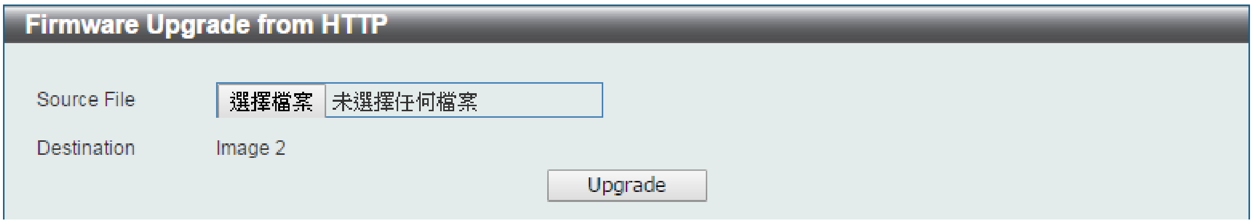
Click the **Boot UP** button of image 1 or image 2 for boot up.

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:



Firmware Upgrade from HTTP

Source File: 選擇檔案 未選擇任何檔案

Destination: Image 2

Figure 3-3 Firmware Upgrade from HTTP window

The fields that can be configured are described below:

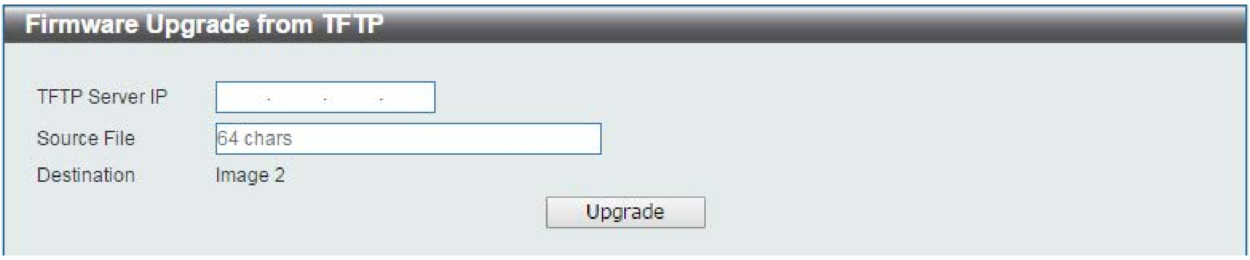
Parameter	Description
Source File	Click the **Browse** button to navigate to the location of the firmware file located on the local PC.
Destination	The destination Image ID is automatically assigned to new upgrade firmware by system.

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:



Firmware Upgrade from TFTP

TFTP Server IP: . . .

Source File: 64 chars

Destination: Image 2

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:

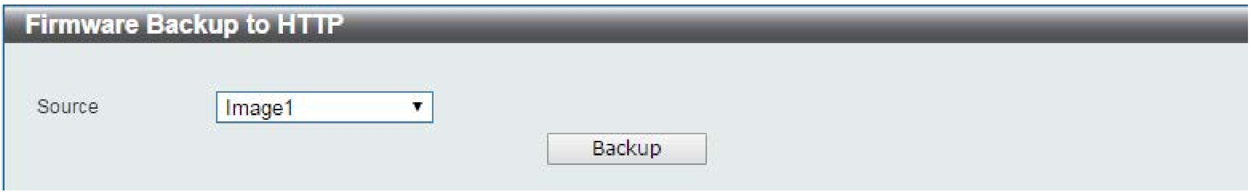


Figure 3-5 Firmware Backup to HTTP window

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:

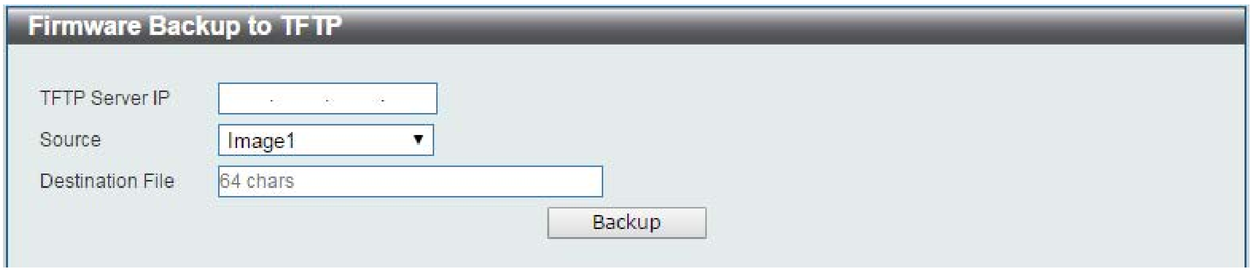


Figure 3-6 Firmware Backup to TFTP window

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.

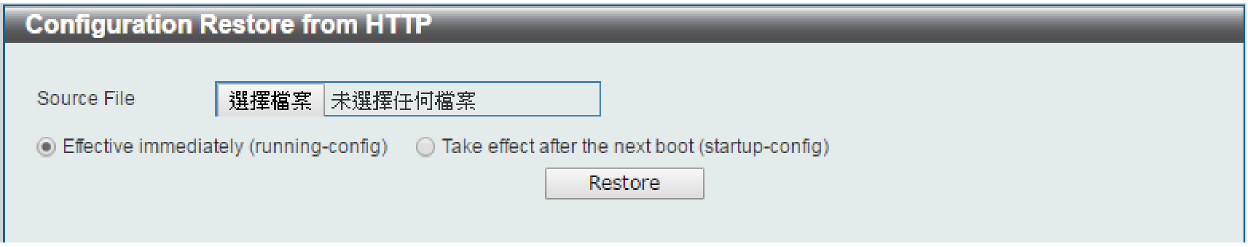
Click the **Backup** button to initiate the firmware backup.

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:



Configuration Restore from HTTP

Source File: 選擇檔案 未選擇任何檔案

● Effective immediately (running-config) ○ Take effect after the next boot (startup-config)

Figure 3-7 Configuration Restore from HTTP window

The fields that can be configured are described below:

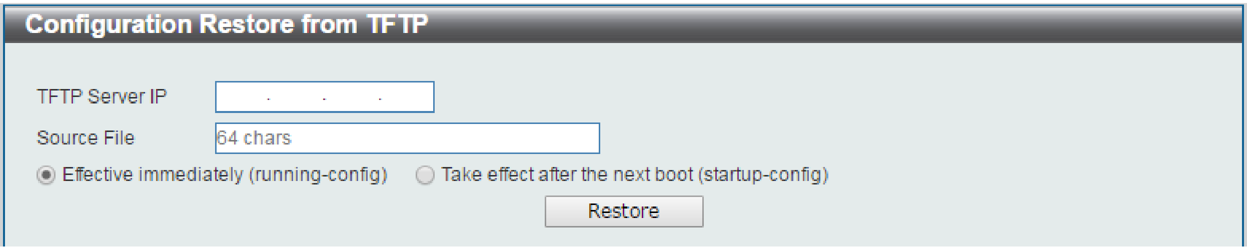
Parameter	Description
Source File	Click the **Browse** button to navigate to the location of the configuration file located on the local PC.
Effective immediately (running-config)	**Specify** this radio button to restore and overwrite the running configuration file on the Switch.
Take effect after the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



Configuration Restore from TFTP

TFTP Server IP: . . .

Source File: 64 chars

● Effective immediately (running-config) ○ Take effect after the next boot (startup-config)

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.

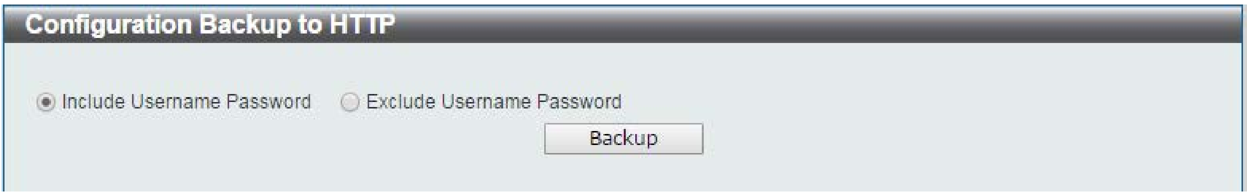
Effective immediately (running-config)	Specify this radio button to restore and overwrite the running configuration file on the Switch.
Take effect after the next boot (startup-config)	Specify this radio button to restore and overwrite the start-up configuration file on the Switch.

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:



Configuration Backup to HTTP

● Include Username Password ○ Exclude Username Password

Figure 3-9 Configuration Backup to HTTP window

The fields that can be configured are described below:

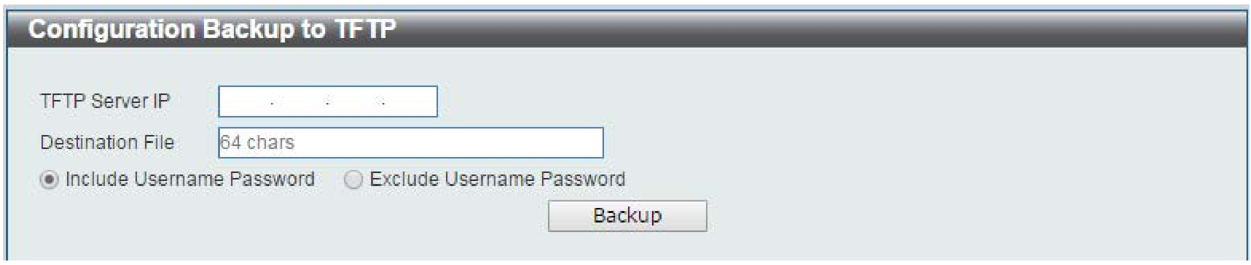
Parameter	Description
Include Username Password	Specify this radio button to back up the running configuration file include username password from the Switch.
Exclude Username Password	Specify this radio button to back up the running configuration file exclude username password from the Switch.

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:



Configuration Backup to TFTP

TFTP Server IP . . .

Destination File 64 chars

● Include Username Password ○ Exclude Username Password

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:

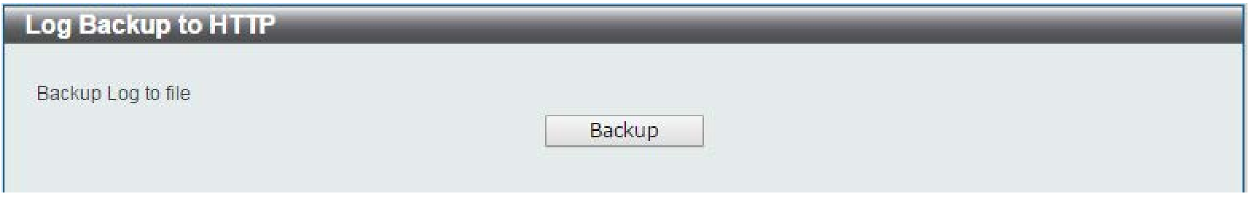


Figure 3-11 Log Backup to HTTP window

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:

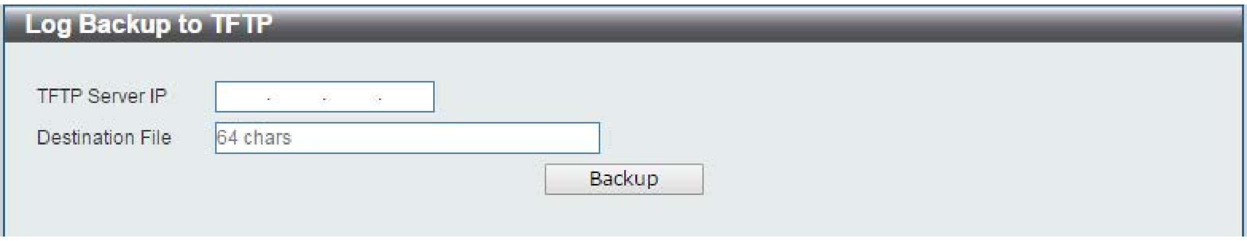


Figure 3-12 Log Backup to TFTP window

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:

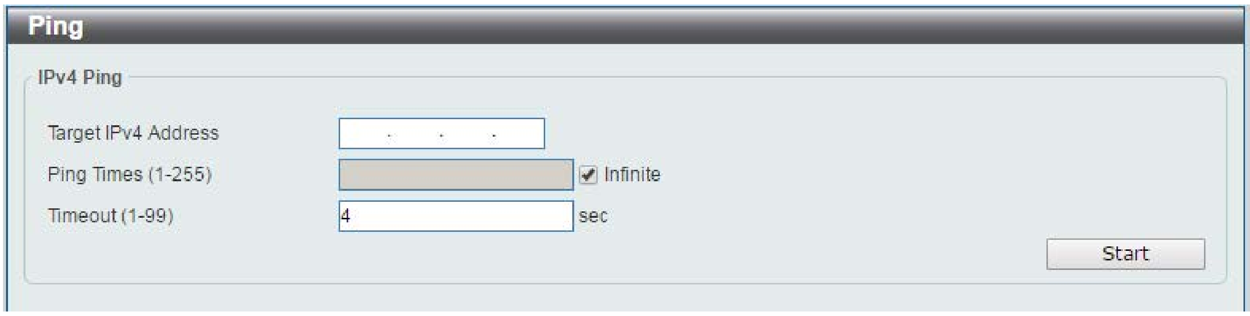


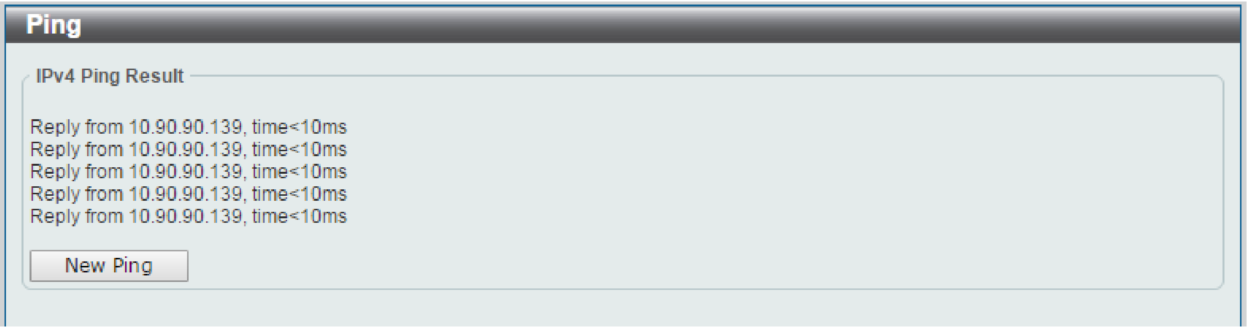
Figure 3-13 Ping window

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:



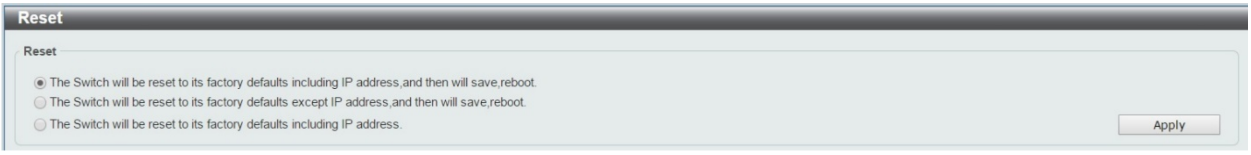
```
Reply from 10.90.90.139, time<10ms
Reply from 10.90.90.139, time<10ms
Reply from 10.90.90.139, time<10ms
Reply from 10.90.90.139, time<10ms
Reply from 10.90.90.139, time<10ms
```

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:



Reset

Reset

● The Switch will be reset to its factory defaults including IP address,and then will save,reboot.

○ The Switch will be reset to its factory defaults except IP address,and then will save,reboot.

○ The Switch will be reset to its factory defaults including IP address.

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.

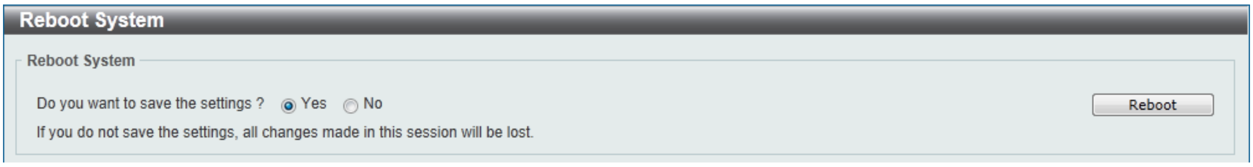
Select the **The Switch will be reset to its factory default except IP address, and then will save, reboot** option to reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

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:



Reboot System

Reboot System

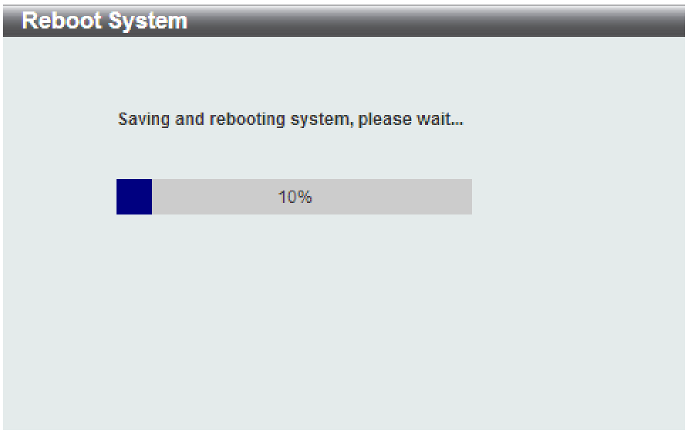
Do you want to save the settings ? ● Yes ○ No

If you do not save the settings, all changes made in this session will be lost.

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.



Reboot System

Saving and rebooting system, please wait...

Figure 3-17 Reboot System - Rebooting window

4. System

Device Information

System Information Settings Port Configuration

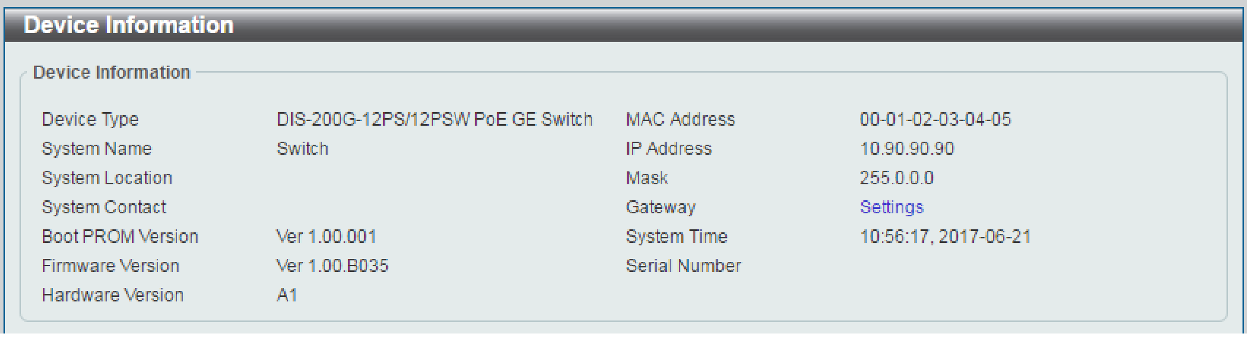
PoE

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 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		

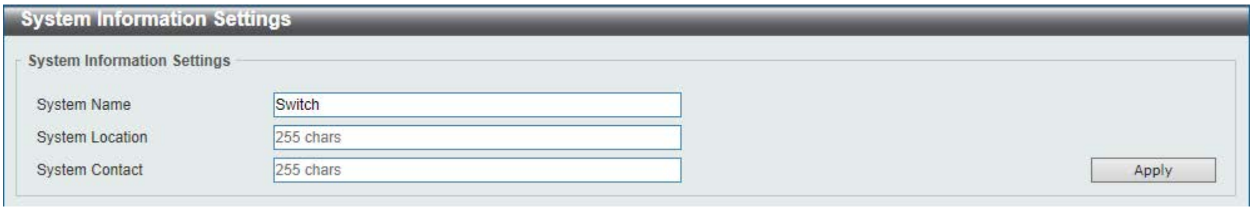
Figure 4-1 Device Information window

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 Name: Switch

System Location: 255 chars

System Contact: 255 chars

Figure 4-2 System Information Settings window

The fields that can be configured are described below:

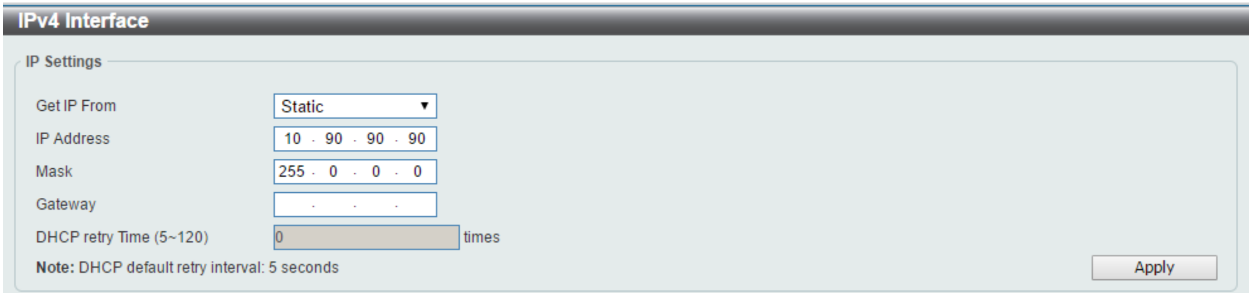
Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired. This string can be up to 255 characters long.
System Contact	Enter a contact name for the Switch, if 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:



IPv4 Interface

IP Settings

Get IP From: Static

IP Address: 10 . 90 . 90 . 90

Mask: 255 . 0 . 0 . 0

Gateway: . . .

DHCP retry Time (5~120): 0 times

Note: DHCP default retry interval: 5 seconds

Figure 4-3 IPv4 Interface window

The fields that can be configured are described below:

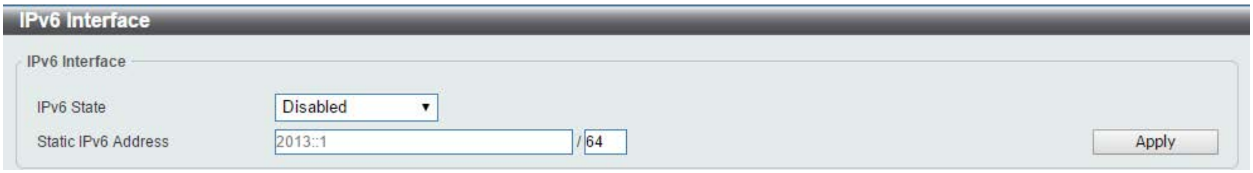
Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are Static and **DHCP**. When the **Static** option is selected, users can enter the IPv4 address of this interface manually in the fields provided. When the **DHCP** option is selected, this interface will obtain 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:



IPv6 Interface

IPv6 Interface

IPv6 State: Disabled

Static IPv6 Address: 2013::1 / 64

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.

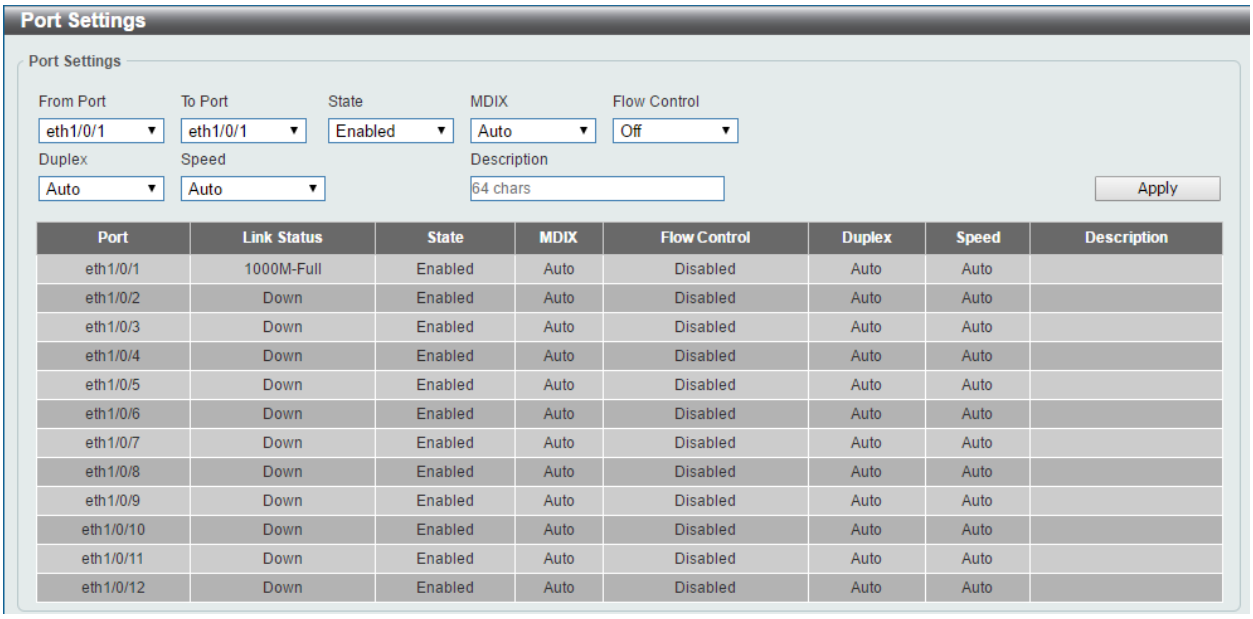
Click the **Apply** button to accept the changes made.

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 Settings

Port Settings

From Port: eth1/0/1

To Port: eth1/0/1

State: Enabled

MDIX: Auto

Flow Control: Off

Duplex: Auto

Speed: Auto

Description: 64 chars

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

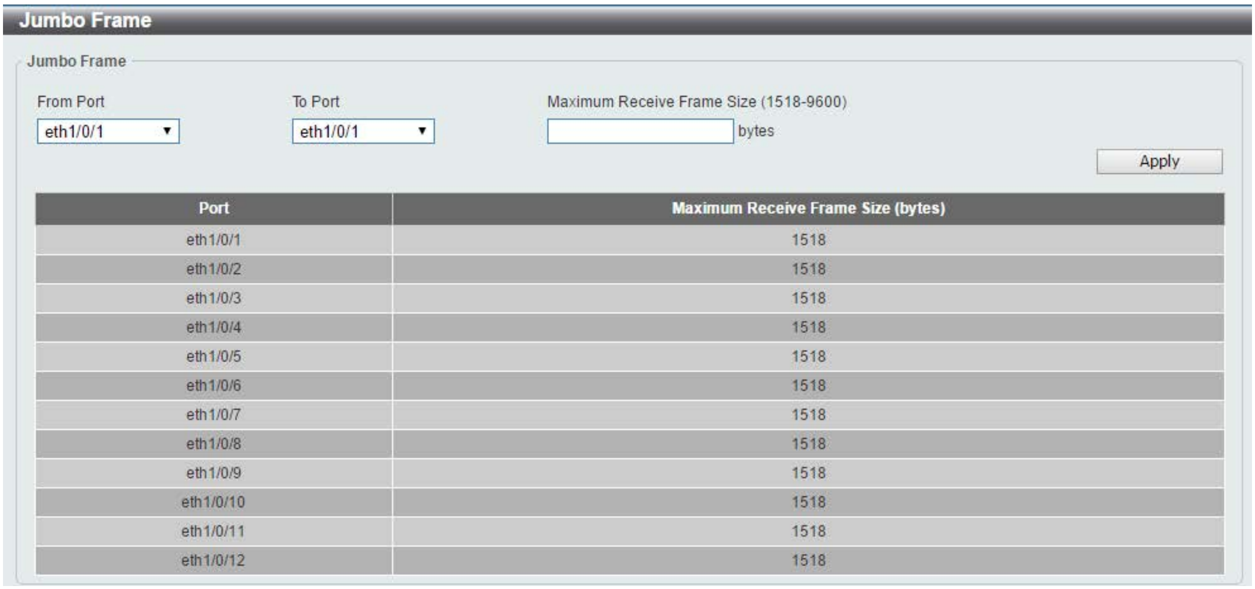
Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are **Auto**, **Normal**, 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:



Jumbo Frame

Jumbo Frame

From Port: eth1/0/1 ▼ To Port: eth1/0/1 ▼ Maximum Receive Frame Size (1518-9600): ____ bytes

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

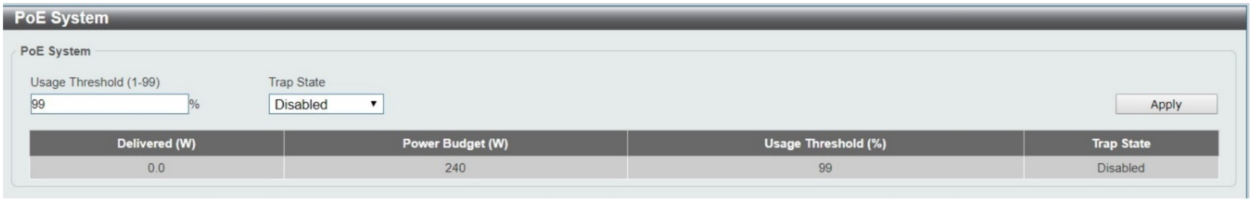
PSE provides power according to the following classification:

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:



PoE System

PoE System

Usage Threshold (1-99): 99 %

Trap State: Disabled

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:

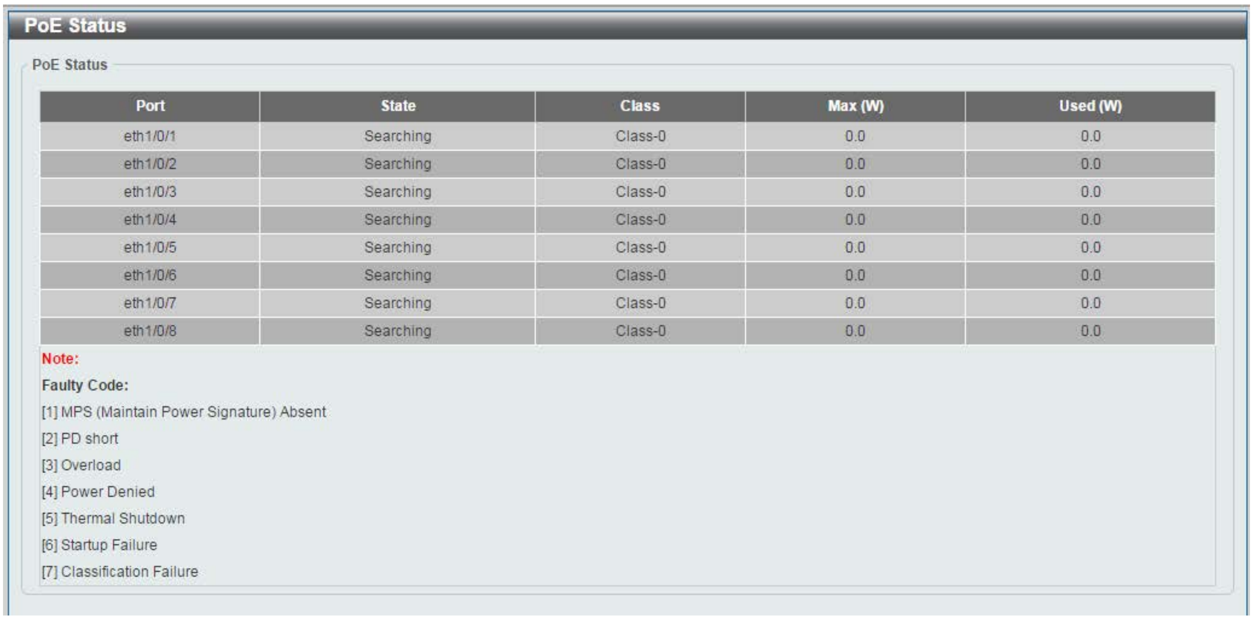
Parameter	Description
Usage Threshold	Enter the usage threshold to generate a log and send the corresponding standard notification. The range is from 1 to 99 percent.
Trap State	Select this option to enable or disable the sending of PoE notifications.

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

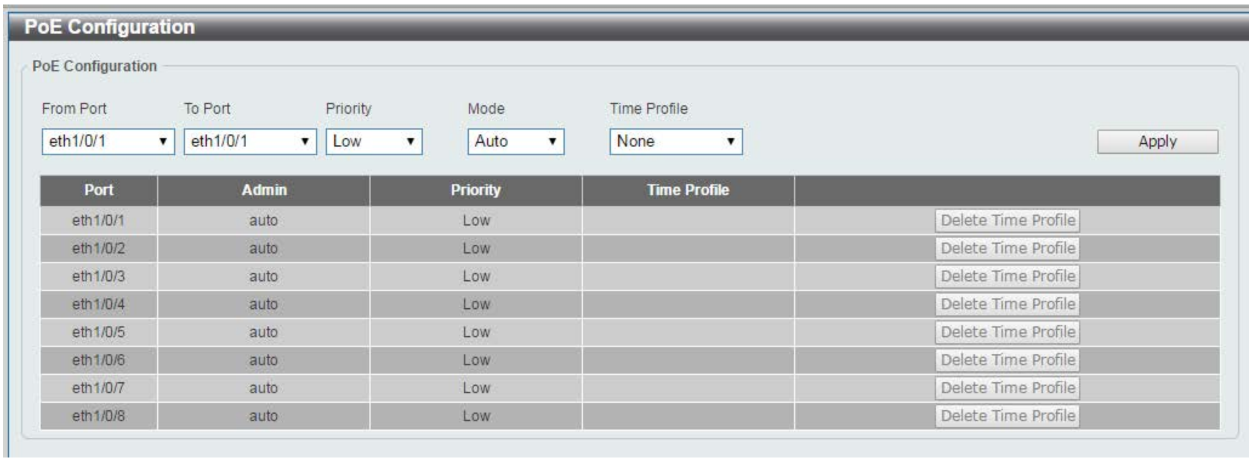
[7] Classification Failure

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

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.

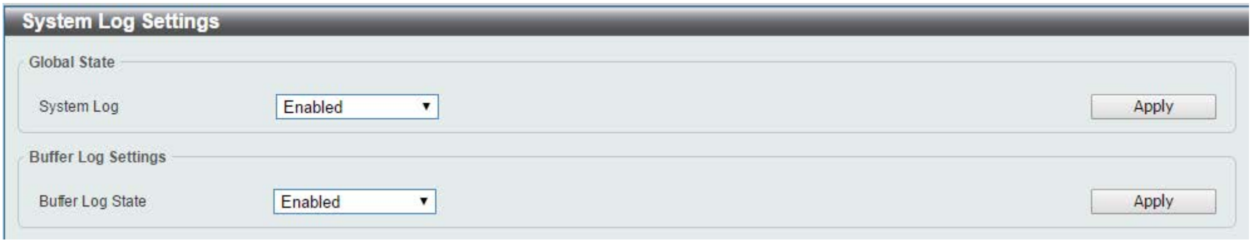
Click the **Apply** button to accept the changes made.

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:



System Log Settings

Global State

System Log: Enabled

Buffer Log Settings

Buffer Log State: Enabled

Figure 4-10 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:

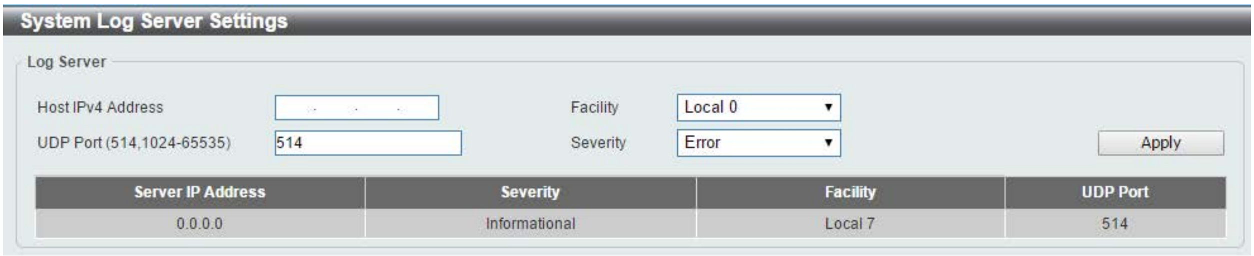
Parameter	Description
Buffer Log State	Select whether the enable or disable the buffer log's global state.

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:



System Log Server Settings

Log Server

Host IPv4 Address: . . .

UDP Port (514,1024-65535): 514

Facility: Local 0

Severity: Error

Server IP Address	Severity	Facility	UDP Port
0.0.0.0	Informational	Local 7	514

Figure 4-11 System Log Server Settings window

The fields that can be configured are described below:

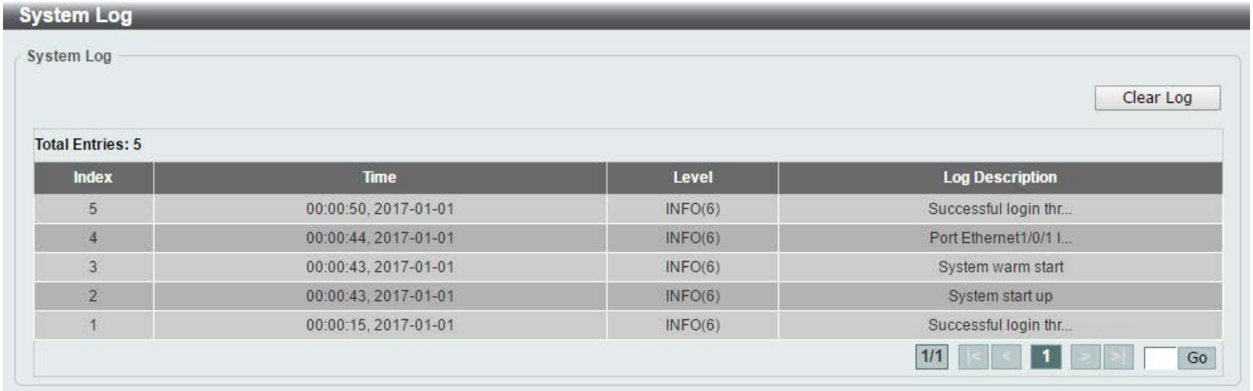
Parameter	Description
Host IPv4 Address	Enter the system log server's IPv4 address here.
UDP Port	Enter the system log server's UDP port number here. This value must be 514 or between 1024 and 65535. By default, this value is 514.
Severity	Select the severity value of the type of information that will 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:



System Log

System Log

Total Entries: 5

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...

Figure 4-12 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.

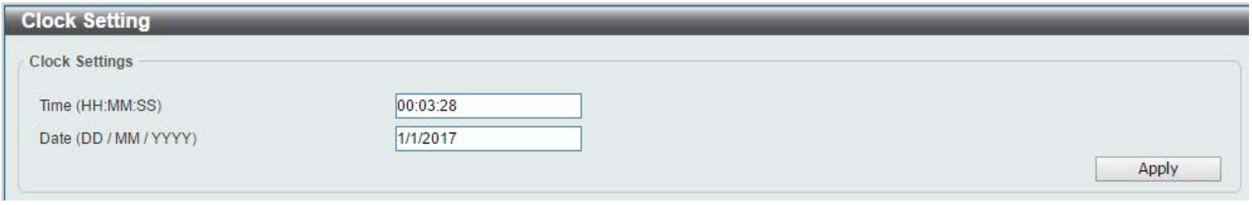
Time and SNTP

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:



Clock Setting

Clock Settings

Time (HH:MM:SS) 00:03:28

Date (DD / MM / YYYY) 1/1/2017

Figure 4-13 Clock Settings window

The fields that can be configured are described below:

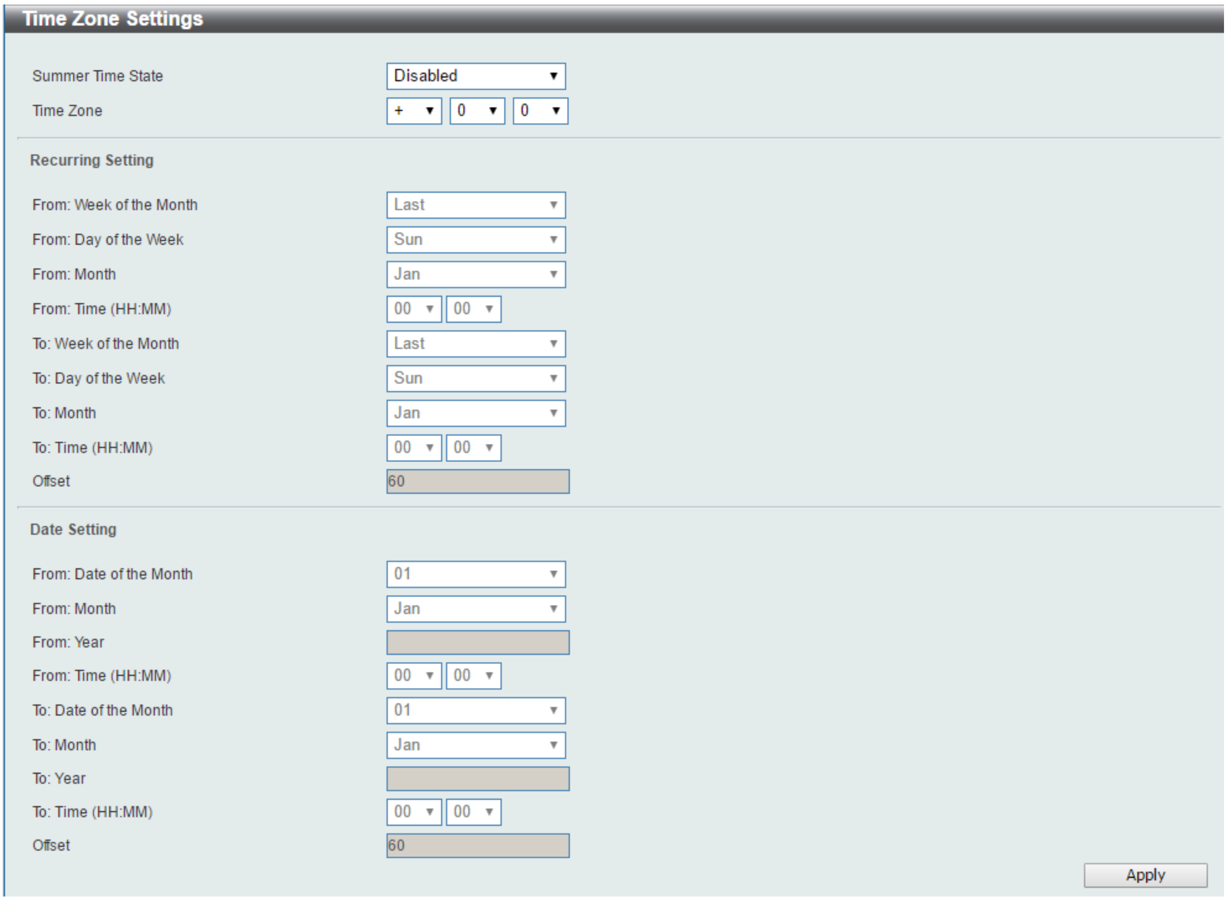
Parameter	Description
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.
Date (DD / MM / YYYY)	Enter the current day, month, and year to update the system clock.

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:



Time Zone Settings

Summer Time State: Disabled

Time Zone: + 0 0

Recurring Setting

From: Week of the Month: Last

From: Day of the Week: Sun

From: Month: Jan

From: Time (HH:MM): 00 00

To: Week of the Month: Last

To: Day of the Week: Sun

To: Month: Jan

To: Time (HH:MM): 00 00

Offset: 60

Date Setting

From: Date of the Month: 01

From: Month: Jan

From: Year:

From: Time (HH:MM): 00 00

To: Date of the Month: 01

To: Month: Jan

To: Year:

To: Time (HH:MM): 00 00

Offset: 60

Figure 4-14 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:

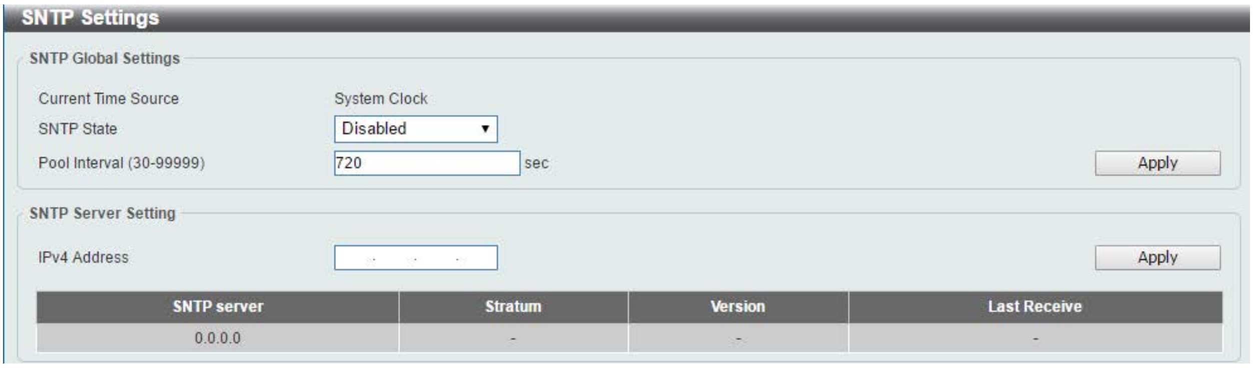
Parameter	Description
From: Date of the Month	Select date of the month that summer time will start.
From: Month	Select the month that summer time will start.
From: Year	Enter the year that the summer time will start.
From: Time (HH:MM)	Select the time of the day that summer time will start.
To: Date 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:



SNTP Settings

SNTP Global Settings

Current Time Source: System Clock

SNTP State: Disabled

Pool Interval (30-99999): 720 sec

SNTP Server Setting

IPv4 Address: . . .

SNTP server	Stratum	Version	Last Receive
0.0.0.0	-	-	-

Figure 4-15 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:

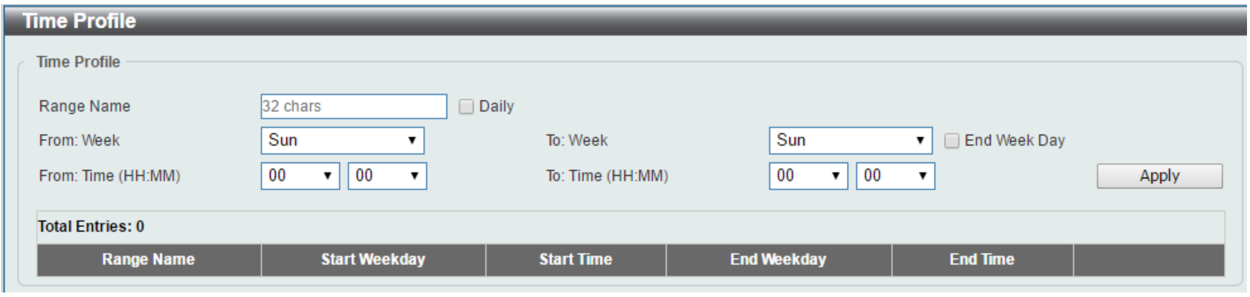
Parameter	Description
IPv4 Address	Enter the IP address of the SNTP server which provides the clock synchronization.

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:



Time Profile

Time Profile

Range Name: 32 chars □ Daily

From: Week: Sun · To: Week: Sun □ End Week Day

From: Time (HH:MM): 00 00 · To: Time (HH:MM): 00 00

Total Entries: 0

Range Name	Start Weekday	Start Time	End Weekday	End Time	

Figure 4-16 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

HTTP/HTTPS

D-Link Discovery Protocol

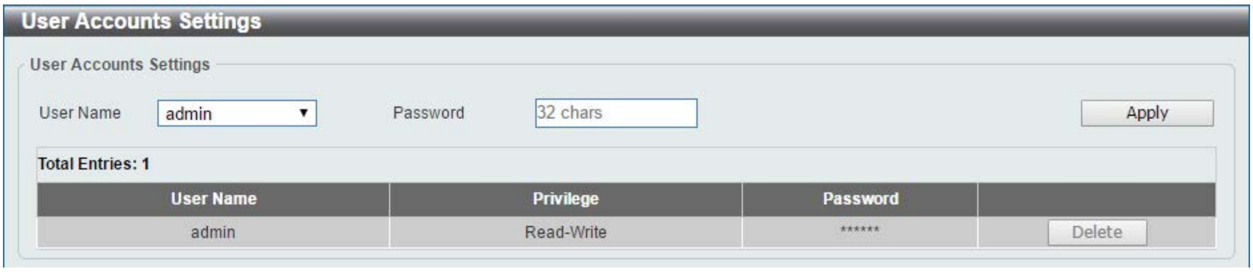
User Account Settings

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 Accounts Settings

User Accounts Settings

User Name: admin

Password: 32 chars

Total Entries: 1

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 and 2c. The two 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.

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, Port Link State Change and System Reboot.

MIBs

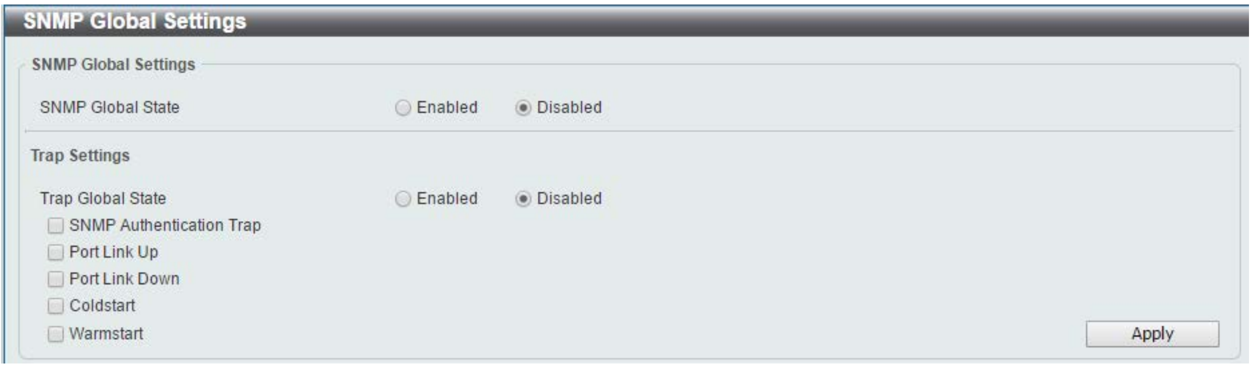
The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, 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.

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:



SNMP Global Settings

SNMP Global Settings

SNMP Global State ○ Enabled ● Disabled

Trap Settings

Trap Global State ○ Enabled ● Disabled

□ SNMP Authentication Trap

□ Port Link Up

□ Port Link Down

□ Coldstart

□ Warmstart

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.

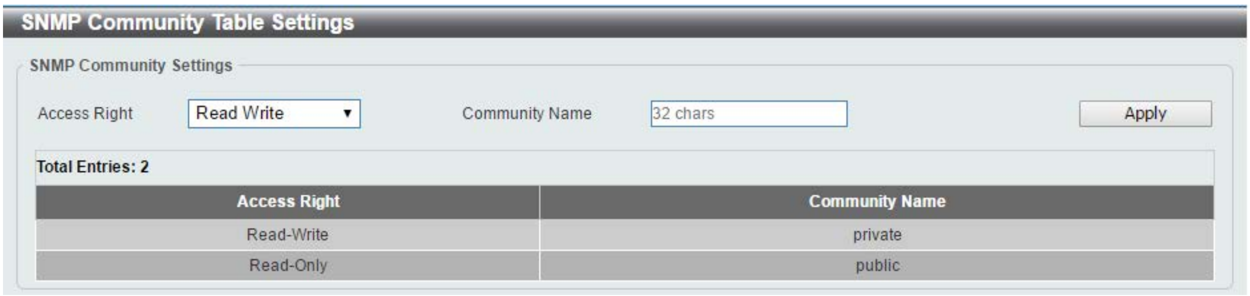
Click the **Apply** button to accept the changes made.

SNMP 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

Access Right: Read Write

Community Name: 32 chars

Total Entries: 2

Access Right	Community Name
Read-Write	private
Read-Only	public

Figure 5-3 SNMP Community Table Settings window

The fields that can be configured are described below:

Parameter	Description
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.
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.

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

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:

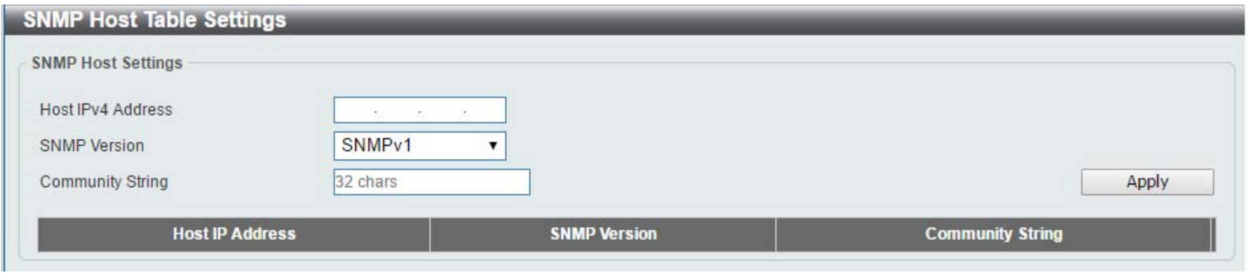


Figure 5-4 SNMP Host Table Settings window

The fields that can be configured are described below:

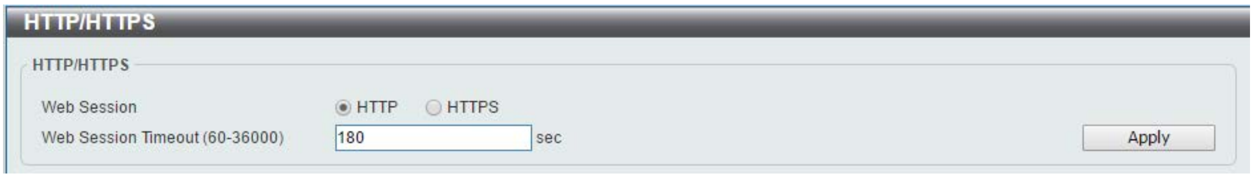
Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
SNMP Version	Choose SNMP version to use for notification messages
Community String	Enter the community string to be sent with the notification packet.

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

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:



Web Session ● HTTP ○ HTTPS

Web Session Timeout (60-36000) 180 sec

Figure 5-5 HTTP/HTTPS window

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

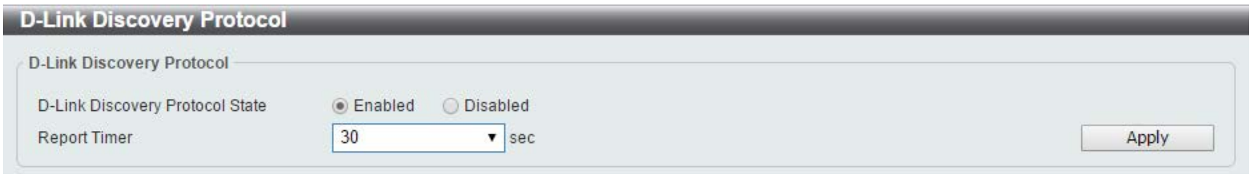
Parameter	Description
WEB Session	Select the protocol for web server.
Web Session Timeout	Enter the session timeout value for web session. The range of this value is from 60 to 36000 seconds.

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:



D-Link Discovery Protocol State ● Enabled ○ Disabled

Report Timer 30 sec

Figure 5-6 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

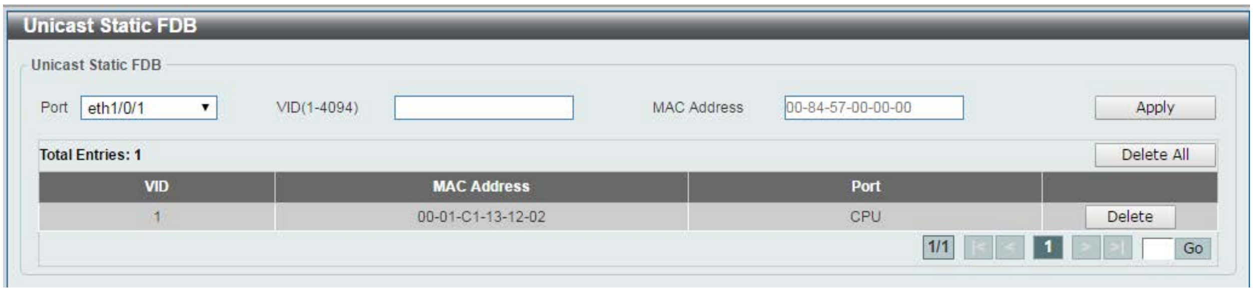
FDB

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:



Unicast Static FDB

Unicast Static FDB

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

Total Entries: 1

VID	MAC Address	Port	
1	00-01-C1-13-12-02	CPU	Delete

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.

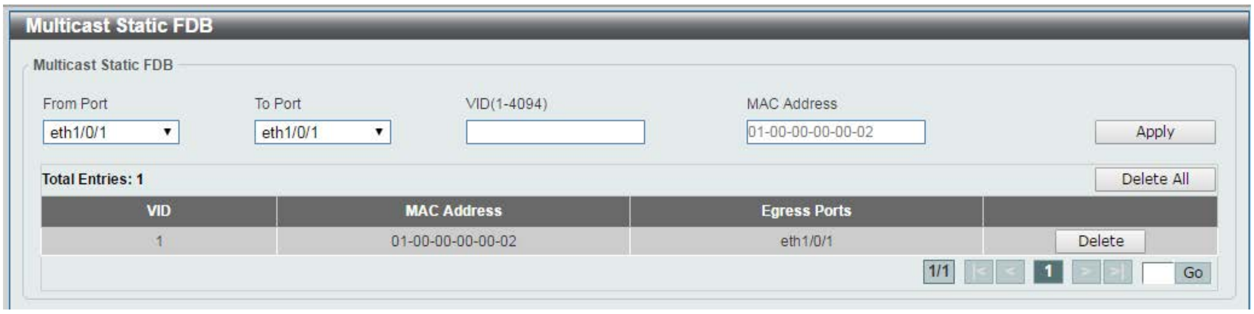
Click the **Delete** button to remove the specified entry.

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:



Multicast Static FDB

Multicast Static FDB

From Port: eth1/0/1
To Port: eth1/0/1
VID(1-4094):
MAC Address: 01-00-00-00-00-02

Total Entries: 1

VID	MAC Address	Egress Ports	
1	01-00-00-00-00-02	eth1/0/1	Delete

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.

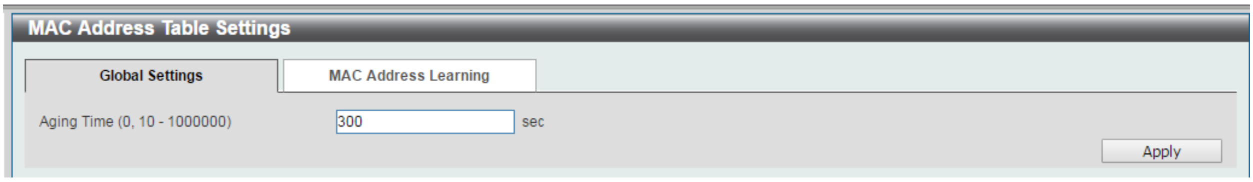
Click the **Delete** button to remove the specific entry.

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:



MAC Address Table Settings

Aging Time (0, 10 - 1000000): 300 sec

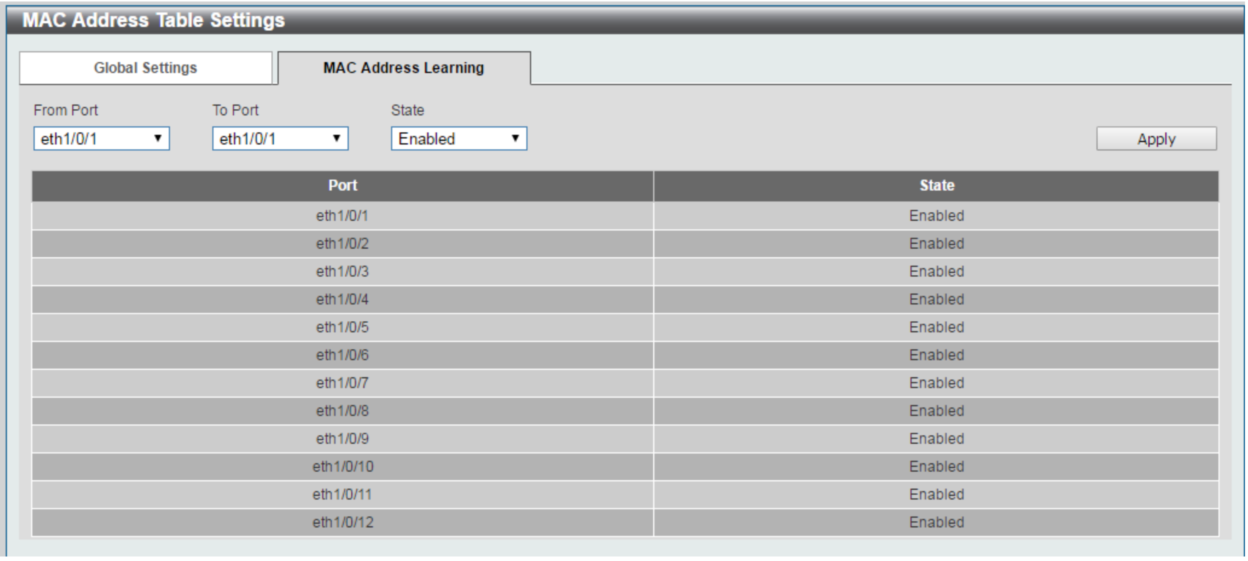
Figure 6-3 MAC Address Table Settings (Global Settings) window

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.



From Port: eth1/0/1

To Port: eth1/0/1

State: Enabled

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

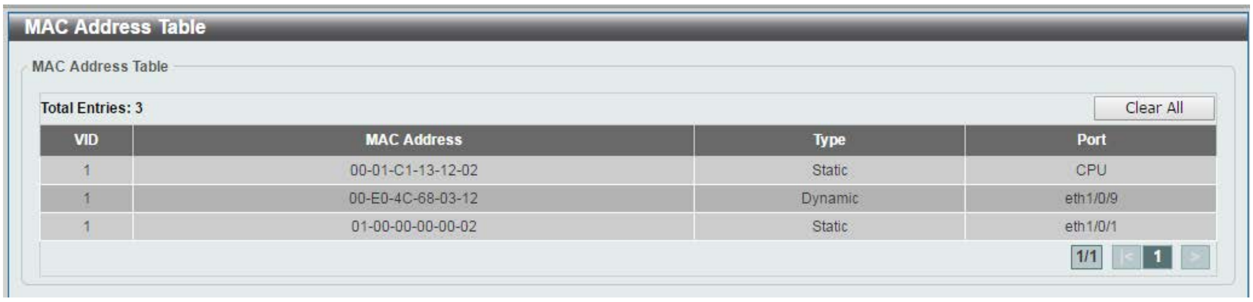
Parameter	Description
From Port / To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the MAC address learning function on the ports specified here.

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:



Total Entries: 3

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

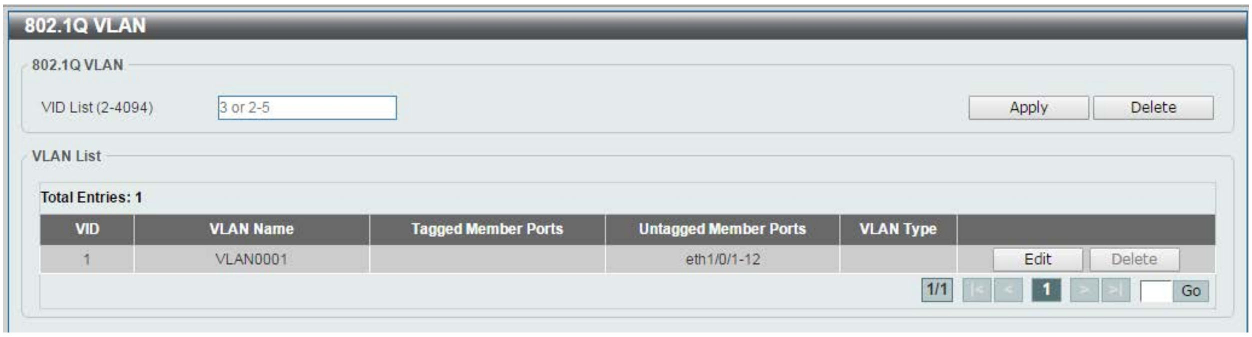
Click the **Clear All** button to clear all dynamic MAC addresses.

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:



802.1Q VLAN

802.1Q VLAN

VID List (2-4094): 3 or 2-5

VLAN List

Total Entries: 1

VID	VLAN Name	Tagged Member Ports	Untagged Member Ports	VLAN Type	
1	VLAN0001		eth1/0/1-12		Edit Delete

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.

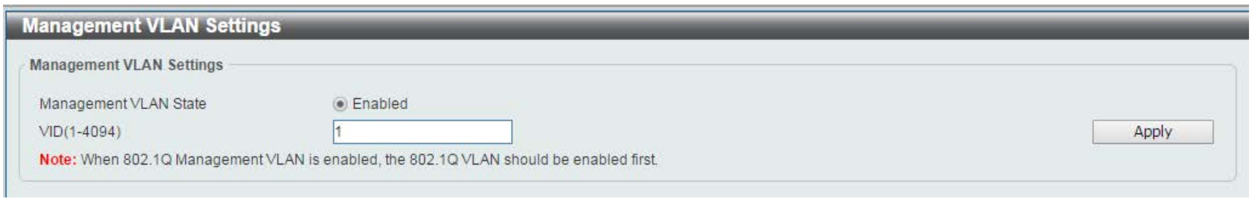
Click the **Edit** button to re-configure the specific entry.

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:



Management VLAN Settings

Management VLAN Settings

Management VLAN State ● Enabled

VID(1-4094): 1

Note: When 802.1Q Management VLAN is enabled, the 802.1Q VLAN should be enabled first.

Figure 6-7 Management VLAN window

The fields that can be configured are described below:

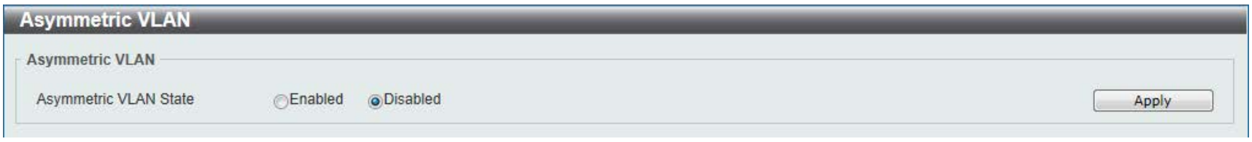
Parameter	Description
VID	Enter the VID to allow user use this VLAN to manage the switch.

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

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:



Asymmetric VLAN

Asymmetric VLAN

Asymmetric VLAN State ○Enabled ●Disabled

Figure 6-8 Asymmetric VLAN window

The fields that can be configured are described below:

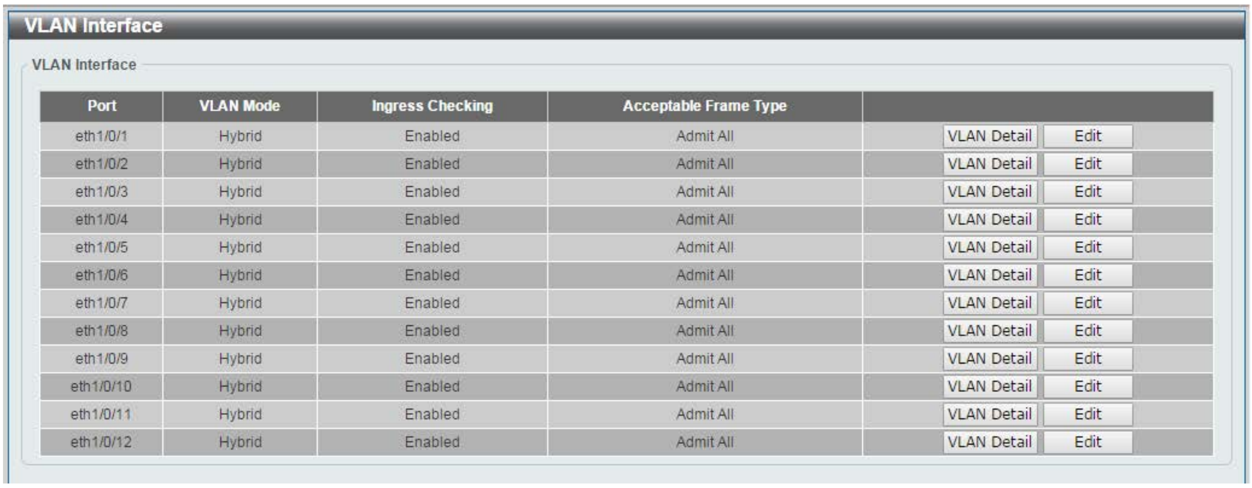
Parameter	Description
Asymmetric VLAN State	Select this option to enable or disable the asymmetric VLAN function

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:



VLAN Interface

VLAN Interface

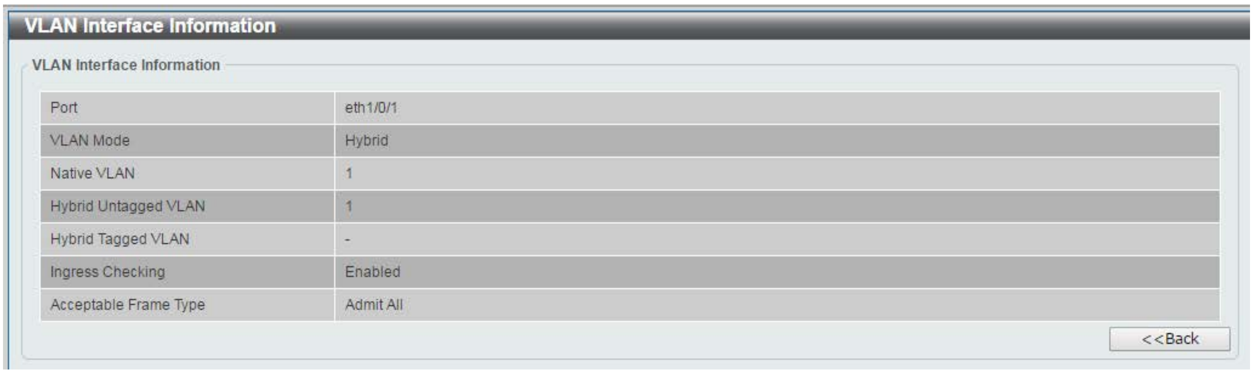
Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	
eth1/0/1	Hybrid	Enabled	Admit All	VLAN Detail Edit
eth1/0/2	Hybrid	Enabled	Admit All	VLAN Detail Edit
eth1/0/3	Hybrid	Enabled	Admit All	VLAN Detail Edit
eth1/0/4	Hybrid	Enabled	Admit All	VLAN Detail Edit
eth1/0/5	Hybrid	Enabled	Admit All	VLAN Detail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

VLAN Interface Information

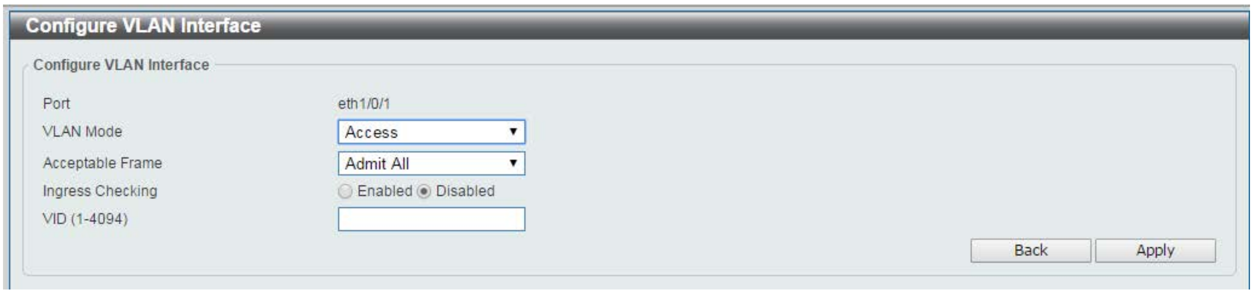
Port	eth1/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	-
Ingress Checking	Enabled
Acceptable Frame Type	Admit All

Figure 6-10 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.



Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/1
VLAN Mode: Access
Acceptable Frame: Admit All
Ingress Checking: ○ Enabled ● Disabled
VID (1-4094):

Figure 6-11 Configure VLAN Interface - Access window

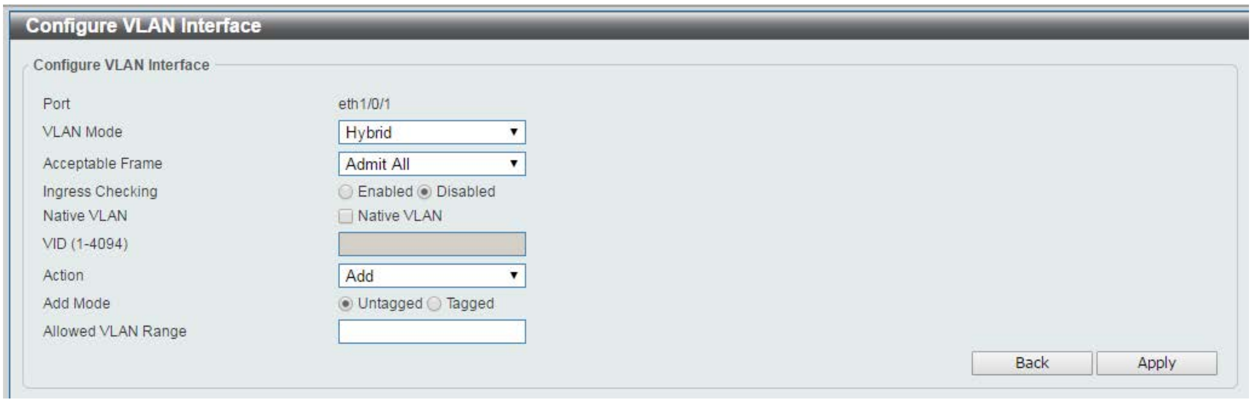
The fields that can be configured are described below:

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.



Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/1

VLAN Mode: Hybrid

Acceptable Frame: Admit All

Ingress Checking: ○ Enabled ● Disabled

Native VLAN: □ Native VLAN

VID (1-4094):

Action: Add

Add Mode: ● Untagged ○ Tagged

Allowed VLAN Range:

Figure 6-12 Configure VLAN Interface - Hybrid window

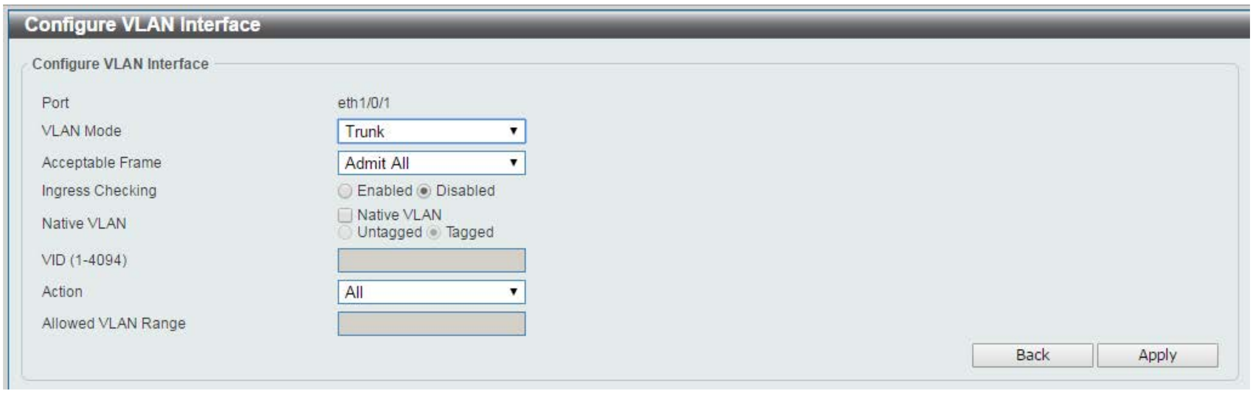
The fields that can be configured are described below:

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.



Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/1

VLAN Mode: Trunk

Acceptable Frame: Admit All

Ingress Checking: ○ Enabled ● Disabled

Native VLAN: □ Native VLAN
○ Untagged ● Tagged

VID (1-4094):

Action: All

Allowed VLAN Range:

Figure 6-13 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.

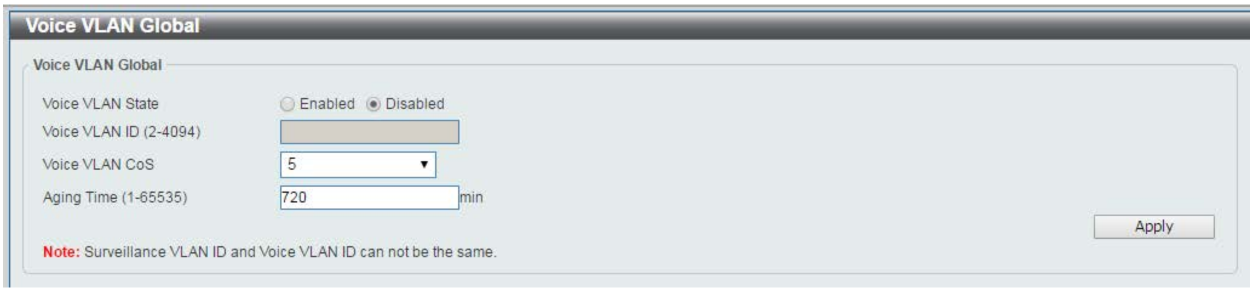
Voice VLAN

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:



Voice VLAN Global

Voice VLAN Global

Voice VLAN State ○ Enabled ● Disabled

Voice VLAN ID (2-4094)

Voice VLAN CoS 5

Aging Time (1-65535) 720 min

Note: Surveillance VLAN ID and Voice VLAN ID can not be the same.

Figure 6-14 Voice VLAN Global window

The fields that can be configured are described below:

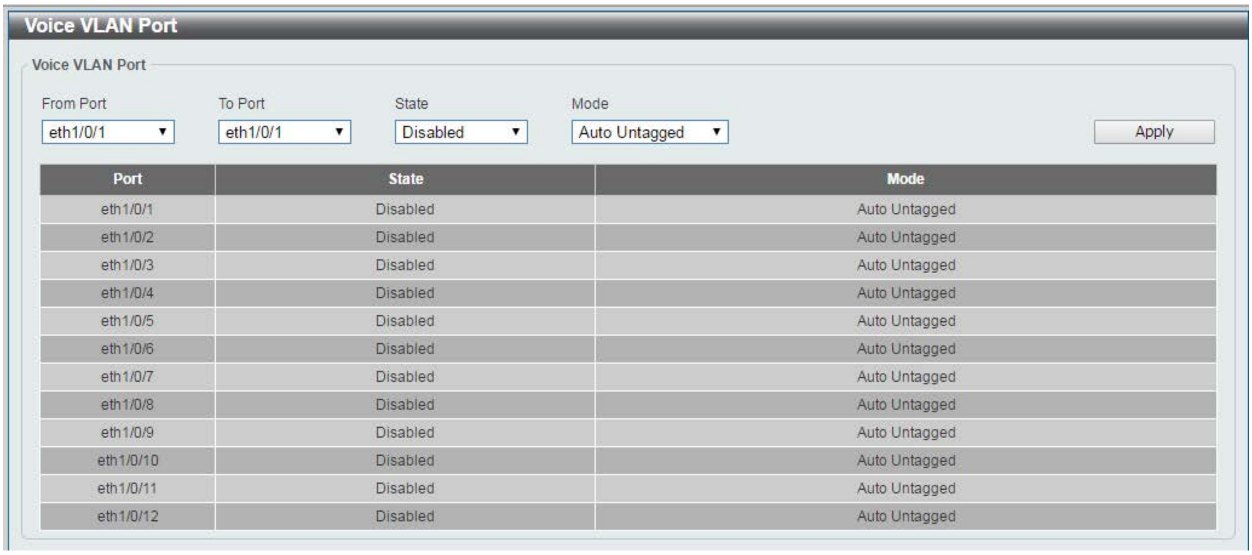
Parameter	Description
Voice VLAN State	Select this option to enable or disable the voice VLAN.
Voice VLAN ID	Enter the voice VLAN ID. The value is range from 2 to 4094.
Voice VLAN CoS	Select the priority of the voice VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is 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:



Voice VLAN Port

Voice VLAN Port

From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled
Mode: Auto Untagged

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 6-15 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.

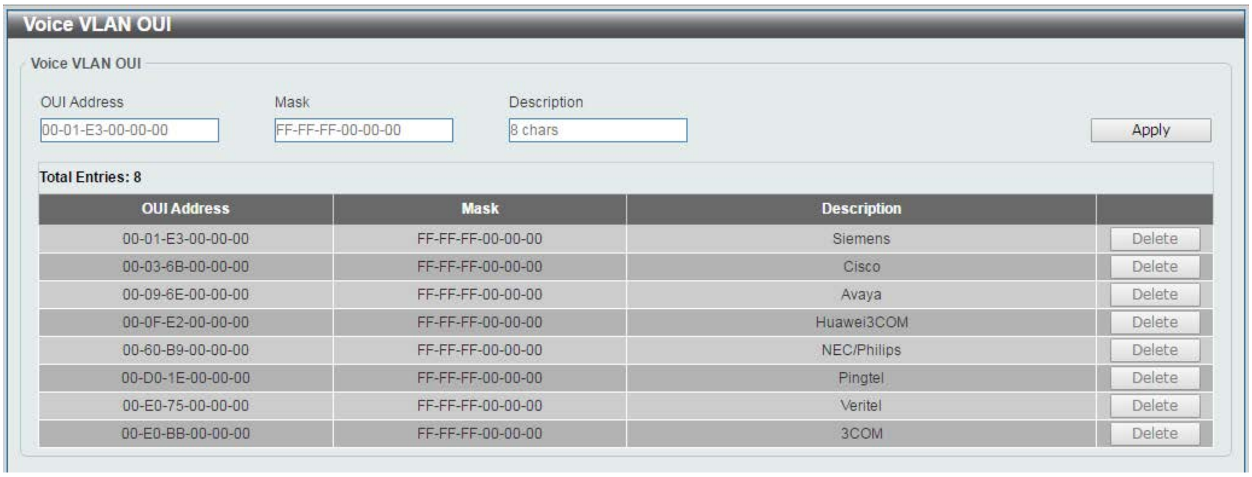
Mode	Select the mode of the port. Options to choose from are Auto **Untagged**, **Auto Tagged**, and **Manual**.

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:



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	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Delete
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei3COM	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC/Philips	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Delete
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	Delete
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	Delete

Figure 6-16 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.

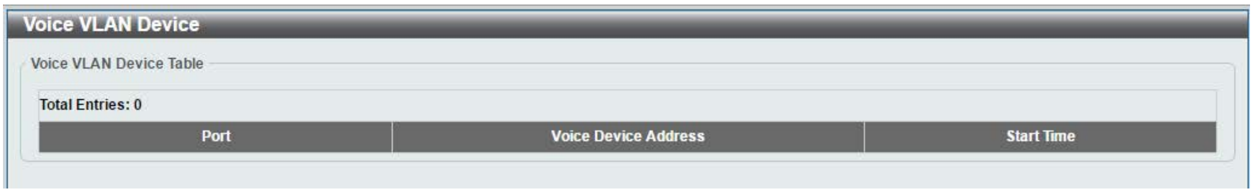
Click the **Apply** button to accept the changes made.

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:



Total Entries: 0

Port	Voice Device Address	Start Time

Figure 6-17 Voice VLAN Device window

Spanning Tree

This Switch supports two versions of the Spanning Tree Protocol: 802.1D-1998 STP and 802.1D-2004 Rapid STP. 802.1D-1998 STP will be familiar to most networking

professionals. However, since 802.1D-2004 RSTP 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, and 802.1D-2004 RSTP.

802.1D-2004 Rapid Spanning Tree

The Switch implements two versions of the Spanning Tree Protocol, 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 two 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. 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 port state discard- ing, 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 two 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.

802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	No	No
Discarding	Blocking	No	No
Discarding	Listening	No	No
Learning	Learning	No	**Yes**
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.

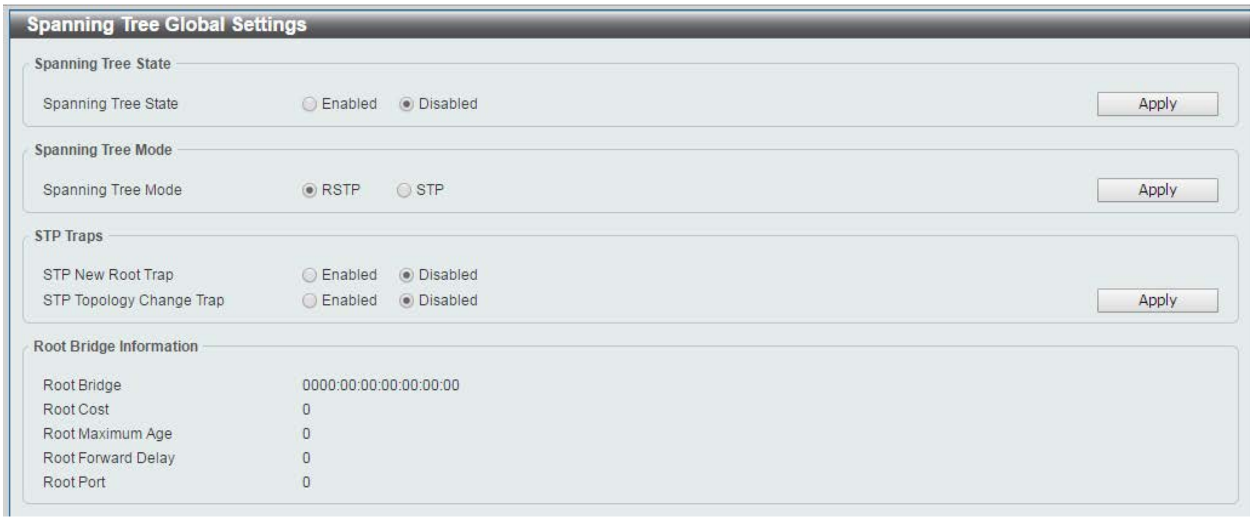
The Spanning Tree Protocol (STP) operates on two levels:

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:



Spanning Tree Global Settings

Spanning Tree State

Spanning Tree State ○ Enabled ● Disabled

Spanning Tree Mode

Spanning Tree Mode ● RSTP ○ STP

STP Traps

STP New Root Trap ○ Enabled ● Disabled

STP Topology Change Trap ○ Enabled ● Disabled

Root Bridge Information

Root Bridge	0000:00:00:00:00:00:00
Root Cost	0
Root Maximum Age	0
Root Forward Delay	0
Root Port	0

Figure 6-18 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 **RSTP**, and **STP**.

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

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

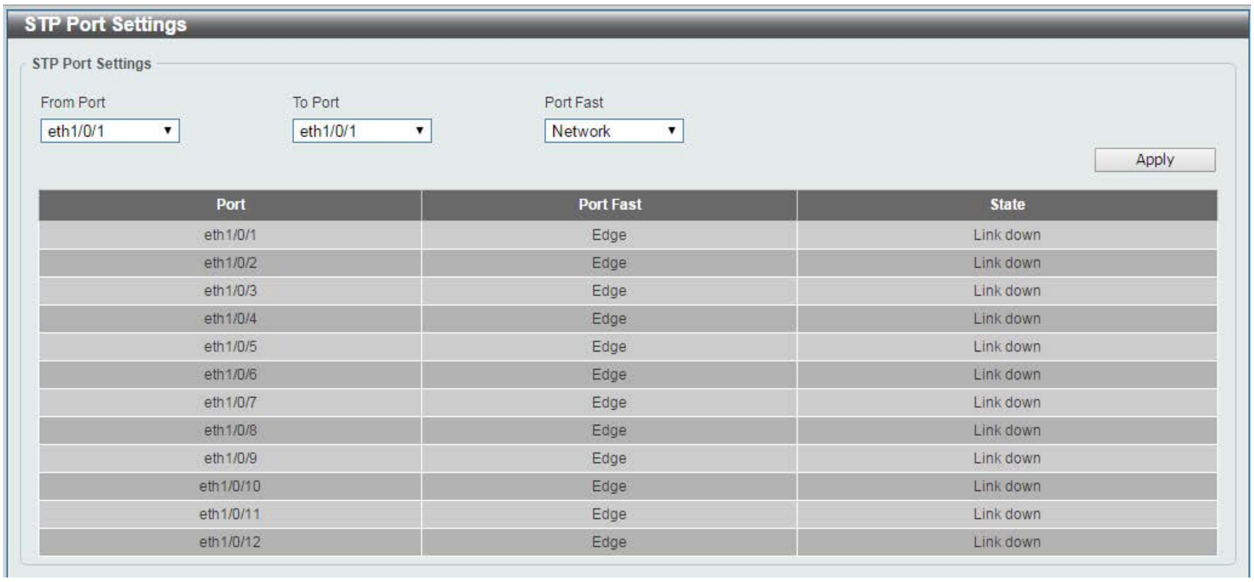
Parameter	Description
STP New Root Trap	Select this option to enable or disable the STP new root trap option here.
STP Topology Change Trap	Select this option to enable or disable the STP topology change trap option here.

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

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:



STP Port Settings

STP Port Settings

From Port: eth1/0/1 ▼
To Port: eth1/0/1 ▼
Port Fast: Network ▼

Apply

Port	Port Fast	State
eth1/0/1	Edge	Link down
eth1/0/2	Edge	Link down
eth1/0/3	Edge	Link down
eth1/0/4	Edge	Link down
eth1/0/5	Edge	Link down
eth1/0/6	Edge	Link down
eth1/0/7	Edge	Link down
eth1/0/8	Edge	Link down
eth1/0/9	Edge	Link down
eth1/0/10	Edge	Link down
eth1/0/11	Edge	Link down
eth1/0/12	Edge	Link down

Figure 6-19 STP Port Settings window

The fields that can be configured are described below:

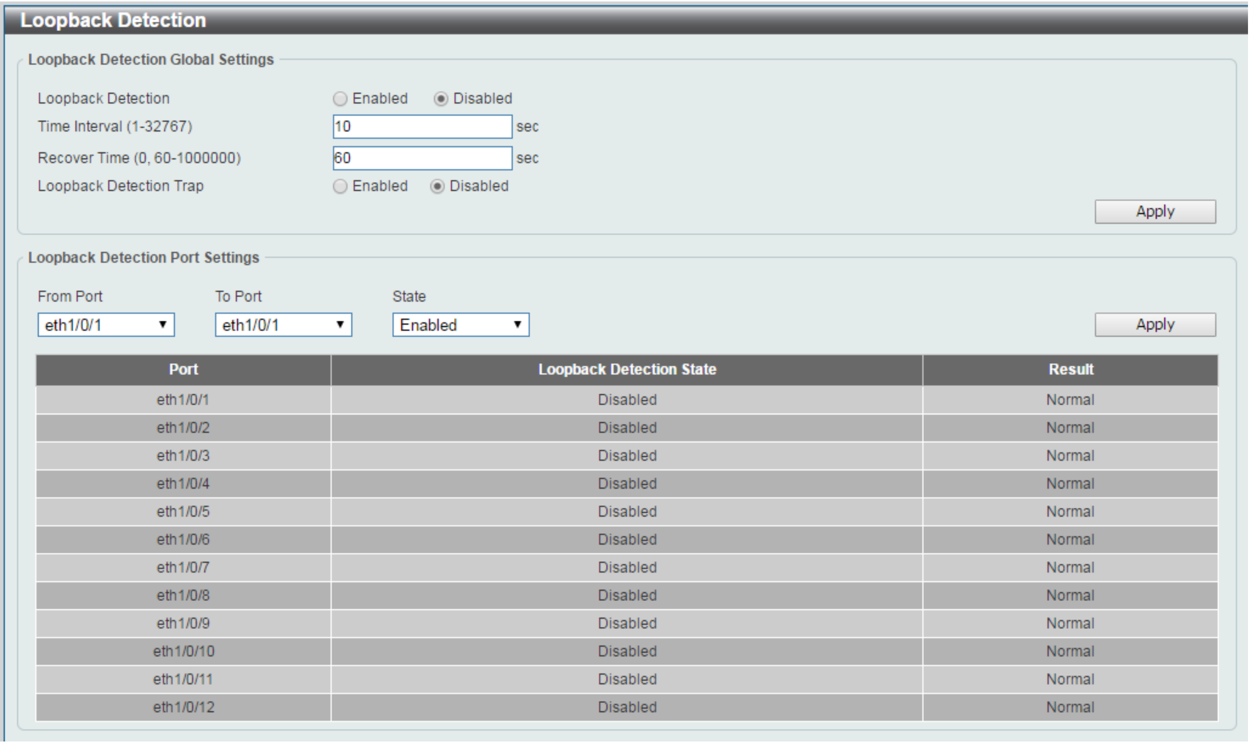
Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Port Fast	Select the port fast option here. Options to choose from are **Network**, **Disabled**, and **Edge**. In the **Network** mode, the port will remain in the non-port-fast state for three 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.

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) 10 sec

Recover Time (0, 60-1000000) 60 sec

Loopback Detection Trap ○ Enabled ● Disabled

Loopback Detection Port Settings

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

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 6-20 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.

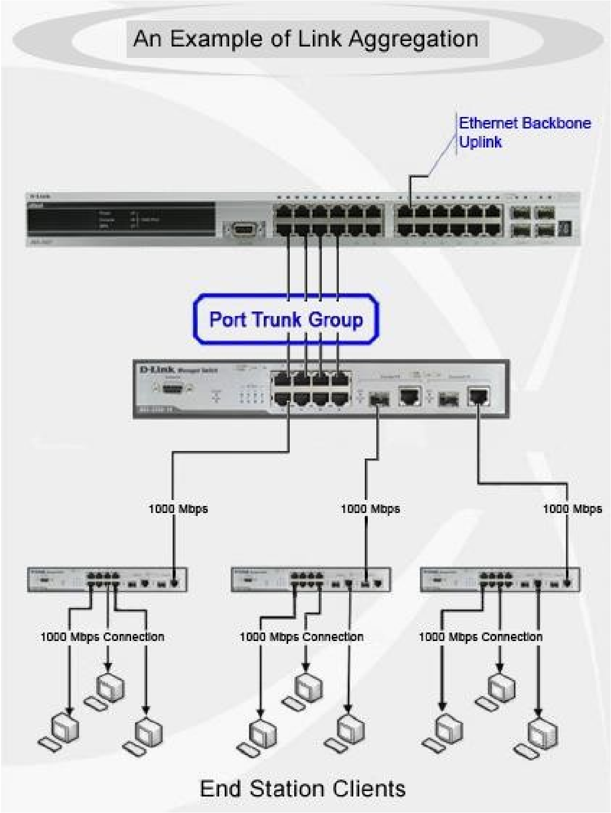


Figure 6-21 Example of Port Trunk Group

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

Link aggregation allows several ports to be grouped together and to act as a single link. This 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.

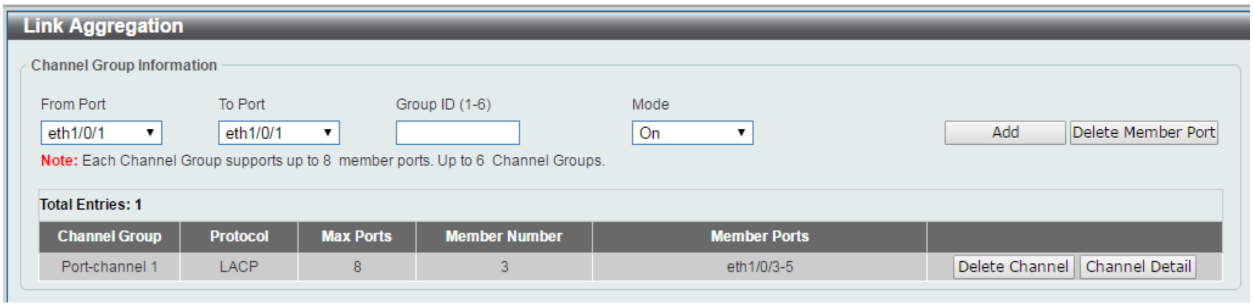
Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

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:



From Port: eth1/0/1
To Port: eth1/0/1
Group ID (1-6):
Mode: On

Note: Each Channel Group supports up to 8 member ports. Up to 6 Channel Groups.

Total Entries: 1

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

Figure 6-22 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.

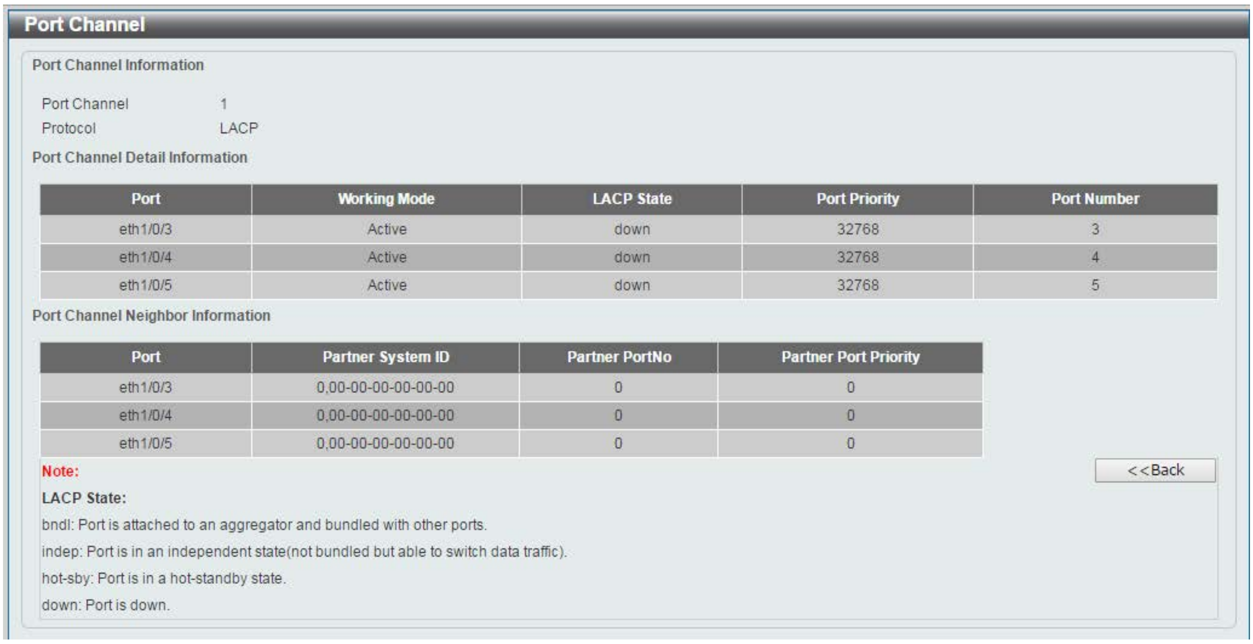
Click the **Add** button to add a new entry based on the information entered.

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 6-23 Port Channel window

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

L2 Multicast Control

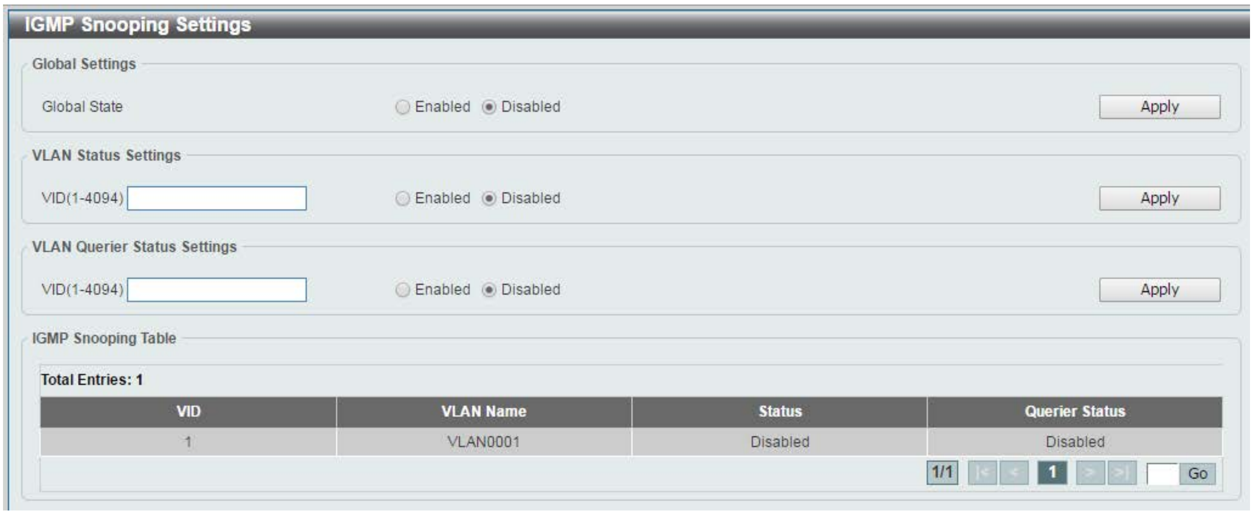
IGMP Snooping

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:



IGMP Snooping Settings

Global Settings

Global State ○ Enabled ● Disabled

VLAN Status Settings

VID(1-4094) ○ Enabled ● Disabled

VLAN Querier Status Settings

VID(1-4094) ○ Enabled ● Disabled

IGMP Snooping Table

Total Entries: 1

VID	VLAN Name	Status	Querier Status
1	VLAN0001	Disabled	Disabled

Figure 6-24 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:

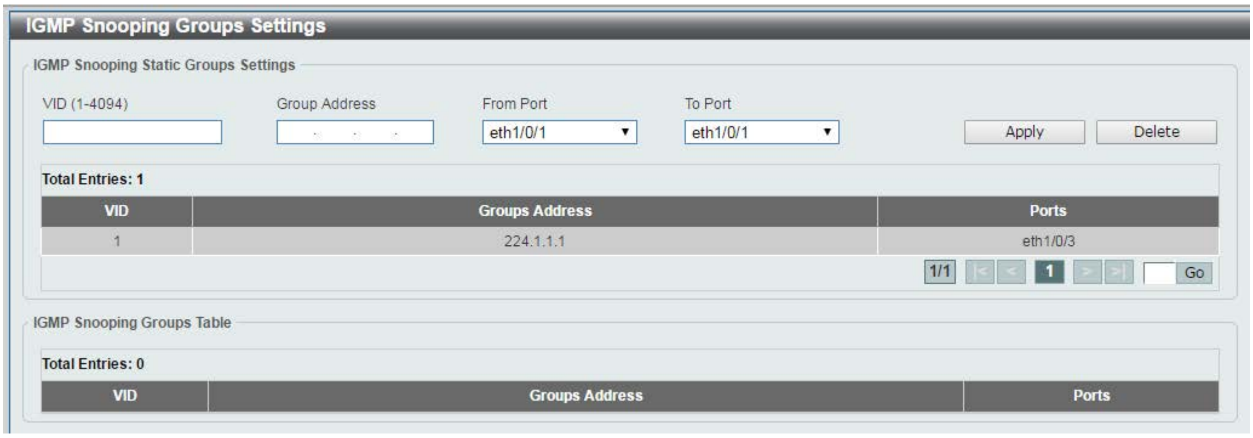
Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable IGMP snooping querier on the VLAN.

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

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:



IGMP Snooping Groups Settings

IGMP Snooping Static Groups Settings

VID (1-4094):

Group Address: . . .

From Port: eth1/0/1

To Port: eth1/0/1

Total Entries: 1

VID	Groups Address	Ports
1	224.1.1.1	eth1/0/3

IGMP Snooping Groups Table

Total Entries: 0

VID	Groups Address	Ports

Figure 6-25 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

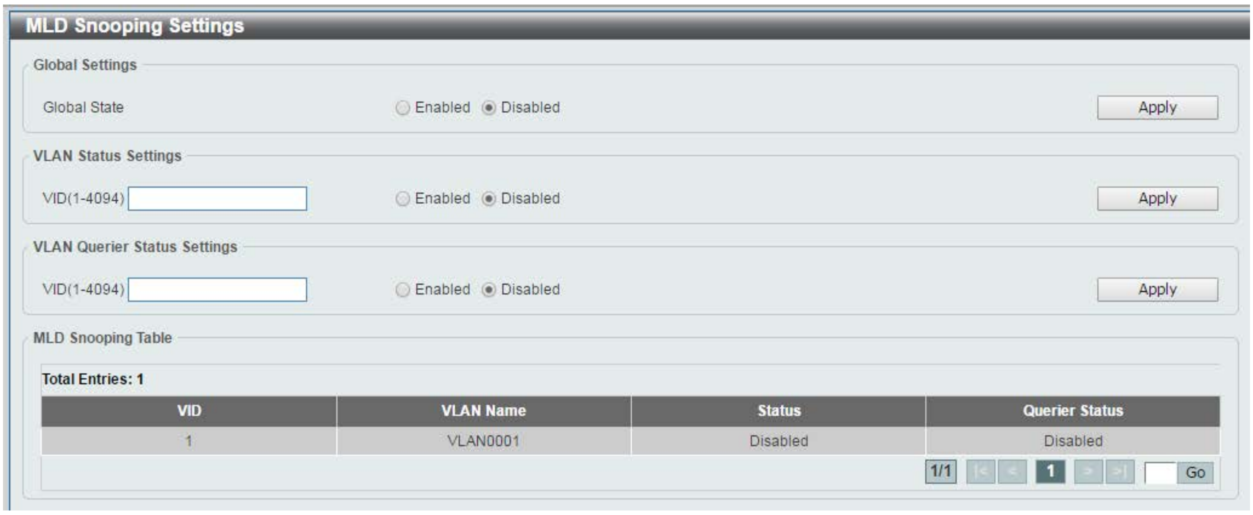
Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

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.

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:



MLD Snooping Settings

Global Settings

Global State ○ Enabled ● Disabled

VLAN Status Settings

VID(1-4094) ○ Enabled ● Disabled

VLAN Querier Status Settings

VID(1-4094) ○ Enabled ● Disabled

MLD Snooping Table

Total Entries: 1

VID	VLAN Name	Status	Querier Status
1	VLAN0001	Disabled	Disabled

Figure 6-26 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.

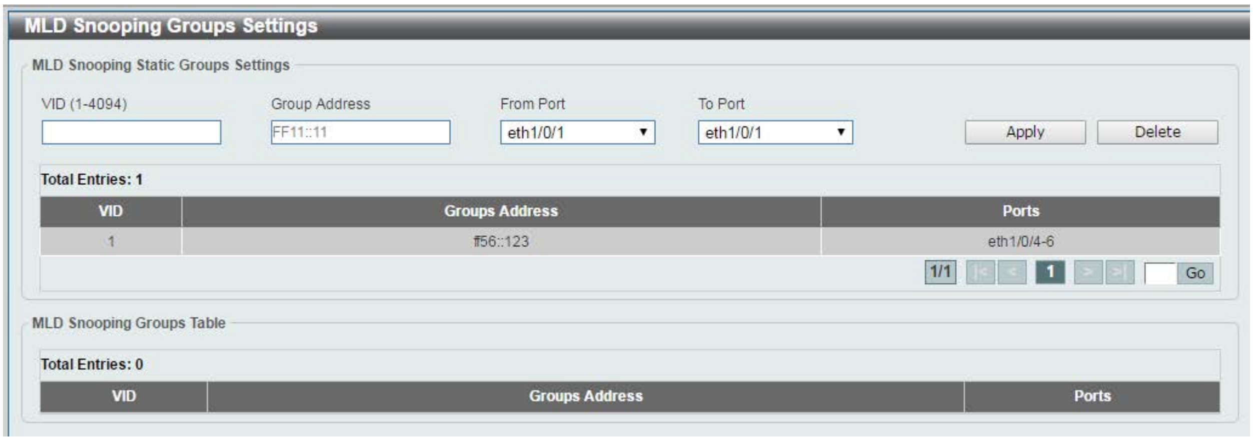
Click the **Apply** button to accept the changes made.

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:



MLD Snooping Groups Settings

MLD Snooping Static Groups Settings

VID (1-4094):

Group Address: FF11::11

From Port: eth1/0/1

To Port: eth1/0/1

Total Entries: 1

VID	Groups Address	Ports
1	ff56::123	eth1/0/4-6

MLD Snooping Groups Table

Total Entries: 0

VID	Groups Address	Ports

Figure 6-27 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.

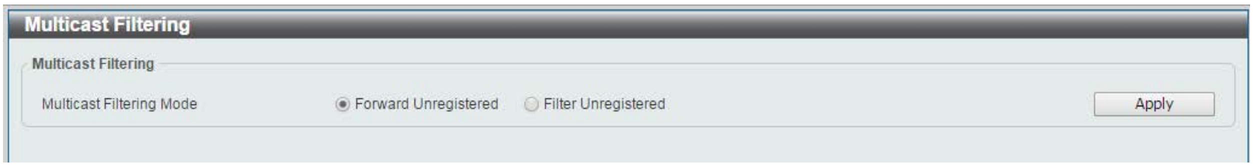
Click the **Delete** button to remove the specified entry.

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:



Multicast Filtering

Multicast Filtering

Multicast Filtering Mode: ● Forward Unregistered ○ Filter Unregistered

Figure 6-28 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.

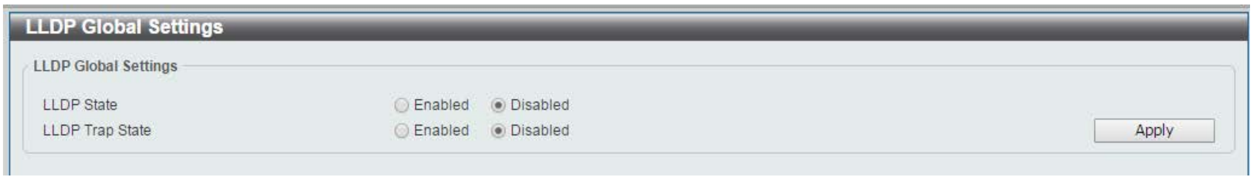
Click the **Apply** button to accept the changes made.

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:



LLDP Global Settings

LLDP Global Settings

LLDP State ○ Enabled ● Disabled

LLDP Trap State ○ Enabled ● Disabled

Apply

Figure 6-29 LLDP Global Settings window

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

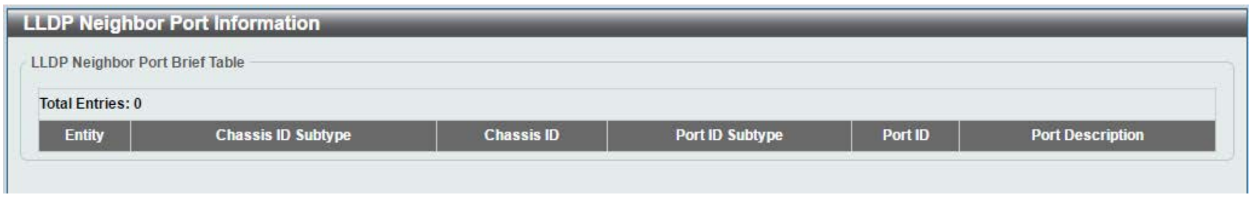
Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Trap State	Select this option to enable or disable the LLDP trap state.

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:



LLDP Neighbor Port Information

LLDP Neighbor Port Brief Table

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description

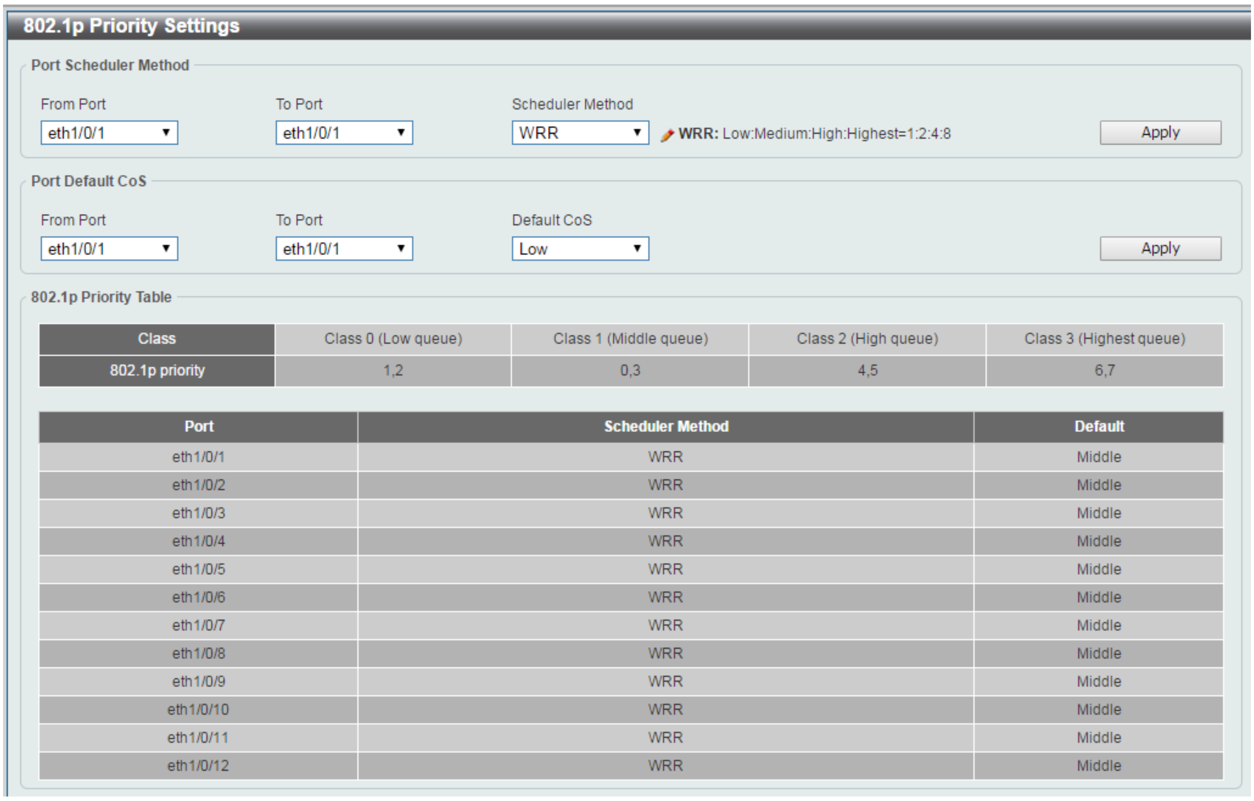
Figure 6-30 LLDP Neighbor Port Information window

7. Quality of Service (QoS)

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	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**. To set a CoS queue in the **SP** mode, any higher priority CoS queue must also be in the strict priority mode. **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.

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

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

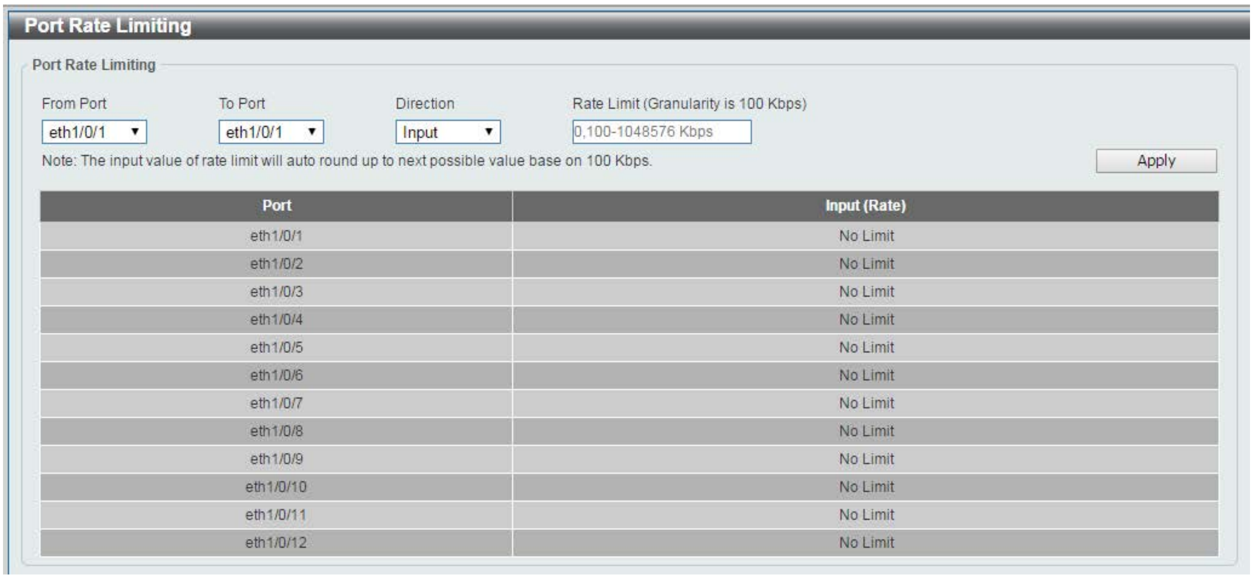
Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are **Low**, **Medium**, **High**, and **Highest**.

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.

8. Security

Safeguard Engine

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

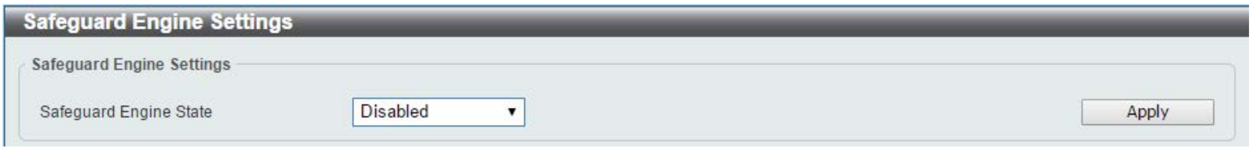
The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

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:



Safeguard Engine Settings

Safeguard Engine Settings

Safeguard Engine State: Disabled

Figure 8-1 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.

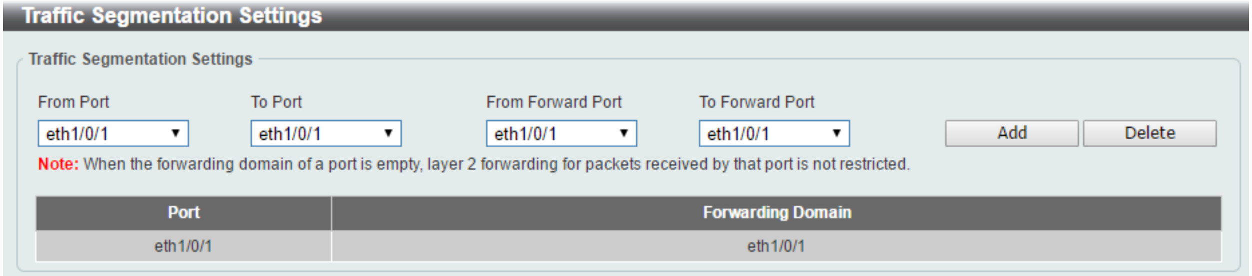
Traffic Segmentation Settings

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:



Traffic Segmentation Settings

Traffic Segmentation Settings

From Port: eth1/0/1
To Port: eth1/0/1
From Forward Port: eth1/0/1
To Forward Port: eth1/0/1

Note: When the forwarding domain of a port is empty, layer 2 forwarding for packets received by that port is not restricted.

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

Figure 8-2 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.

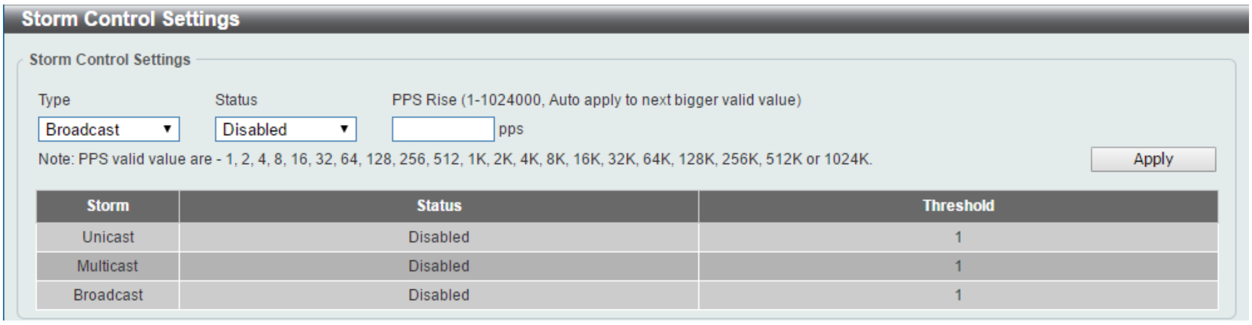
Click the **Add** button to add a new entry based on the information entered.

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 Control Settings

Storm Control Settings

Type: Broadcast
Status: Disabled
PPS Rise (1-1024000, Auto apply to next bigger valid value): pps

Note: PPS valid value are - 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

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

Figure 8-3 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.

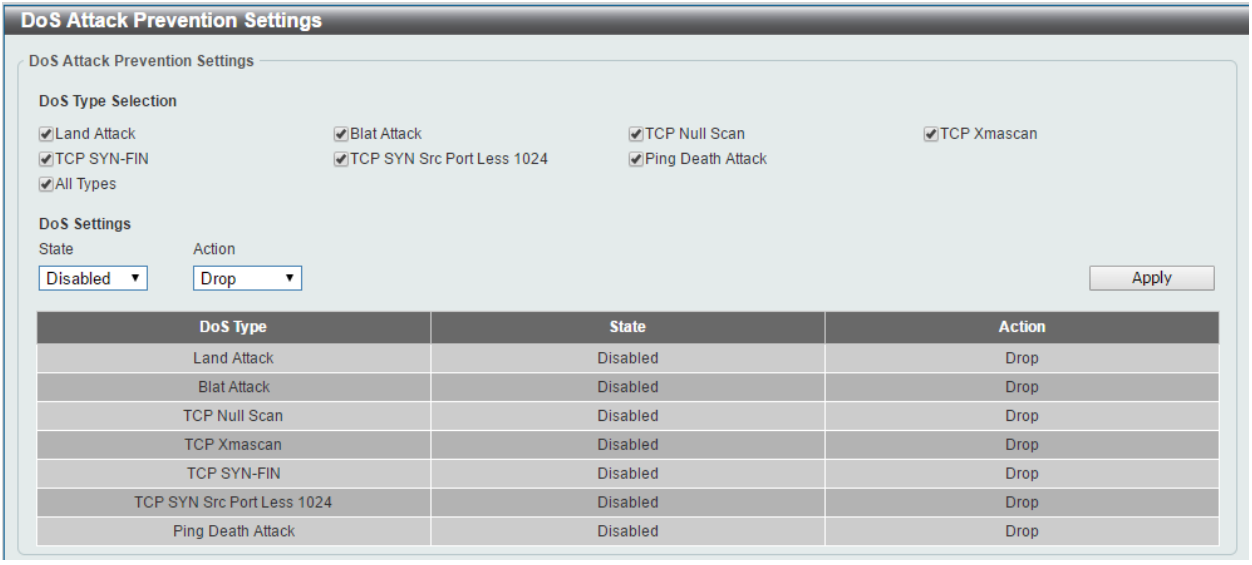
Click the **Apply** button to accept the changes made.

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 Attack Prevention Settings

DoS Attack Prevention Settings

DoS Type Selection

☑ Land Attack ☑ Blat Attack ☑ TCP Null Scan ☑ TCP Xmascan
☑ TCP SYN-FIN ☑ TCP SYN Src Port Less 1024 ☑ Ping Death Attack
☑ All Types

DoS Settings

State: Disabled
Action: Drop

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 8-4 DoS Attack Prevention Settings window

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

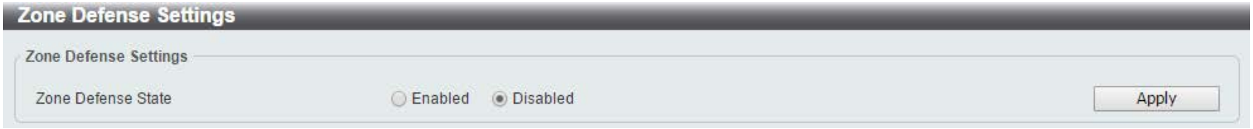
Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
State	Select to enable or disable the DoS attack prevention feature's global state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is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



Zone Defense Settings

Zone Defense Settings

Zone Defense State ○ Enabled ● Disabled

Figure 8-5 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

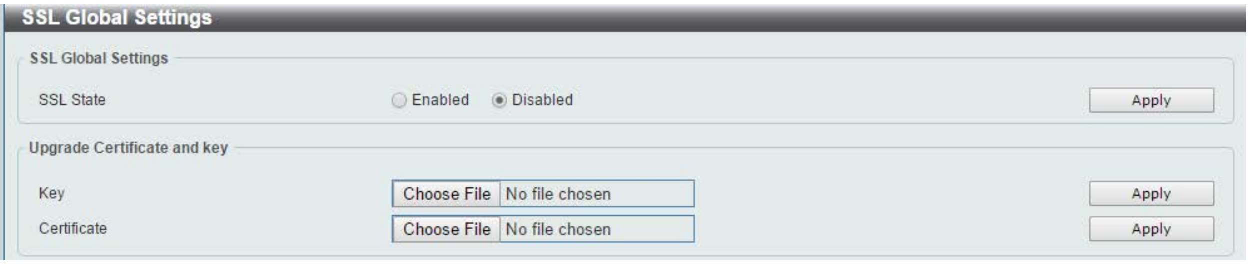
SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

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:



SSL Global Settings

SSL Global Settings

SSL State ○ Enabled ● Disabled Apply

Upgrade Certificate and key

Key Choose File No file chosen Apply

Certificate Choose File No file chosen Apply

Figure 8-6 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.

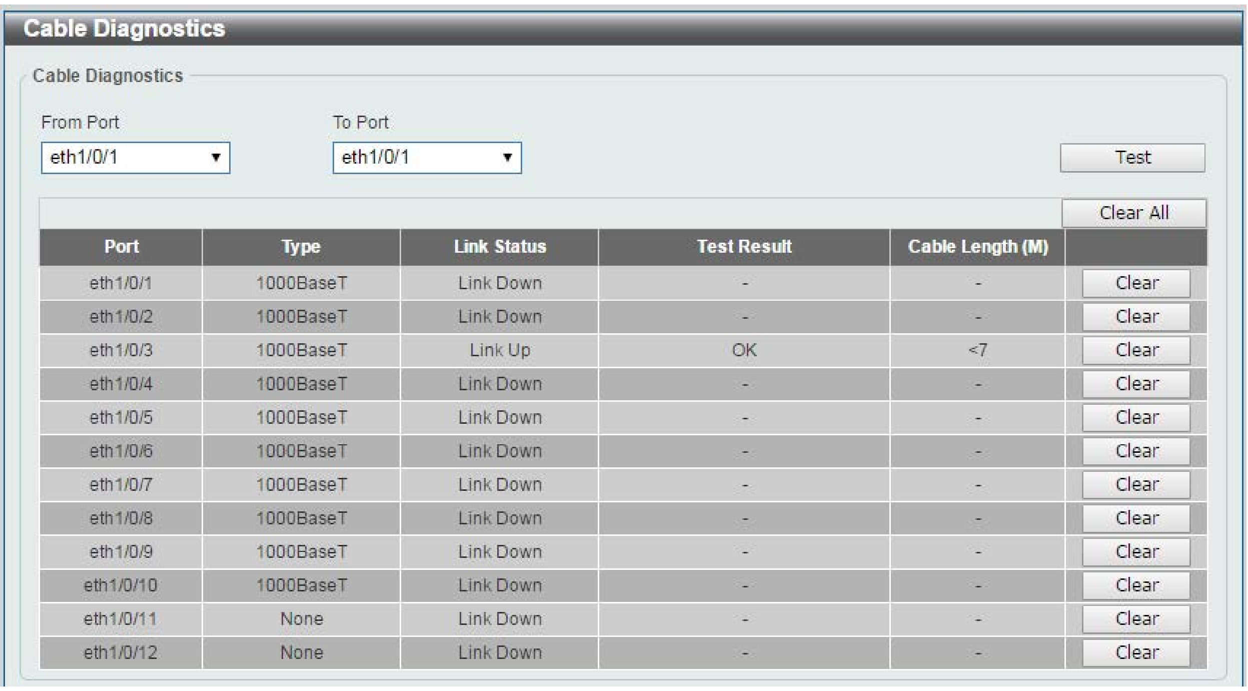
9. OAM

Cable Diagnostics

Cable Diagnostics

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

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



Port	Type	Link Status	Test Result	Cable Length (M)	
eth1/0/1	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

The fields that can be configured are described below:

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

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

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

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

10. Monitoring

__Statistics__

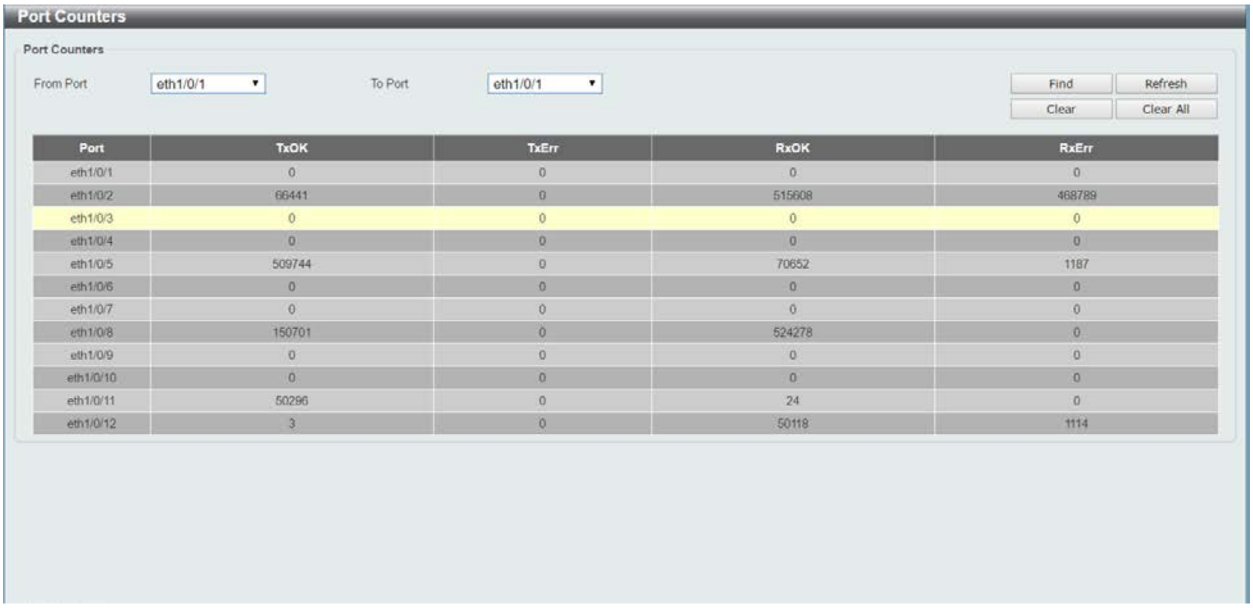
__Mirror Settings__

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:



From Port: eth1/0/1 ▼ To Port: eth1/0/1 ▼

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.

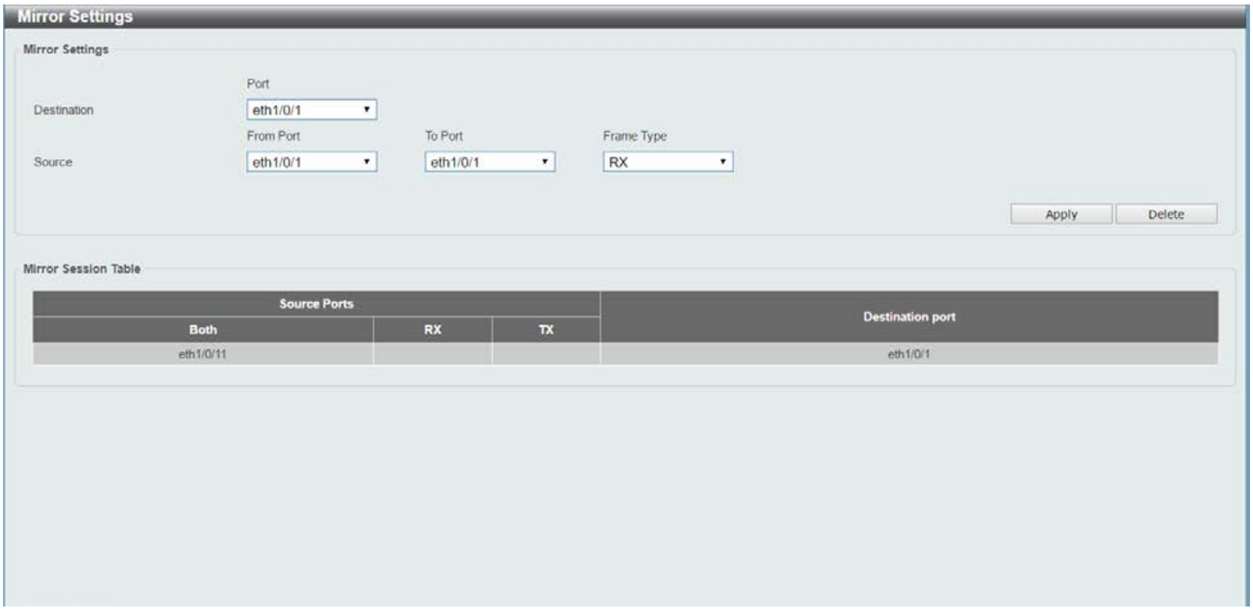
Click the **Clear** button to clear all error counters of the specific port.

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:



Mirror Settings

Mirror Settings

Destination: Port eth1/0/1

Source: From Port eth1/0/1, To Port eth1/0/1, Frame Type RX

Mirror Session Table

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

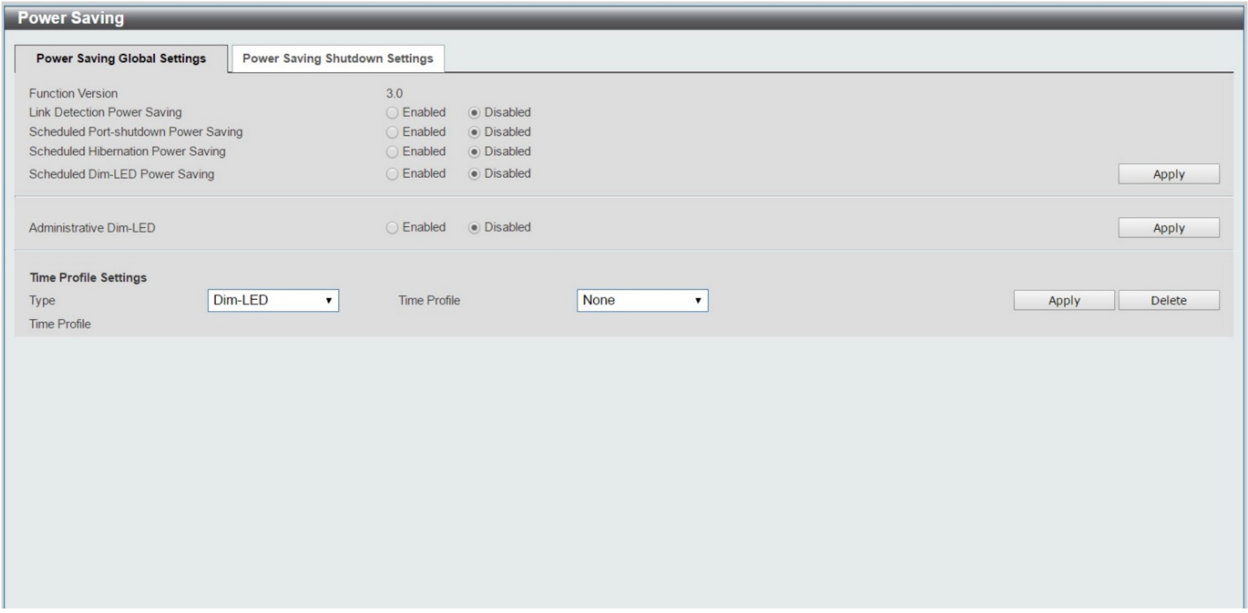
Power Saving

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:



Power Saving

Power Saving Global Settings | Power Saving Shutdown Settings

Function Version 3.0

Link Detection Power Saving ○ Enabled ● Disabled

Scheduled Port-shutdown Power Saving ○ Enabled ● Disabled

Scheduled Hibernation Power Saving ○ Enabled ● Disabled

Scheduled Dim-LED Power Saving ○ Enabled ● Disabled

Administrative Dim-LED ○ Enabled ● Disabled

Time Profile Settings

Type: Dim-LED ▾ Time Profile: None ▾

Time Profile

Figure 11-1 Power Saving window

The fields that can be configured are described below:

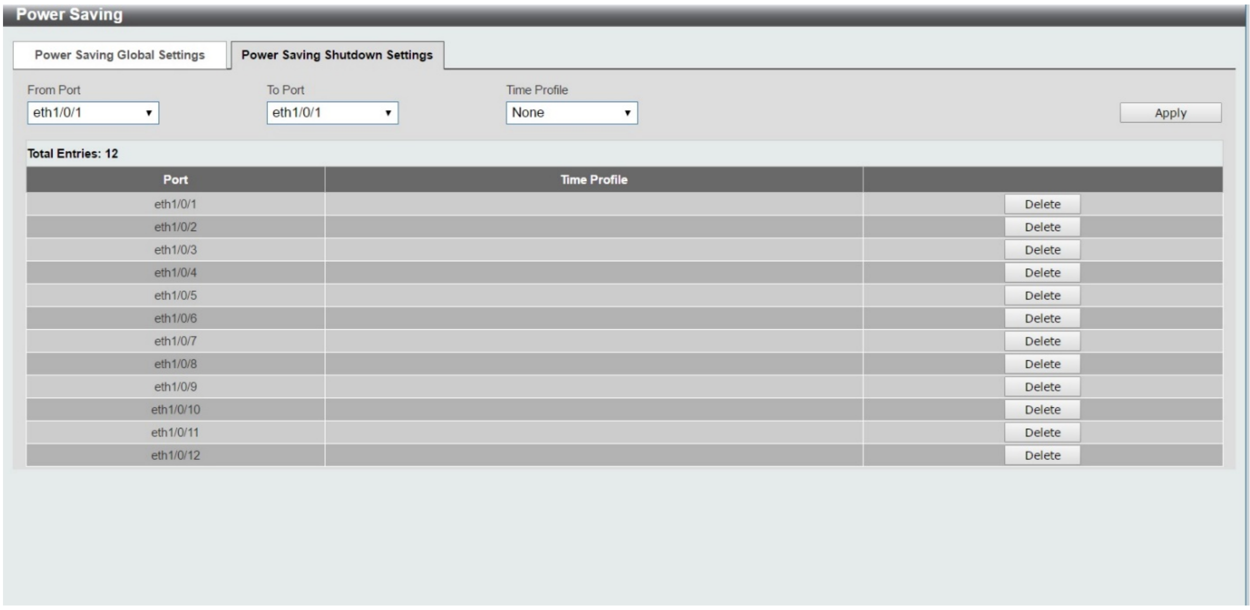
Parameter	Description
Link Detection Power Saving	Select this option to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port’s capabilities when the port status is link up.
Scheduled 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.



From Port: eth1/0/1

To Port: eth1/0/1

Time Profile: None

Total Entries: 12

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.

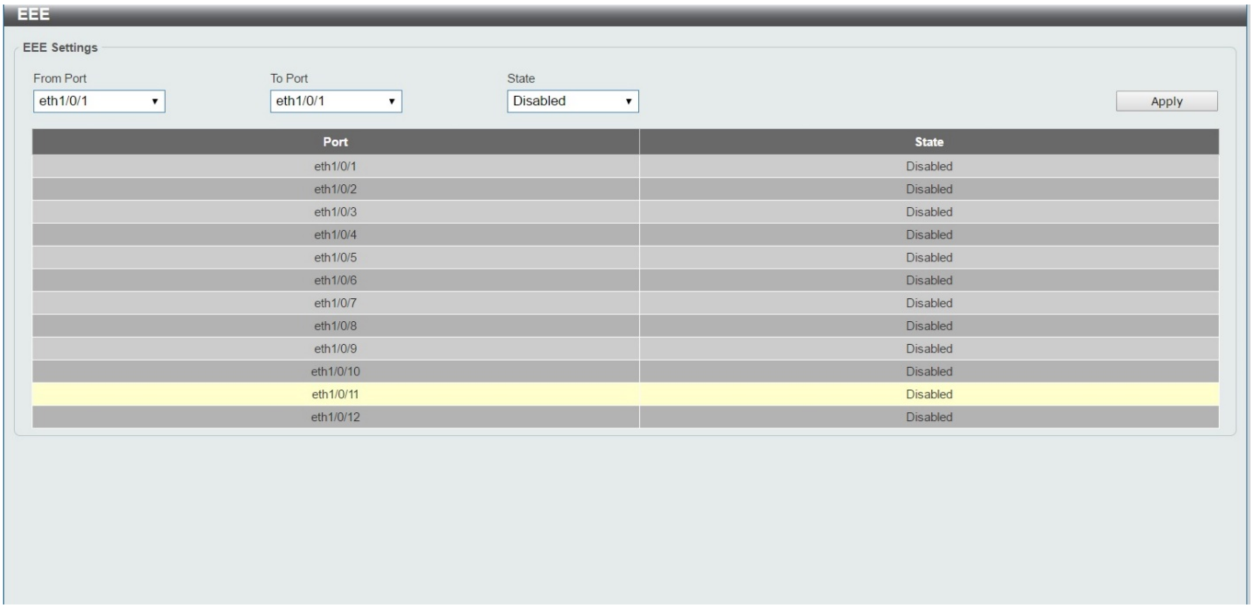
Click the **Apply** button to accept the changes made.

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:



EEE

EEE Settings

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

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

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.

Interface

Log Description	Severity
Event description: When port is down Log Message: Port <port-type>< interface-id> link down Parameters description: port-type: port type interface-id: Interface name	Informational
Event description: When port is up Log Message: Port <port-type>< interface-id> link up, <link-speed> Parameters description: port-type: port type 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: [Unit <unitID>,]Successful login through Console (Username: <username>) Parameters description: unitID: The unit ID.	Informational

username: Represent current login user.	
vent description: Login through console unsuccessfully. Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Warning
Event description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

PoE

Log Description	Severity
Event description: Total power usage threshold is exceeded Log Message: Unit <unit-id> usage threshold <percentage> is exceeded Parameters description: unit-id : box id percentage : usage threshold	Warning
Event description: Total power usage threshold is recovered. Log Message: Unit <unit-id> usage threshold <percentage> is recovered Parameters description: unit-id : box id percentage : usage threshold	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
Event description: Successful login through Telnet.	Informational

Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	
Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning
Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>). Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational

Voice-VLAN

Log Description	**Severity**
Event description: When a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: < mac-address >) Parameters description: interface-id: Interface name. mac-address: Voice device MAC address	Informational
Event description: When an interface which is in auto voice VLAN mode joins the voice VLAN Log Message: < interface-id > add into voice VLAN <vid > Parameters description: interface-id: Interface name. vid:VLAN ID	Informational
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. Log Message: < interface-id > remove from voice VLAN <vid > Parameters description:	Informational

interface-id: Interface name. vid:VLAN ID	

Web

Log Description	Severity
Event description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event description: Web session timed out. Log Message: Web session timed out (Username: <usrname>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Logout through Web. Log Message: Logout through Web (Username: %S, IP: %S). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational

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

LBD

Trap Name	Description	OID
isLbdLoopOccurred	his trap is sent when an interface loop occurs. Binding objects: (1) isLbdNotifyInfoIfIndex	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) isLbdNotifyInfoIfIndex	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	1.0.8802.1.1.2.0.0.1

	(4) lldpStatsRemTablesAgeouts	

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 trap is sent for the same transition. Implementation of this trap is optional	1.3.6.1.2.1.17.0.2

PoE

Trap Name	Description	OID
pethMainPowerUsageOnNotification	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
pethMainPowerUsageOffNotification	This trap indicates PSE Threshold usage indication is off, the usage power is below the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3

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

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