Version 1.81 | 02/29/2024

Web UI Reference Guide

Gigabit Ethernet SmartPro Switch

DGS-1510 Series

Table of Contents

1. Introduction

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DGS-1510 Series switch, which will be generally be referred to simply as the 'Switch' within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

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

- *DGS-1510 Series Gigabit Ethernet SmartPro Switch Hardware Installation Guide*
- *DGS-1510 Series Gigabit Ethernet SmartPro Switch CLI Reference Guide*

Conventions

Convention	Description
Boldface Font	This indicates a button, a toolbar icon, menu, or menu item. For example, Open the **File** menu and choose **Cancel**. Used for emphasis. This 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	This indicates a window name. Names of keys on the keyboard have initial capitals. For example, click Enter.
Menu Name > Menu Option	This indicates the menu structure. **Device > Port > Port Properties** means the **Port Properties** menu option under the **Port** menu option that is located under the **Device** menu.

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.

Web User Interface (Web UI)

The Switch can be managed through any of the RJ4/SFP/SFP+ ports on the front panel of the Switch by means of an HTTP/HTTPS connection using a Web browser like Microsoft® Internet Explorer, Mozilla Firefox, Safari, or Google Chrome.

Command Line Interface (CLI)

The Switch can be managed, Out-Of-Band (OOB), through the RJ45 Console port on the front panel of the Switch. Alternatively, the Switch can also be managed, in-band, through any of the RJ4/SFP/SFP+ ports on the front panel of the Switch by means of a Telnet connection. 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 SNMPv1, SNMPv2c, and SNMPv3. 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.

Connecting using the Web UI

Most software functions of the DGS-1510 Series switches can be managed, configured, and monitored through the Web UI. 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 UI

To access the Web UI, 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**.

Figure 2-1 IP address in Internet Explorer

NOTE: By default, one user account is already configured on the Switch. Both the username and password for this account is **admin**.

NOTE: After upgrading the firmware on the Switch and no user accounts were created, the default **admin** user account will automatically be created after rebooting the Switch with the new boot-up configuration file.

NOTE: After upgrading the firmware on the Switch and user accounts were created, the default **admin** user account will not be created automatically. Only after a factory reset was performed on the Switch will the default **admin** user account be created.

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

Figure 2-2 User Authentication Window

Enter the **User Name** and **Password** in the corresponding fields and click **Login**. This will open the Web UI. Management features available in the Web UI of the Switch are explained below.

Smart Wizard

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

Step 1 - Web Mode

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

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

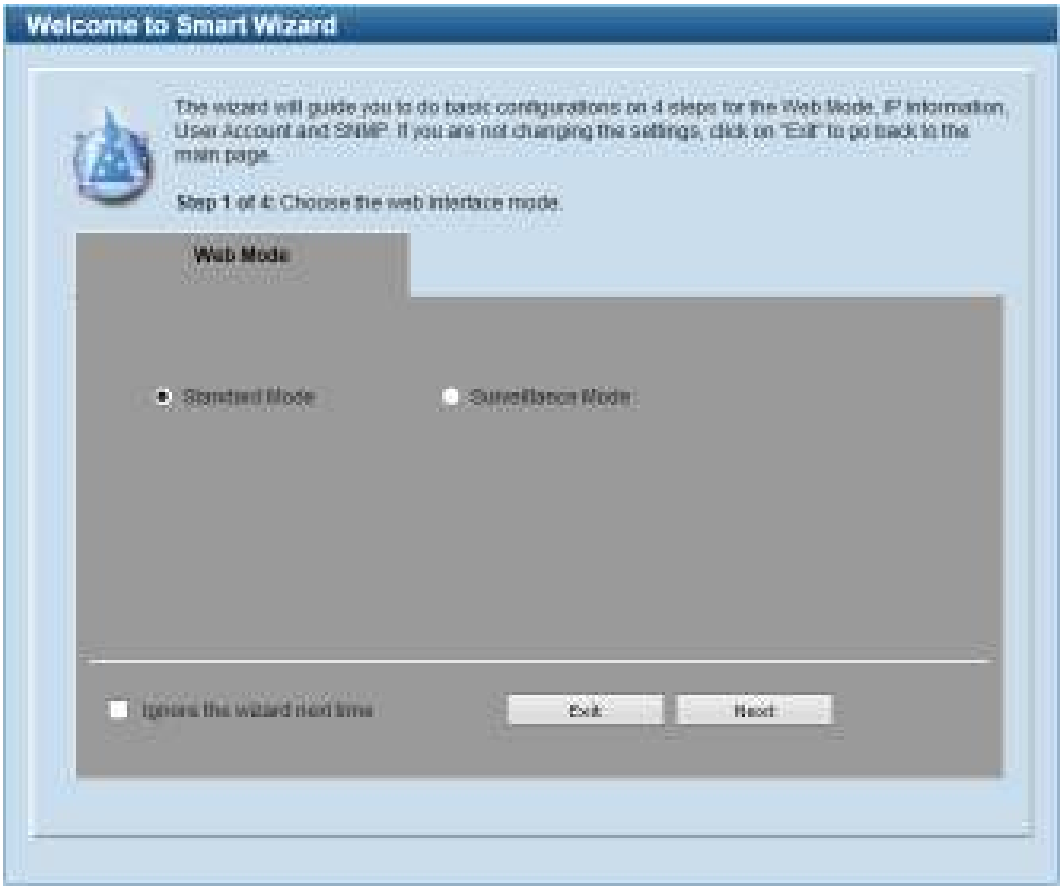


Figure 2-3 Web Mode

The fields that can be configured are described below:

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

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

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

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

Step 2 - System IP Information

In this step, we can configure System IP Information.

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

Figure 2-4 System IP Information

The fields that can be configured are described below:

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

Parameter	Description
Gateway	After selecting the **Static** option, manually enter the IP address of the default gateway here.

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

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

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

Step 3 - User Accounts Settings

In this step, we can configure the user account settings. This step can only be modified by a user account with the privilege level of 15.

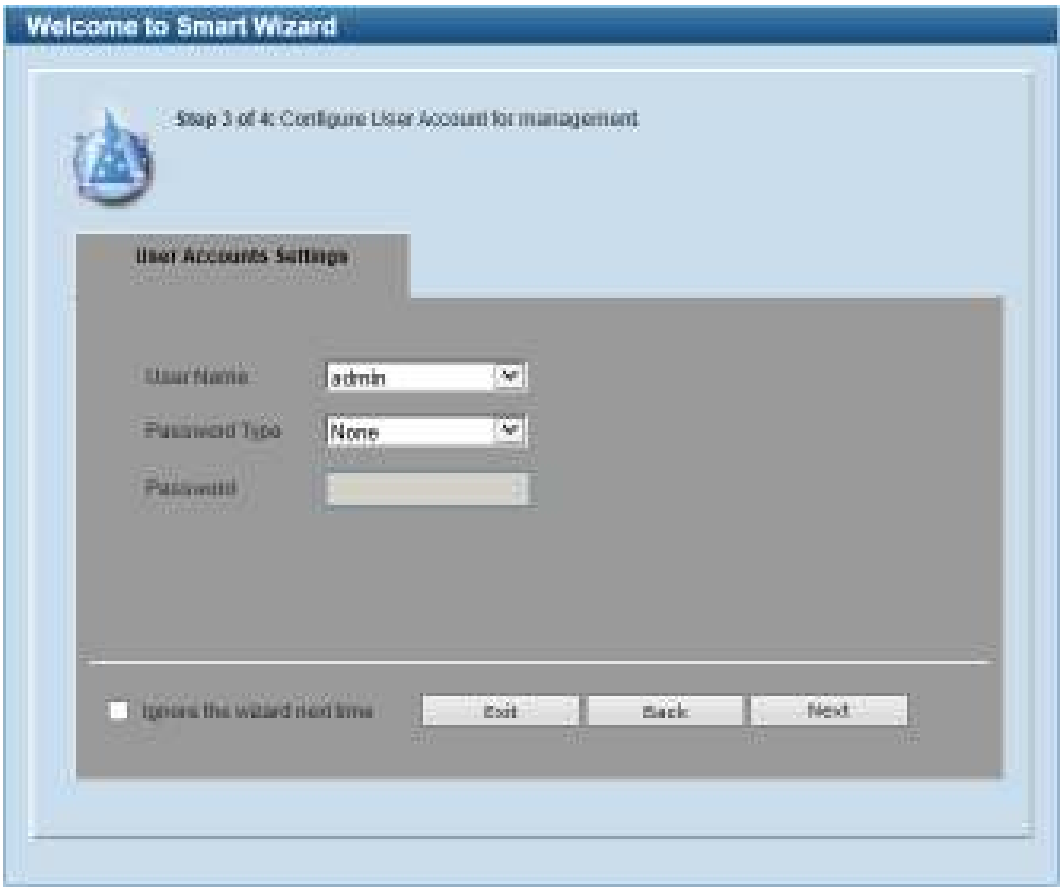


Figure 2-5 User Account Settings

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user name of the administrator level account with the privilege level of 15.
Password Type	Select the password type here. Options to choose from are: • **None** - Specifies that no password will be configured for this user account. • **Plain Text** - Specifies that the password for this user account will be in the plain text form. • **Encrypted-SHA1** - Specifies that the password for this user account will be in the encrypted form using the SHA1 encryption method.

Parameter	Description
	• **Encrypted-MD5** - Specifies that the password for this user account will be in the encrypted form using the MD5 encryption method.
Password	Enter the password for the user account either in the plain text format or the encrypted format here based on the previous selection made. In the encrypted format, the password will not be encrypted from plain text to the encrypted format. Instead, the encrypted password must be entered. To encrypt the password from plain text to the encrypted format, refer to the **Password Encryption** window.

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** button to accept the changes made and continue to the Web UI.

Step 4 - SNMP Settings

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

Figure 2-6 SNMP Window

The fields that can be configured are described below:

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

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

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

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

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

Web User Interface (Web UI)

Areas of the User Interface

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

Standard Mode

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

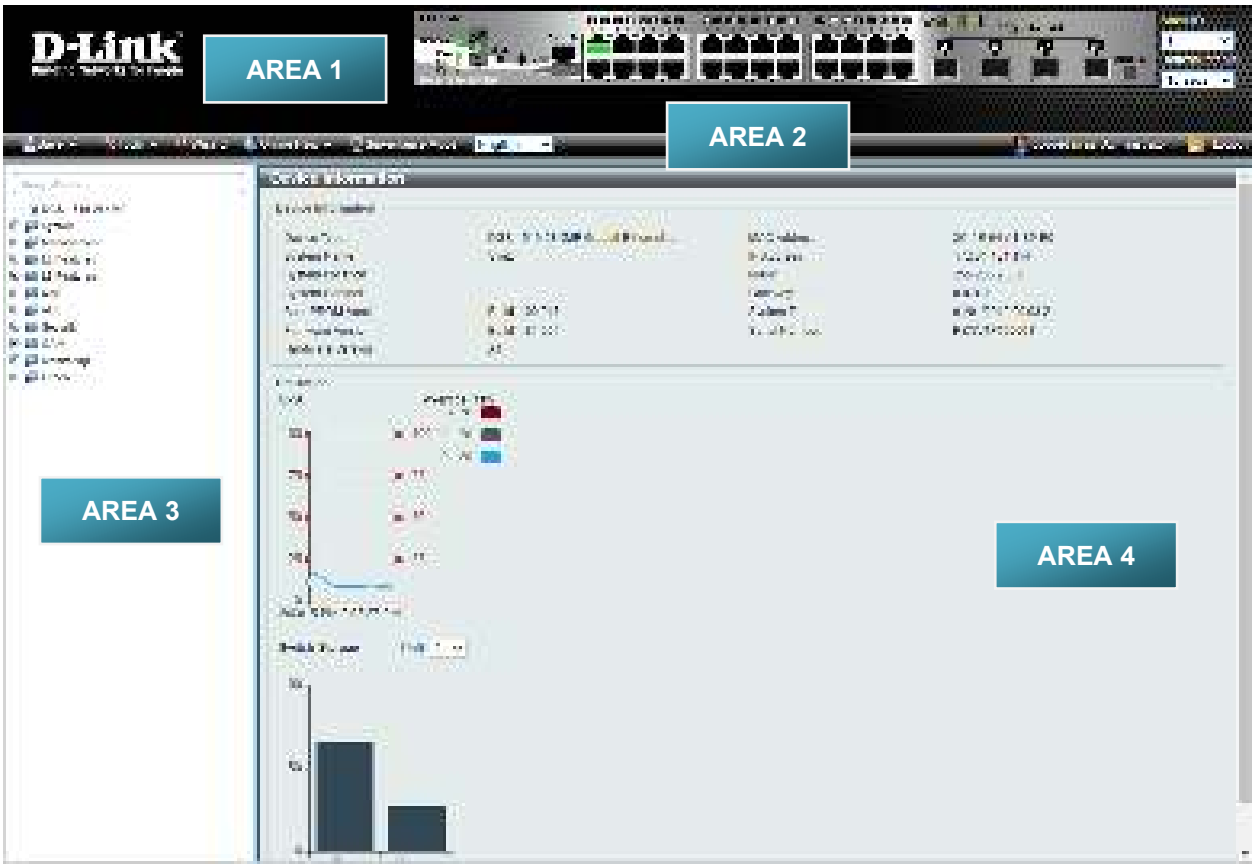


Figure 2-7 Web UI (Standard Mode)

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

Area Number	Description
AREA 1	In this area, a graphical near real-time image of the front panel of the Switch is displayed with ports and expansion modules. Port activity is displayed, depending on the specified mode. Some management functions like port monitoring are also accessible here. Click the D-Link logo to go to the D-Link website.
AREA 2	In this area is a toolbar used to access functions like **Save**, **Tools**, the **Wizard**, **Online Help**, accessing the Web UI in the **Surveillance Mode**, customized **Language** preference, and a **Logout** option. Click the **Surveillance Mode** option to change the switch mode from Standard Mode to Surveillance Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.

Area Number	Description
AREA 3	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in area 4. There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to easily find the link to the set of features.
AREA 4	In this area, configuration and monitoring window frames are available based on the selections made in area 3.

Surveillance Mode

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

Figure 2-8 Web UI (Surveillance Mode)

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

Area Number	Description
AREA 1	In this area is a toolbar used to access functions like the **Wizard**, **Tools**, **Save**, **Help**, **Online Help**, accessing the Web UI in the **Standard Mode**, customized **Language** preference, and a **Logout** option. Click the **Standard Mode** option to change the switch mode from Surveillance Mode to Standard Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.
AREA 2	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in area 3.

Area Number	Description
	There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to find the link to the set of features.
AREA 3	In this area, configuration and monitoring window frames are available based on the selections made in Area 2. The status of devices, IP cameras, and NVRs discovered on the switch will also be displayed in this area.

NOTE: For more information about the Surveillance Mode, refer to **Surveillance Mode** on page 391.

3. System

Device Information
System Information Settings
Peripheral Settings
Port Configuration
Interface Description
PoE
System Log
Time and SNTP
Time Range

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 **DGS-1510-28XMP** link.

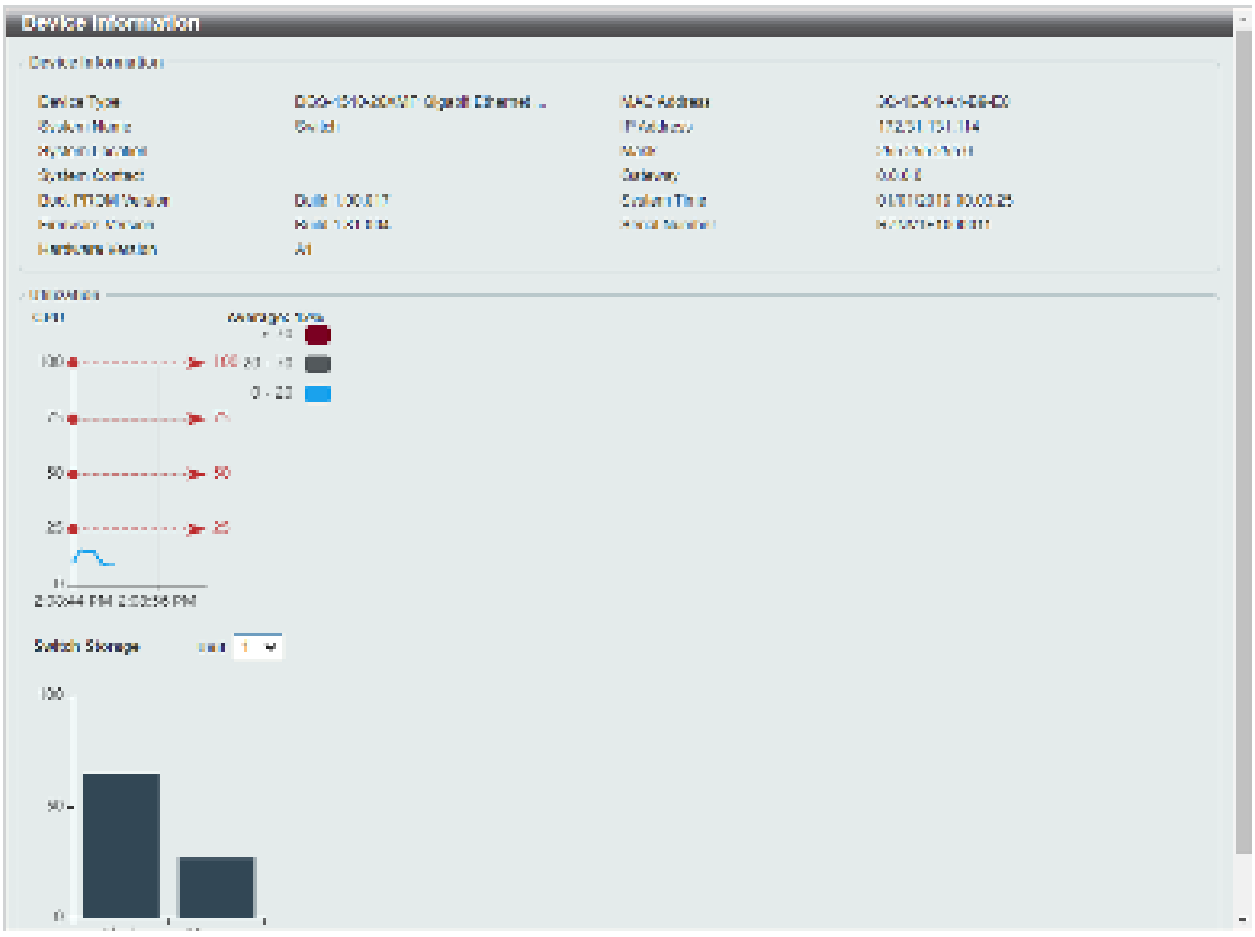


Figure 3-1 Device Information Window

System Information Settings

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:

Figure 3-2 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.

Peripheral Settings

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

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

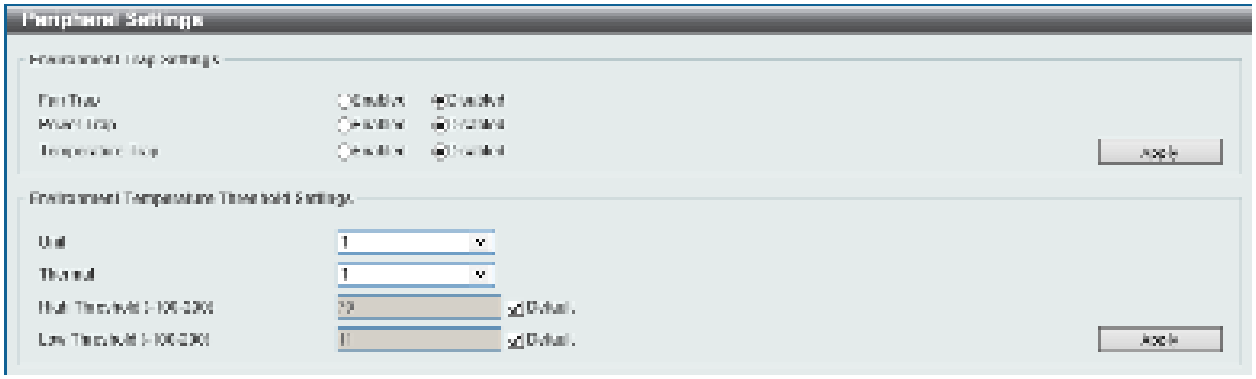


Figure 3-3 Peripheral Settings Window

The fields that can be configured are described below:

Parameter	Description
Fan Trap	Click to enable or disable the fan trap state for waning fan event (fan failed or fan recover).

Parameter	Description
Power Trap	Click to enable or disable the power trap state for waning power event (power failed or power recover).
Temperature Trap	Click to enable or disable the temperature trap state for waning temperature event (temperature exceeds the thresholds or temperature recover).
Unit	Select the switch unit that will be used for this configuration here.
Thermal	Select the thermal sensor ID.
High Threshold	Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 degree Celsius. Tick the **Default** check box to return to the default value.
Low Threshold	Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 degree Celsius. Tick the **Default** check box to return to the default value.

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

Port Configuration

Port Settings

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

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

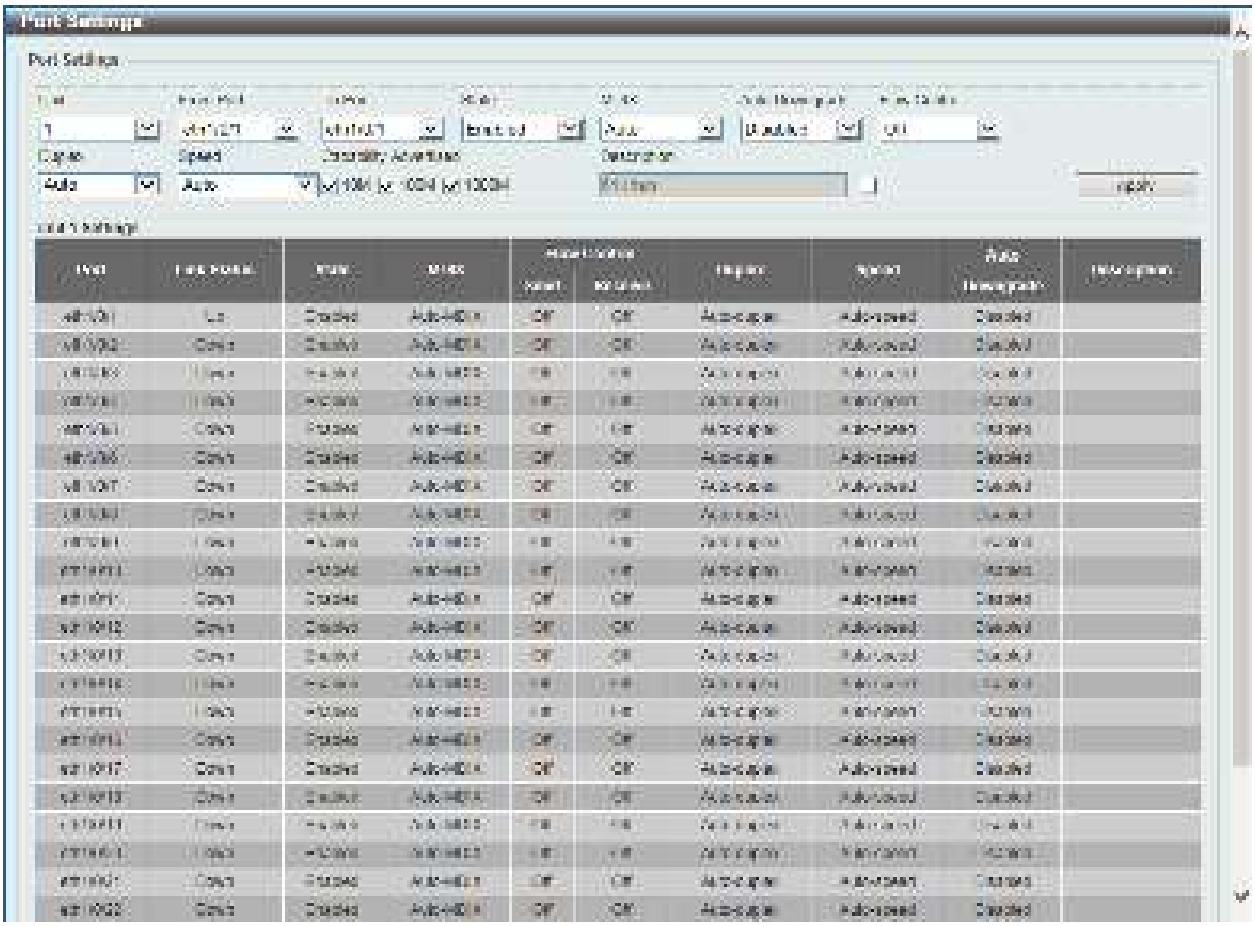


Figure 3-4 Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select 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** - 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 crossover 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.
Auto Downgrade	Select this option to enable or disable automatically downgrading advertised speed in case a link cannot be established at the available speed.
Flow Control	Select to turn flow control **On** or **Off** here. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure 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 connection on the selected port to connect at the speed specified here. Options to choose from are **Auto**, **10M**, **100M**, **1000M**, **1000M Master**, **1000M Slave**, and **10G**. The Switch allows users to configure two types of gigabit connections; **1000M Master** and **1000M Slave**, which refer to connections running a 1000BASE-T cable for connection between the Switch port and another device capable of a gigabit connection. The master setting (1000M Master) will allow the port to advertise capabilities related to duplex, speed, and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M Slave) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M Master, the other side of the connection must be set for 1000M Slave. Any other configuration will result in a link down status for both ports.
Capability Advertised	When the **Speed** is set to **Auto**, these capabilities are advertised during auto-negotiation.
Description	Tick the check box to enter a 64 characters description for the corresponding port here.

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

Port Status

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

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

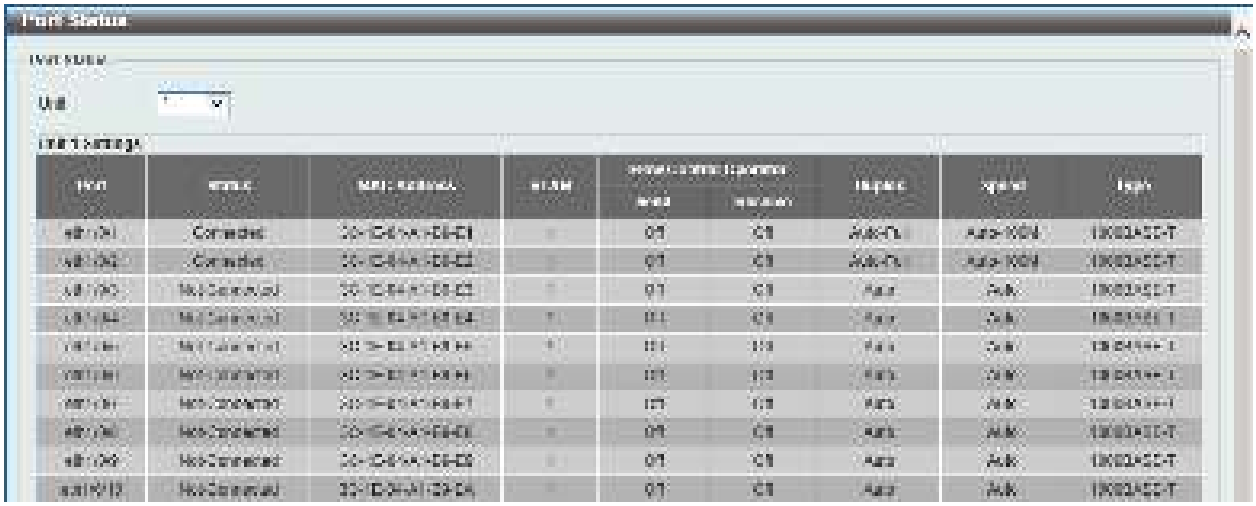


Figure 3-5 Port Status Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Port GBIC

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

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

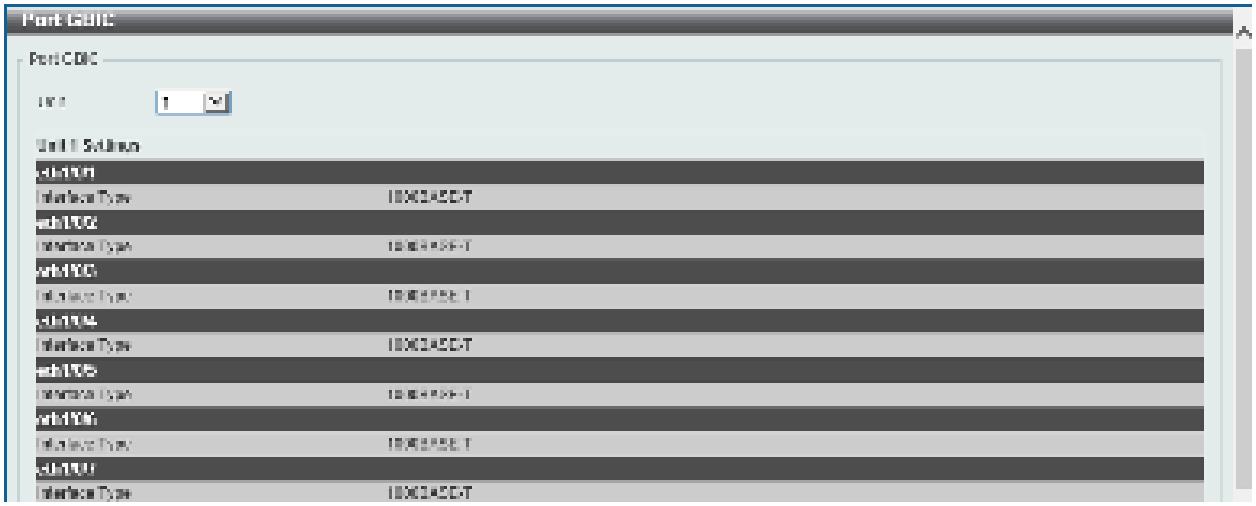


Figure 3-6 Port GBIC Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Port Auto Negotiation

This window is used to view detailed port auto-negotiation information.

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

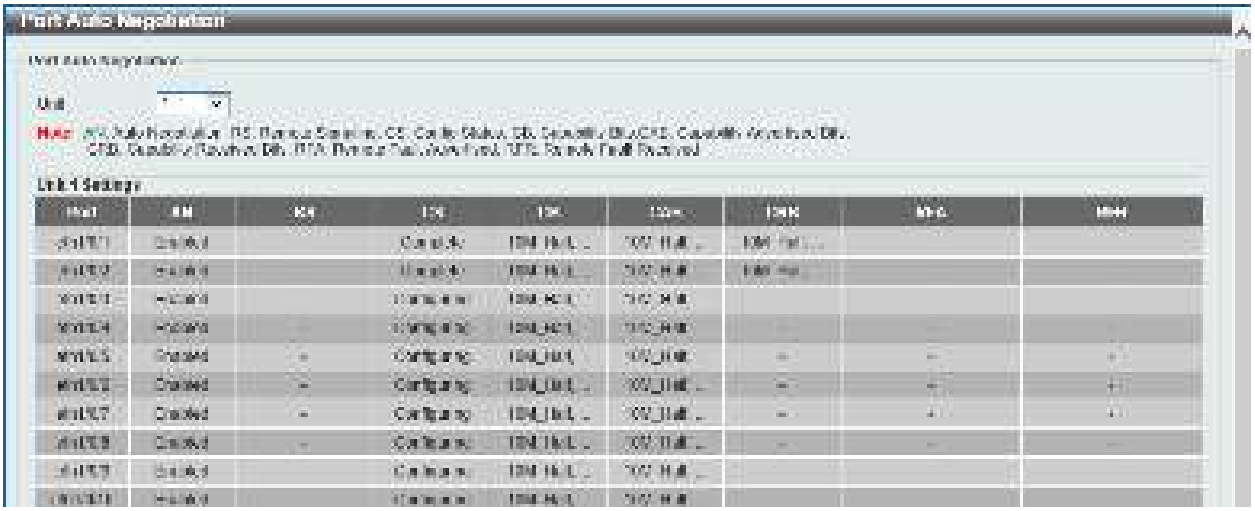


Figure 3-7 Port Auto Negotiation Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

Error Disable Settings

This window is used to configure the sending of SNMP notifications for error disable state.

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

Figure 3-8 Error Disable Settings Window

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

Parameter	Description
Asserted	Select this option to enable or disable the notifications when entering into the error disabled state.
Cleared	Select this option to enable or disable the notifications when exiting from the error disabled state.
Notification Rate	Enter the number of traps per minute. The packets that exceed the rate will be dropped. The value is between 0 and 1000.

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

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

Parameter	Description
ErrDisable Cause	Select the error disable causes here. Options to choose from are **All**, **Port Security**, **Storm Control**, **BPDU Attack Protection**, **Dynamic ARP Inspection**, **DHCP Snooping**, and **Loopback Detect**.
State	Select this option to enable or disable the auto-recovery for an error port caused by the specified cause.
Interval	Enter the time between 5 and 86400 seconds to recover the port.

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 1518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 9216 bytes.

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

Figure 3-9 Jumbo Frame Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 9216 bytes. By default, this value is 1536 bytes.

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

Interface Description

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

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

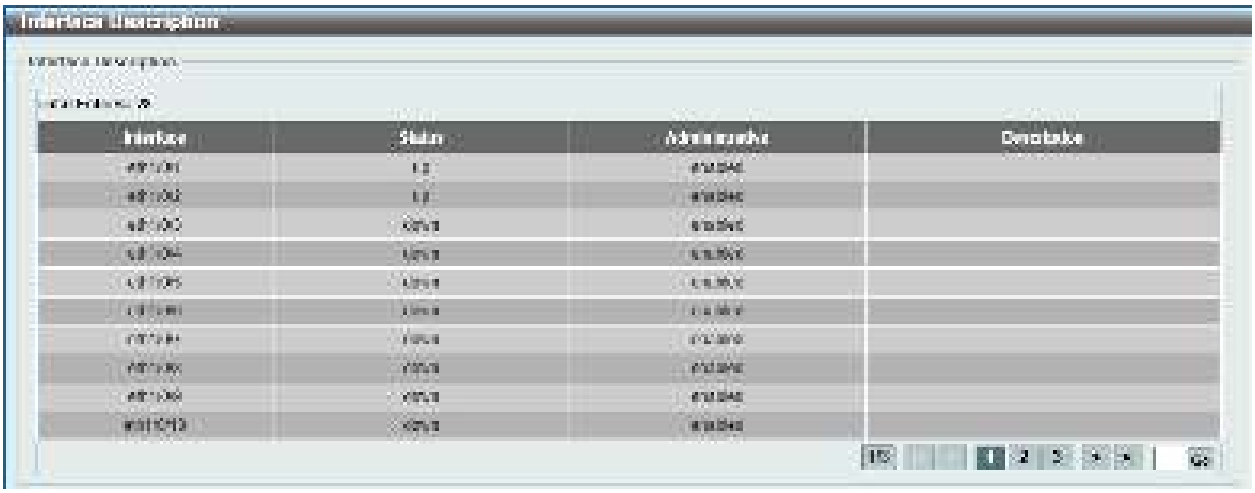


Figure 3-10 Interface Description Window

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

PoE (PoE Switches Only)

The **DGS-1510-28P**, **DGS-1510-28XMP**, and **DGS-1510-52XMP** switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at.

NOTE: The Power over Ethernet (PoE) settings are only available on the **DGS-1510-28P**, **DGS-1510-28XMP**, and **DGS-1510-52XMP**.

All ports can support PoE up to 30W. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. 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 and automatically sends power to it.
- The Auto-disable feature occur 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 IEEE 802.3af/at, power is received and supplied according to the following classifications:

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

PoE System

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

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

Figure 3-11 PoE System 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.
Usage Threshold	Enter the usage threshold to generate a log and send the corresponding standard notification. The range is from 1 to 99 percent.
Policy Preempt	Select to enable or disable the policy preempt function. When this function is **Enabled**, under the power shortage condition, power provisioned to PDs with lower priority will instead be provisioned to PDs with higher priority. When this function is **Disabled**, the power management mode will use the first in, first serviced method.
Trap State	Select this option to enable or disable the sending of PoE notifications.

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

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

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

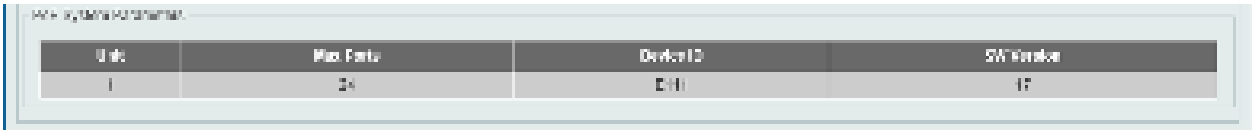


Figure 3-12 PoE System (Show Detail) Window

PoE Status

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

One of the following PoE port states will be displayed in the table:

- **Disabled**
- **Searching** (remote PD is not connected)
- **Requesting** (remote PD is inserted but no power is provided yet)
- **Delivering** (remote PD is inserted and power is provided)
- **Faulty** (maintain power signature absent, PD short, overloading, power denied, thermal shutdown, startup failure, or classification failure)

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

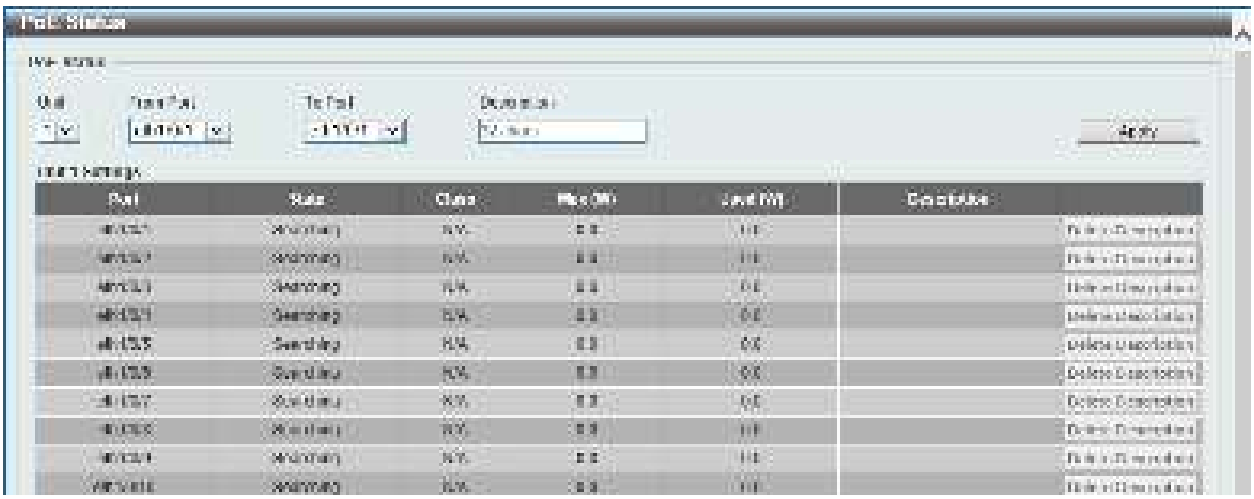


Figure 3-13 PoE Status Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Description	Enter the text that describes the PD connected to a PoE interface. The maximum length is 32 characters.

Click the **Delete Description** button to clear the setting in the corresponding Description field.

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

PoE Configuration

This window is used to configure the PoE port.

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

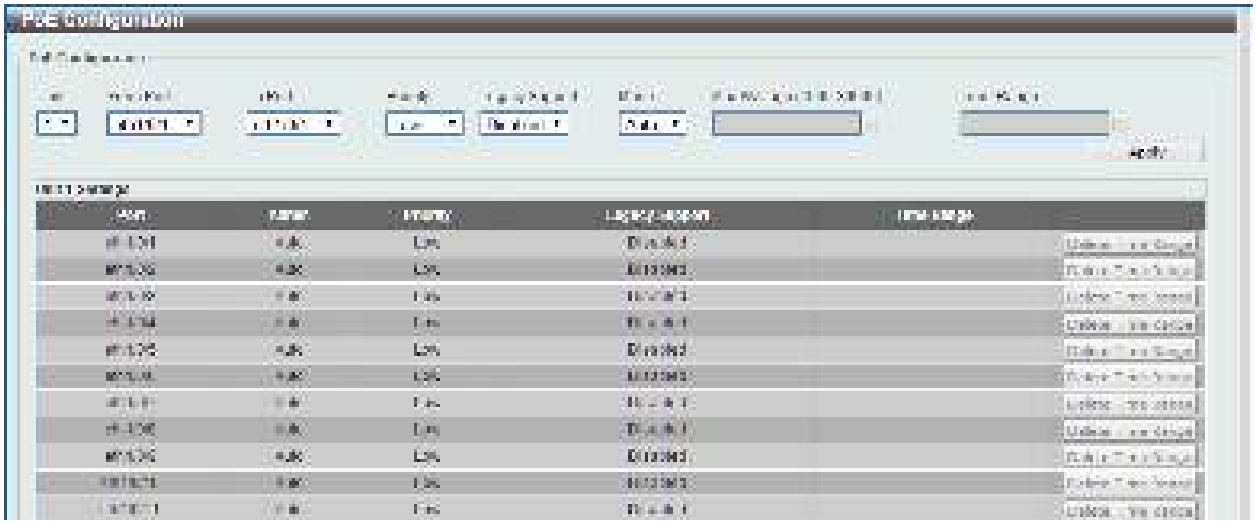


Figure 3-14 PoE Configuration Window

The fields that can be configured are described below:

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

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

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

PD Alive

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

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

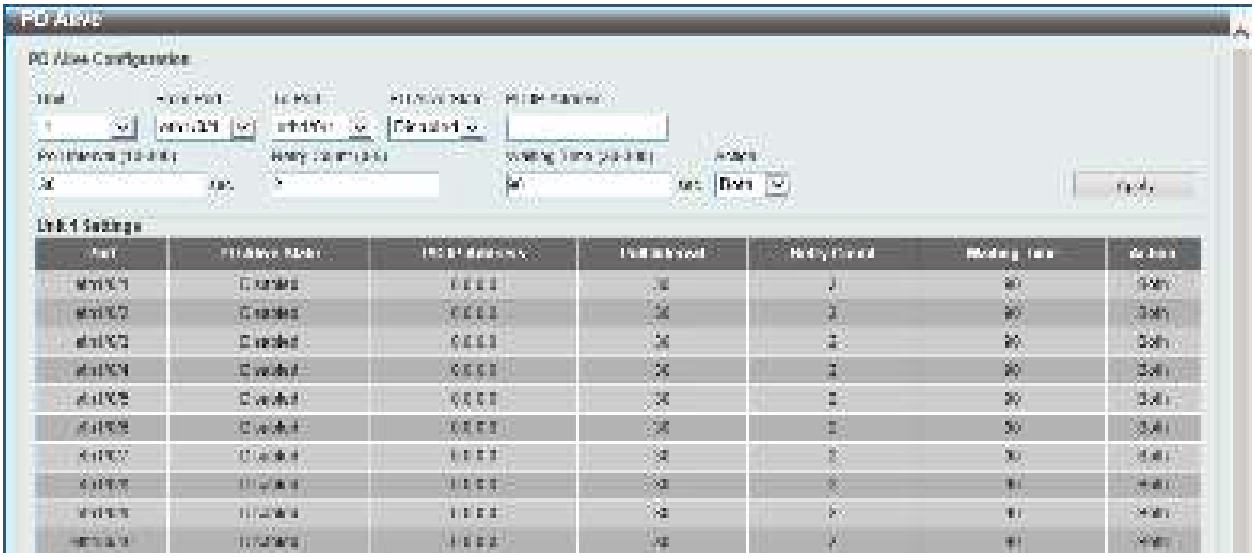


Figure 3-15 PD Alive Window

The fields that can be configured are described below:

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

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

PoE Statistics

This window is used to display the PoE statistics.

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

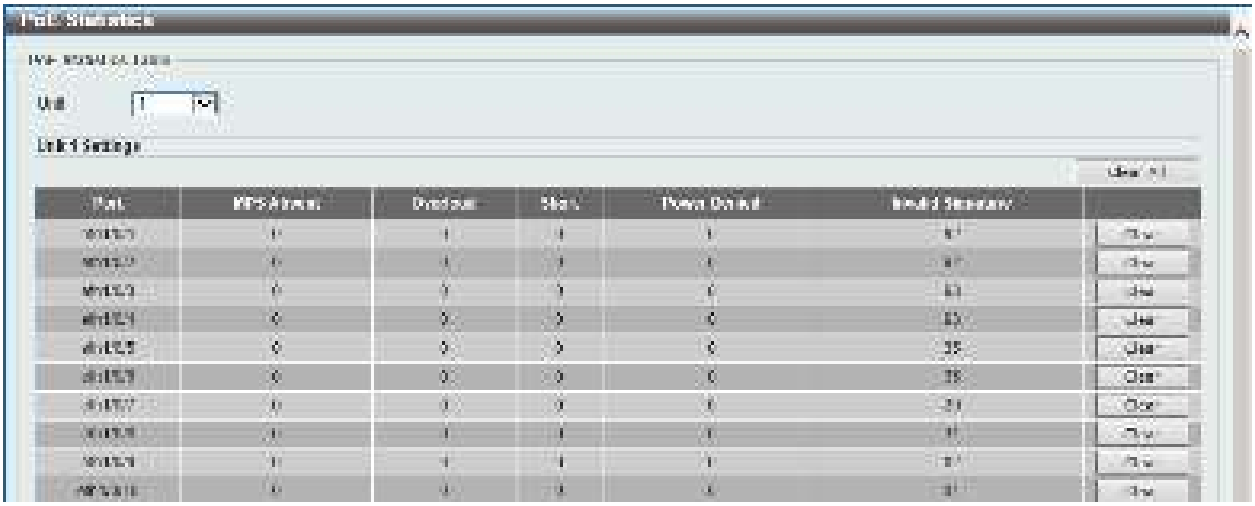


Figure 3-16 PoE Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

The fields that are displayed in the table are described below:

Parameter	Description
MPS Absent	This field is incremented when the PD's Maintain Power Signature (MPS) is absent.
Overload	This field is incremented when the power demand exceeds the maximum output power supplied.
Short	This field is incremented when the internal circuit of the PD shorted out.
Power Denied	This field is incremented when power was denied to the PD by the system.
Invalid Signature	This field is incremented when an invalid PD signature was detected by the system.

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

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

PoE Measurement

This window is used to display the PoE measurement.

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

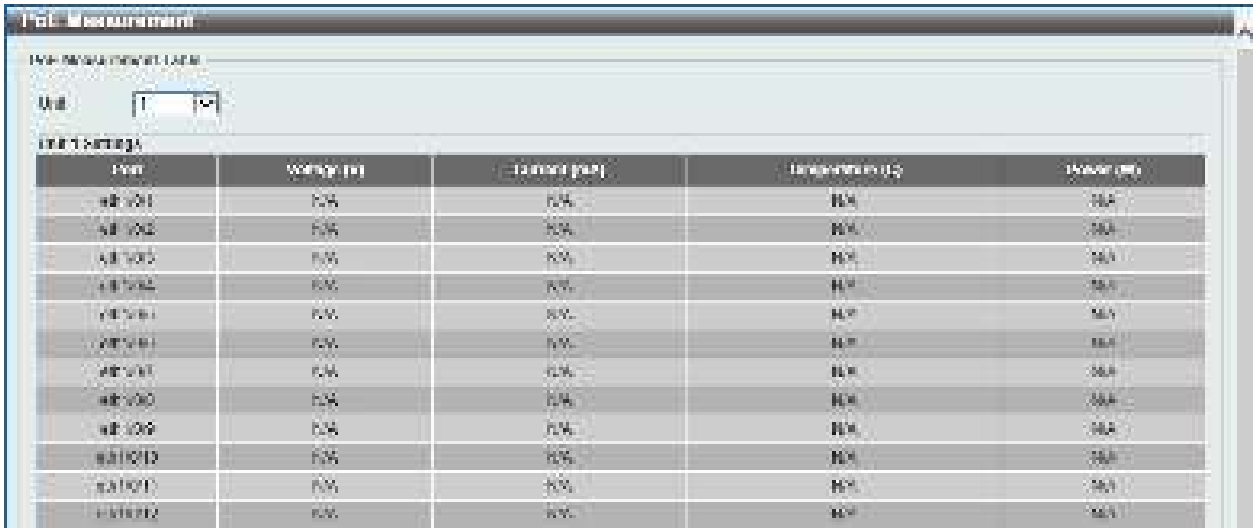


Figure 3-17 PoE Measurement Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

PoE LLDP Classification

This window is used to display the PoE LLDP Classification.

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

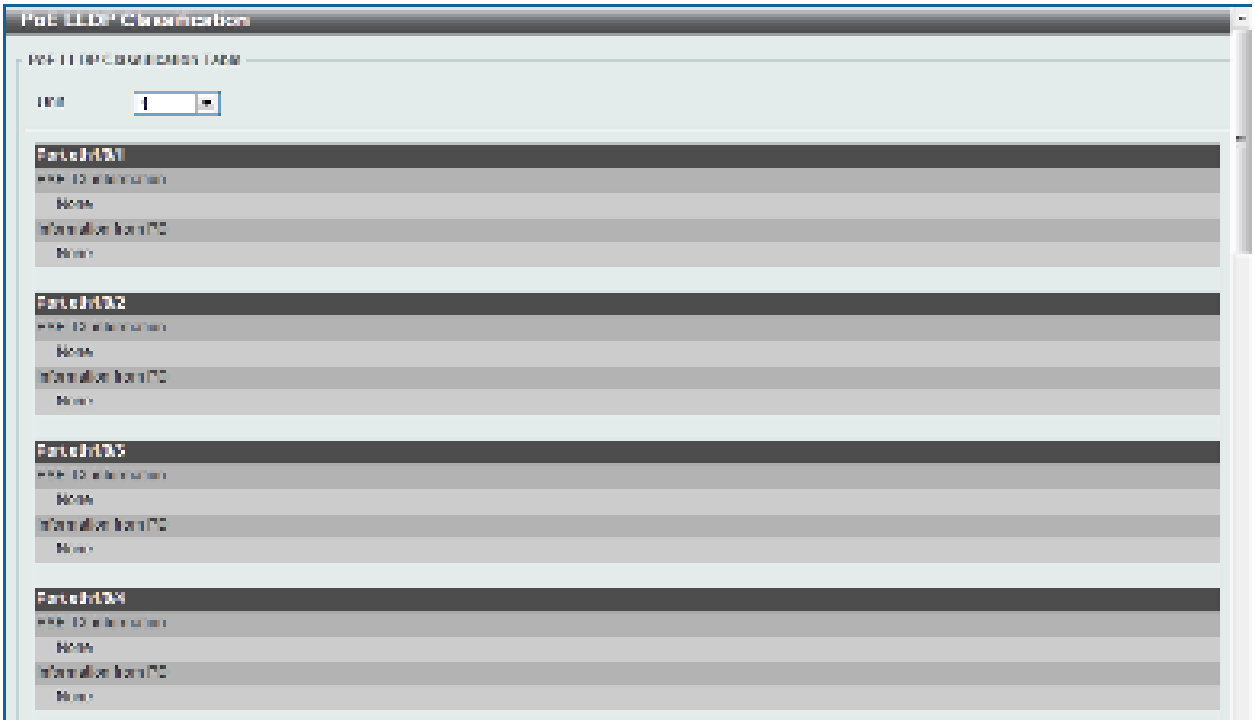


Figure 3-18 PoE LLDP Classification Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.

System Log

System Log Settings

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

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

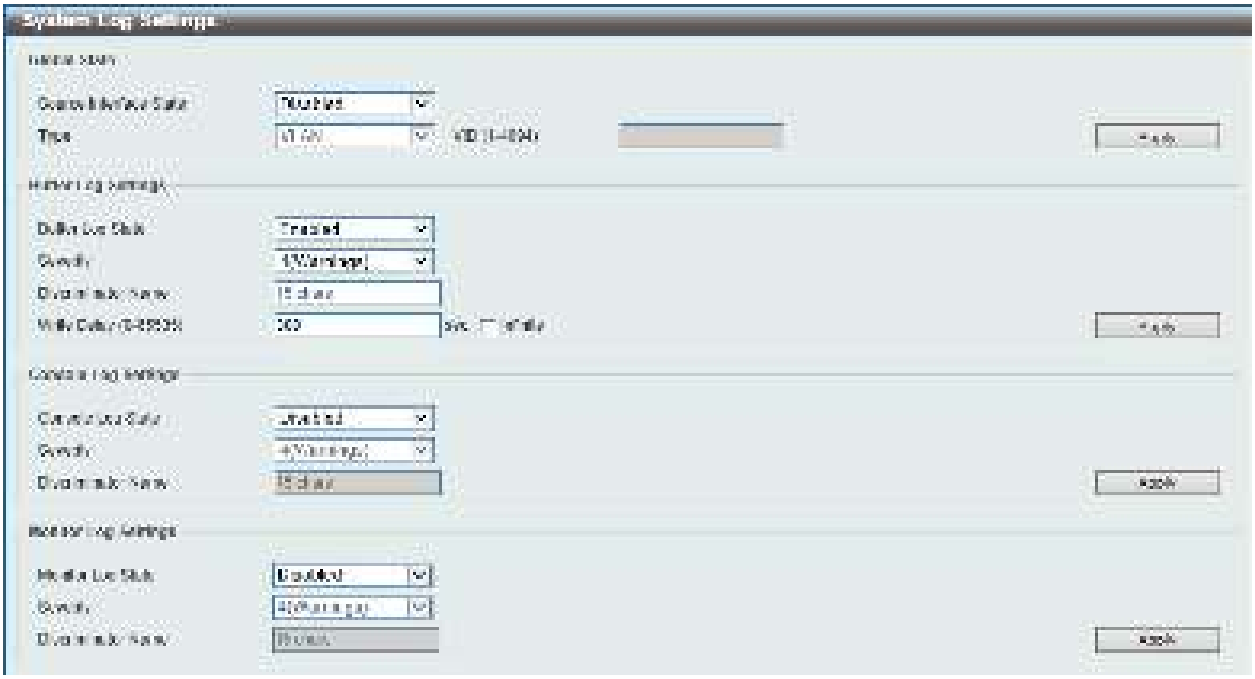


Figure 3-19 System Log Settings Window

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

Parameter	Description
Source Interface State	Select this option to enable or disable the source interface's global state.
Type	Select the type of interface that will be used. Option to choose from is **VLAN**.
VID	Enter the VLAN ID used here. The value is between 1 and 4094.

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 here. Options to choose from are **Enable**, **Disabled**, and **Default**. When selecting the **Default** option, the buffer log's global state will follow the default behavior.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long.

Parameter	Description
Write Delay	Enter the interval for periodic writing of the logging buffer to FLASH. This value must be between 0 and 65535 seconds. By default, this value is 300 seconds. Tick the **Infinite** option, to disable the write delay feature.

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

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

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

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

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

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

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

System Log Discriminator Settings

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

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

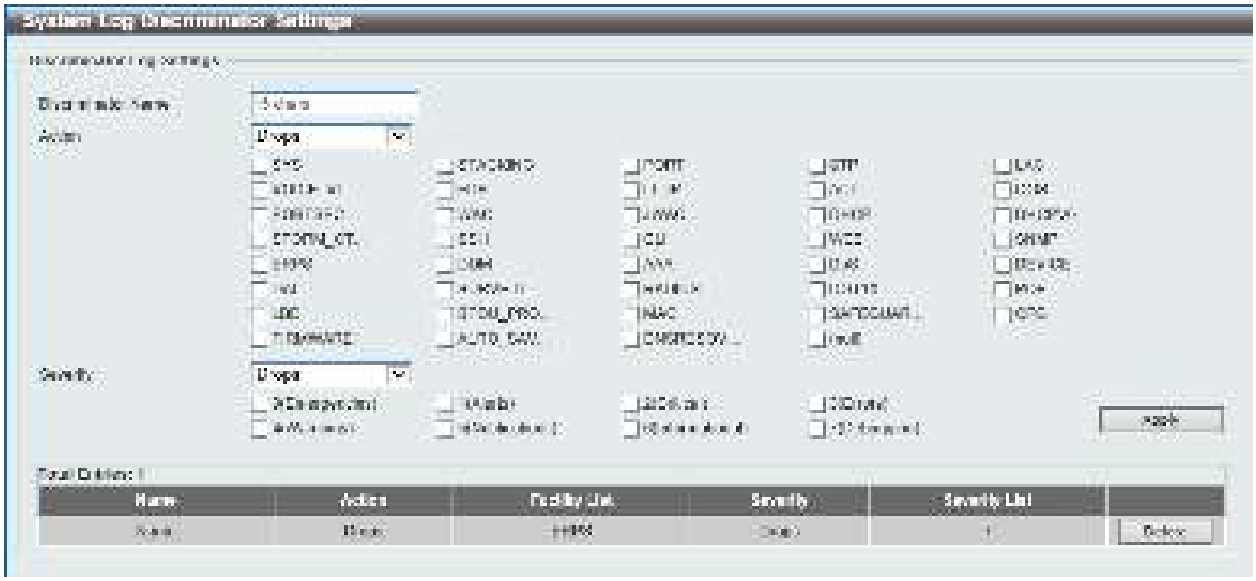


Figure 3-20 System Log Discriminator Settings Window

The fields that can be configured are described below:

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

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

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

System Log Server Settings

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

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

Figure 3-21 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.
Host IPv6 Address	Enter the system log server's IPv6 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 **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.
Facility	Select the facility value here. Options to choose from are 0 to 23.
Discriminator Name	Enter the discriminator name here. This name can be up to 15 characters long.

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

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

System Log

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

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

Figure 3-22 System Log Window

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

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

System Attack Log

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

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

Figure 3-23 System Attack Log 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.

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

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 and SNTP > Clock Settings**, as shown below:

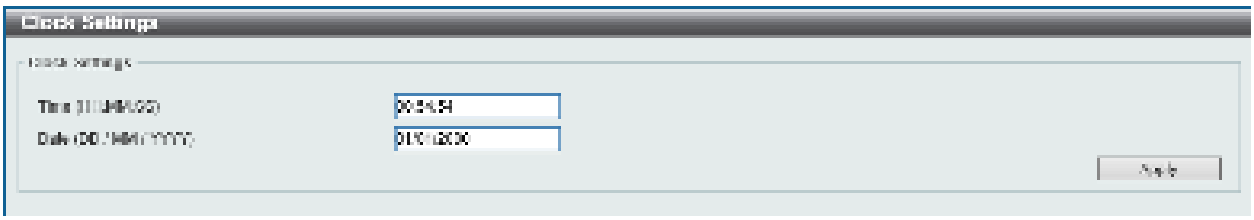


Figure 3-24 Clock Settings Window

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 and SNTP > Time Zone Settings**, as shown below:

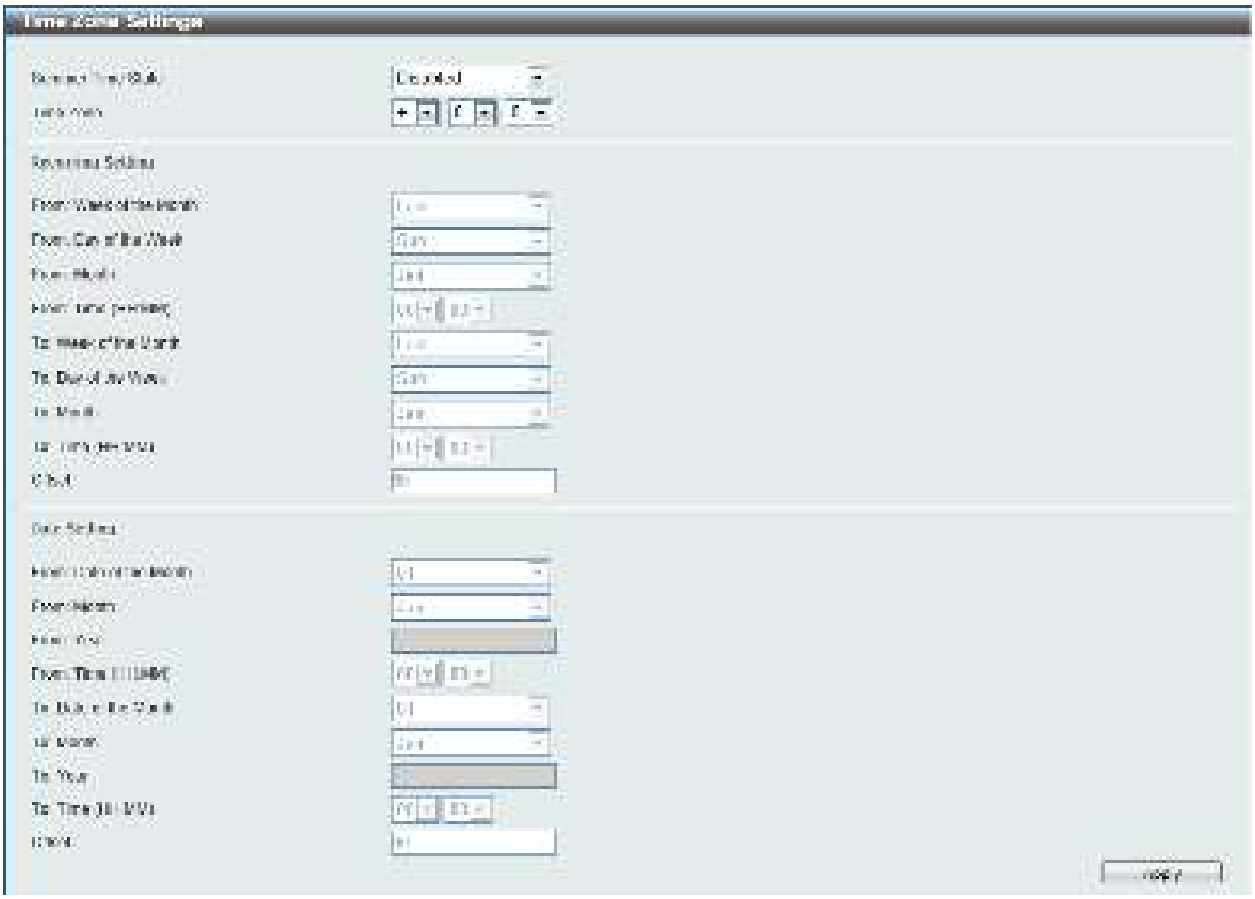


Figure 3-25 Time Zone Settings Window

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** - Select to disable the summer time setting. • **Recurring Setting** - Select to configure the summer time that should start and end on the specified weekday of the specified month. • **Date Setting** - Select to configure the summer time that should start and end on the specified date of the specified month.
Time Zone	Select to specify the offset of the local time zone from the 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.

Parameter	Description
From: Day of the Week	Select the day of the week that summer time will start.
From: Month	Select the month that summer time will start.
From: Time (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 and SNTP > SNTP Settings**, as shown below:

Figure 3-26 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.
IPv6 Address	Enter the IPv6 address of the SNTP server, which provides the clock synchronization.

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

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

Time Range

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

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

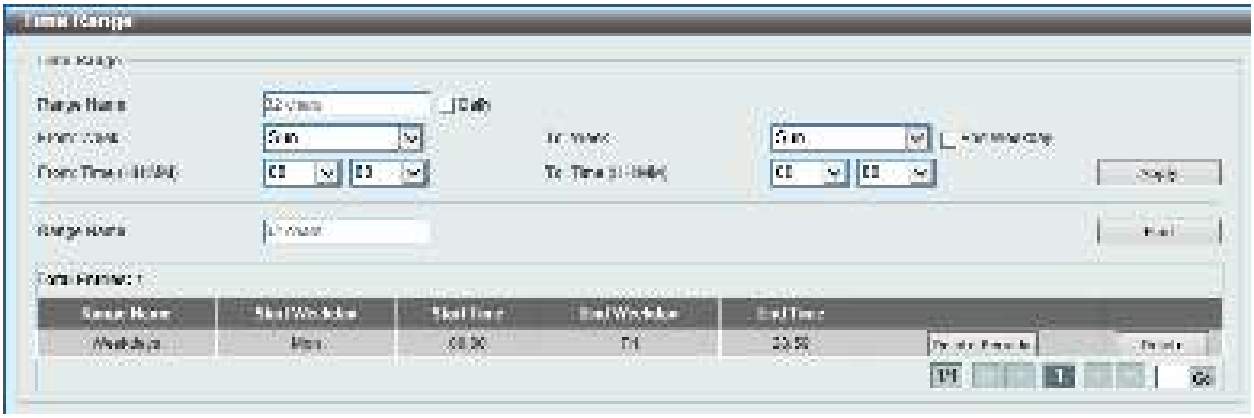


Figure 3-27 Time Range Window

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.

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

Click the **Delete Periodic** button to delete the periodic entry.

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

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

4. Management

User Account Settings
Password Encryption
Login Method
SNMP
RMON
Telnet/Web
Session Timeout
DHCP
DNS
NTP
IP Source Interface
File System
Physical Stacking
Virtual Stacking (SIM)
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.

There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**. A user account created with a higher privilege level will be given access to configure more features than a user account created with a lower privilege level.

The pre-defined privilege levels for user accounts are:

- **Basic User (Privilege Level 1)** - 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.
- **Operator (Privilege Level 12)** - This user account level is used to grant system configuration rights for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings.
- **Administrator (Privilege Level 15)** - 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:

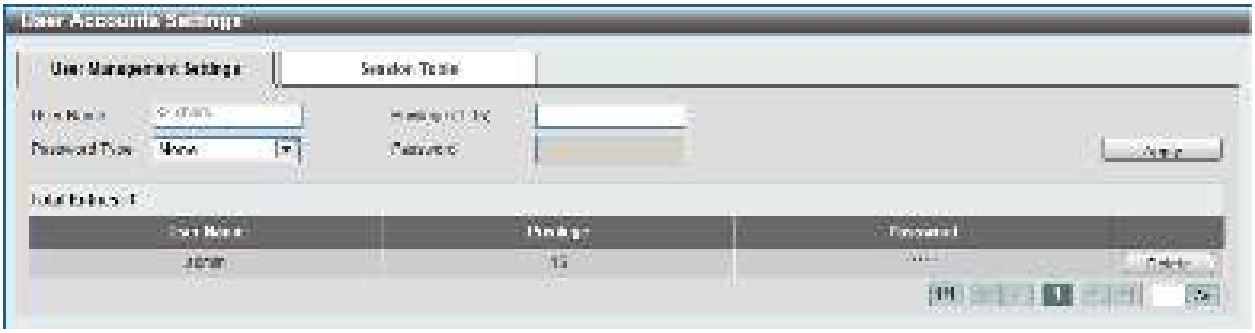


Figure 4-1 User Management Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.

Parameter	Description
Privilege	Enter the privilege level for this account here. This value must be between 1 and 15.
Password Type	Select the password type for this user account here. Options to choose from are **None**, **Plain Text**, **Encrypted-SHA1**, and **Encrypted-MD5**. When selecting **Encrypted-SHA1** or **Encrypted-MD5**, the password will not be encrypted from the plain-text format to the encrypted format. Instead, the encrypted password must be entered. To encrypt the password from the plain-text format to the encrypted format, refer to the **Password Encryption** window.
Password	After selecting **Plain Text**, **Encrypted-SHA1**, or **Encrypted-MD5** as the **Password Type**, enter the password for this user account here.

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

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

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

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

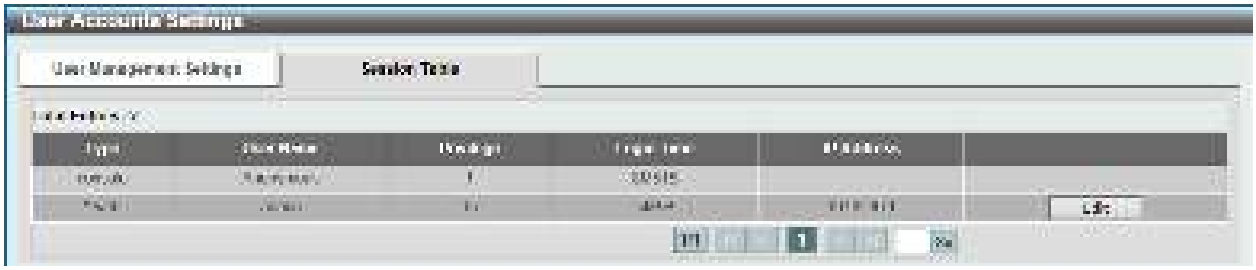


Figure 4-2 Session Table Window

A list of active user account session will be displayed.

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

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

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

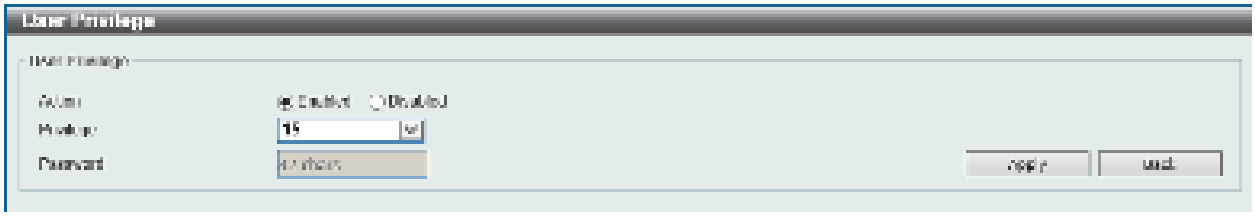


Figure 4-3 User Privilege Window

The fields that can be configured are described below:

Parameter	Description
Action	Select to enable or disable user level security.
Privilege	Select the privilege level here. The range is from 1 to 15.
Password	Enter the password here. This can be up to 32 characters long.

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

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

Password Encryption

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

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

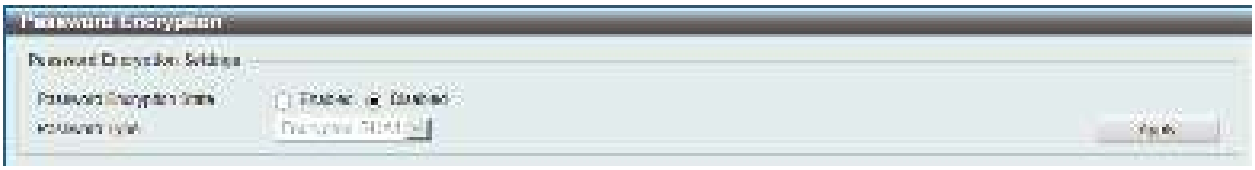


Figure 4-4 Password Encryption Window

The fields that can be configured are described below:

Parameter	Description
Password Encryption State	Select this option to enable or disable the encryption of the password before stored in the configuration file.
Password Type	After the **Password Encryption State** is **Enabled**, this filed will be available. Options to choose from are **Encrypted-SHA1** and **Encrypted-MD5**.

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

Login Method

This window is used to configure the login method for each management interface that this Switch supports.

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

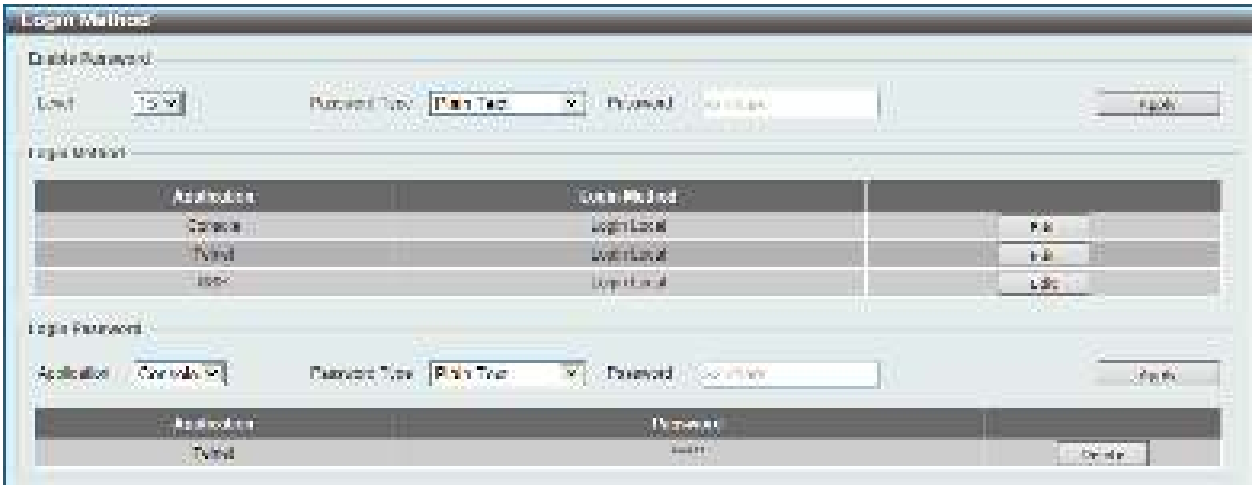


Figure 4-5 Login Method Window

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

Parameter	Description
Level	Select the password level here. This value must be between 1 and 15.
Password Type	Select the password type here. Options to choose from are **Plain Text**, **Encrypted-SHA1**, and **Encrypted-MD5**. When selecting **Encrypted-SHA1** or **Encrypted-MD5**, the password will not be encrypted from the plain-text format to the encrypted format. Instead, the encrypted password must be entered. To encrypt the password from the plain-text format to the encrypted format, refer to the **Password Encryption** window.
Password	After selecting **Plain Text**, **Encrypted-SHA1**, or **Encrypted-MD5** as the **Password Type**, enter the password for this user account here.

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

The **Login Method** section will only be available when Authentication, Authorization, and Accounting (AAA) feature is disabled. The fields that can be configured for **Login Method** settings are described below:

Parameter	Description
Login Method	After clicking the **Edit** button, this parameter can be configured. Select the login method for the specified application here. Options to choose from are **No Login**, **Login**, and **Login Local**. **No Login**, as the name implies, requires no login authentication to access the specified application. **Login** will require the user to enter a password when trying to access the application specified. **Login Local** requires the user to enter a username and a password to access the specified application.

Click the **Edit** button to modify the corresponding login method.

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

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

Parameter	Description
Application	Select the application that will be configured here. Options to choose from are **Console**, **Telnet** and **SSH**.
Password Type	Select the password encryption type that will be used here. Options to choose from are **Plain Text**, **Encrypted-SHA1**, and **Encrypted-MD5**.
Password	Enter the password for the selected application here. This password will be used when the **Login Method** for the specified application is set as **Login**.

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

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

SNMP

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

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

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

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

The default community strings for the Switch used for SNMPv1 and SNMPv2c management access are:

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

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

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

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

Traps

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

MIBs

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

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

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

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

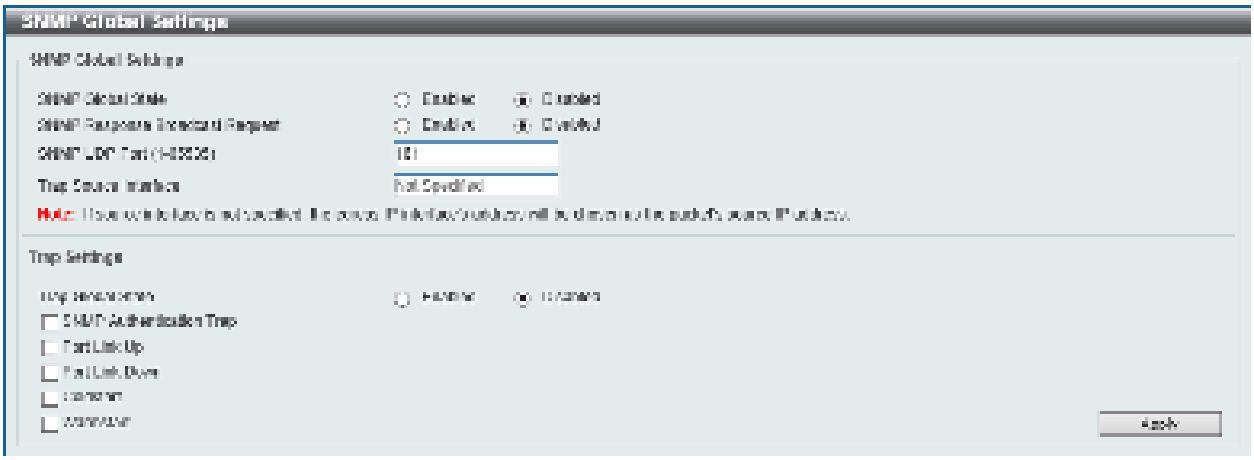


Figure 4-6 SNMP Global Settings Window

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.
SNMP Response Broadcast Request	Select this option to enable or disable the server to response to broadcast SNMP GetRequest packets.
SNMP UDP Port	Enter the SNMP UDP port number. The range is from 1 to 65535.
Trap Source Interface	Enter the interface whose IP address will be used as the source address for sending the SNMP trap packet.

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. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.

Parameter	Description
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 Linkchange Trap Settings

This window is used to configure the SNMP Linkchange trap settings.

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

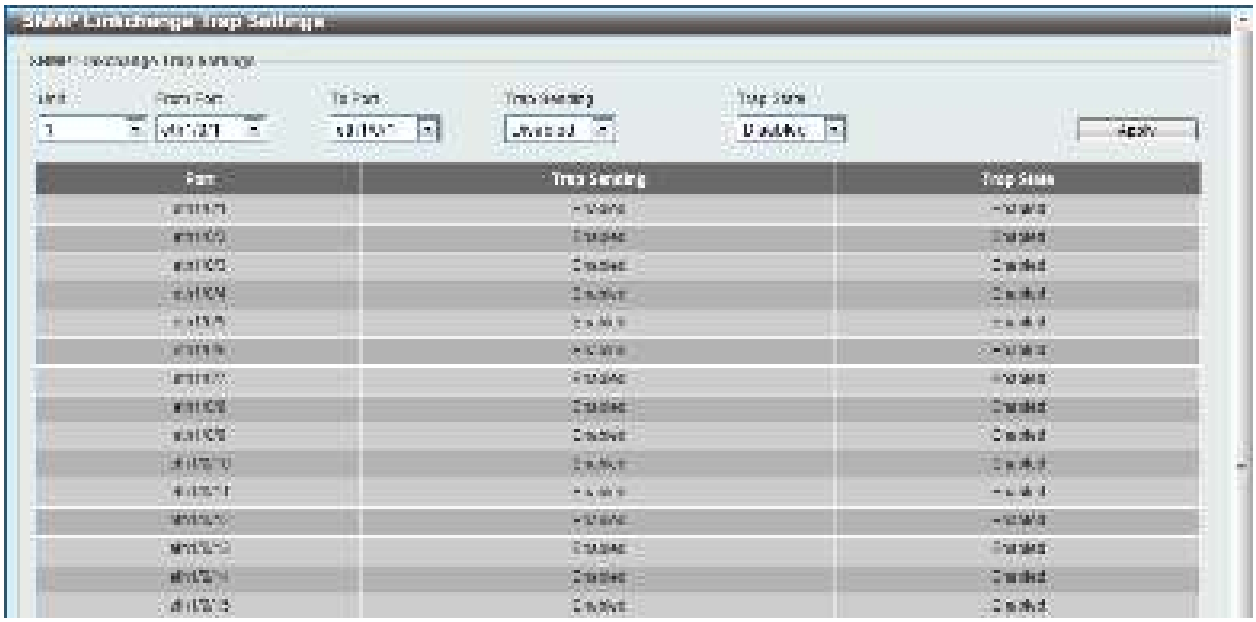


Figure 4-7 SNMP Linkchange Trap Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Trap Sending	Select this option to enable or disable the sending of the SNMP notification traps that is generated by the system.
Trap State	Select this option to enable or disable the SNMP link change trap.

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

SNMP View Table Settings

This window is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

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

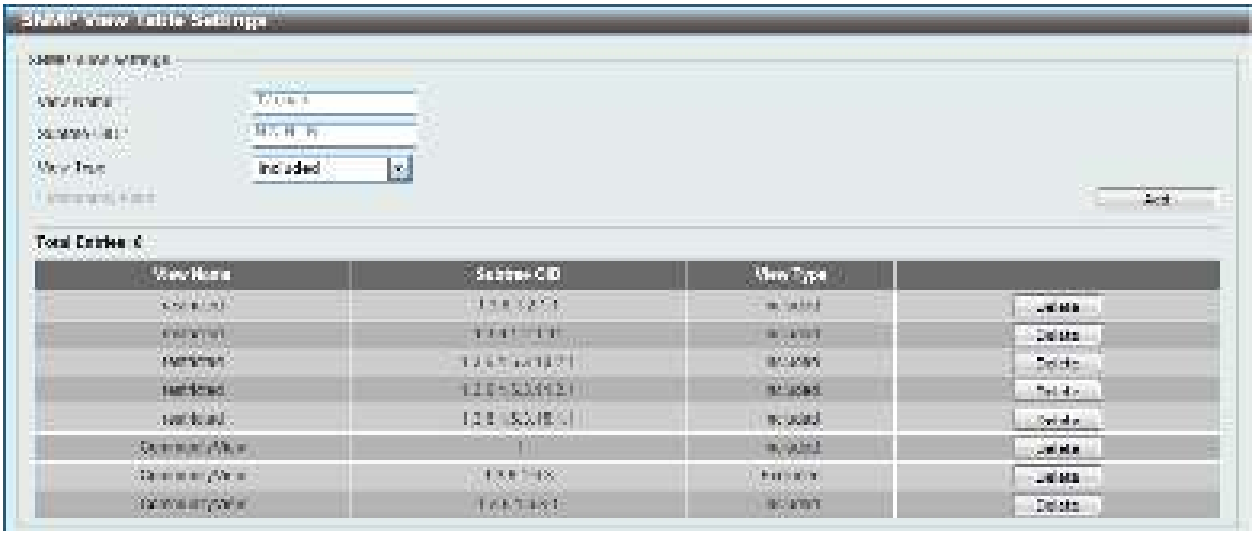


Figure 4-8 SNMP View Table Settings Window

The fields that can be configured are described below:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select the view type here. Options to choose from are: • **Included** - Select to include this object in the list of objects that an SNMP manager can access. • **Excluded** - Select to exclude this object from the list of objects that an SNMP manager can access.

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

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

SNMP Community Table Settings

This window is used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch.

One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.

- 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:

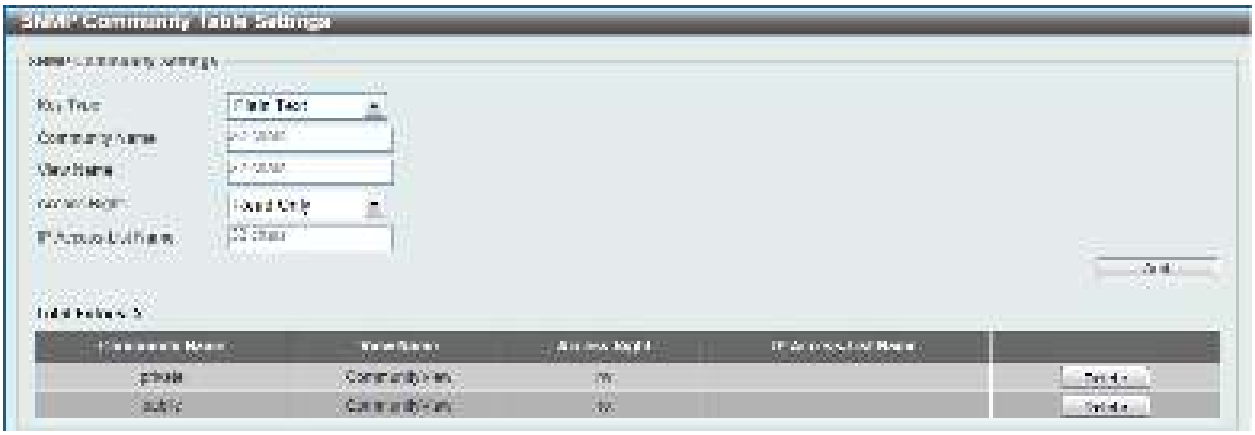


Figure 4-9 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Key Type	Select the key type for the SNMP community. Options to choose from are **Plain Text**, and **Encrypted**.
Community Name	Enter an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Enter an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	Select the access right here. Options to choose from are: • **Read Only** - SNMP community members using the community string created can only read the contents of the MIBs on the Switch. • **Read Write** - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.
IP Access-List Name	Enter the name of the standard access list to control the user to use this community string to access to the SNMP agent.

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

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

SNMP Group Table Settings

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

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

Figure 4-10 SNMP Group Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the group name of a maximum of 32 characters. The syntax is general string that does not allow space.
User-based Security Model	Select the security model here. Options to choose from are: • **SNMPv1** - Select to allow the group user to use the SNMPv1 security model. • **SNMPv2c** - Select to allow the group user to use the SNMPv2c security model. • **SNMPv3** - Select to allow the group user to use the SNMPv3 security model.
Security Level	When selecting **SNMPv3** in the **User-based Security Model** drop-down list, this option is available. • **NoAuthNoPriv** - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthNoPriv** - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthPriv** - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the group.
Read View Name	Enter the read view name that the group user can access.
Write View Name	Enter the write view name that the group user can access.
Notify View Name	Enter a write view name that the group user can access. The notify view describes the object that can be reported its status via trap packets to the group user.

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

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

SNMP Engine ID Local Settings

The Engine ID is a unique identifier used for SNMP V3 implementations on the Switch.

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

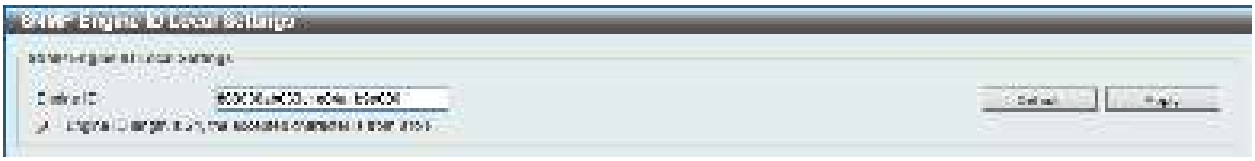


Figure 4-11 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

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

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

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

SNMP User Table Settings

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

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

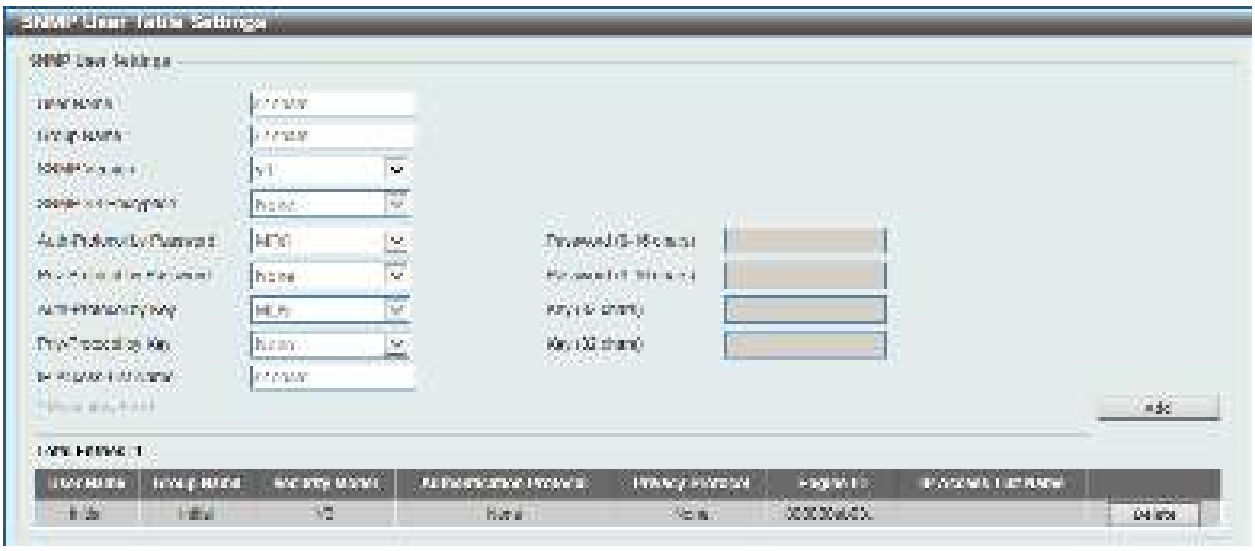


Figure 4-12 SNMP User Table Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP users.

Parameter	Description
Group Name	Enter the SNMP group name to which the user belongs. The syntax is general string that does not allow spaces.
SNMP Version	Select the SNMP version. Options to choose from are **v1**, **v2c**, and **v3**.
SNMP V3 Encryption	After selecting **v3** in the **SNMP Version** drop-down list, this option is available. Options to choose from are **None**, **Password**, and **Key**.
Auth-Protocol	After selecting **v3** in the **SNMP Version** drop-down list, and selecting either **Password** or **Key** in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are: • **MD5** - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. • **SHA** - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.
Priv-Protocol	After selecting **v3** in the **SNMP Version** drop-down list, and selecting either **Password** or **Key** in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are: • **None** - Specify that no authorization protocol is in use. • **DES56** - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the user.

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

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

SNMP Host Table Settings

This window is used to 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 4-13 SNMP Host Table Settings

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	Select the security model here. Options to choose from are: • **SNMPv1** - Select to allow the group user to use the SNMPv1 security model. • **SNMPv2c** - Select to allow the group user to use the SNMPv2c security model. • **SNMPv3** - Select to allow the group user to use the SNMPv3 security model.
Security Level	When selecting **SNMPv3** in the **User-based Security Model** drop-down list, this option is available. • **NoAuthNoPriv** - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthNoPriv** - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthPriv** - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
UDP Port	Enter the UDP port number. The default UDP port number of the trap is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string to be sent with the notification packet.

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

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

RMON

RMON Global Settings

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

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

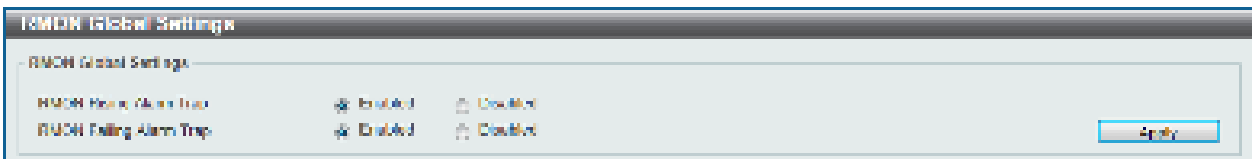


Figure 4-14 RMON Global Settings Window

The fields that can be configured are described below:

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

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

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

RMON Statistics Settings

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

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

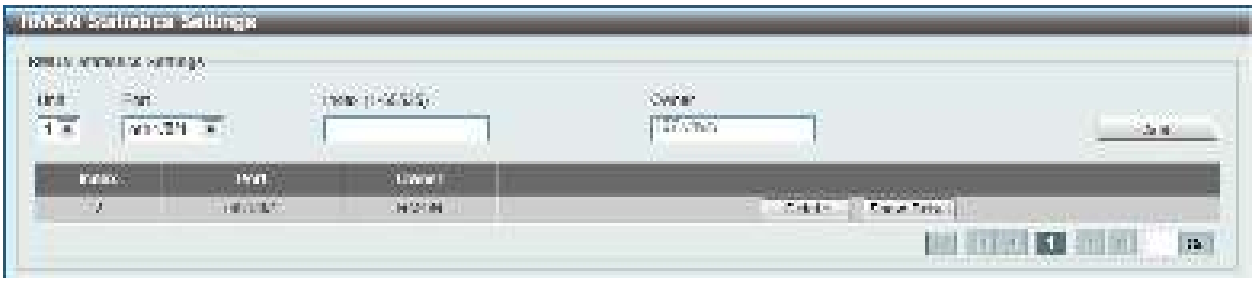


Figure 4-15 RMON Statistics Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select to choose the port.
Index	Enter the RMON table index. The value is from 1 to 65535
Owner	Enter the owner string. The string can be up to 127 characters.

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

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

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

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

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

Figure 4-16 RMON Statistics Table Window

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

RMON History Settings

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

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

Figure 4-17 RMON History Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

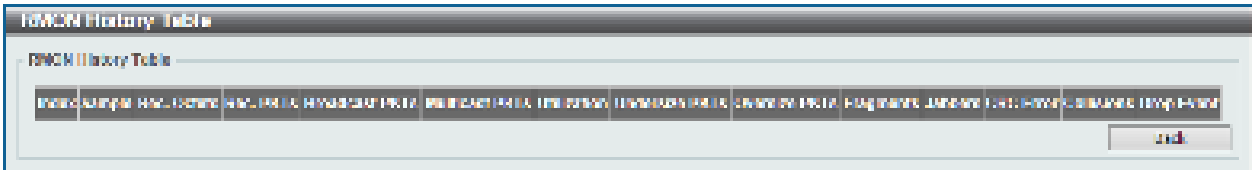


Figure 4-18 RMON History Table Window

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

RMON Alarm Settings

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

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

Figure 4-19 RMON Alarm Settings Window

The fields that can be configured are described below:

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

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

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

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

RMON Event Settings

This window is used to configure and display event entries.

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

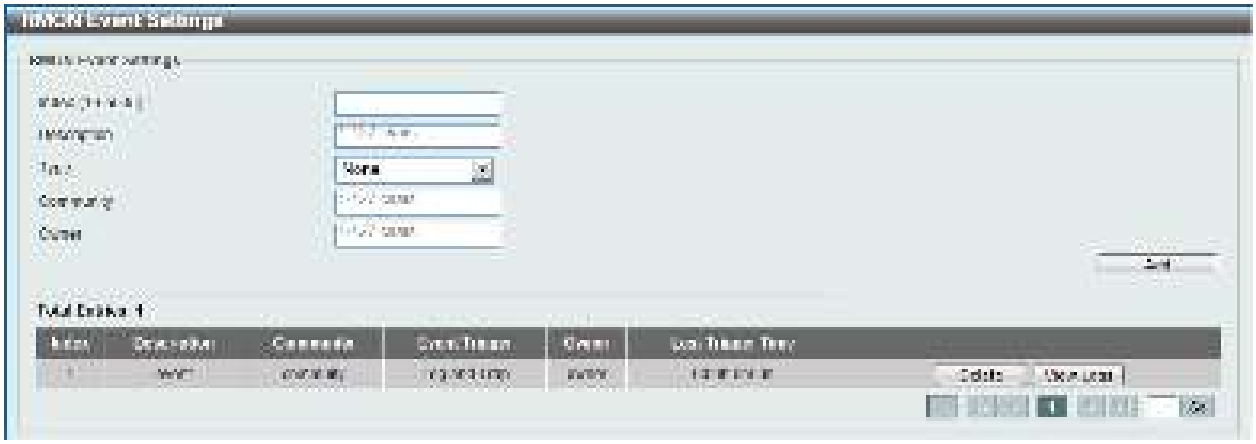


Figure 4-20 RMON Event Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

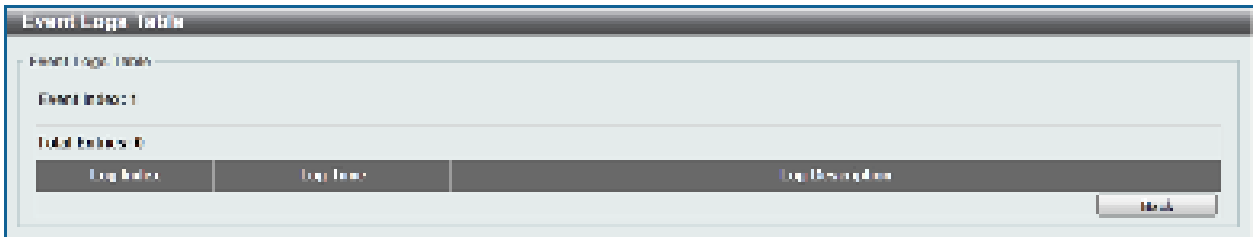


Figure 4-21 Event Logs Table Window

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

Telnet/Web

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

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

Figure 4-22 Telnet/Web Window

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

Parameter	Description
Telnet State	Select this option to enable or disable the configuration through Telnet.
Port	Enter the TCP port number used for Telnet management of the Switch. The default TCP port for the Telnet protocol is 23.

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

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

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

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

Session Timeout

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

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

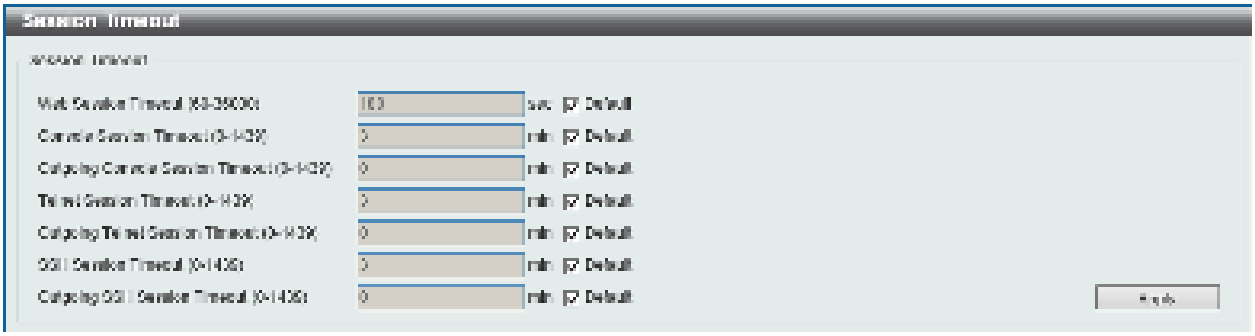


Figure 4-23 Session Timeout Window

The fields that can be configured are described below:

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

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

DHCP

Service DHCP

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

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

Figure 4-24 Service DHCP Window

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

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

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

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

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

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

DHCP Class Settings

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

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

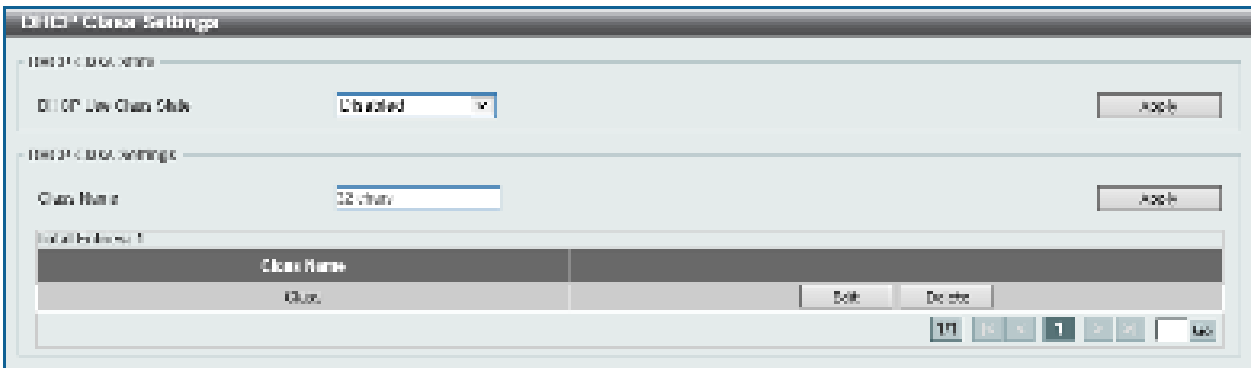


Figure 4-25 DHCP Class Settings Window

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

Parameter	Description
DHCP Use Class State	Select to enable or disable the DHCP class function here.

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

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

Parameter	Description
Class Name	Enter the DHCP class name with a maximum of 32 characters.

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

Click the **Edit** button to modify the DHCP option-matching pattern for the corresponding DCHP class.

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

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

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

Figure 4-26 DHCP Class Option Settings Window

The fields that can be configured are described below:

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

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

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

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

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) allows the Switch to designate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it will allocate an IP address to the client. The DHCP client may be then utilize the IP address allocated by the DHCP server as its local configuration.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allocated IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the range so as not to make identical entries

on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to assign the same IP addresses to important devices.

DHCP Server Global Settings

This window is used to display and configure the global DHCP server parameters.

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

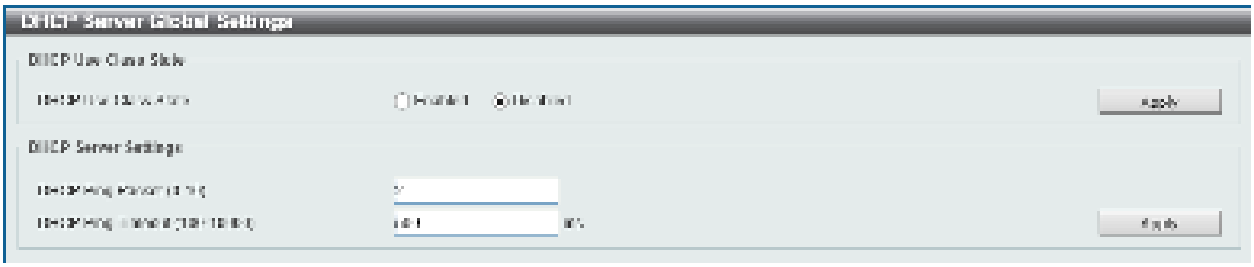


Figure 4-27 DHCP Server Global Settings Window

The fields that can be configured in **DHCP Use Class State** are described below:

Parameter	Description
DHCP Use Class State	Select to enable or disable the DHCP Use Class State here. When enabled, the DHCP server will use DHCP classes for address allocation.

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

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

Parameter	Description
DHCP Ping Packet	Enter the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. A value of 0 means there is no ping test. The range is from 0 to 10. The default value is 2.
DHCP Ping Timeout	Enter the amount of time the DHCP server must wait before timing out a ping packet. The range is from 100 to 10000 milliseconds. The default value is 500 milliseconds.

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

DHCP Server Pool Settings

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

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

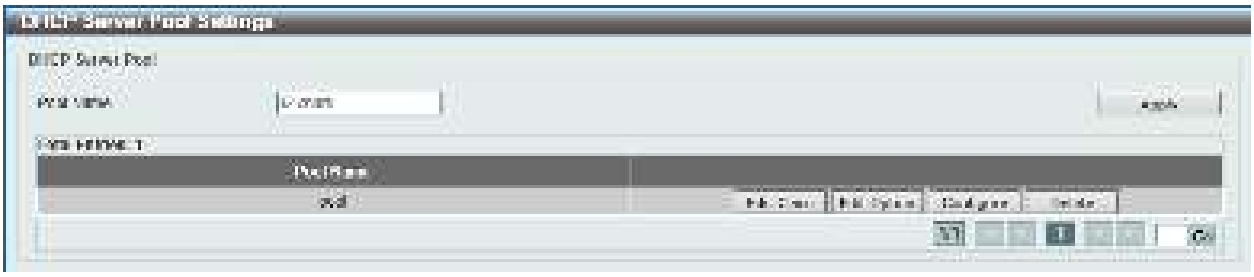


Figure 4-28 DHCP Server Pool Settings Window

The fields that can be configured are described below:

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

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

Click the **Edit Class** button to configure the DHCP class.

Click the **Edit Option** button to configure the DHCP server pool option settings.

Click the **Configure** button to configure the DHCP server pool settings.

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

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

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

Figure 4-29 DHCP Server Pool Class Settings Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select an existing DHCP class name here that will be associated with this DHCP pool.
Start Address	Enter the starting IPv4 address that will be associated with the DHCP class in the DHCP pool here.
End Address	Enter the ending IPv4 address that will be associated with the DHCP class in the DHCP pool here.

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

Click the **Delete by Name** button to remove the DHCP class association by name.

Click the **Delete by Address** button to remove the DHCP class association by address.

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

After clicking the **Edit Option** button, the following page will appear.

Figure 4-30 DHCP Server Pool Option Settings Window

The fields that can be configured are described below:

Parameter	Description
Option	Enter the DHCP option number here. The range is from 1 to 254.
Type	Select the DHCP option type here. Options to choose from are: • **ASCII** - Enter the ASCII string in the space provided. This string can be up to 255 characters long. • **Hex** - Enter the hexadecimal string in the space provided. This string can be up to 254 characters long. Select the **None** option to specify a zero-length hexadecimal string. • **IP** - Enter the IPv4 address(es) in the space(s) provided. Up to 8 IPv4 addresses can be entered.

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

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

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

After clicking the **Configure** button, the following page will appear.

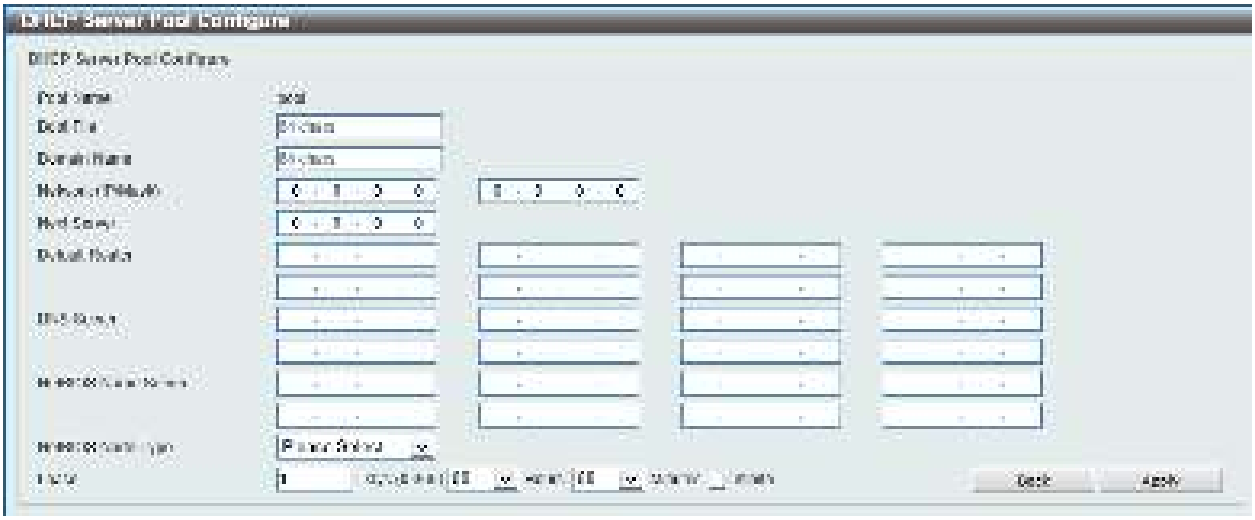


Figure 4-31 DHCP Server Pool Configure Window

The fields that can be configured are described below:

Parameter	Description
Boot File	Enter the boot file name here. This can be up to 64 characters long.
Domain Name	Enter the domain name for the DHCP client here. This can be up to 64 characters long.
Network (IP/Mask)	Enter the network IPv4 address and subnet mask for the DHCP client here.
Next Server	Enter the next server IPv4 address here. The boot image file is stored on this server and can be retrieved by DHCP clients using this IP address. The server is typically a TFTP server. Only one next server IP address can be specified.
Default Router	Enter the IPv4 address of the default router for the DHCP client here. Up to 8 IPv4 addresses can be entered here. The IP address of the router should be on the same subnet as the client's subnet. Routers are listed in the order of preference. If default routers are already configured, the default routers configured later will be added to the default interface list.
DNS Server	Enter the IPv4 address to be used by the DHCP client as the DNS server here. Up to 8 IPv4 addresses can be entered here. Servers are listed in the order of preference. If DNS servers are already configured, the DNS servers configured later will be added to the DNS server list.
NetBIOS Name Server	Enter the WINS name server IPv4 address for the DHCP client here. Up to 8 IPv4 addresses can be entered here. Servers are listed in the order of preference. If name servers are already configured, the name server configured later will be added to the default interface list.
NetBIOS Node Type	Select the NetBIOS node type for Microsoft DHCP clients here. The node type determines the method that NetBIOS uses to register and resolve names. Options to choose from are: • **Broadcast** - This system uses broadcasts. • **Peer To Peer** - This system (p-node) uses only point-to-point name queries to a name server (WINS). • **Mixed** - This system (m-node) broadcasts first, and then queries the name server. • **Hybrid** - This system (h-node) queries the name server first, and then broadcasts. This is the recommended type.
Lease	Enter and select the lease time for an IPv4 address that is assigned from the address pool here. Enter the **Days** in the range from 0 to 365. Select the **Hours** and **Minutes** from the drop-down menus. Alternatively, the **Infinite** option can be selected to specify that the lease time is unlimited.

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

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

DHCP Server Exclude Address

This window is used to view and exclude a range of IPv4 addresses from being allocated to the DHCP client. The DHCP server automatically allocates addresses in DHCP address pools to DHCP clients. All the addresses except the interface's IP address on the router and the excluded address(es) specified here are available for allocation. Multiple ranges of addresses can be excluded. To remove

a range of excluded addresses, administrators must specify the exact range of addresses previously configured.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Exclude Address**, as shown below:

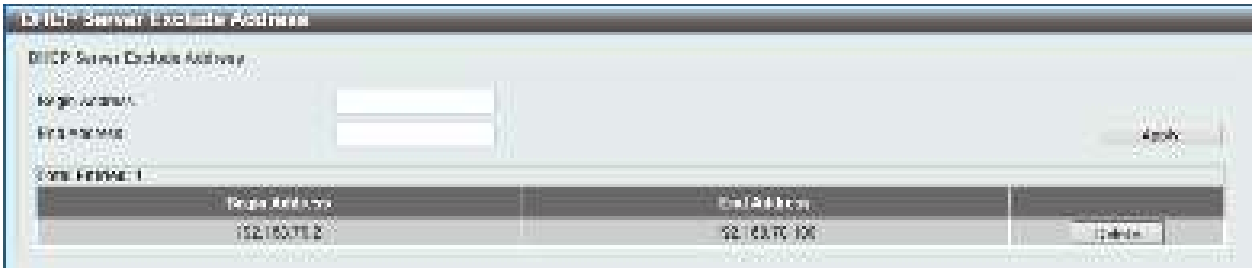


Figure 4-32 DHCP Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
Begin Address	Enter the first IPv4 address of a range of addresses to be excluded here.
End Address	Enter the last IPv4 address of a range of addresses to be excluded here.

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

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

DHCP Server Manual Binding

This window is used to display and configure the DHCP server manual binding settings. With a manual binding entry, the IP address can be bound with a client-identifier or bound with the hardware address of the host.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Manual Binding**, as shown below:

Figure 4-33 DHCP Server Manual Binding Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.
Host	Enter the DHCP host IPv4 address here.
Mask	Enter the DHCP host network subnet mask here.
Hardware Address	Enter the DHCP host MAC address here.

Parameter	Description
Client Identifier	Enter the DHCP host identifier in hexadecimal notation here. The client identifier is formatted by the media type and the MAC address.

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

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

DHCP Server Dynamic Binding

This window is used to view and clear the DHCP server dynamic binding entries.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Dynamic Binding**, as shown below:

Figure 4-34 DHCP Server Dynamic Binding Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the binding entry IPv4 address here.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the **All** option to clear the binding entries for all pools.

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

Click the **Clear** button to clear the entries based on the information specified.

DHCP Server IP Conflict

This window is used to view and clear the DHCP conflict entries from the DHCP server database.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server IP Conflict**, as shown below:

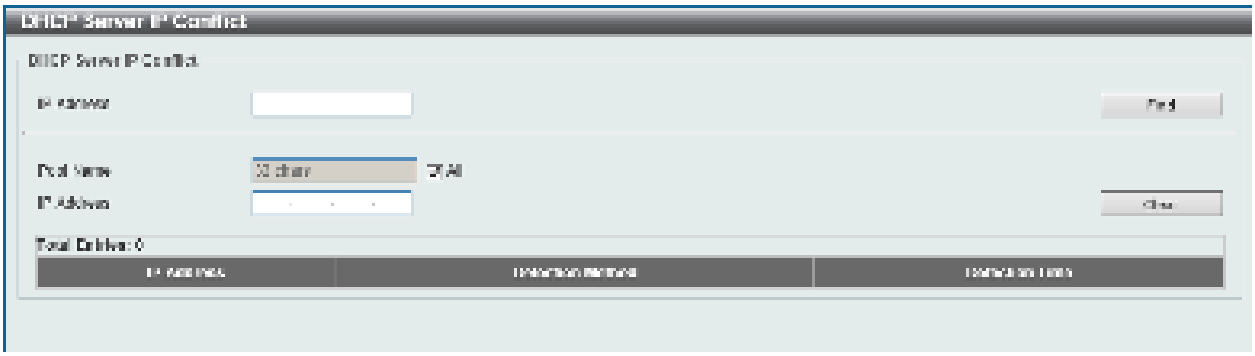


Figure 4-35 DHCP Server IP Conflict Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address of the conflict entry to be located or cleared.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the **All** option to clear the conflict entries for all pools.

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

Click the **Clear** button to clear the entries based on the information specified.

DHCP Server Statistic

This window is used to display DHCP server statistics.

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

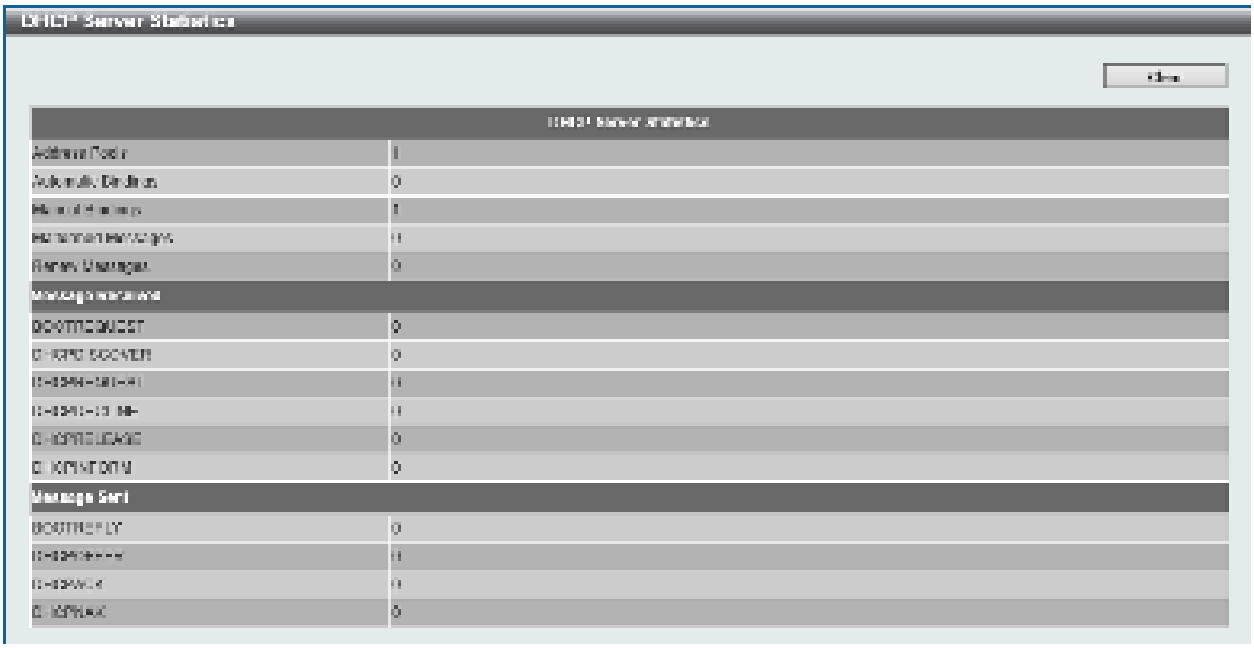


Figure 4-36 DHCP Server Statistic Window

Click the **Clear** button to clear the statistics information displayed here.

DHCPv6 Server

DHCPv6 Server Pool Settings

This window is used to display and configure the DHCPv6 server pool settings.

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

Figure 4-37 DHCPv6 Server Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.

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

Click the **Configure** button to configure the DHCPv6 server pool settings.

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

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

After clicking the **Configure** button, the following page will appear.

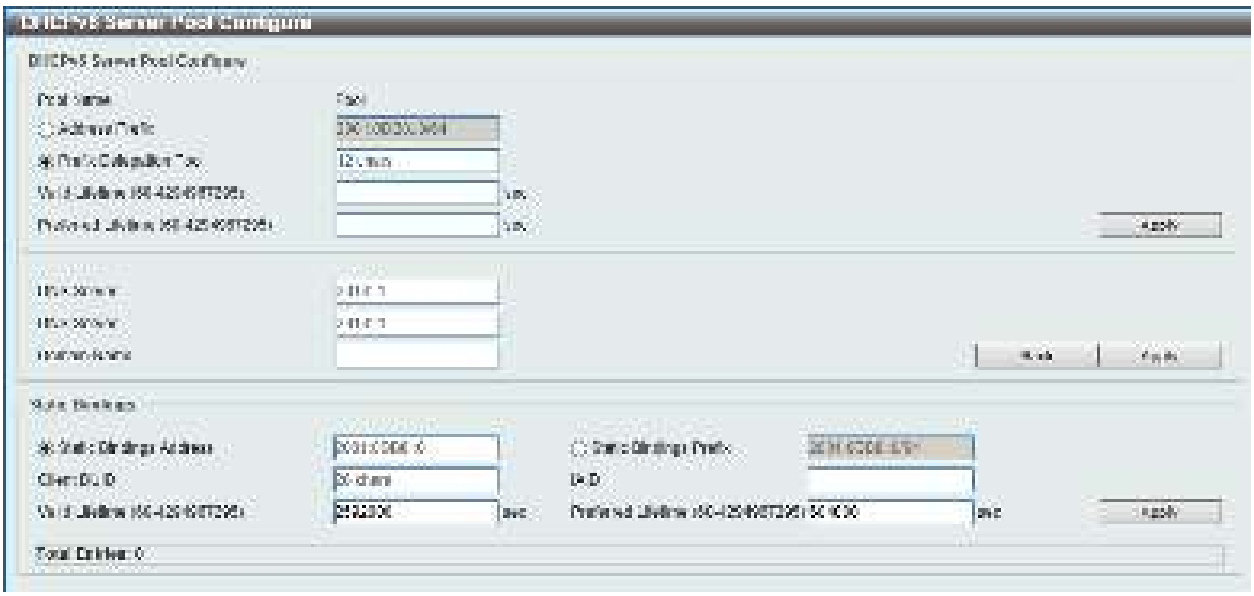


Figure 4-38 DHCPv6 Server Pool Configure Window

The fields that can be configured in **DHCPv6 Server Pool Configure** are described below:

Parameter	Description
Address Prefix	Select and enter the DHCPv6 server pool IPv6 network address and prefix length here. For example, 2015::0/64.
Prefix Delegation Pool	Select and enter the DHCPv6 server pool prefix delegation name here. This name can be up to 12 characters long.
Valid Lifetime	Enter the valid lifetime value here. The range is from 60 to 4294967295 seconds. The valid lifetime should be greater than preferred lifetime. If this value is not specified, then the default valid lifetime will be 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. If this value is not specified, the preferred lifetime will be 604800 seconds (7 days).
DNS Server	Enter the DNS server IPv6 address to be assigned to requesting DHCPv6 clients here.
Domain Name	Enter the domain name to be assigned to requesting DHCPv6 clients here.

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

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

The fields that can be configured in **Static Bindings** are described below:

Parameter	Description
Static Bindings Address	Enter the static binding IPv6 address assign to the specific client here.
Static Bindings Prefix	Enter the static binding IPv6 network address and prefix length here.
Client DUID	Enter the client DHCP Unique Identifier (DUID) here. This string can be up to 28 characters long.
IAID	Enter the Identity Association Identifier (IAID) here. The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client.
Valid Lifetime	Enter the valid lifetime value here. The valid lifetime should be greater than the preferred lifetime. The range is from 60 to 4294967295 seconds. By default, this value is 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. By default, this value is 604800 seconds (7 days).

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

DHCPv6 Server Local Pool Settings

This window is used to display and configure the DHCPv6 server local pool settings.

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

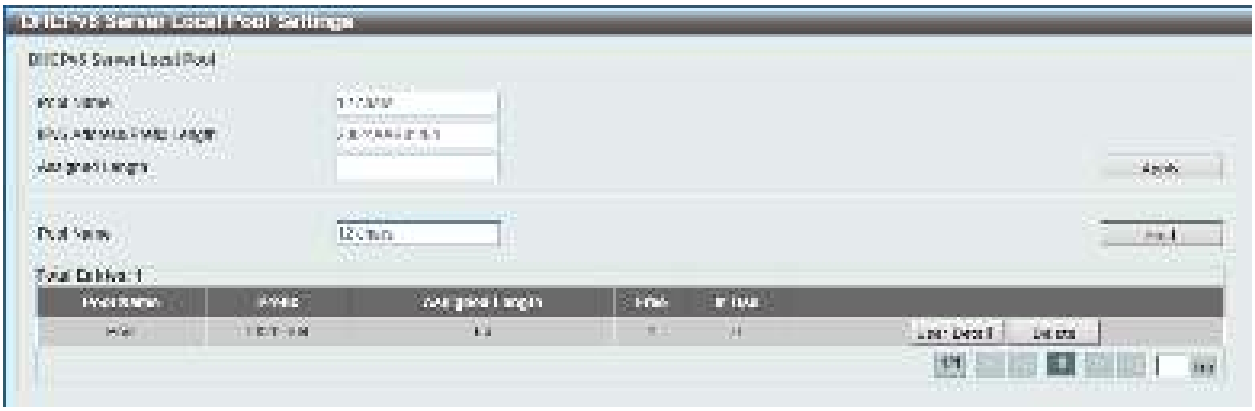


Figure 4-39 DHCPv6 Server Local Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
IPv6 Address / Prefix Length	Enter the IPv6 prefix address and prefix length of the local pool here.
Assigned Length	Enter the prefix length to be delegated to the user from the pool here. The value of the assigned length cannot be less than the value of the prefix length.

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

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

Click the **User Detail** button to view the user information displayed in the lower 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.

DHCPv6 Server Exclude Address

This window is used to specify IPv6 addresses that a DHCPv6 server should not assign to DHCPv6 clients. The DHCPv6 server assumes that all addresses (excluding the Switch's IPv6 address) can be

assigned to clients. Use this window to exclude a single IPv6 address or a range of IPv6 addresses. The excluded addresses are only applied to the pool(s) for address assignment.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Exclude Address**, as shown below:

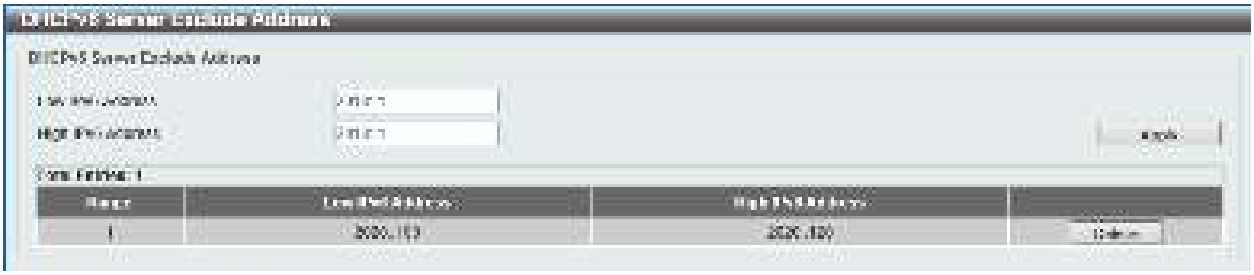


Figure 4-40 DHCPv6 Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
Low IPv6 Address	Enter the excluded IPv6 address or first IPv6 address in the excluded address range here.
High IPv6 Address	Enter the last IPv6 address in the excluded address range here (optional).

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

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

DHCPv6 Server Binding

This window is used to view and clear the DHCPv6 server binding entries.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Binding**, as shown below:

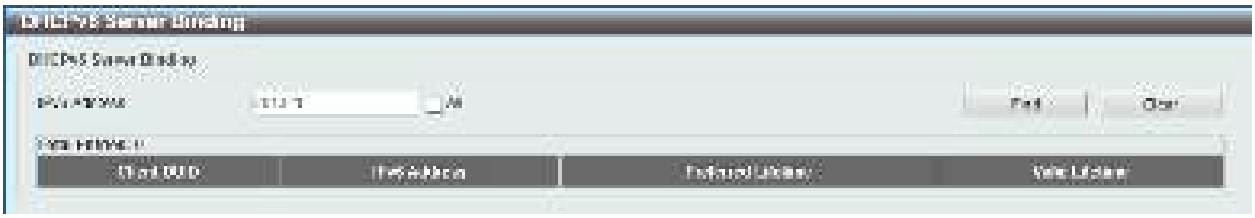


Figure 4-41 DHCPv6 Server Binding Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Enter the binding entry IPv6 address to be displayed or cleared here. Select the **All** option to display or clear all DHCPv6 client prefix bindings in or from the binding table.

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

Click the **Clear** button to clear the entries based on the information specified.

DHCPv6 Server Interface Settings

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

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

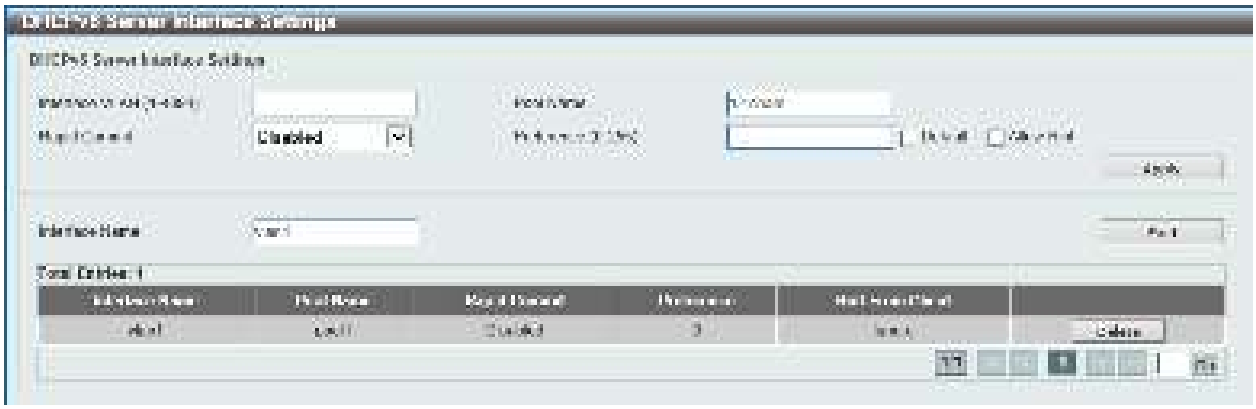


Figure 4-42 DHCPv6 Server Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
Rapid Commit	Select to enable or disable two-message exchange here. By default, two-message exchange is not allowed.
Preference	Enter the preference value here. The range is from 0 to 255. Select the **Default** option to use the default value. Select the **Allow Hint** option to allow hints.
Interface Name	Enter the interface name here.

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

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

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

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

DHCPv6 Server Operational Information

This window is used to display the DHCPv6 server operational information.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Operational Information**, as shown below:

Figure 4-43 DHCPv6 Server Operational Information Window

DHCP Relay

DHCP Relay Global Settings

This window is used to configure the smart relay feature of the DHCP relay agent.

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

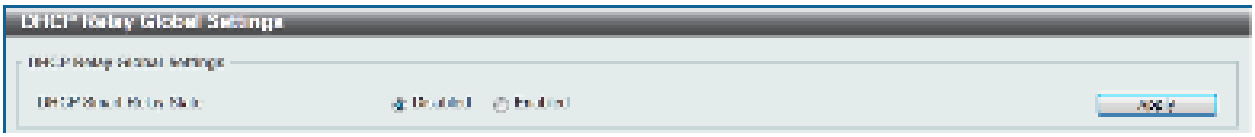


Figure 4-44 DHCP Relay Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DCHP Smart Relay State	Select this option to enable or disable the DHCP smart relay.

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

DHCP Relay Pool Settings

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

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

Figure 4-45 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

Figure 4-46 DHCP Relay Pool Source Settings Window

The fields that can be configured are described below:

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

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

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

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

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

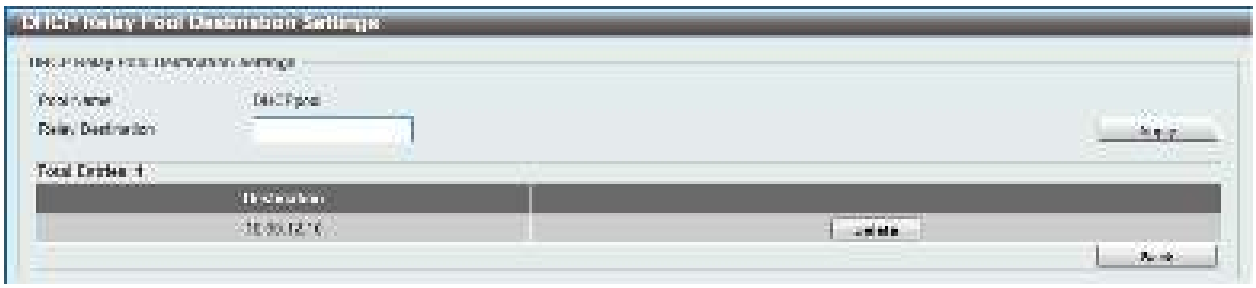


Figure 4-47 DHCP Relay Pool Destination Settings Window

The fields that can be configured are described below:

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

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

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

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

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

Figure 4-48 DHCP Relay Pool Class Settings Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

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

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

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

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

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

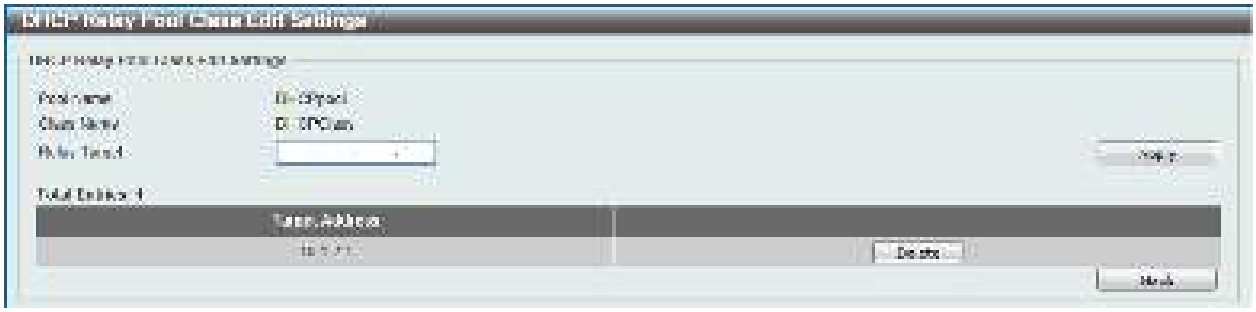


Figure 4-49 DHCP Relay Pool Class Edit Settings Window

The fields that can be configured are described below:

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

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

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

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

DHCP Relay Information Settings

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

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

Figure 4-50 DHCP Relay Information Settings Window

The fields that can be configured are described below:

Parameter	Description
Information Trust All	Select this option to enable or disable the DHCP relay agent to trust the IP DHCP relay information for all interfaces.
Information Check	Select this option to enable or disable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet.
Information Policy	Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are: • **Keep** - Select to discard the packet that already has the relay option. • **Drop** - Select that the DHCP request packet that already has the relay option is left unchanged and directly relayed to the DHCP server. • **Replace** - Select that the DHCP request packet that already has the relay option will be replaced by a new option.
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets.

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

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

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

DHCP Relay Information Option Format Settings

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

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

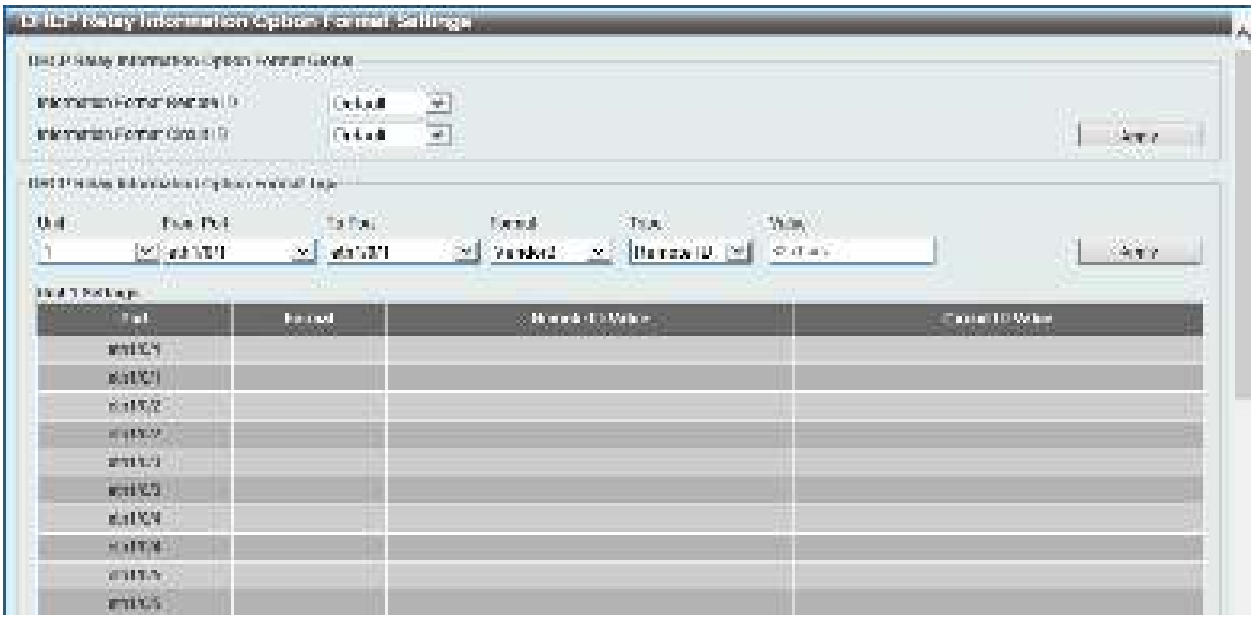


Figure 4-51 DHCP Relay Information Option Format Settings Window

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

Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: • **Default** - Select to use the Switch's system MAC address as the remote ID. • **User Define** - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor2** - Select to use vender 2 as the remote ID. • **Vendor3** - Select to use vender 3 as the remote ID. • **Export UDF** - Select to use the expert UDF remote ID. Select the **Standalone Unit Format** after this selection here.
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are: • **Default** - Select to use the default circuit ID sub-option. • **User Define** - Select to use a user-defined circuit ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor1** - Select to use vender 1 as the circuit ID. • **Vendor2** - Select to use vender 2 as the circuit ID. • **Vendor3** - Select to use vender 3 as the circuit ID. • **Vendor4** - Select to use vender 4 as the circuit ID. • **Vendor5** - Select to use vender 5 as the circuit ID. • **Vendor6** - Select to use vender 6 as the circuit ID. • **Export UDF** - Select to use the expert UDF circuit ID. Select the **Standalone Unit Format** after this selection here.

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

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

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Format	Select the DHCP information circuit ID format. Options to choose from are **Vendor3** and **Expert UDF**.
Type	Select the DHCP information circuit ID format typ. Options to choose from are **Remote ID** and **Circuit ID**.
Value	Enter the vendor-defined string.

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

DHCP Relay Information Profile Settings

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

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

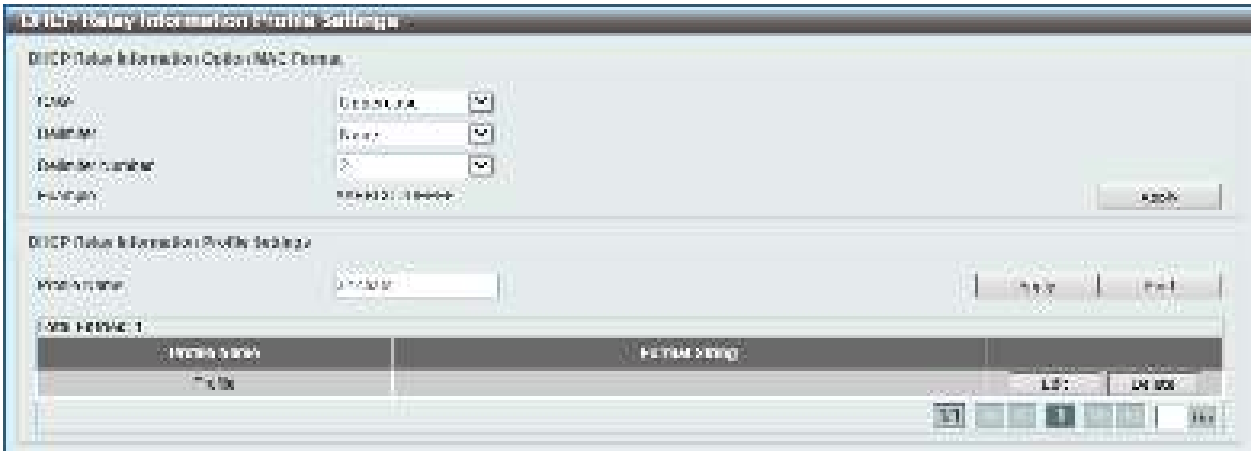


Figure 4-52 DHCP Relay Information Profile Settings Window

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

Parameter	Description
Case	Select the case that will be used here. Options to choose from are: • **Lowercase** - Specifies that when using the lowercase format, the Option 82 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff. • **Uppercase** - Specifies that when using the uppercase format, the Option 82 MAC address for the user-defined profile username will be formatted as: AA-BB-CC-DD-EE-FF.
Delimiter	Select the delimiter that will be used here. Options to choose from are: • **Hyphen** - Specifies that the format will be AA-BB-CC-DD-EE-FF. • **Colon** - Specifies that the format will be AA:BB:CC:DD:EE:FF. • **Dot** - Specifies that the format will be AA.BB.CC.DD.EE.FF. • **None** - Specifies that when not using any delimiter, the format will be AABBCCDDEEFF.

Parameter	Description
Delimiter Number	Select the delimiter number here. Options to choose from are: • **1** - Single delimiter, the format is: AABBCC.DDEEFF. • **2** - Double delimiters, the format is: AABB.CCDD.EEFF. • **5** - Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF.

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

The fields that can be configured in **DHCP Relay Information Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the Option 82 profile name here. The profile can be used to define the flexible, user-defined Option 82 entry.
Format String	After clicking the **Edit** button, enter the user-defined DHCP Option 82 format string here. This string can be up to 251 characters long. The following rules need to be considered: • This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks (“”) like “Ethernet”. Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, **“%” +“$”+“1~32”+ “keyword”+ “:”:** ○ **%** - Indicates that the string that follows this character is a formatted key string. ○ **“$”** or **“0”** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either “$” or “0”, and cannot be specified as both at the same time. ▪ **“$”** - Indicates to fill the leading space (0x20). ▪ **“0”** - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting. ○ **1~32** - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. ○ **keyword** - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: ▪ **devtype** - The model name of the device. Only an ASCII string is allowed. ▪ **sysname** - Indicates the System name of the Switch. Only an ASCII string is allowed. ▪ **ifdescr** - Derived from *ifDescr* (IF-MIB). Only an ASCII string is allowed. ▪ **portmac** - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands. When in the format of a hexadecimal value, the MAC

Parameter	Description
	address will be encapsulated in order in hexadecimal. ▪ **sysmac** - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal. ▪ **unit** - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0. ▪ **module** - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value. ▪ **port** - Indicates the local port number. This can be either an ASCII string or a hexadecimal value. ▪ **svlan** - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. ▪ **cvlan** - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value. ○ **:** - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#$%^&*()_+|-=\[]{};:'"/?.,<>`, and space characters. "\" is the escape character. The special character after "\" is the character itself, for example, "\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

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

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

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

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

DHCP Local Relay VLAN

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

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

Figure 4-53 DHCP Local Relay VLAN Window

The fields that can be configured are described below:

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

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

DHCPv6 Relay

DHCPv6 Relay Global Settings

This window is used to configure the DHCPv6 relay remote ID.

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

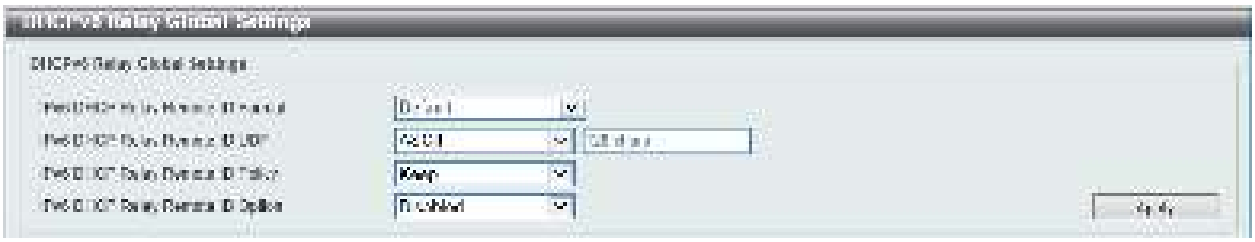


Figure 4-54 DHCPv6 Relay Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select to choose the sub-type of the remote ID. Options to choose from are **Default**, **CID With User Define**, and **User Define**.
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for remote ID. Options to choose from are: • **ASCII** - Select to enter the ASCII string with a maximum of 128 characters in the text box. • **HEX** - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are:

Parameter	Description
	• **Keep** - Select to discard the packet that already has the relay agent Remote-ID Option 37. • **Drop** - Select that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server.
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.

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

DHCPv6 Relay Interface Settings

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

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

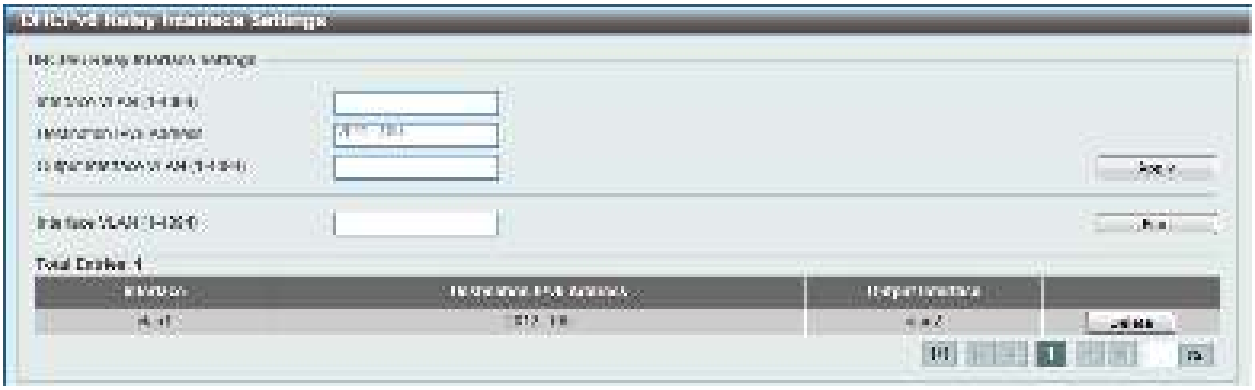


Figure 4-55 DHCPv6 Relay Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN from 1 to 4094 for DHCPv6 relay.
Destination IPv6 Address	Enter the DHCPv6 relay destination address.
Output Interface VLAN	Enter the output interface for the relay destination.

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

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

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

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

DHCP Auto Configuration

This window is used to configure the DHCP auto-configuration function.

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

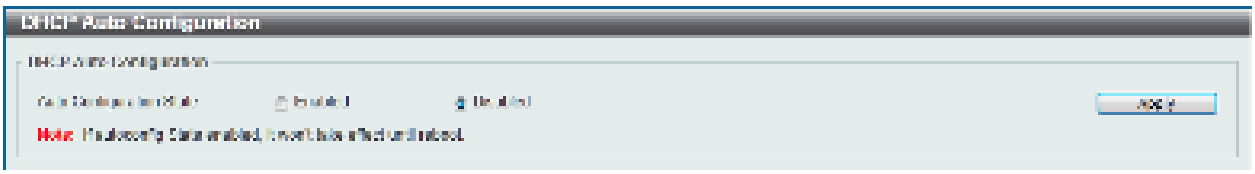


Figure 4-56 DHCP Auto Configuration Window

The fields that can be configured are described below:

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

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

DNS

Computer users usually prefer to use text names for computers for which they may want to open a connection. Computers themselves, require 32-bit IP addresses. Somewhere, a database of network devices' text names and their corresponding IP addresses must be maintained.

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets. For two DNS servers to communicate across different subnets, the DNS Relay of the Switch must be used. The DNS servers are identified by IP addresses.

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name server. The client program is called a Name resolver. A Name resolver may need to contact several Name servers to translate a name to an address.

The Domain Name System (DNS) servers are organized in a somewhat hierarchical fashion. A single server often holds names for a single network, which is connected to a root DNS server - usually maintained by an ISP.

Domain Name Resolution

The domain name system can be used by contacting the name servers one at a time, or by asking the domain name system to do the complete name translation. The client makes a query containing the name, the type of answer required, and a code specifying whether the domain name system should do the entire name translation, or simply return the address of the next DNS server if the server receiving the query cannot resolve the name.

When a DNS server receives a query, it checks to see if the name is in its sub domain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution. This requires the server to contact

other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it will return the address of the next DNS server the client contacted.

Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

The address of the machine that supplies domain name service is often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Global Settings

This window is used to configure the DNS global settings.

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

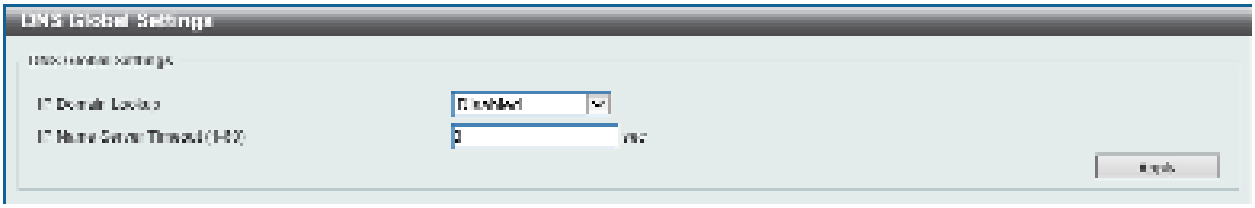


Figure 4-57 DNS Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Domain Lookup	Select this option to enable or disable the DNS to carry out the domain name resolution.
IP Name Server Timeout	Enter the maximum time to wait for a response from a specified name server. This value is between 1 and 60 seconds.

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

DNS Name Server Settings

This window is used to configure and display the IP address of a domain name server.

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

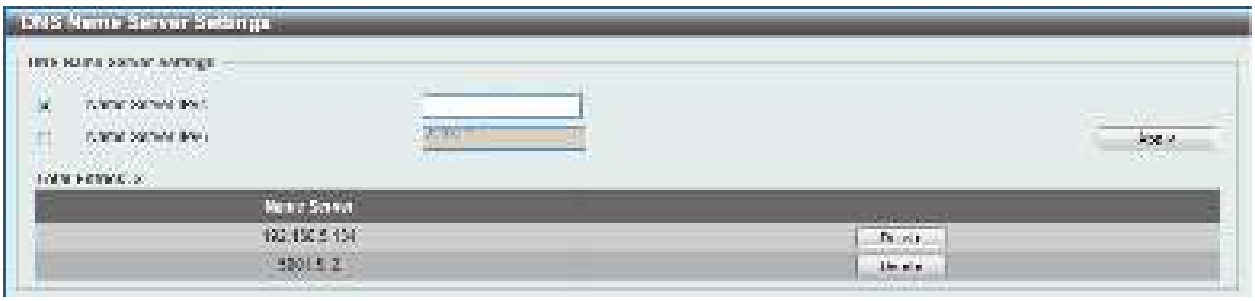


Figure 4-58 DNS Name Server Settings Window

The fields that can be configured are described below:

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

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

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

DNS Host Settings

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

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

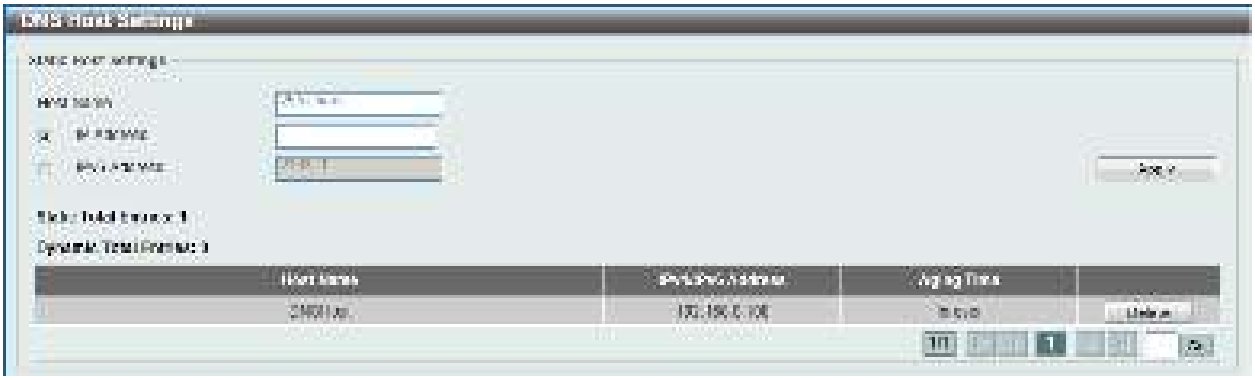


Figure 4-59 DNS Host Settings Window

The fields that can be configured are described below:

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

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

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

NTP

NTP Global Settings

This window is used to view and configure the Network Time Protocol (NTP) global settings.

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

Figure 4-60 NTP Global Settings Window

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

Parameter	Description
NTP State	Select the NTP feature's global state here. Options to choose from are **Enabled** and **Disabled**.

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

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

Parameter	Description
NTP Authentication State	Select the NTP feature's authentication state here. Options to choose from are **Enabled** and **Disabled**.

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

The fields that can be configured for **NTP Update Calendar** are described below:

Parameter	Description
NTP Update Calendar	Select the NTP feature's update calendar state here. Options to choose from are **Enabled** and **Disabled**.

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

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

Parameter	Description
NTP Master Stratum	Enter the NTP master stratum value here. This value must be between 1 and 15. Select the **Default** option to use the default value.
NTP Max Associations	Enter the NTP maximum amount of associations here. This value must be between 1 and 64.

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

NTP Server Settings

This window is used to view and configure the NTP server's settings.

To view the following window, click **Management > NTP > NTP Server Settings**, as shown below:

Figure 4-61 NTP Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the NTP server's IPv4 address here.
IPv6 Address	Select and enter the NTP server's IPv6 address here.
Version	Enter the NTP server's version number here. This value must be between 1 and 4.
Key ID	Enter the authentication key ID here. This ID must be between 1 and 255.
Min Poll	Enter the minimum poll intervals for NTP messages here. This value must be between 3 and 16 seconds.
Max Poll	Enter the maximum poll intervals for NTP messages here. This value must be between 4 and 17 seconds.
Prefer	Select whether this server is the preferred server in the list or not. Options to choose from are **True** and **False**.

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

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

NTP Peer Settings

This window is used to view and configure the NTP peer settings.

To view the following window, click **Management > NTP > NTP Peer Settings**, as shown below:

Figure 4-62 NTP Peer Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the NTP peer's IPv4 address here.
IPv6 Address	Select and enter the NTP peer's IPv6 address here.
Version	Enter the NTP peer's version number here. This value must be between 1 and 4.
Key ID	Enter the authentication key ID here. This ID must be between 1 and 255.
Min Poll	Enter the minimum poll intervals for NTP messages here. This value must be between 3 and 16 seconds.
Max Poll	Enter the maximum poll intervals for NTP messages here. This value must be between 4 and 17 seconds.
Prefer	Select whether this peer is the preferred peer in the list or not. Options to choose from are **True** and **False**.

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

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

NTP Access Group Settings

This window is used to view and configure the NTP access group settings.

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

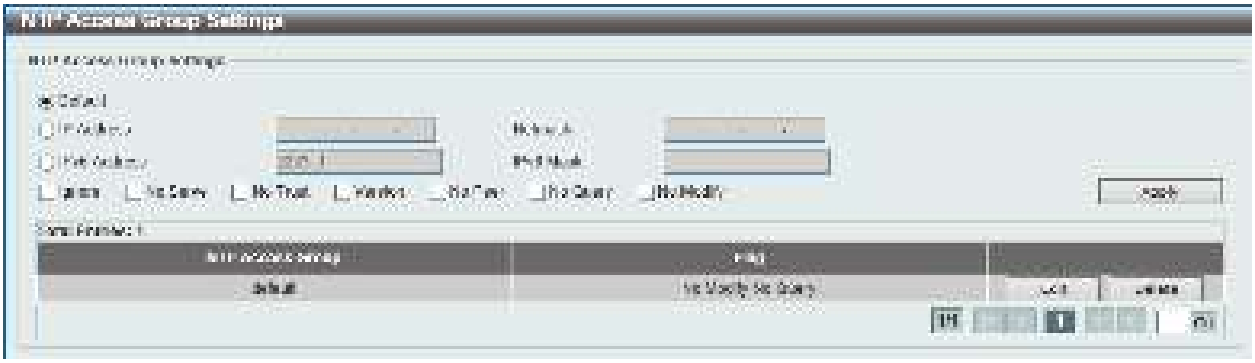


Figure 4-63 NTP Access Group Settings Window

The fields that can be configured are described below:

Parameter	Description
Default	Select this option to specify that a default entry (address 0.0.0.0, mask 0.0.0.0) will always be included and is the lowest priority in the list.
IP Address	Select and enter the IPv4 address of the host or network here.
Netmask	Select and enter the IPv4 network mask of the host or network here.
IPv6 Address	Select and enter the IPv6 address of the host or network here.
IPv6 Mask	Select and enter the IPv6 network mask of the host or network here.
Ignore	Select this option to ignore all NTP related packets.
No Serve	Select this option to deny all NTP related packets, except for NTP control queries.
No Trust	Select this option to deny all NTP related packets that are not cryptographically authenticated.
Version	Select this option to deny all NTP related packets that don't match the current NTP version.
No Peer	Select this option to deny all NTP related packets that might mobilize an association unless authenticated.
No Query	Select this option to deny all NTP control queries.
No Modify	Select this option to deny NTP control queries that attempted to modify the state of the server.

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

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

NTP Key Settings

This window is used to view and configure the NTP key settings.

To view the following window, click **Management > NTP > NTP Key Settings**, as shown below:

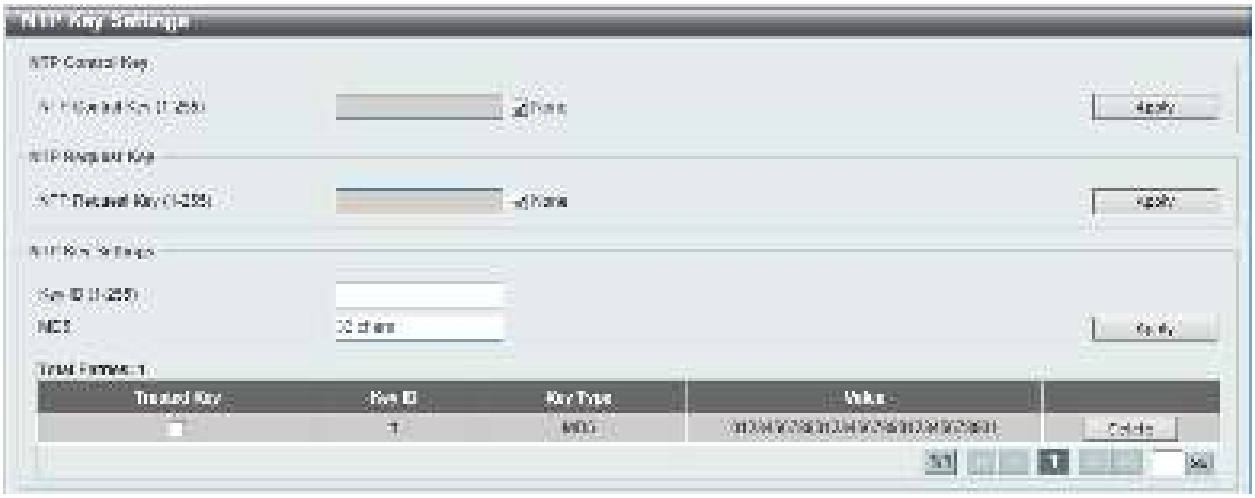


Figure 4-64 NTP Key Settings Window

The fields that can be configured for **NTP Control Key** are described below:

Parameter	Description
NTP Control Key	Enter the NTP control key here. This key must be between 1 and 255. Select the **None** option not to use an NTP control key.

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

The fields that can be configured for **NTP Request Key** are described below:

Parameter	Description
NTP Request Key	Enter the NTP request key here. This key must be between 1 and 255. Select the **None** option not to use an NTP request key.

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

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

Parameter	Description
Key ID	Enter the NTP key number here. This authentication key number must be between 1 and 255.
MD5	Enter the MD5 NTP key here. This key can be up to 32 characters long.

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

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

NTP Interface Settings

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

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

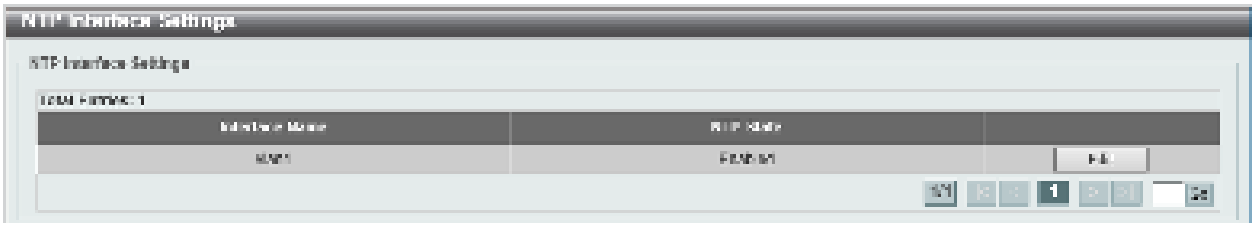


Figure 4-65 NTP Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
NTP State	After click the **Edit** button, select the NTP feature's state on the interface specified. Options to choose from are **Enabled** and **Disabled**.

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

NTP Associations

This window is used to view a list of NTP associations.

To view the following window, click **Management > NTP > NTP Associations**, as shown below:

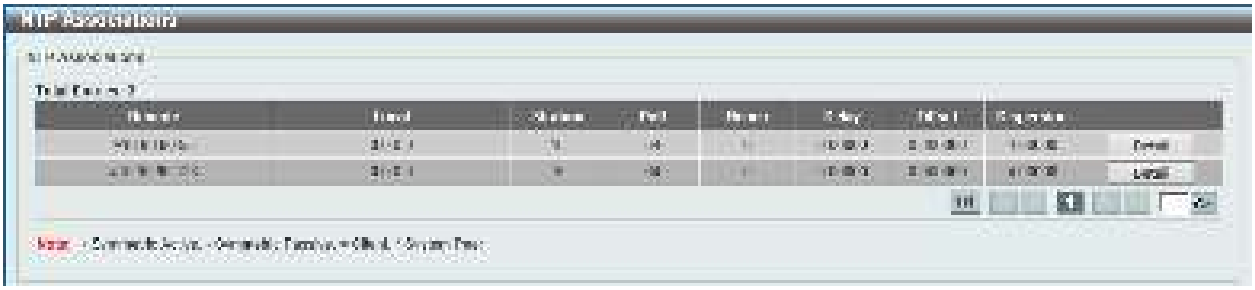


Figure 4-66 NTP Associations Window

Click the **Detail** button, next to the specified entry, to view more information about the NTP association, as shown below:

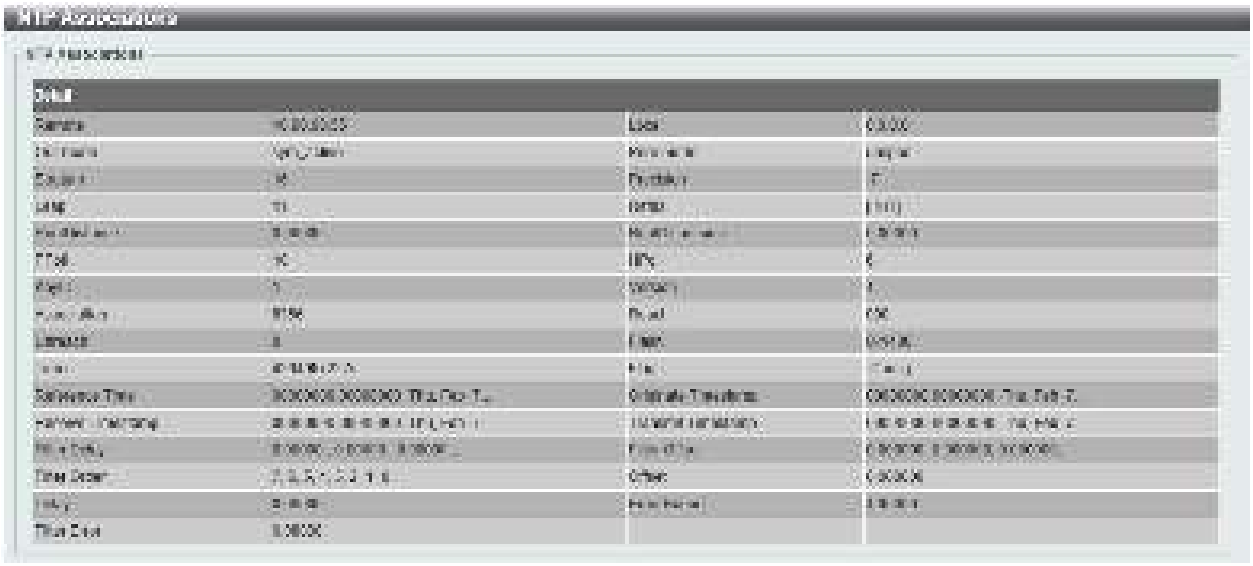


Figure 4-67 NTP Associations (Detail) Window

NTP Status

This window is used to view NTP status information.

To view the following window, click **Management > NTP > NTP Status**, as shown below:

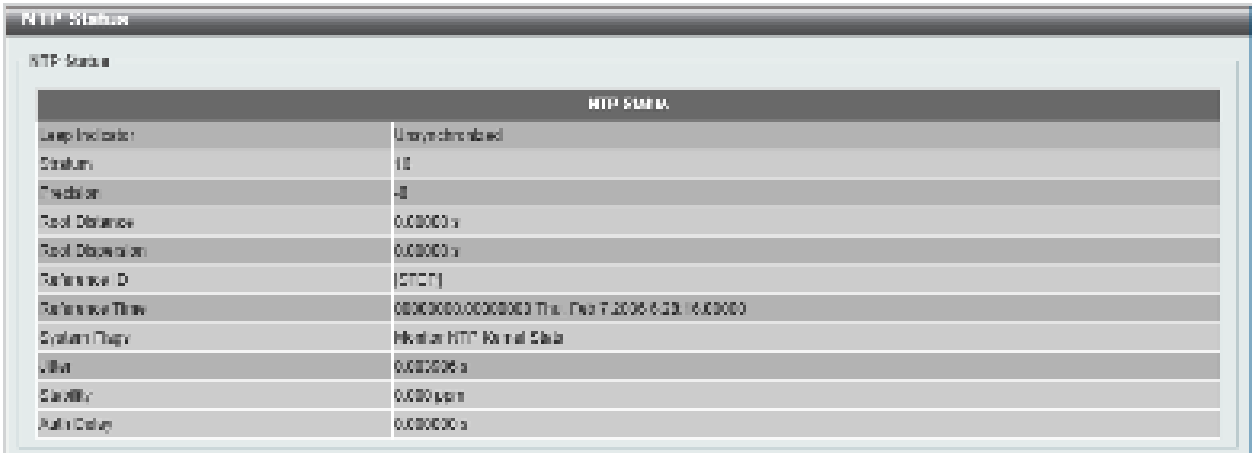


Figure 4-68 NTP Status Window

IP Source Interface

This window is used to configure the IP source interface settings.

To view the following window, click **Management > IP Source Interface**, as shown below:

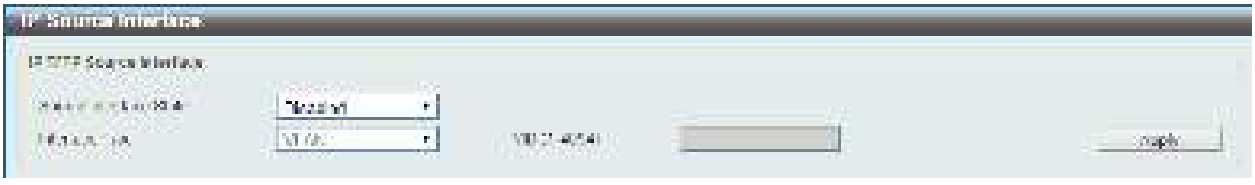


Figure 4-69 IP Source Interface Window

The fields that can be configured are described below:

Parameter	Description
Source Interface State	Select to **Enable** or **Disable** the source interface feature's global state here.
Interface Type	After enabling the **Source Interface State** option, select the interface type here. The only option available is **VLAN**.
VID (1-4094)	After selecting the **VLAN** as the **Interface Type**, enter the VLAN ID used here. This value must be between 1 and 4094.

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

File System

Why use flash file system?

In old switch system, the firmware, configuration, and log information are saved in a flash with fixed addresses and size. This means that the maximum configuration file can only be 2Mb, and even if the current configuration is only 40Kb, it will still take up 2Mb of flash storage space. The configuration file number and firmware numbers are also fixed. A compatible issue will occur in the event that the configuration file or firmware size exceeds the originally designed size.

Flash File System (FFS) in our system:

The Flash File System is used to provide the user with flexible file operation on the Flash. All the firmware, configuration information, and system log information are stored in the Flash as files. This means that the Flash space taken up by all the files are not fixed, it is the real file size. If the Flash space is enough, the user could download more configuration files or firmware files and use commands to display Flash file information, rename file names, and delete it. Furthermore, the user can also configure the **boot up runtime image** or the **running configuration file** if needed.

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

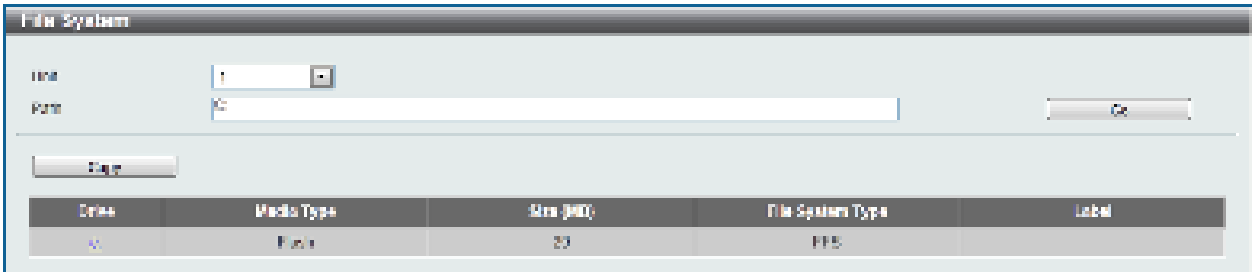


Figure 4-70 File System Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Path	Enter the path string

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

Click the c: hyperlink to navigate the C: drive.

After clicking the c: hyperlink, the following window will appear:

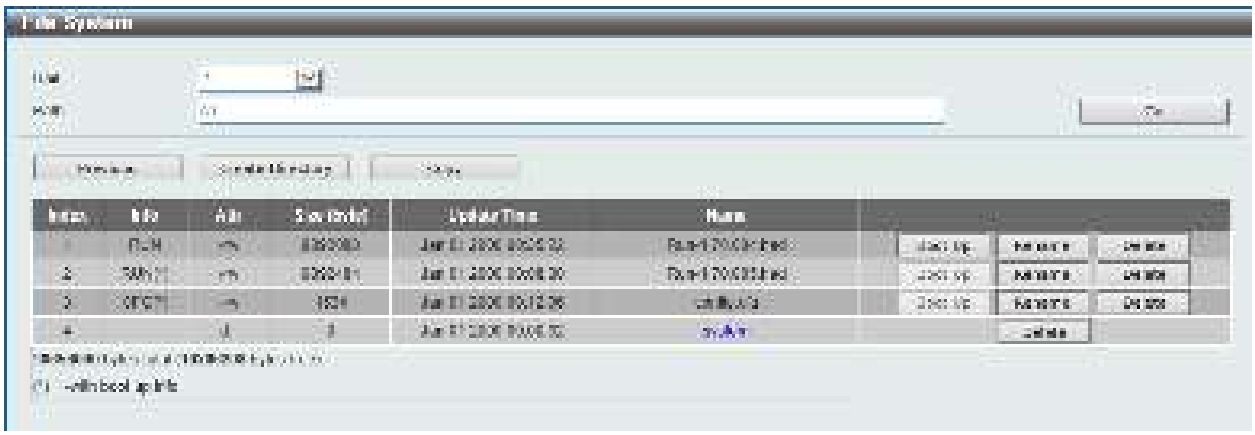


Figure 4-71 File System - Search for Drive Window

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

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

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

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

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

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

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

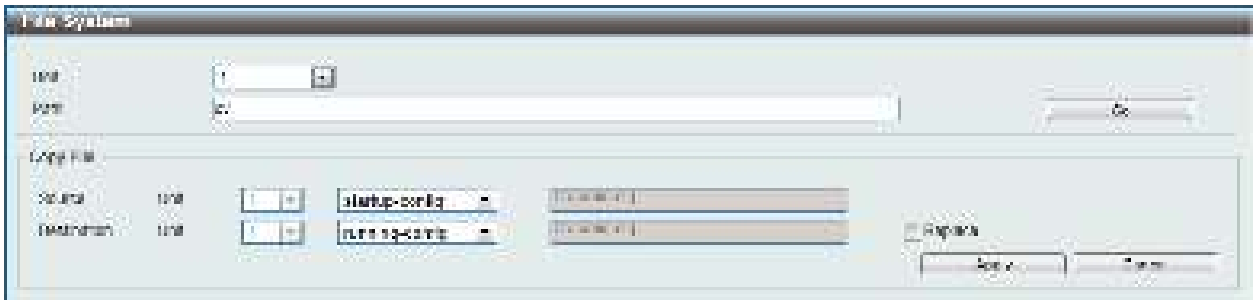


Figure 4-72 File System - Copy Window

When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path. Tick the **Replace** check box to replace the current running configuration with the indicated configuration file.

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

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

Physical Stacking

The Switch supports switch stacking, where a set of six switches can be combined and managed by one IP address through Telnet, the Web UI, the RJ45 console port, or through SNMP. Each switch of this series has two stacking ports located at the front of the device, which can be used to connect other devices and make them stack together. After adding these stacking ports, the user may connect

these ports together using fiber cables or Direct Attach Cables (DAC) in one of two possible topologies.

- **Duplex Chain** -The Duplex Chain topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will obviously be affected.
- **Duplex Ring** -The Duplex Ring stacks switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient because if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack.

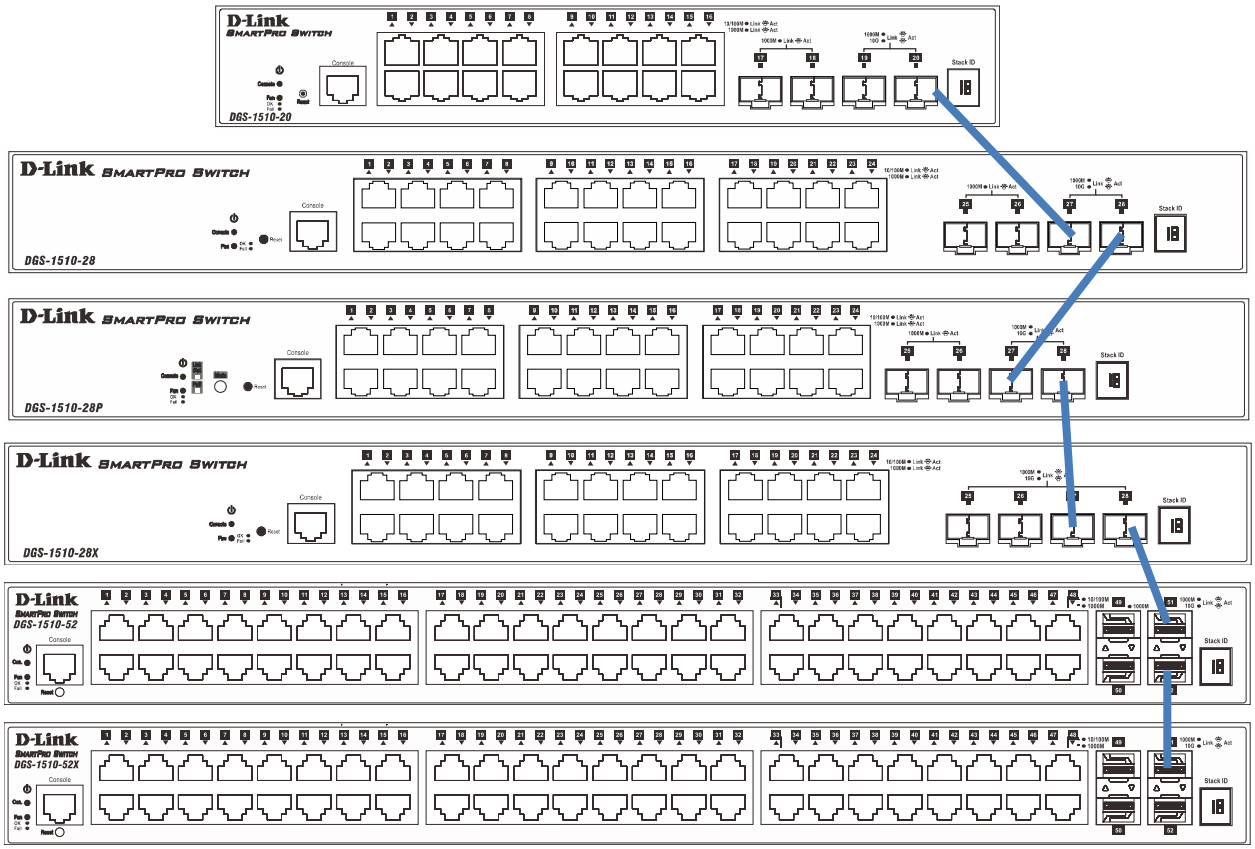


Figure 4-73 Switches stacked in a Duplex Chain

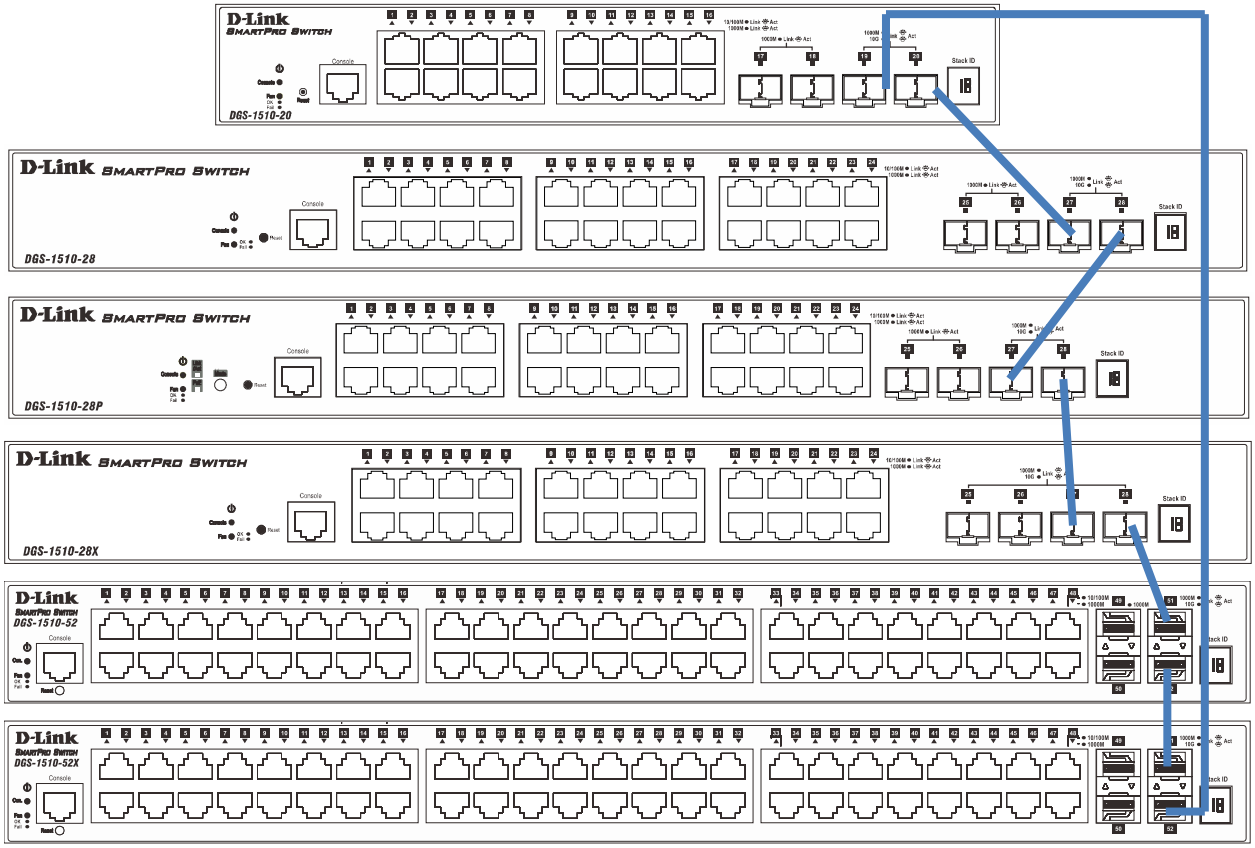


Figure 4-74 Switches stacked in a Duplex Ring

Within each of these topologies, each switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the Switch stack. Three possible roles exist when stacking with the Switch.

Primary Master - The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This switch will also assign Stack Unit IDs, synchronize configurations, and transmit commands to remaining switches in the switch stack. The Primary Master can be configured manually by assigning the Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack or it can be determined automatically, by the stack, through an election process which determines the lowest MAC address and will assign that switch as the Primary Master, if all priorities are the same. The Primary master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and ‘H’.

Backup Master - The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority before physically assembling the stack, or it can be determined automatically by the stack through an election process that determines the second lowest MAC address and then will assign that switch as the Backup Master, if all priorities are the same. The Backup master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and ‘h’.

Slave - Slave switches constitute the rest of the switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave switches perform operations requested by the master, monitor the status of neighbor switches in the stack and the stack topology, and adhere to the Backup Master’s commands once it becomes a Primary Master. Slave switches will do a self-check to determine if it is to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, it will determine if it is to become the Primary Master. These roles will be determined, first by priority and if the priority is the same, the lowest MAC address.

Once switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

Initialization State - This is the first state of the stack, where the runtime codes are set and initialized and the system conducts a peripheral diagnosis to determine each individual switch is functioning properly.

Master Election State - Once the codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.

Synchronization State - Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to switches in the stack, synchronize configurations for all switches and then transmit commands to the rest of the switches based on the users configurations of the Primary Master.

Once these steps have been completed, the switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the Switch supports “hot swapping” of switches in and out of the running stack. Users may remove or add switches to the stack without powering down or largely affecting the transfer of data between switches in the stack, with a few minor provisions.

When switches are “hot inserted” into the running stack, the new switch may take on the Primary Master, Backup Master or Slave role, depending on configurations set on the newly added switch, such as configured priority or MAC address. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master’s roles for all new switches that were hot inserted. This process is done using discovery packets that circulate through the switch stack every 1.5 seconds until the discovery process has been completed.

The “hot remove” action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master, or Slave, may be removed from the stack, yet different processes occur for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configurations of the unit removed. Dynamically learned databases, such as ARP, will also be cleared.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configurations of the unit removed. Dynamically learned databases, such as ARP, will also be cleared. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master’s role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configurations of the unit removed. Dynamically learned databases, such as ARP, will also be cleared. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

If both the Primary Master and the Backup Master are removed, the election process is immediately processed, and a new Primary Master and Backup Master are determined. Switches in the stack will clear the configurations of the units removed, and dynamically learned databases, such as ARP, will be cleared as well. Static switch configurations still remain in the database of the remaining switches in the stack and those functions will not be affected.

NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack.

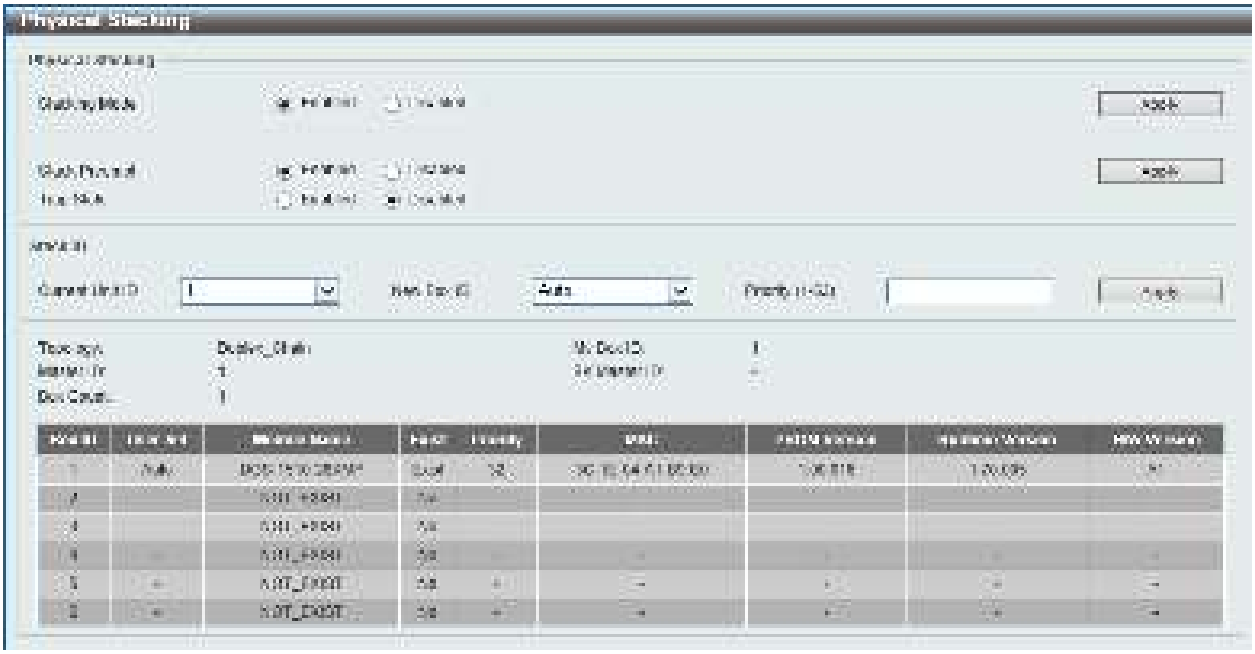


Figure 4-75 Physical Stacking Window

The fields that can be configured for **Physical Stacking** are described below:

Parameter	Description
Stacking Mode	Select this option to enable or disable the stacking mode.
Stack Preempt	Select this option to enable or disable preemption of the master role to come into play when a unit with a better priority is added to the Switch later.
Trap State	Select this option to enable or disable sending of stacking related traps.

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

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

Parameter	Description
Current Unit ID	Select the unit ID of the switch in the stack.
New Box ID	Select the new box ID for the switch that is selected in the **Current Unit ID**. The user may choose any number between 1 and 6 to identify the switch in the switch stack. **Auto** will automatically assign a box number to the switch in the switch stack.
Priority	Enter the priority of the Switch stacking unit. The range is from 1 to 63.

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

Virtual Stacking (SIM)

D-Link Single IP Management (SIM) is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the Single IP Management feature:

- SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
- SIM can reduce the number of IP address needed in your network.

- SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.
- There are three classifications for switches using SIM. The **Commander Switch (CS)**, which is the master switch of the group, **Member Switch (MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch (CaS)**, which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- A SIM group accepts up to 32 switches (numbered 1-32), not including the Commander Switch (numbered 0).
- Members of a SIM group cannot cross a router.
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain); however, a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the management VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The Switch may take on three different roles:

- **Commander Switch (CS)** - This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
    - It has an IP Address.
    - It is not a command switch or member switch of another Single IP group.
    - It is connected to the member switches through its management VLAN.
- **Member Switch (MS)** - This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
    - It is not a CS or MS of another IP group.
    - It is connected to the CS through the CS management VLAN.
- **Candidate Switch (CaS)** - This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of the Switch by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:
    - It is not a CS or MS of another Single IP group.
    - It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

- Each device begins in a Candidate state.
- A CS must change its role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.
- The user can manually configure a CS to become a CaS.
- A MS can become a CaS by:
    - Being configured as a CaS through the CS.
    - If report packets from the CS to the MS time out.
- The user can manually configure a CaS to become a CS
- The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DGS-1510 Series switches may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (includes read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

Upgrade to Version 1.61

To better improve SIM management, the DGS-1510 Series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including the Commander Switch (CS) now having the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This is accomplished through the use of Discover packets and Maintenance packets that previously configured SIM members will send and receive after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS Switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group.

- **Firmware** - The switch now supports MS firmware downloads from a TFTP server.
- **Configuration Files** - This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server.
- **Log** - The Switch now supports uploading MS log files to a TFTP server.

The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configurations.

Single IP Settings

This window is used to configure the SIM settings. The Switch is set as a Candidate (CaS) as the factory default configuration and Single IP Management is disabled.

To view the following window, click **Management > Virtual Stacking (SIM) > Single IP Settings**, as shown below:

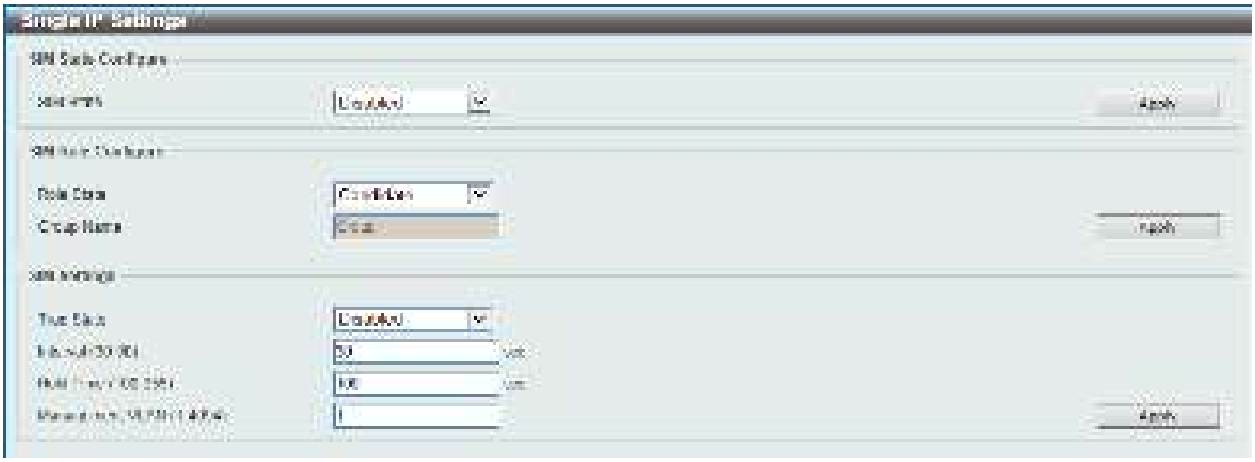


Figure 4-76 Single IP Settings Window

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

Parameter	Description
SIM State	Select this option to enable or disable the SIM state on the Switch. Select **Disabled** to render all SIM functions on the Switch inoperable.

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

The fields that can be configured for **SIM Role Configure** are described below:

Parameter	Description
Role State	Select to change the SIM role of the Switch. Options to choose from are: • **Candidate** - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the Switch. • **Commander** - Select to make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	Enter a group name. This is optional. This name is used to segment switches into different SIM groups.

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

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

Parameter	Description
Traps State	Select to enable or disable the SIM trap state.
Interval	Enter the interval in seconds. The range is from 30 to 90.
Hold Time	Enter the hold-time in seconds. The range is from 100 to255.

Parameter	Description
Management VLAN	Enter the single IP management message VLAN ID.

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

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade**, **Configuration Backup/Restore**, and **Upload Log File**.

Topology

This window is used to configure and manage the Switch within the SIM group.

To view the following window, click **Management > Virtual Stacking (SIM) > Topology**, as shown below:

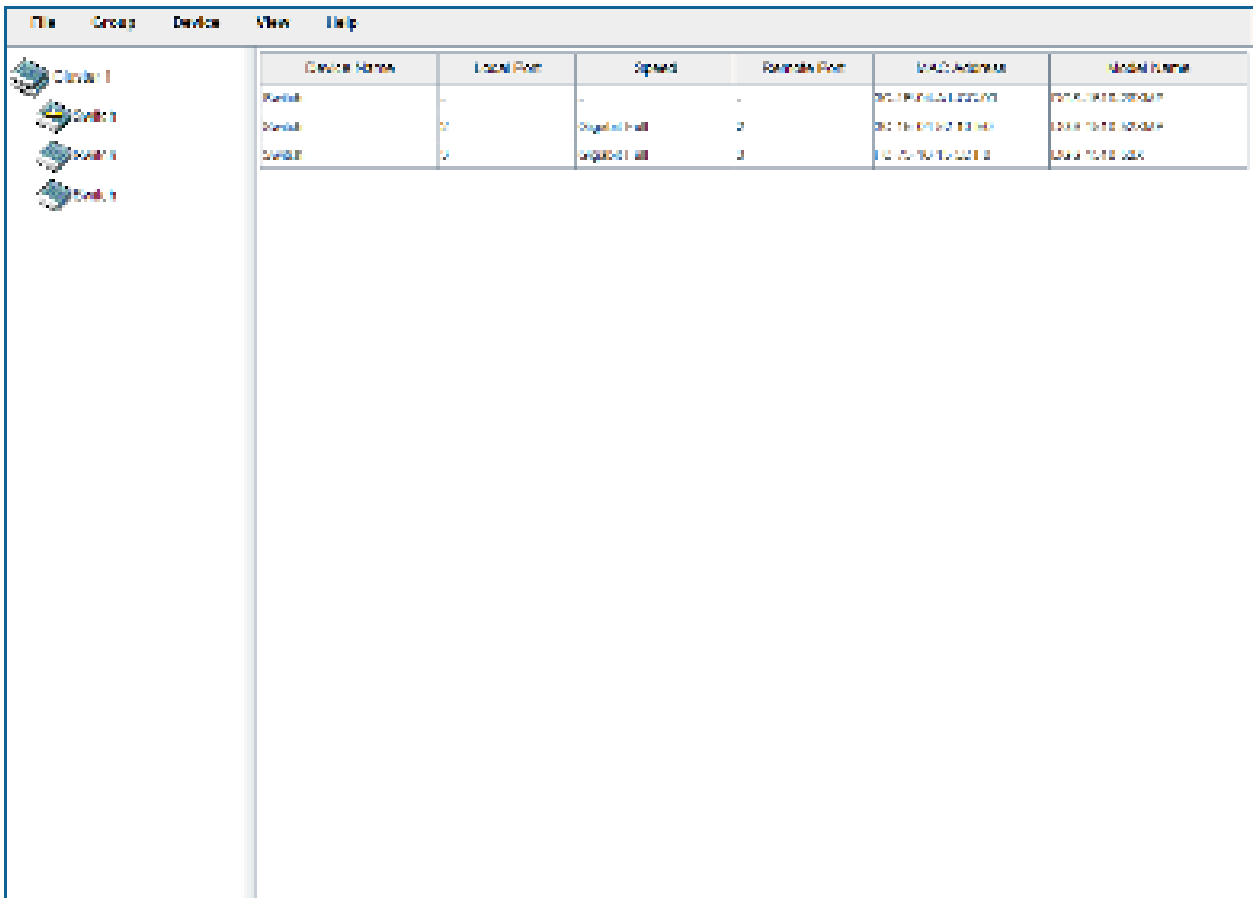


Figure 4-77 Topology Window

There is a menu bar at the top of the window containing **File**, **Group**, **Device**, **View**, and **Help**.

File

Print Topology

On the **File** menu, select **Print Topology** to print the SIM topology map to any of the printers configured on the PC accessing the Web UI.

Preference

On the **File** menu, select **Preference** to configure the display properties for the SIM topology map.

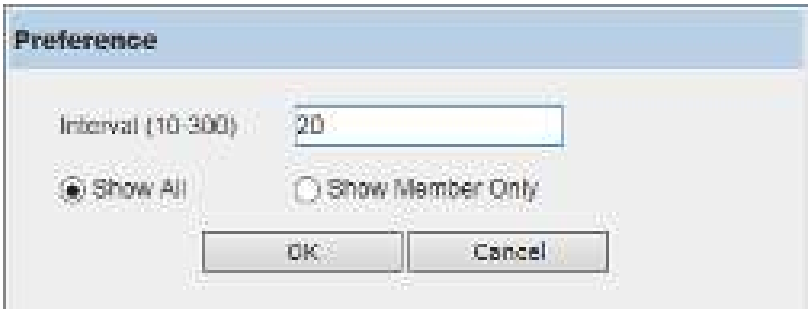


Figure 4-78 Preference

The fields that can be configured are described below:

Parameter	Description
Interval	Enter the SIM topology display refresh interval value here. The range is from 10 to 300.
Show All	Select this option to display all available SIM devices in the topology.
Show Member Only	Select this option to only display SIM member devices in the topology.

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

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

Group

Add to Group

Select a Candidate Switch (CaS) from the list and then select **Add to Group** on the **Group** menu to add the selected CaS to the SIM group. Password authentication is required when a CaS is added to the SIM group.

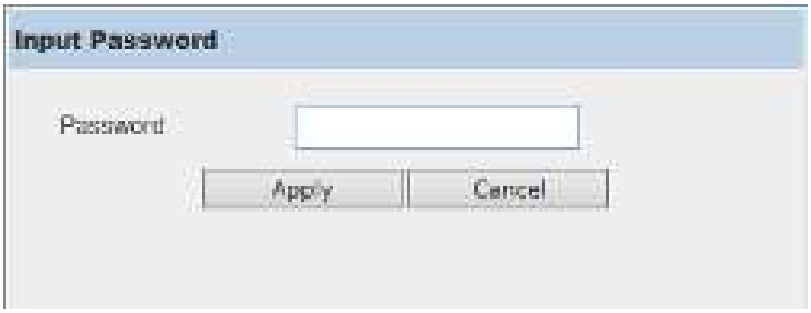


Figure 4-79 Add to Group (Input Password)

The fields that can be configured are described below:

Parameter	Description
Password	Enter the password of the CaS.

Click the **Apply** button to add the CaS to the SIM group.

Click the **Cancel** button to discard the addition and return to the Topology window.

Remove from Group

Select a Member Switch (MS) from the list and then select **Remove from Group** on the **Group** menu to remove the selected MS from the SIM group.

Device

Configure

Select a device from the list and then select **Configure** on the **Device** menu to connect to the Web User Interface (if available) on the selected device.

View

Refresh

On the **View** menu, select **Fresh** to refresh the items displayed in the page.

Topology

On the **View** menu, select **Topology** to view the following:

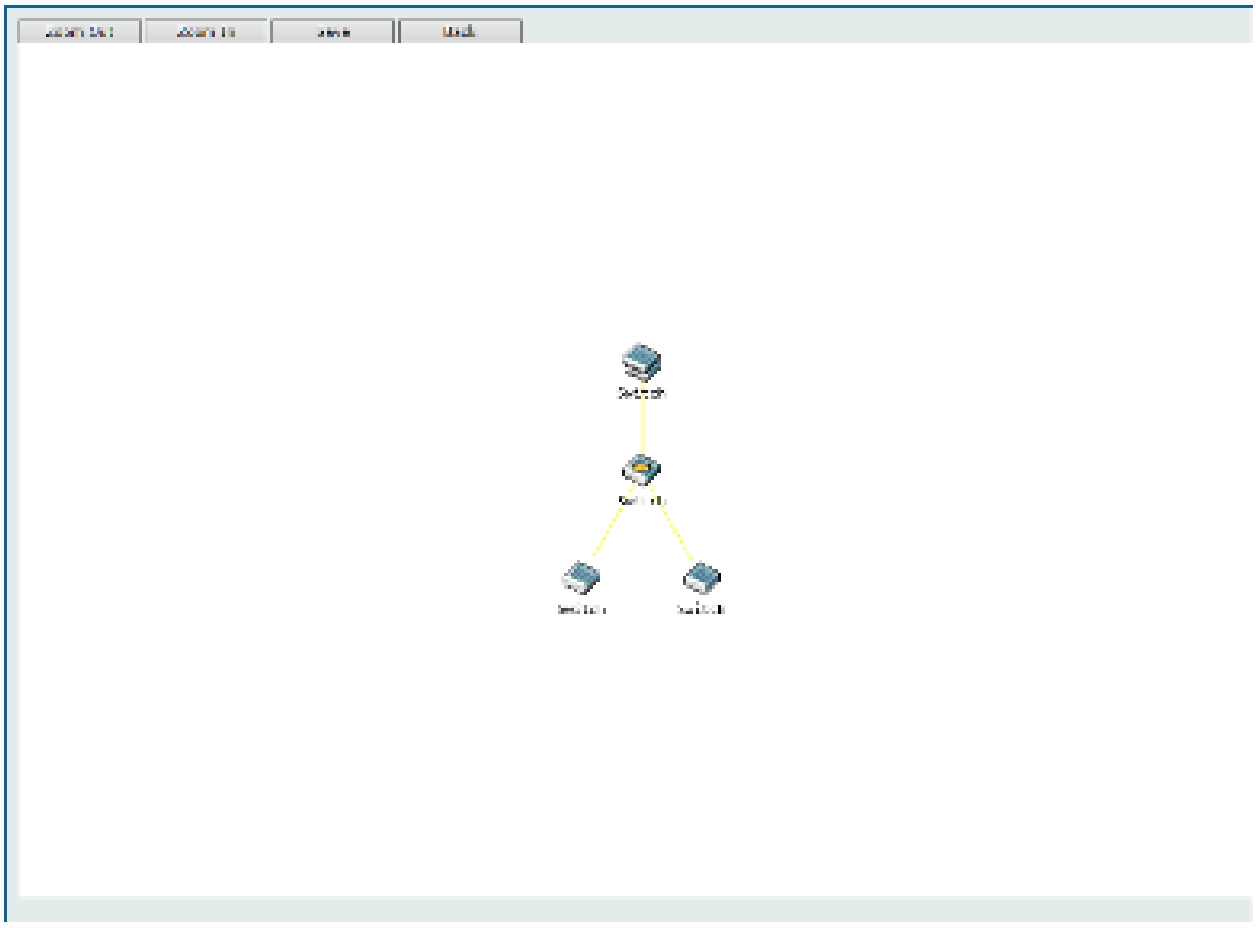


Figure 4-80 Topology Window

Click the **Zoom In** button enlarge the size of the displayed items.

Click the **Zoom Out** button reduce the size of the displayed items.

Click the **Save** button to save the display.

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

This window will display how the devices within the SIM Group connect to other groups and devices. Possible icons on this window are as follows:

Icon	Description	Icon	Description
	Group		Layer 3 Member Switch
	Layer 2 Commander Switch		Member Switch of other group
	Layer 3 Commander Switch		Layer 2 Candidate Switch
	Commander Switch of other group		Layer 3 Candidate Switch
	Layer 2 Member Switch		Unknown device
	Non-SIM devices		

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Point to a specific device in the Topology window to display more information about the device

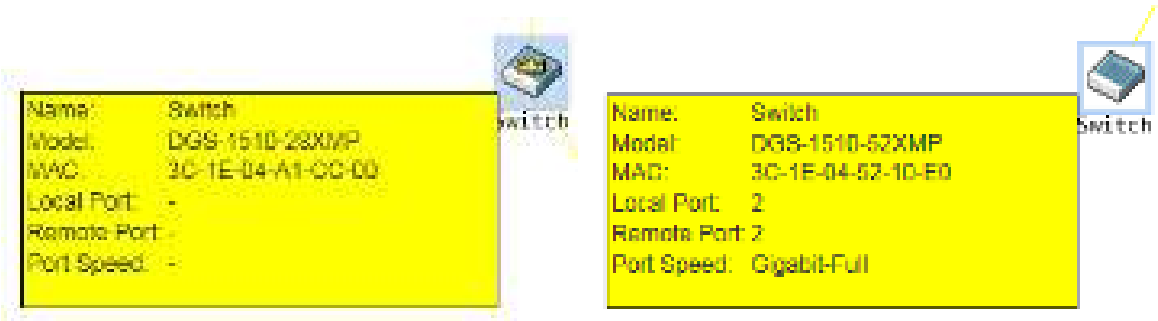


Figure 4-81 Device Information Utilizing the Tool Tip

Point to a line between two devices to display the connection speed between the two devices.

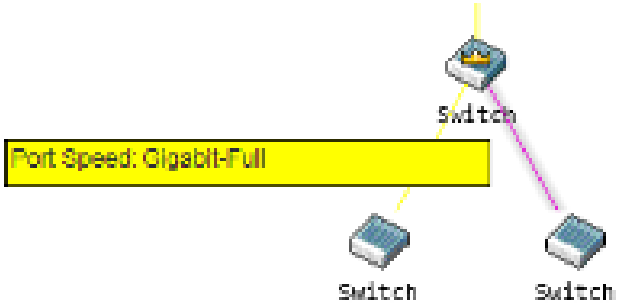
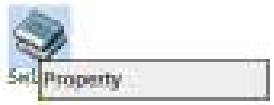
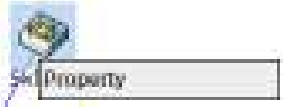


Figure 4-82 Port Speed Utilizing the Tool Tip

Righ-Click

Right-click a device to allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group	Commander Switch	Member Switch	Candidate Switch
			

The fields that can be configured are described below:

Parameter	Description
Property	Specifies to display more information about the device.
Configure	(Member Switch Only) Specifies to connect to the Web User Interface (if available) on the selected device.
Add to Group	(Candidate Switch Only) Specifies to add the selected CaS to the SIM group. Password authentication is required when a CaS is added to the SIM group.
Remove from Group	(Member Switch Only) Specifies to remove the selected MS from the SIM group.

Figure 4-83 Group Property

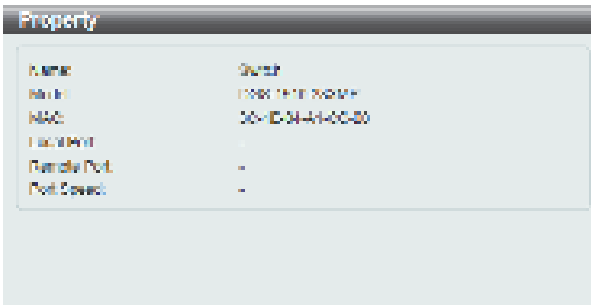


Figure 4-84 Commander Switch Property

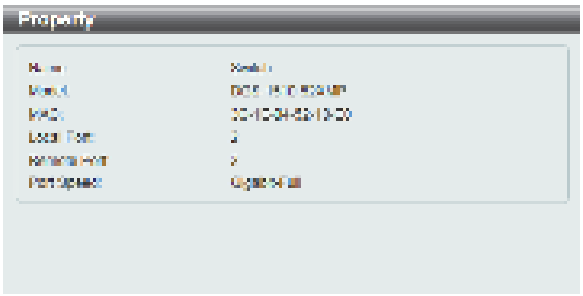


Figure 4-85 Member Switch Property

Figure 4-86 Candidate Switch Property

The fields displayed are described below:

Parameter	Description
Name	Displays the Device Name of the Switches in the SIM group configured. If the device is not configured with a name, it will be given the name default and tagged with the last six digits of the MAC address to identify it.

Parameter	Description
Model	Displays the model name of the Switch.
MAC	Displays the MAC address of the Switch.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS.

Help

About

On the **Help** menu, select **About** to display the SIM Copyright information and release date.

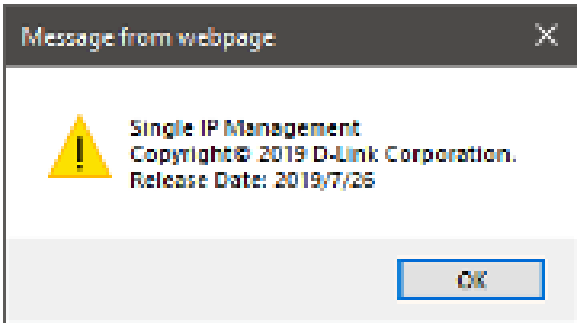


Figure 4-87 About Window

Firmware Upgrade

This window is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table.

To view the following window, click **Management > Virtual Stacking (SIM) > Firmware Upgrade**, as shown below:

Figure 4-88 Firmware Upgrade Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path\Filename	Enter the path and file name.

Click the **Download** button to update the firmware.

To specify a certain Switch for firmware download, tick its corresponding check box.

Configuration File Backup/Restore

This window is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table.

To view the following window, click **Management > Virtual Stacking (SIM) > Configuration File Backup/Restore**, as shown below:

Figure 4-89 Configuration File Backup/Restore Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path\Filename	Enter the path and file name.

Click the **Restore** button to update the configuration from a TFTP server to the member switch.

Click the **Backup** button to back up the configuration file to a TFTP server.

Upload Log File

This window is used to upload log files from SIM member switches to a specified PC.

To view the following window, click **Management > Virtual Stacking (SIM) > Upload Log File**, as shown below:

Figure 4-90 Upload Log File Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path\Filename	Enter the path and file name.

Click the **Upload** button to initiate the file transfer.

D-Link Discovery Protocol

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

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

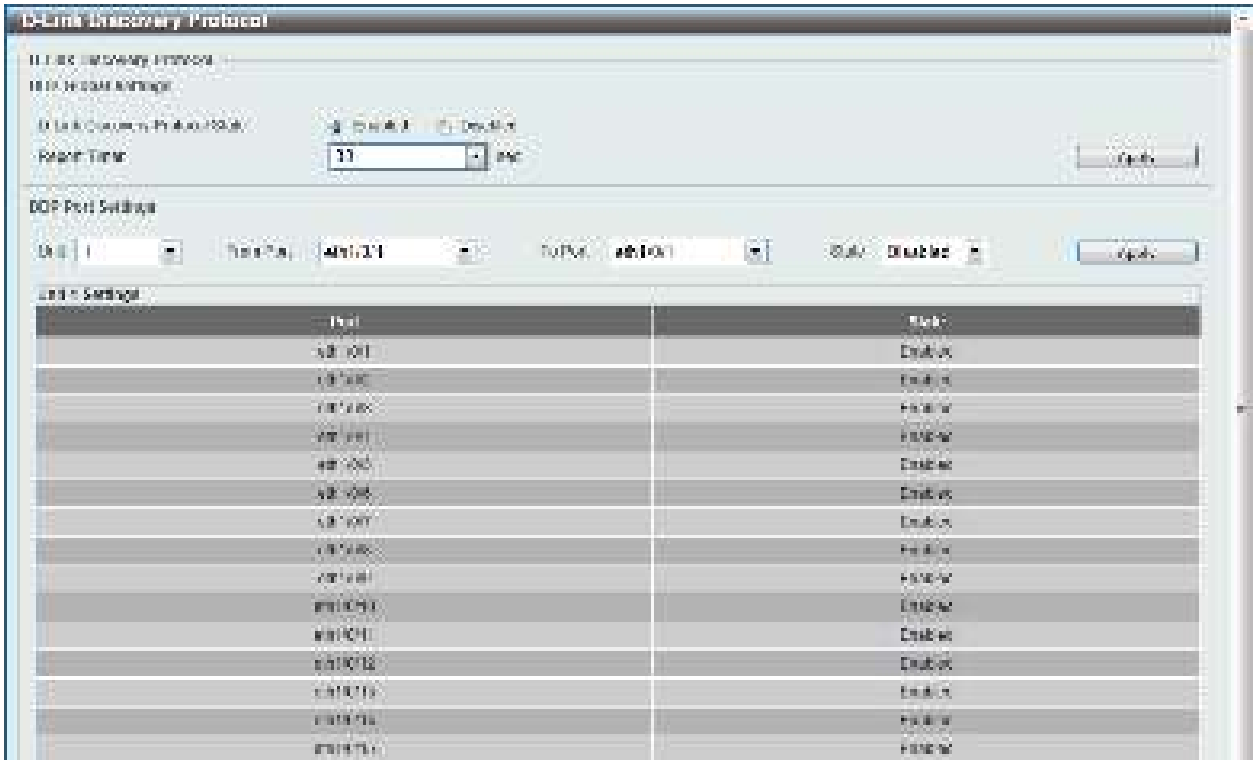


Figure 4-91 D-Link Discovery Protocol Window

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.

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

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable DDP port state.

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

5. Layer 2 Features

FDB
VLAN
STP
ERPS (G.8032)
Loopback Detection
Link Aggregation
L2 Multicast Control
LLDP

FDB

Static FDB

Unicast Static FDB

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

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

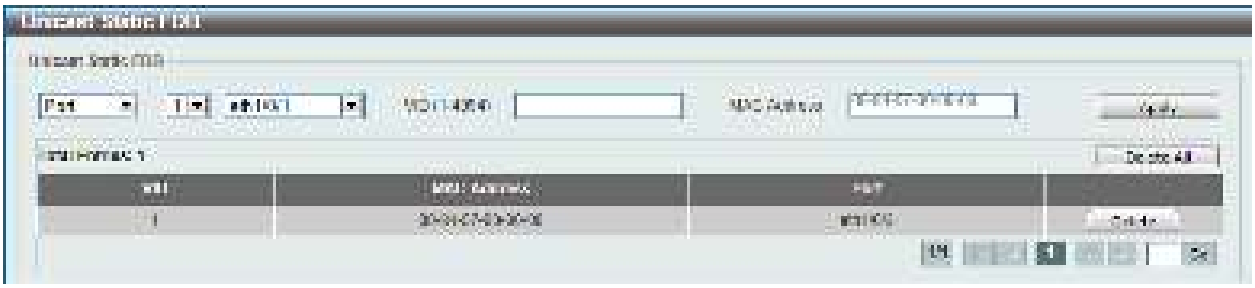


Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Port / Drop	Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. When selecting **Port**, select the switch unit and port number.
Unit Number	Select the switch unit that will be used for this configuration here, when **Port** is selected in the previous drop-down list.
Port Number	Select the port number used here, when **Port** is selected in the previous drop-down list.
VID	Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address	Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address.

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

Click the **Delete All** button to delete all the entries found in the display table.

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

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

Multicast Static FDB

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

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

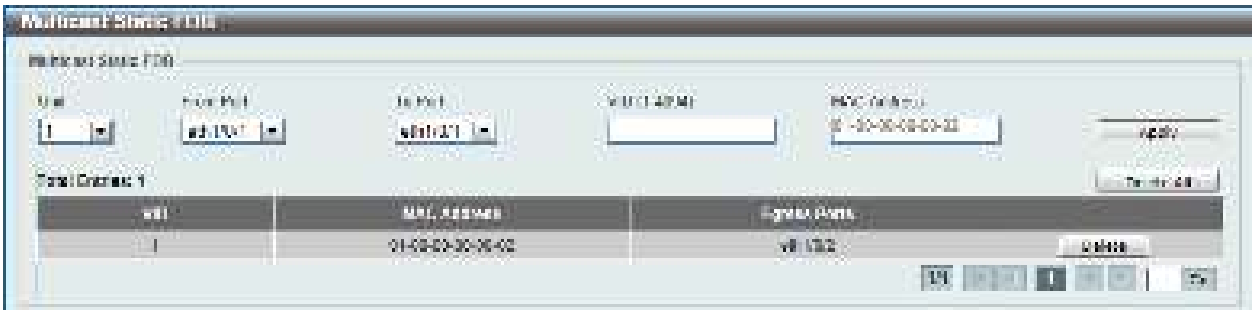


Figure 5-2 Multicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
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 destination MAC address should start with 01. For example, 01-00-00-00-00-02.

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

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

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

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

MAC Address Table Settings

This window is used to view and configure the MAC address table's global settings.

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

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

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table'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.
Aging Destination Hit	Select to enable or disable the aging destination hit function.

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.

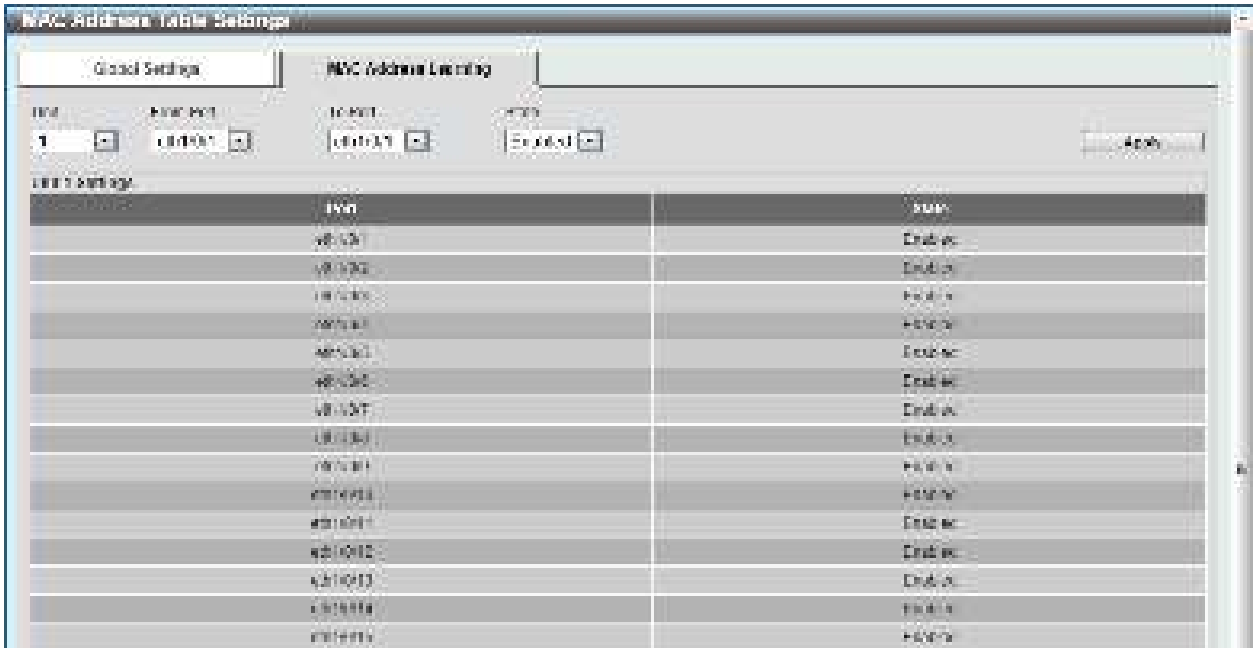


Figure 5-4 MAC Address Table Settings (MAC Address Learning) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the 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:

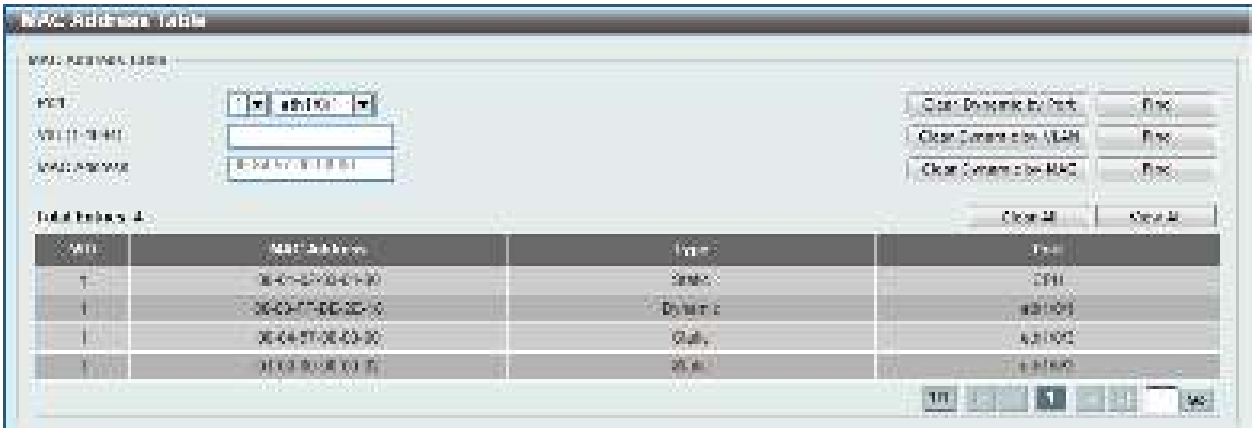


Figure 5-5 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the switch unit and the port that will be used for this configuration here.
VID	Enter the VLAN ID that will be used for this configuration here.
MAC Address	Enter the MAC address that will be used for this configuration here.

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

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

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

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

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

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

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

MAC Notification

This window is used to view and configure MAC notification.

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

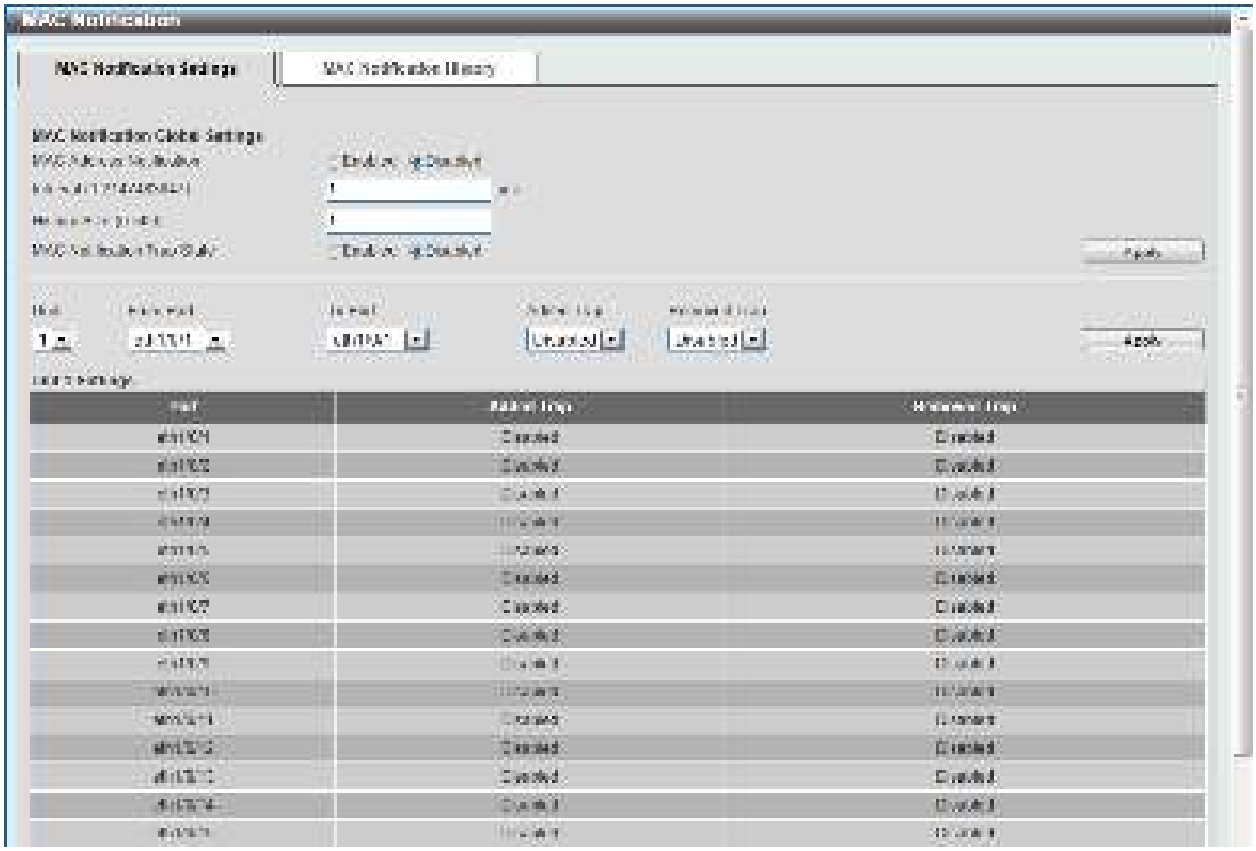


Figure 5-6 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch.
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1.
MAC Notification Trap State	Select this option to enable or disable the MAC notification trap state.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the range of ports that will be used for this configuration here.
Added Trap	Select this option to enable or disable the added trap for the port(s) selected.
Removed Trap	Select this option to enable or disable the removed trap for the port(s) selected.

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

After clicking the **MAC Notification History** tab, the following page will be available.

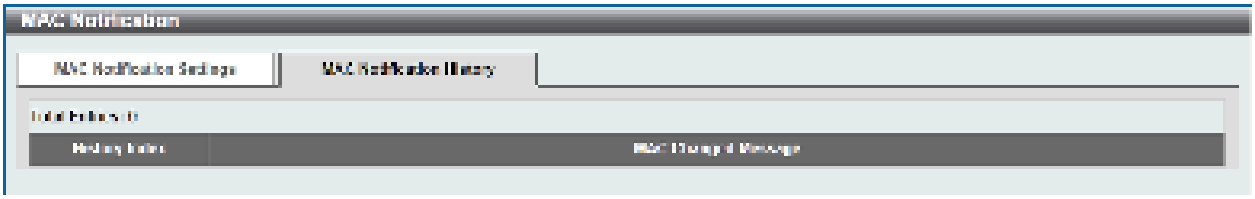


Figure 5-7 MAC Notification (MAC Notification History) Window

A list of MAC notification messages will be displayed.

VLAN

VLAN Configuration Wizard

This window is used to start the VLAN configuration wizard.

Create/Configure VLAN

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

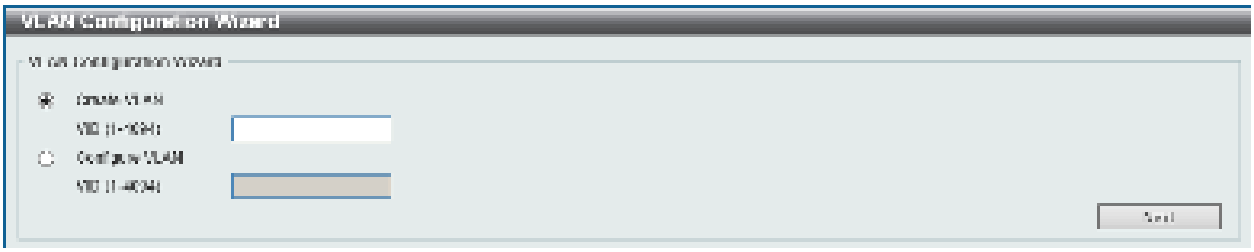


Figure 5-8 VLAN Configuration Wizard (Step 1) Window

The fields that can be configured are described below:

Parameter	Description
Create VLAN	Select this option to create a new VLAN. • **VID** - Enter the VLAN ID here. The range is from 1 to 4094.
Configure VLAN	Select this option to configure an existing VLAN. • **VID** - Enter the VLAN ID here. The range is from 1 to 4094.

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

Create VLAN

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

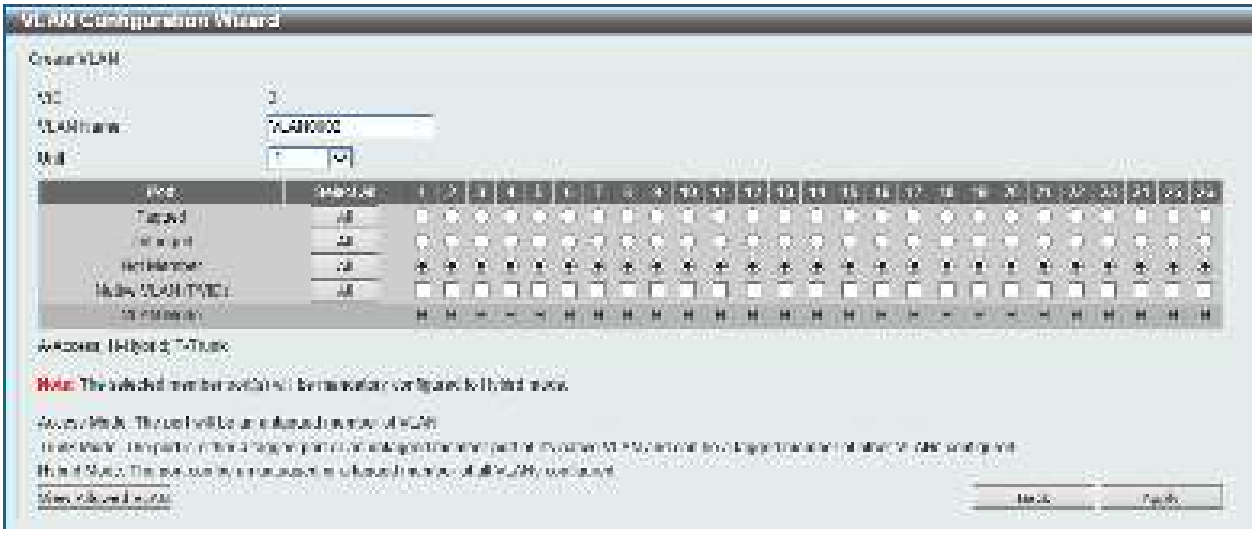


Figure 5-9 VLAN Configuration Wizard (Create VLAN) Window

The fields that can be configured are described below:

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

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

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

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

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

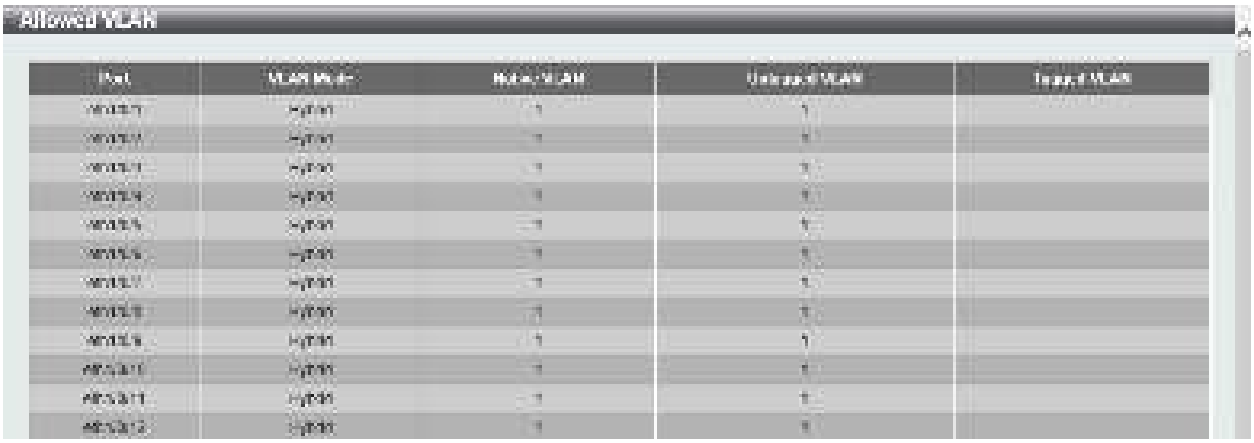


Figure 5-10 Allowed VLAN Window

Configure VLAN

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

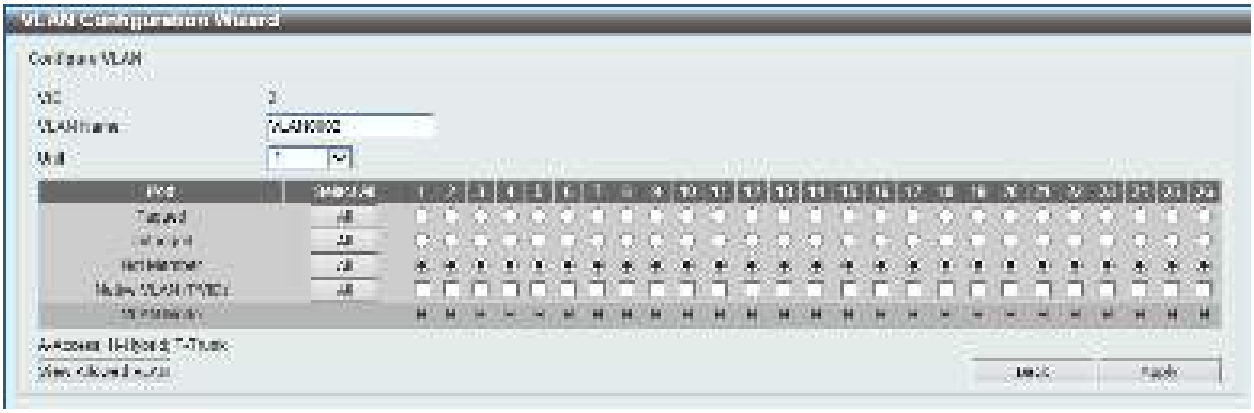


Figure 5-11 VLAN Configuration Wizard (Configure VLAN) Window

The fields that can be configured are described below:

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

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

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

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

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

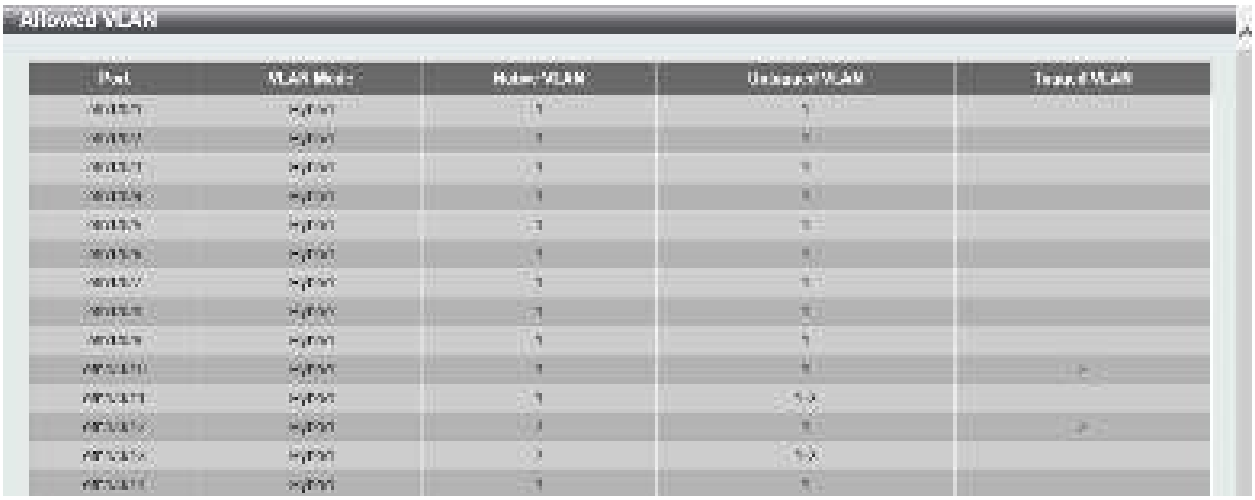


Figure 5-12 Allowed VLAN Window

802.1Q VLAN

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

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

Figure 5-13 802.1Q 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.

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

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

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

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

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.

VLAN Interface

VLAN Interface Settings

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:

Figure 5-14 VLAN Interface 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.

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

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

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

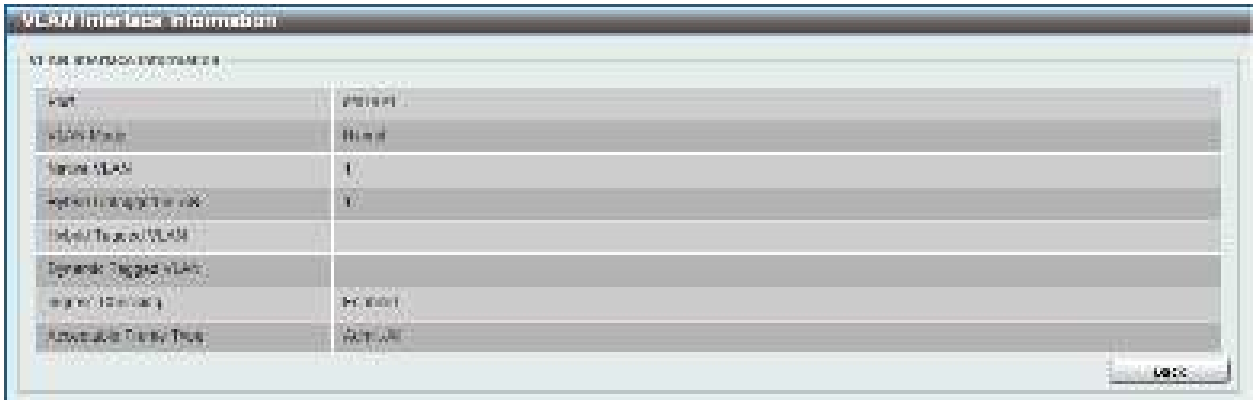


Figure 5-15 VLAN Interface Information Window

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

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

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

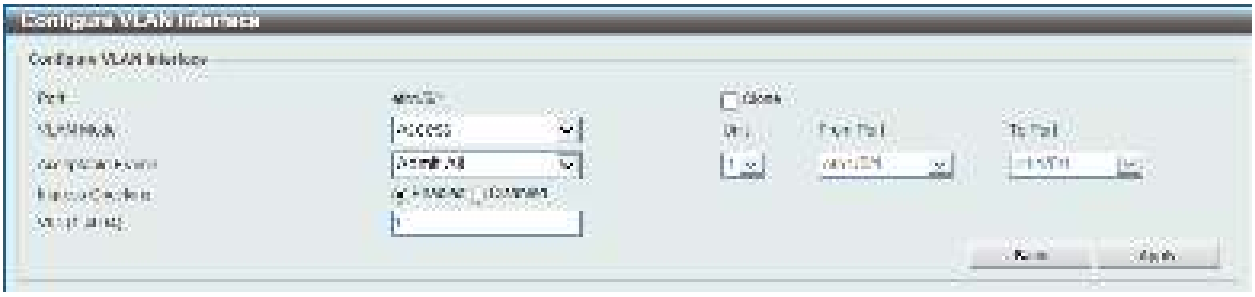


Figure 5-16 Configure VLAN Interface - Access Window

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.
Clone	Tick this option to apply the configuration to the specified ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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.

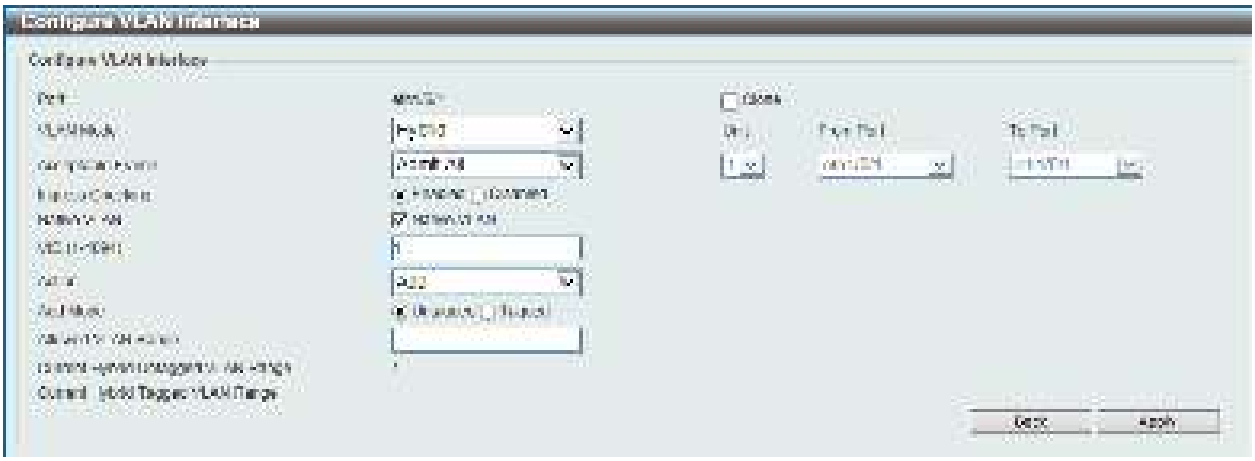


Figure 5-17 Configure VLAN Interface - Hybrid Window

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**.

Parameter	Description
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select 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.
Clone	Tick this option to apply the configuration to the specified ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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.

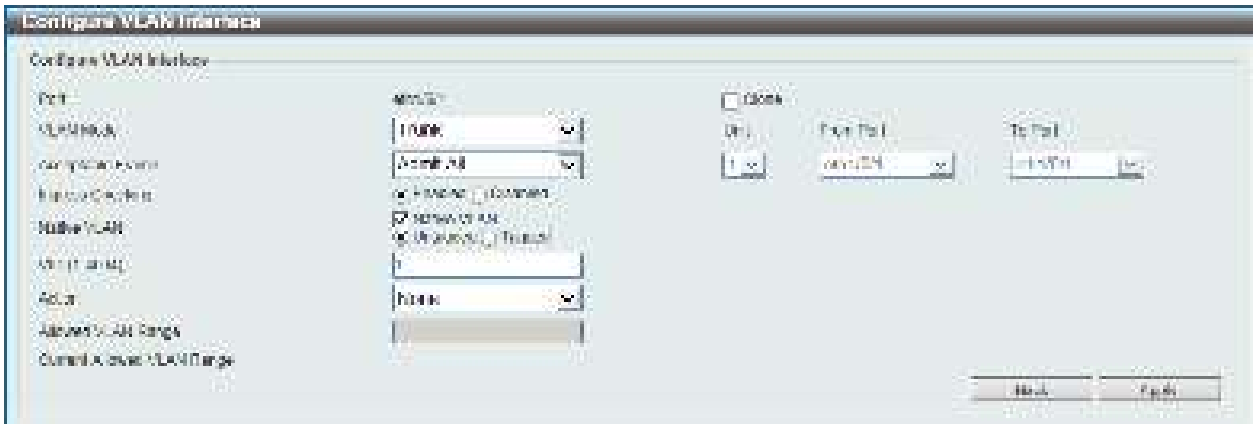


Figure 5-18 Configure VLAN Interface - Trunk Window

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. 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.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **All**, **Add**, **Remove**, **Except**, and **Replace**.
Allowed VLAN Range	Enter the allowed VLAN range information here.
Clone	Tick this option to apply the configuration to the specified ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

Port Summary

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

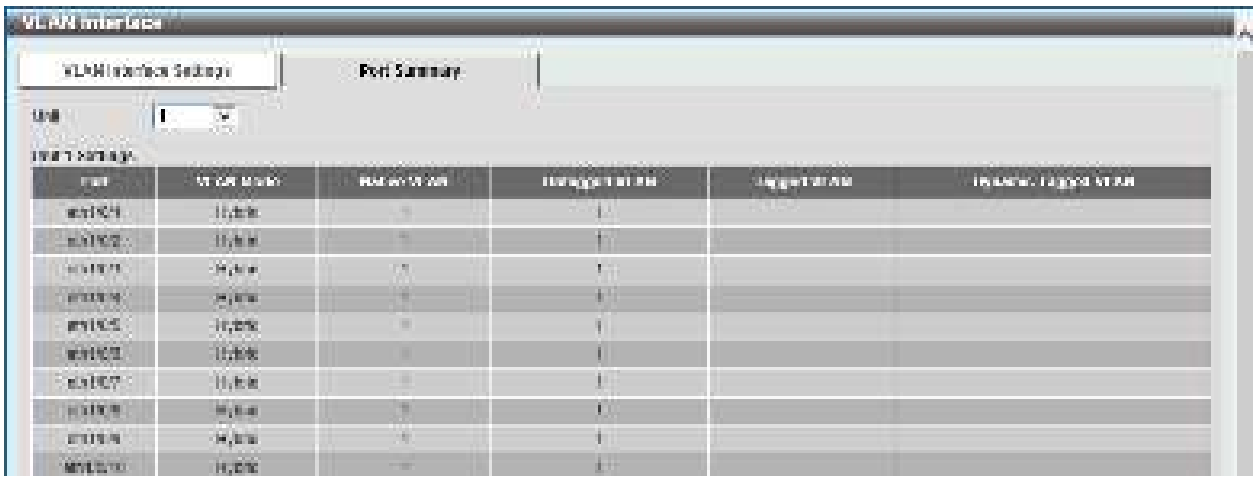


Figure 5-19 VLAN Interface Port Summary Window

802.1v Protocol VLAN

Protocol VLAN Profile

This window is used to view and configure the Protocol VLAN profile.

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

Figure 5-20 9 Protocol VLAN Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the profile ID that will be created here.

Parameter	Description
Frame Type	Select the frame type here. Options to choose from are **Ethernet2**, **SNAP** and **LLC**.
Ether Type	Enter the Ethernet type in hexadecimal form.

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

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

Protocol VLAN Profile Interface

This window is used to view and configure the Protocol VLAN profile interface.

To view the following window, click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface**, as shown below:

Figure 5-21 Protocol VLAN Profile Interface Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the switch unit and the port that will be used for this configuration here.
Profile ID	Select the ID of the protocol group.
VID	Enter the VLAN ID of the Protocol VLAN.
Priority	Select the priority of the Protocol VLAN.

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

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

GVRP

GVRP Global

This window is used to view and configure the GARP VLAN Registration Protocol (GVRP) global settings.

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

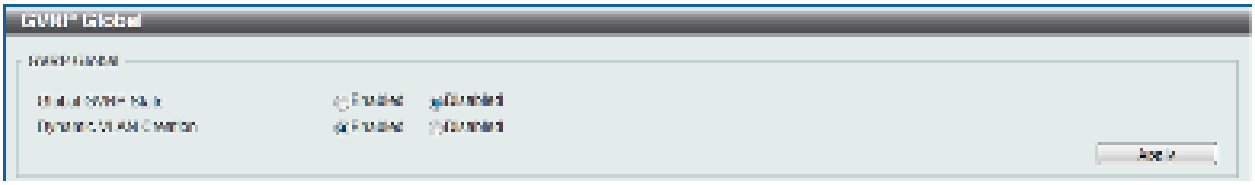


Figure 5-22 GVRP Global Window

The fields that can be configured are described below:

Parameter	Description
Global GVRP State	Select this option to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select this option to enable or disable the dynamic VLAN creation function here.

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

GVRP Port

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

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

Figure 5-23 GVRP Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
GVRP Status	Select this option to enable or disable the GVRP port status. This enables the port to dynamically become a member of a VLAN. By default, this option is disabled.
Join Time	Enter the Join Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 1000 centiseconds.

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

GVRP Advertise VLAN

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

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

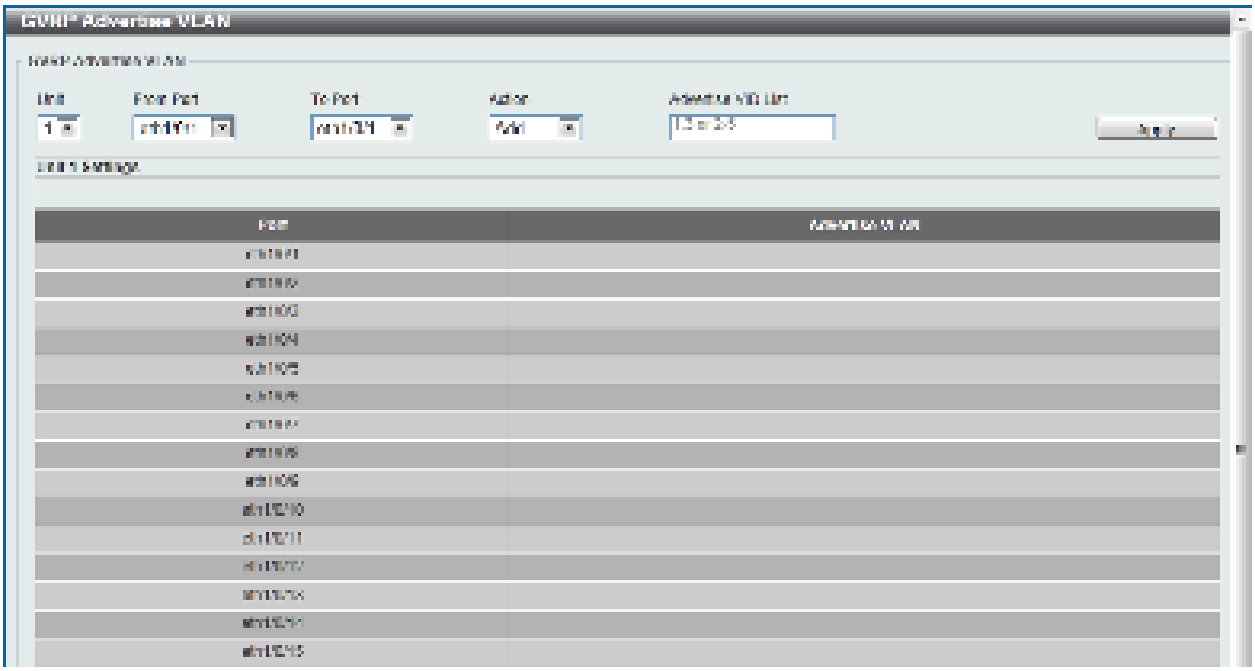


Figure 5-24 GVRP Advertise VLAN Window

The fields that can be configured are described below:

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

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

GVRP Forbidden VLAN

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

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

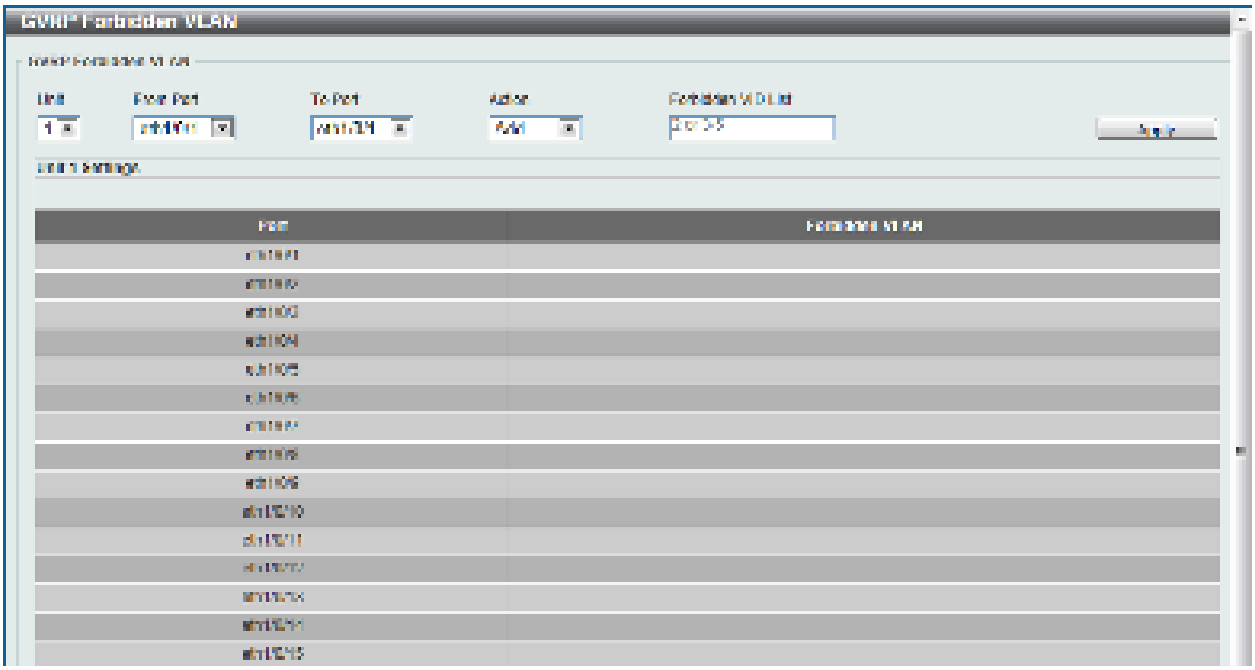


Figure 5-25 GVRP Forbidden VLAN Window

The fields that can be configured are described below:

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

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

GVRP Statistics Table

This window is used to display GVRP statistics information.

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

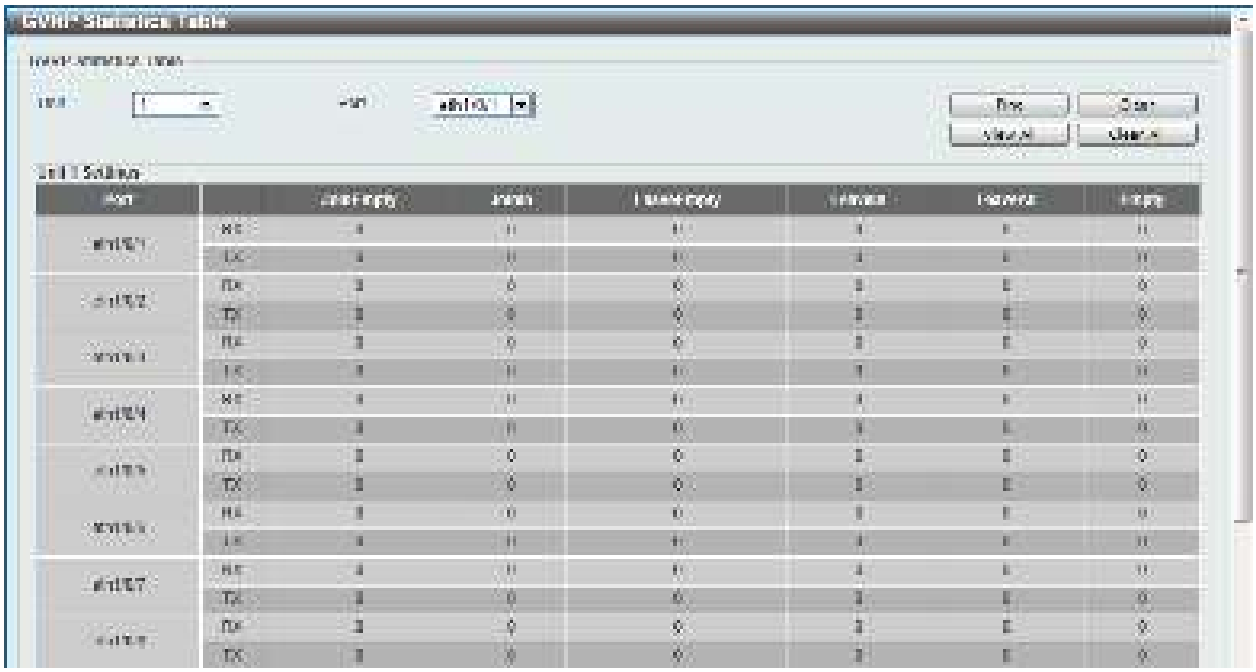


Figure 5-26 GVRP Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port number of which GVRP statistic information will be displayed.

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

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

Click the **View All** button to view all GVRP statistic information.

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

Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

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

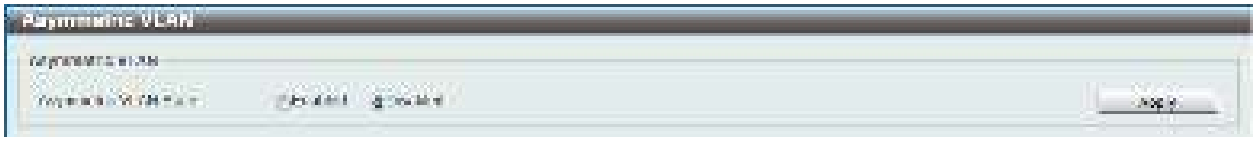


Figure 5-27 Asymmetric VLAN Window

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.

MAC VLAN

This window is used to view and configure MAC-based VLAN settings.

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

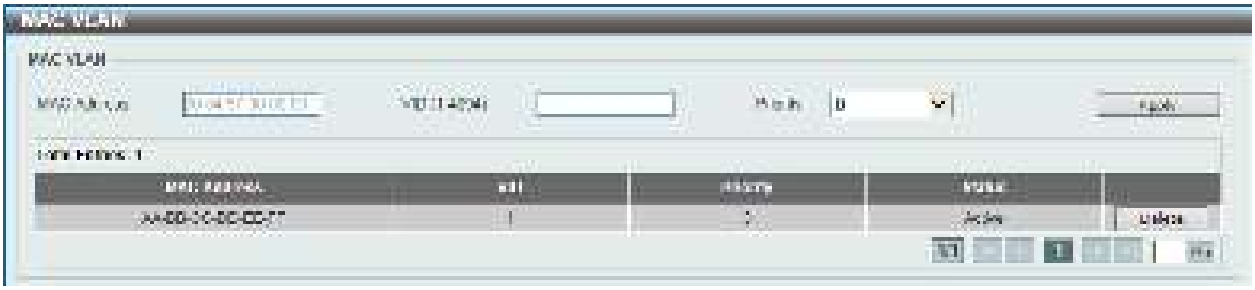


Figure 5-28 MAC VLAN Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address that will be used for this configuration here.
VID	Enter the VLAN ID for the MAC-based VLAN.
Priority	Select the priority of the MAC-based VLAN.

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.

L2VLAN Interface Description

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

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

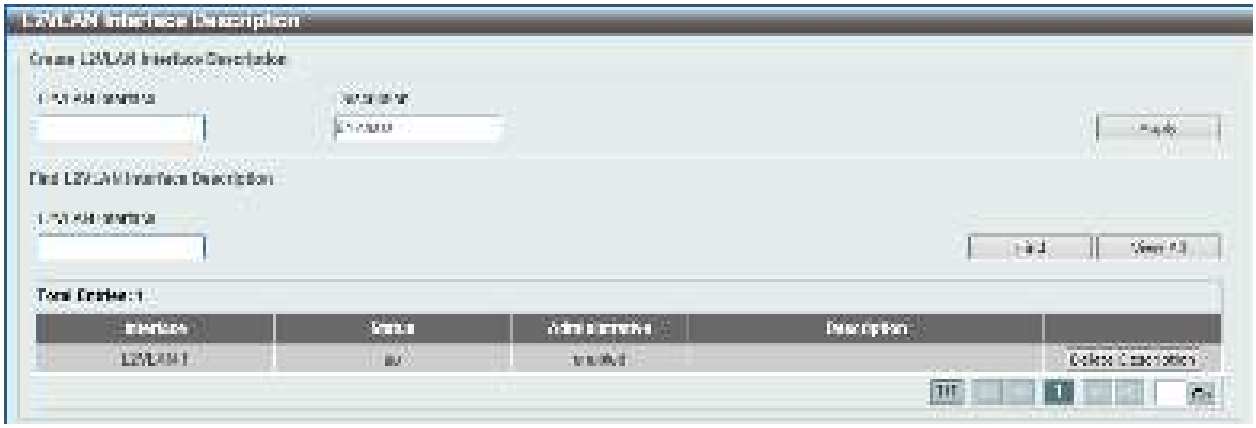


Figure 5-29 L2VLAN Interface Description Window

The fields that can be configured for **Create L2VLAN Interface Description** are described below:

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

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

The fields that can be configured for **Find L2VLAN Interface Description** are described below:

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

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

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

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

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

Auto Surveillance VLAN

Auto Surveillance Properties

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

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

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

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

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

Figure 5-30 Auto Surveillance Properties Window

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

Parameter	Description
Surveillance VLAN State	Select this option to enable or disable the surveillance VLAN state
Surveillance VLAN ID	Enter the surveillance VLAN ID. The range is from 2 to 4094.
Surveillance VLAN CoS	Select the priority of the surveillance VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stop.
ONVIF Discover Port	Enter the TCP/UDP port number here. The range is either 554, or from 1025 to 65535. This is used to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs

Parameter	Description
	by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.

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

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

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

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

MAC Settings and Surveillance Device

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

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

Figure 5-31 User -defined MAC Settings Window

The fields that can be configured are described below:

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

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

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

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

Figure 5-32 Auto Surveillance VLAN Summary 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.

ONVIF IP-Camera Information

This window is used to display ONVIF IP camera information.

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

Figure 5-33 ONVIF IP-Camera Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used in the display here.

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

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

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

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

Figure 5-34 ONVIF IP-Camera Information (More Detail) Window

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

Figure 5-35 ONVIF IP-Camera Information (Edit) Window

The fields that can be configured are described below:

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

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

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

ONVIF NVR Information

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

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

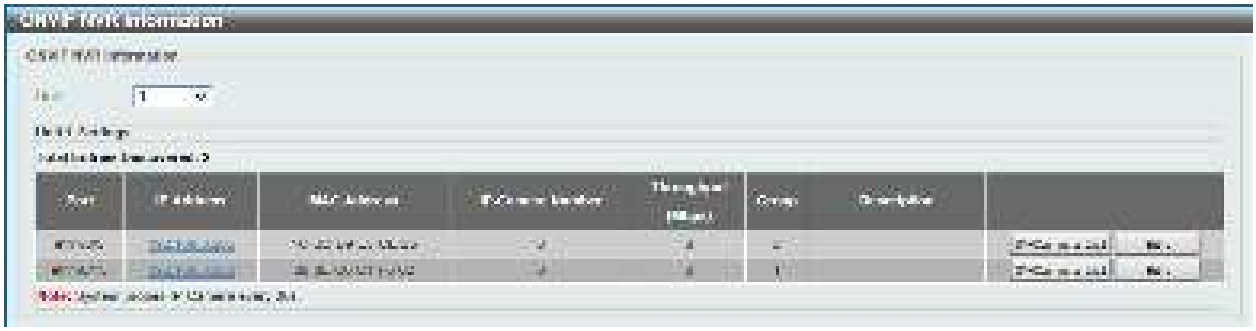


Figure 5-36 ONVIF NVR Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used in the display here.

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

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

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

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

Figure 5-37 ONVIF NVR Information (IP-Camera List) Window

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

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

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

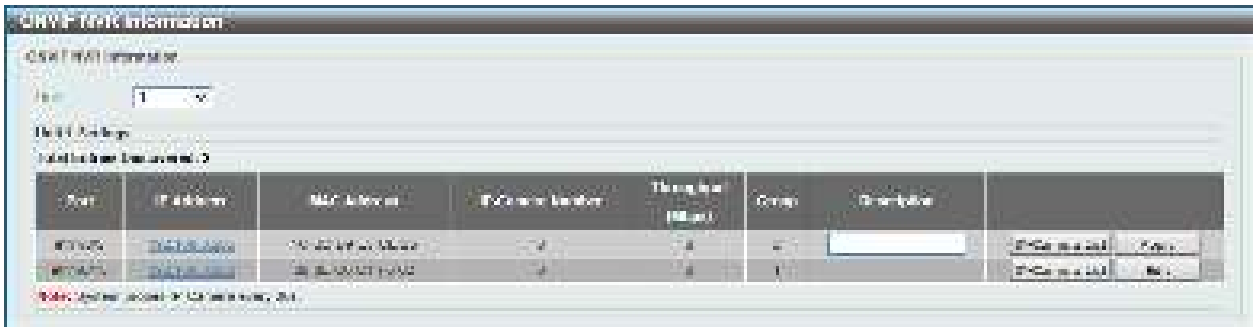


Figure 5-38 ONVIF NVR Information (Edit) Window

The additional fields that can be configured are described below:

Parameter	Description
Description	Enter the description for this NVR here.

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

Voice VLAN

Voice VLAN Global

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

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

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

Figure 5-39 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 shown below:

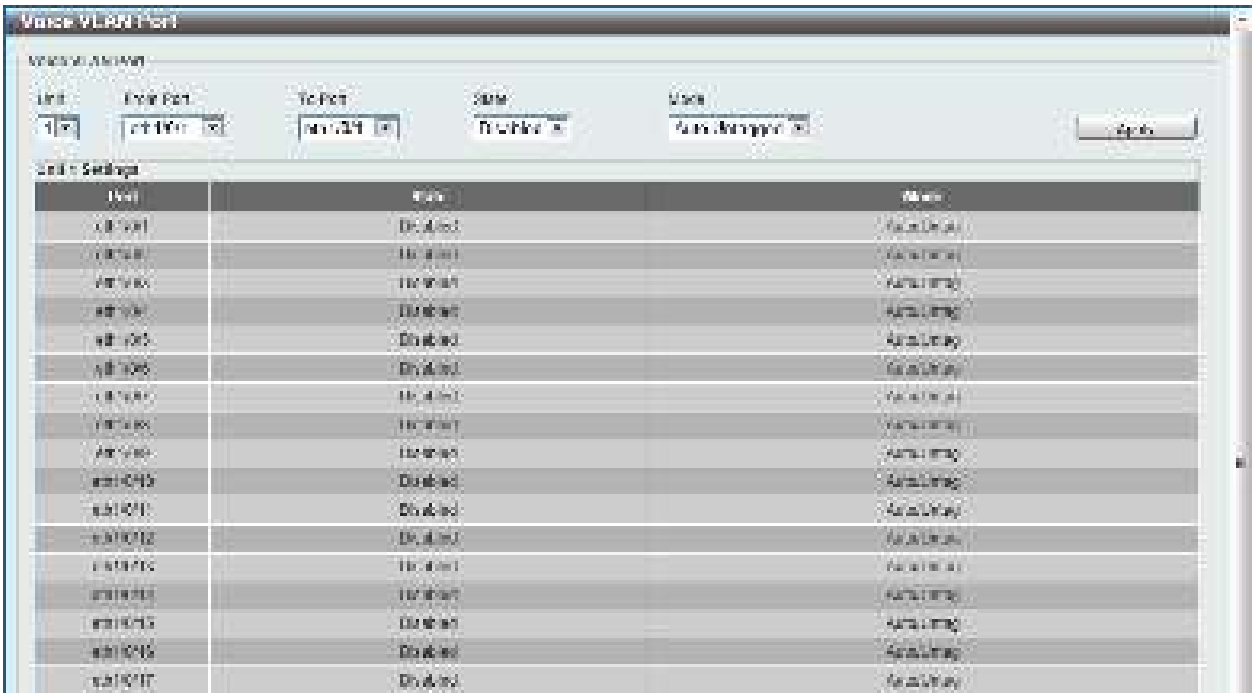


Figure 5-40 Voice VLAN Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select 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 shown below:

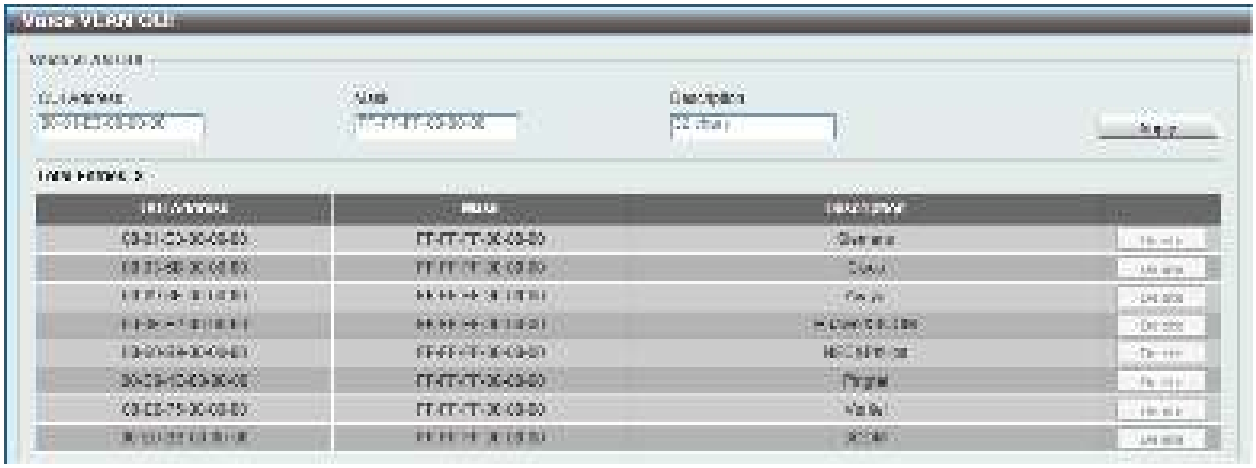


Figure 5-41 Voice VLAN OUI Window

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 shown below:

Figure 5-42 Voice VLAN Device 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.

Voice VLAN LLDP-MED Device

This window displays the voice VLAN LLDP-MED voice devices connected to the Switch.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device**, as shown below:

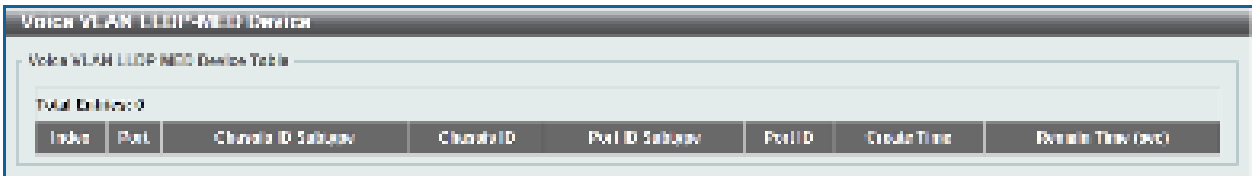


Figure 5-43 Voice VLAN LLDP-MED Device Window

STP

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

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP, or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

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

- A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
- A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;

- A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

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

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

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however, the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way, this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1D-1998 and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

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

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*Listening*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) 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 workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

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

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

MSTP or RSTP can interoperate with legacy equipment and 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:

- On the switch level, the settings are globally implemented.
- 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 > STP > STP Global Settings**, as shown below:

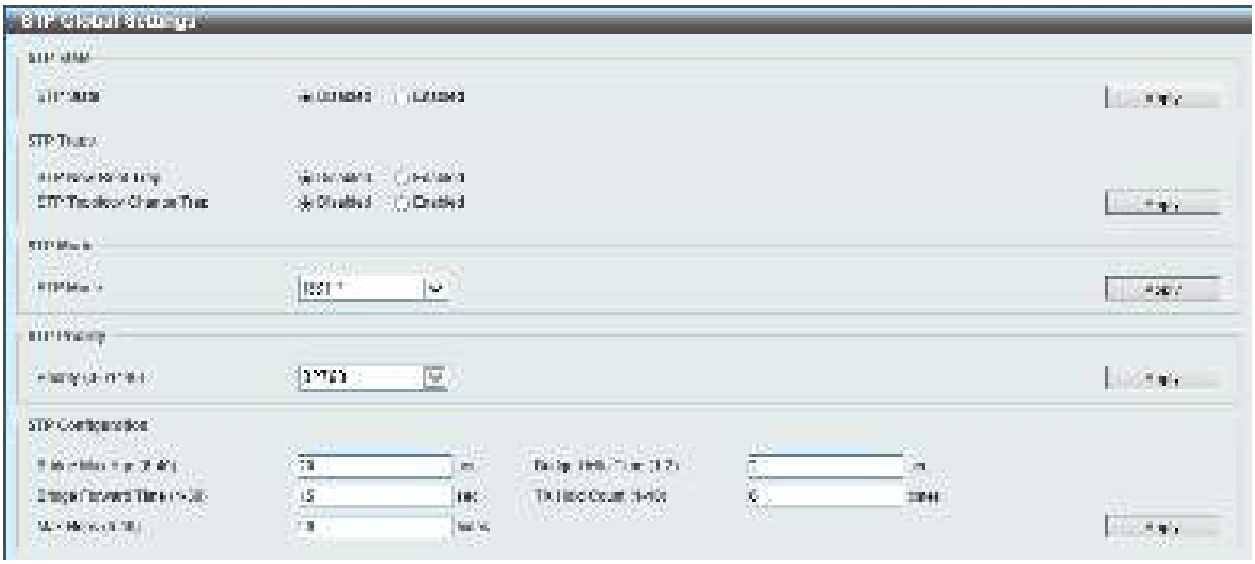


Figure 5-44 STP Global Settings Window

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 Traps** are described below:

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

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

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

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

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

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

Parameter	Description
Priority	Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

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

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

Parameter	Description
Bridge Max Age	Enter the bridge's maximum age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The maximum age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting **RSTP**/**STP** as the **STP Mode**, this parameter will be available. Enter the bridge's hello time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis.
Bridge Forward Time	Enter the bridge's forwarding time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.

Parameter	Description
TX Hold Count	Enter the transmit hold count value here. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. This value must be between 6 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out.

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

STP Port Settings

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

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

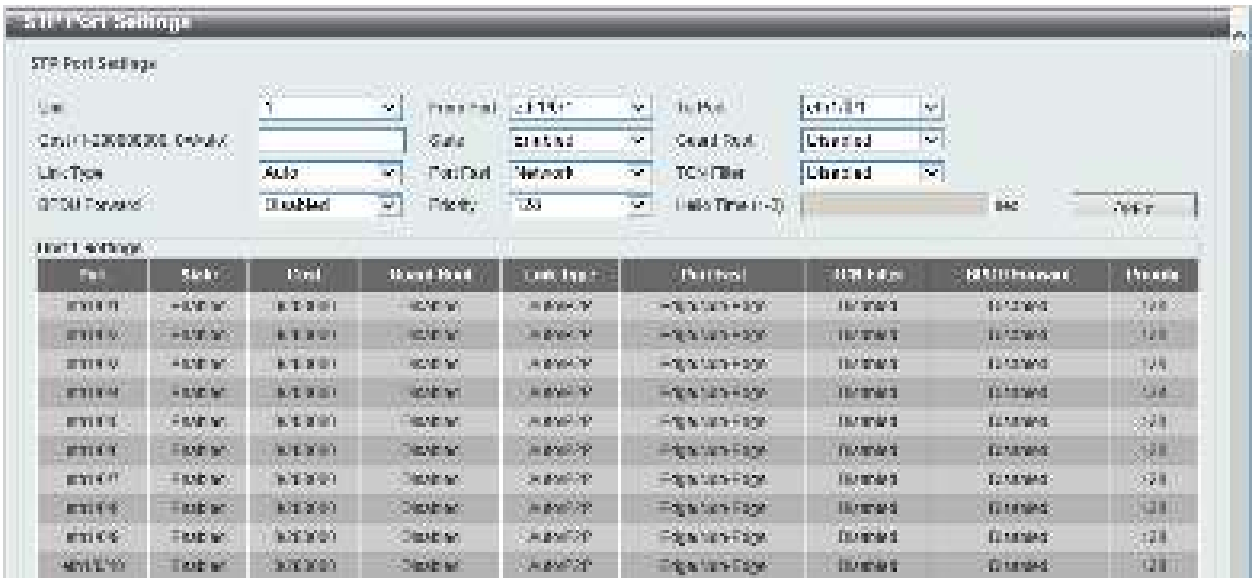


Figure 5-45 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Cost	Enter the cost value here. This value must be between 1 and 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is **0** (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000 and the default port cost for a Gigabit port is 20000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.

Parameter	Description
Guard Root	Select to enable or disable the guard root function.
Link Type	Select the link type option here. Options to choose from are **Auto**, **P2P**, and **Shared**. A full-duplex port is considered to have a point-to-point (**P2P**) connection. On the opposite, a half-duplex port is considered to have a **Shared** connection. The port cannot transit into the forwarding state rapidly by setting the link type to **Shared**. By default, this option is **Auto**.
Port Fast	Select the port fast option here. Options to choose from are: • **Network** - The port remains 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. • **Disabled** - The port is always in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. • **Edge** - The port directly changes 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. This is the default option.
TCN Filter	Select to enable or disable the TCN filter option. Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly, because those bridges are not under the full control of the administrator. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is **Disabled**.
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is **Disabled**.
Priority	Select the priority value here. Options to choose from are **0** to **240**. By default, this option is **128**. A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between 1 and 2 seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.

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

MST Configuration Identification

This window is used to view and configure the MST configuration identification settings. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially

possesses one CIST, or Common Internal Spanning Tree, of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

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

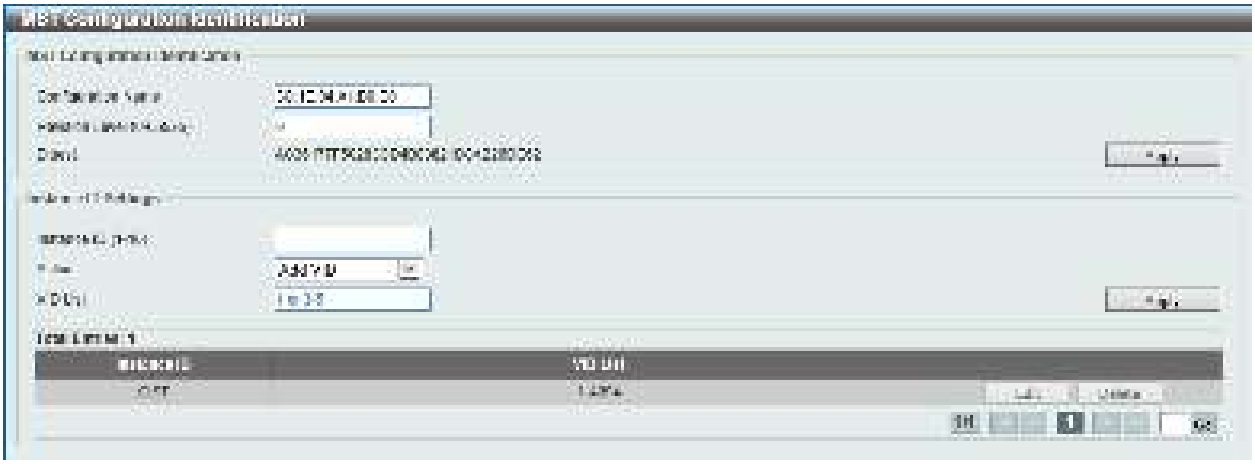


Figure 5-46 MST Configuration Identification Window

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

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

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

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

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 16.
Action	Select the action that will be taken here. Options to choose from are **Add VID** and **Remove VID**.
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

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

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

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

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

STP Instance

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

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

Figure 5-47 STP Instance Window

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

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

MSTP Port Information

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

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

Figure 5-48 MSTP Port Information 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.
Port	Select the port number that will be cleared here.

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

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

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

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

ERPS (G.8032)

For more information, refer to **Appendix E - ERPS Information**.

ERPS

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

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

Figure 5-49 ERPS Window

The fields that can be configured are described below:

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

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

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

Click the **Edit Instance** button to configure the ERP instance.

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

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

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

Figure 5-50 ERPS (Edit Ring) Window

The fields that can be configured are described below:

Parameter	Description
Instance ID	Select the checkbox and enter the ERP instance number here. This value must be between 1 and 32. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
Sub Ring Name	Select the checkbox and enter the physical ring's sub-ring name here. This name can be up to 32 characters long. Select the **Specify** radio button to configure this parameter as per normal.

Parameter	Description
	Select the **None** radio button to revert this parameter to the default setting.
Port0	Select the checkbox and then select the switch's unit ID and the port number that will be the first ring port of the physical ring. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
Port1	Select the checkbox and then select the switch's unit ID and the port number that will be the second ring port of the physical ring. Select the **None** option, from the drop-down menu, specifies that the inter-connected node is a local node endpoint of an open ring. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.

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

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

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

Figure 5-51 ERPS (Edit Instance) Window

The fields that can be configured are described below:

Parameter	Description
Description	Select the checkbox and enter the ERP instance's description here. This description can be up to 64 characters long. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
R-APS Channel VLAN	Select the checkbox and enter the R-APS channel VLAN's ID for the ERP instance here. The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring. This value must be between 1 and 4094. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
Inclusion VLAN List	Select the checkbox and enter the inclusion VLAN list here. A range is identified when a hyphen (-) is used. For example, VLANs 1 to 5 can be entered as 1-5. A list is identified when commas (,) are used. For example, use VLANs 1,3,5. The VLANs specified here will be protected by the ERP mechanism. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.

Parameter	Description
MEL	Select the checkbox and enter the ring MEL value of the ERP instance here. This value must be between 0 and 7. The configured MEL value of all ring nodes that participate in the same ERP instance should be identical. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
Profile Name	Select the checkbox and enter the G.8032 profile's name here that will be associated with this ERP instance. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance. This name can be up to 32 characters long. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
RPL Port	Select the checkbox and then select the RPL port option here. Options to choose from are **Port0** and **Port1**. The option selected will be configured as the RPL port.
RPL Owner	Select the checkbox and then select whether this node is the RPL owner or neighbor. Options to choose from are **Enabled** and **Disabled**. Enabling this option will specify this RPL as an owner.
Activate	Select the checkbox and then select whether or not to active this ERP instance. Options to choose from are **Enabled** and **Disabled**. Enabling this option will active this ERP instance.

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

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

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

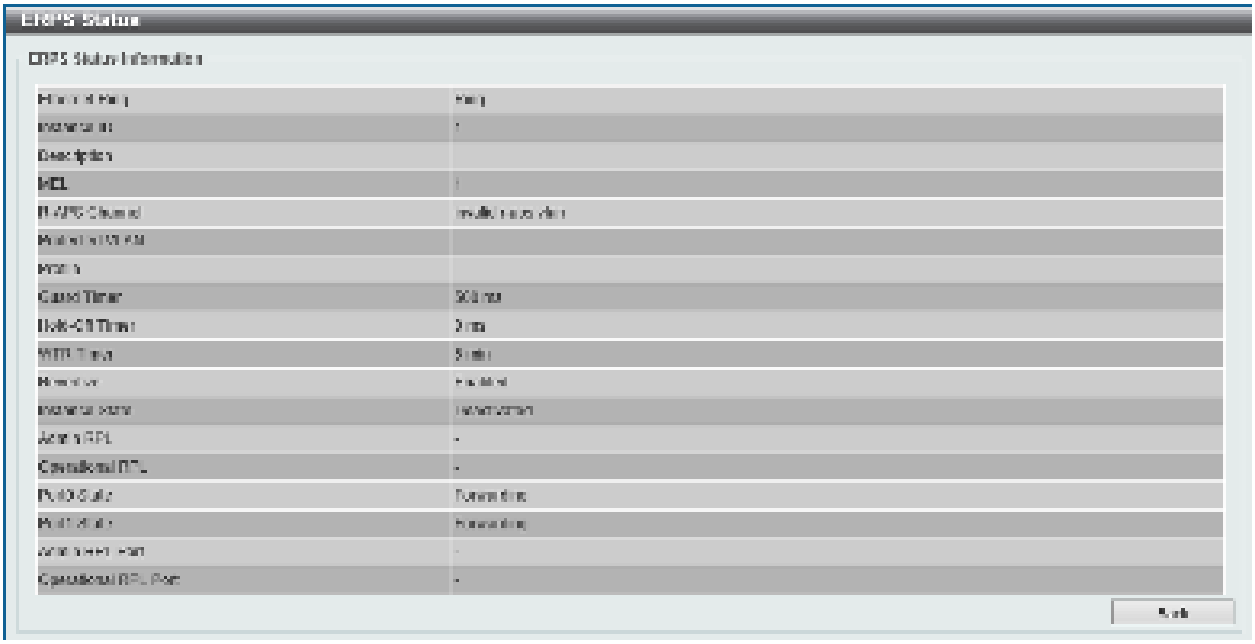


Figure 5-52 ERPS (Show Status) Window

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

ERPS Profile

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

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

Figure 5-53 ERPS Profile Window

The fields that can be configured are described below:

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

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

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

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

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

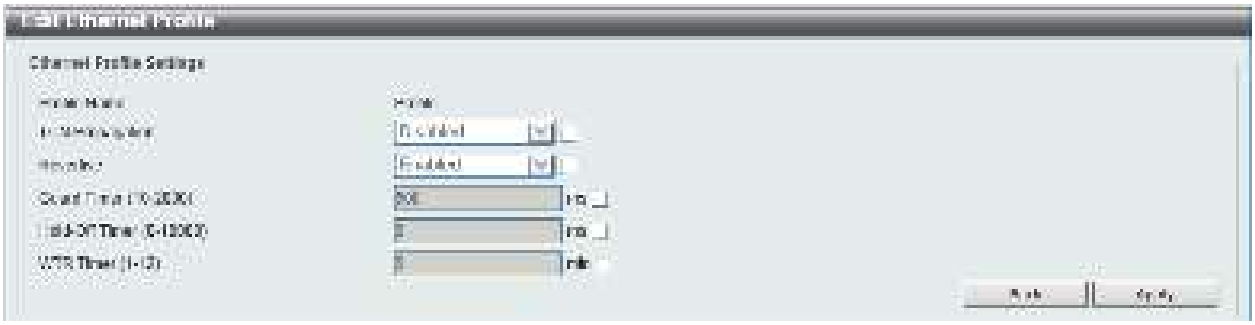


Figure 5-54 ERPS Profile (Edit) Window

The fields that can be configured are described below:

Parameter	Description
TCN Propagation	Select the checkbox and then select the TCN propagation state. Options to choose from are **Enable** and **Disabled**. This function is used to enable the propagation of the topology change notifications from the sub-ERP instance to the major instance.
Revertive	Select the checkbox and then select the revertive state. Options to choose from are **Enable** and **Disabled**. This function is used to revert back to the working transport entity, for example, when the RPL was blocked.

Parameter	Description
Guard Timer	Select the checkbox and enter the guard timer value here. This value must be between 10 and 2000 milliseconds. By default, this value is 500 milliseconds.
Hold-Off Timer	Select the checkbox and enter hold-off timer value here. This value must be between 0 and 10000 milliseconds. By default, this value is 0 milliseconds.
WTR Timer	Select the checkbox and enter the WTR timer value here. This value must be between 1 and 12 minutes. By default, this value is 5 minutes.

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

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

Loopback Detection

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

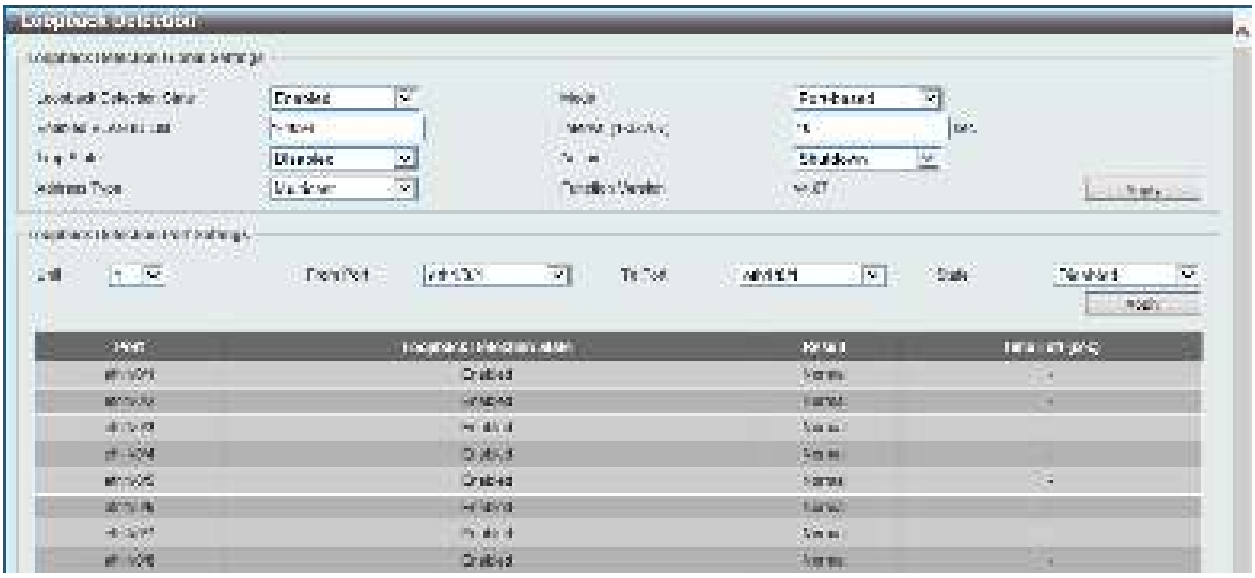


Figure 5-55 Loopback Detection Window

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

Parameter	Description
Loopback Detection State	Select to enable or disable loopback detection. The default is **Disabled**.
Mode	Select the loopback detection mode. Options to choose from are **Port-based** and **VLAN-based**.
Enable VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when the **VLAN-based** is selected in the **Mode** drop-down list.

Parameter	Description
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.
Traps State	Select to enable or disable the loopback detection trap state.
Action	Select the action that will be taken here. Options to choose from are: • **Shutdown** - Specifies that when a loop was detected, the port will be shut down (disabled) in the port-based mode. Traffic will be blocked on the specific VLAN in the VLAN-based mode. • **None** - Specifies that when a loop was detected, the port will not be disabled in the port-based mode. Traffic will not be block on the specific VLAN in the VLAN-based mode. Only log and trap messages will be sent.
Address Type	Select the address type here. This is used to configure the destination address type in LBD packets for loopback detection. Options to choose from are: • **Multicast** - Specifies that only multicast LBD packet will be sent. The destination address is CF-00-00-00-00-00. • **Broadcast** - Specifies that only broadcast LBD packet will be sent. The destination address is FF-FF-FF-FF-FF-FF.

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
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select 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 32 port trunk groups with 1 to 8 ports in each group.

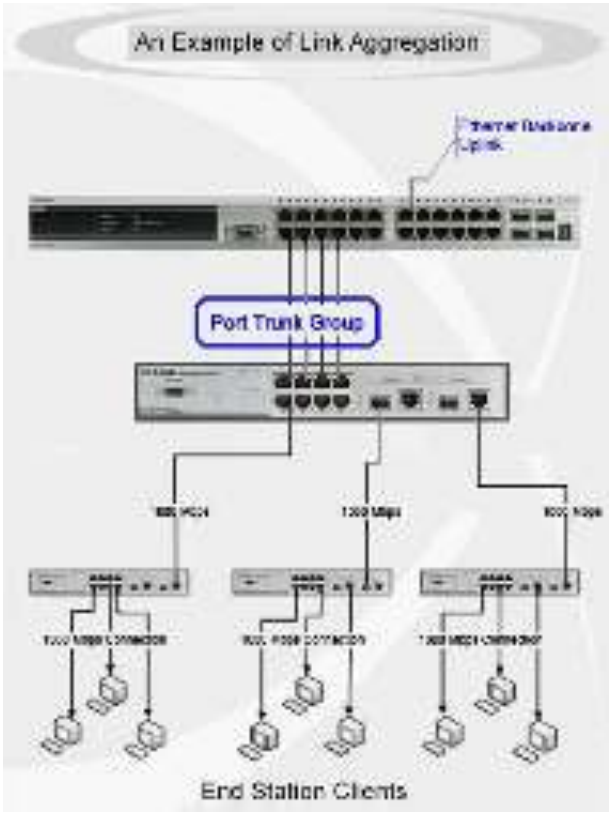


Figure 5-56 Example of Port Trunk Group

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 32 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. Port locking and 802.1X must not be enabled on the trunk group. 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 of the Master Port in the 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:

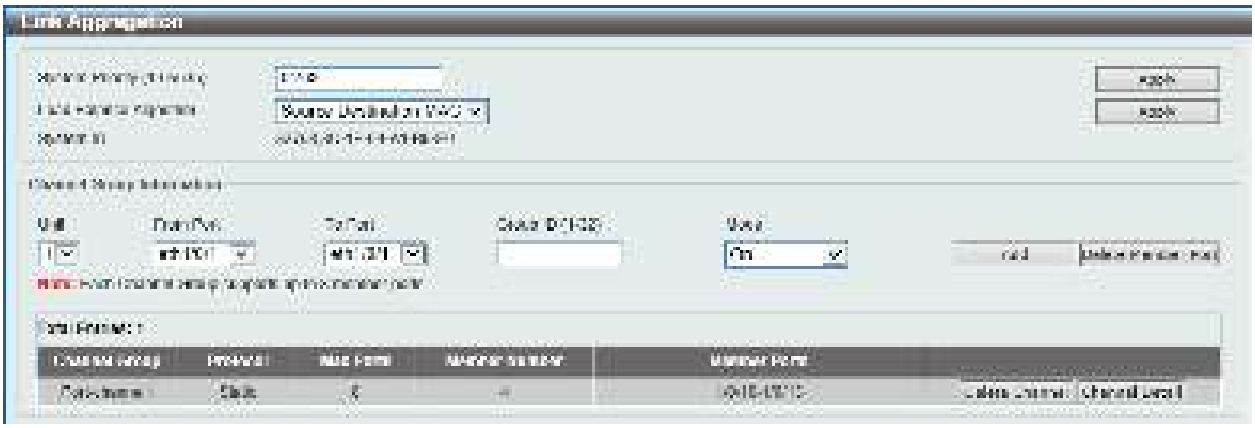


Figure 5-57 Link Aggregation Window

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

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

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

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

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 32. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are **On**, **Active**, and **Passive**. If the mode **On** is specified, the channel

Parameter	Description
	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 detailed information about the channel.

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

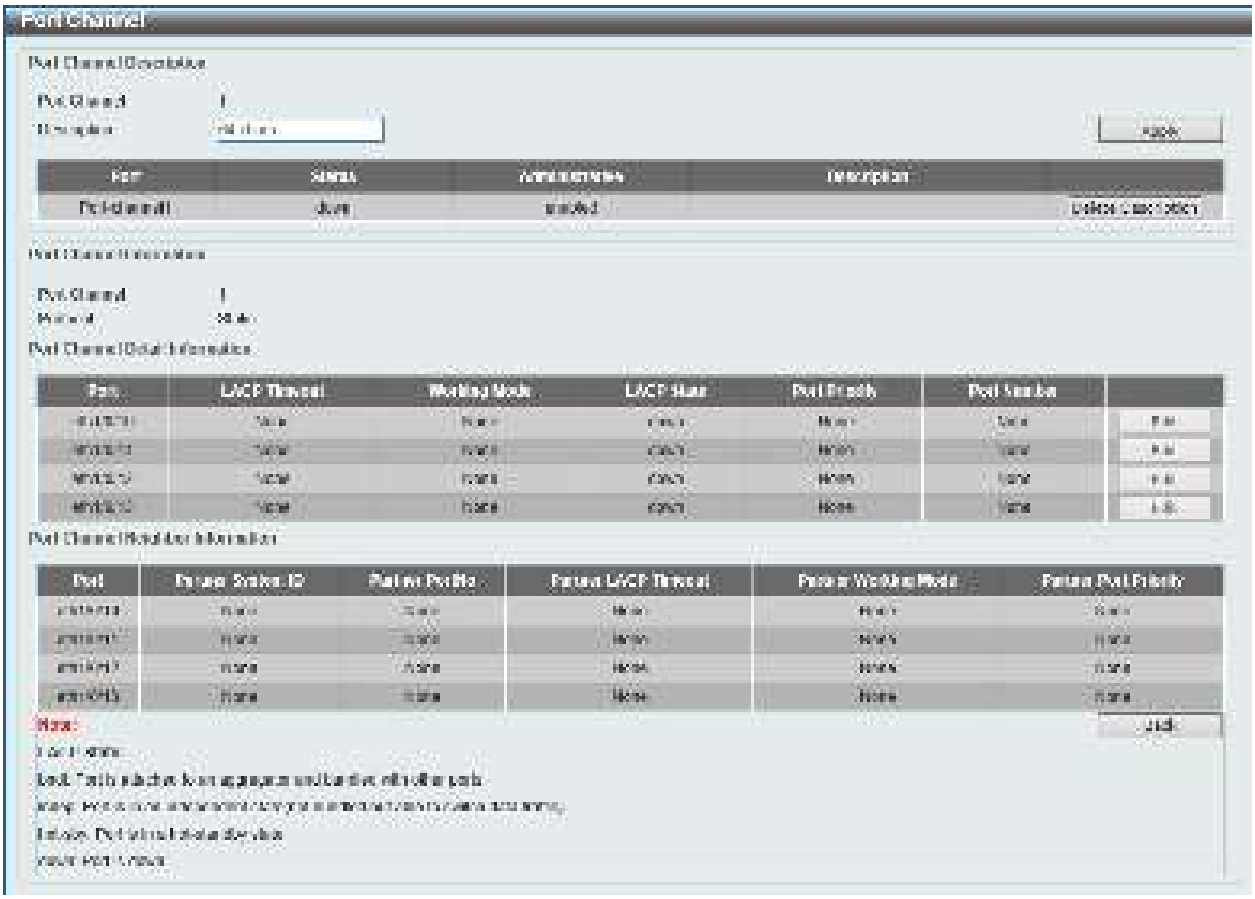


Figure 5-58 Port Channel Window

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

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

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

Click the **Delete Description** button to clear the setting in the corresponding Description field.

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

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

L2 Multicast Control

IGMP Snooping

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

IGMP Snooping Settings

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

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

Figure 5-59 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 **IGMP Snooping Table** are described below:

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

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

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

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

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

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

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

Figure 5-60 IGMP Snooping VLAN Parameters Window

The window displays the detail information about IGMP snooping VLAN. Click the **Modify** button to edit the information in the following window.

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

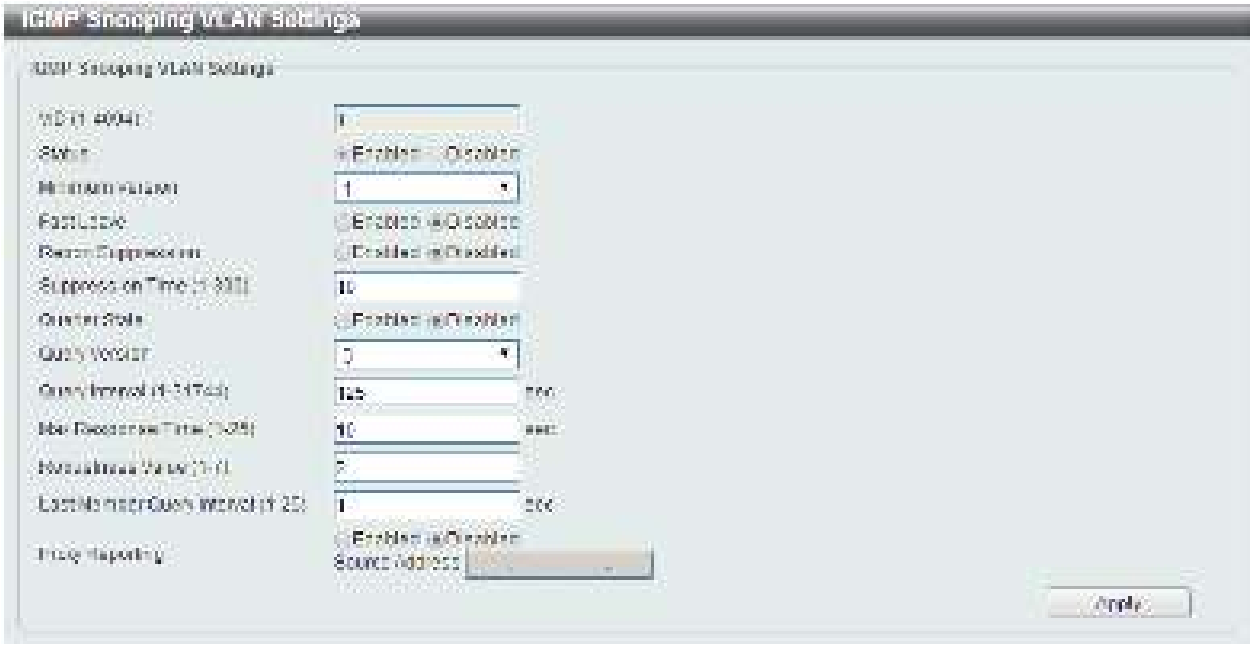


Figure 5-61 IGMP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of IGMP hosts that is allowed on the VLAN.
Fast Leave	Select this option to enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.
Report Suppression	Select this option to enable or disable the report suppression. The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expired. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.
Suppression Time	Enter the interval of suppressing duplicate IGMP reports or leaves. The range is from 1 to 300.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the IGMP snooping querier. Options to choose from are **1**, **2**, and **3**.
Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically.
Max Response Time	Enter the maximum response time, in seconds, advertised in IGMP snooping queries. The range is 1 to 25.
Robustness Value	Enter the robustness variable used in IGMP snooping.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when **Enabled** is selected in **Proxy Reporting**.

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

IGMP Snooping Groups Settings

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

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

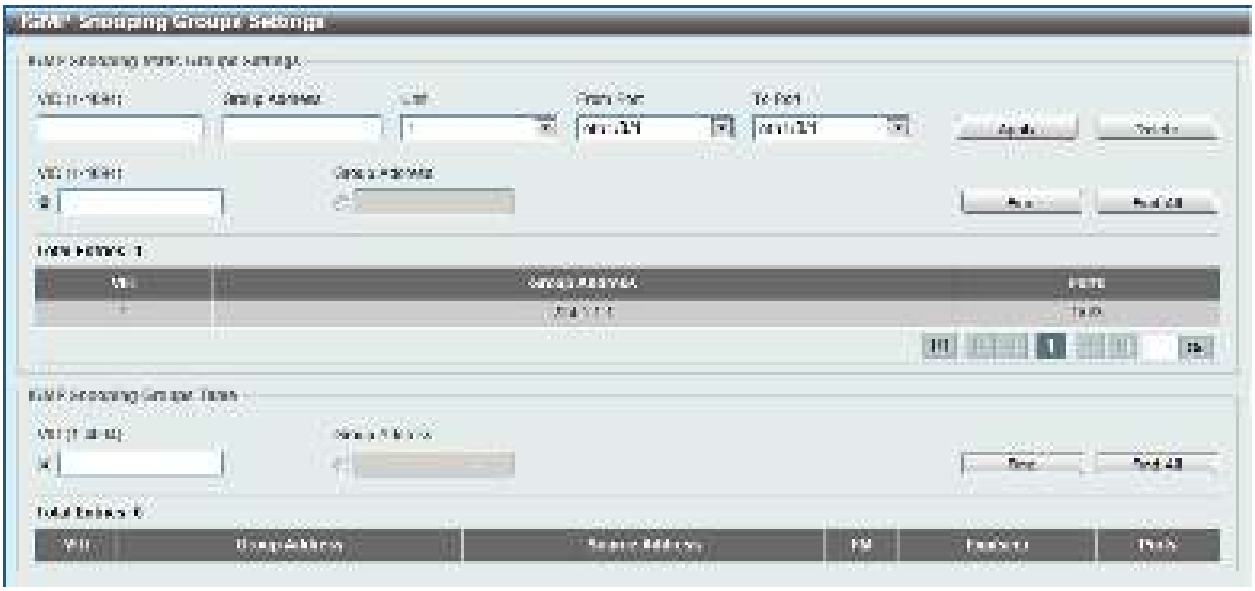


Figure 5-62 IGMP Snooping Groups Settings

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.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IP multicast group address.

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

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

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

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

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

The fields that can be configured or displayed for **IGMP Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IP multicast group address.
FM	Displays the filter mode. The value of the filter mode can be either **IN** (Include) or **EX** (Exclude). • **IN** (Include) - The filter mode is Include.

Parameter	Description
	• **EX** (Exclude) - The filter mode is Exclude.
Exp (sec)	Display the time left in seconds before the entry expires.

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

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

IGMP Snooping Mrouter Settings

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

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

Figure 5-63 IGMP Snooping Mrouter Settings Window

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

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are: • **Port** - Select to have the configured ports to be static multicast router ports. • **Forbidden Port** - Select to have the configured ports not to be multicast router ports.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

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

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

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

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

IGMP Snooping Statistics Settings

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

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

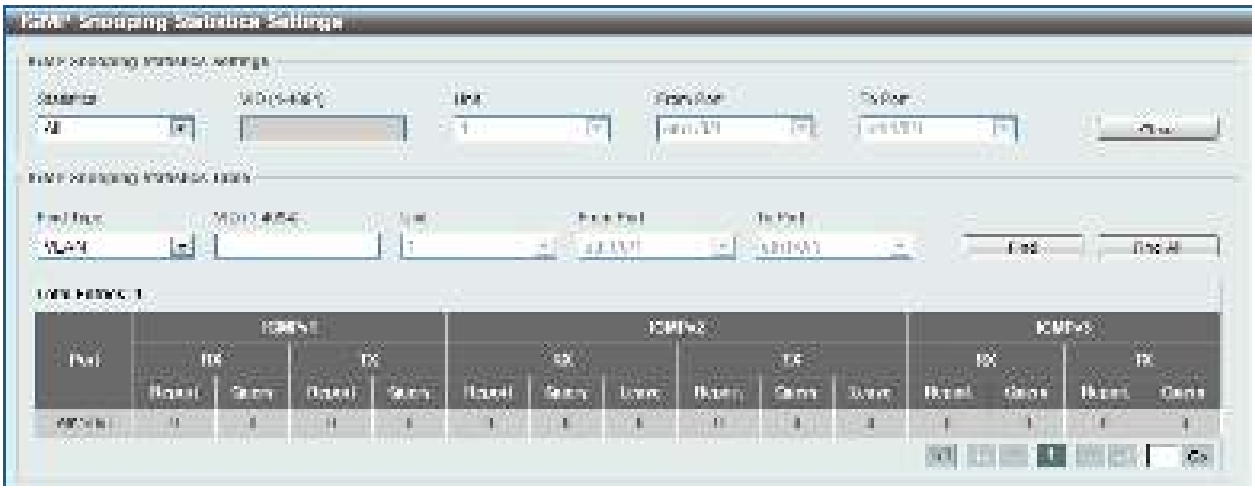


Figure 5-64 IGMP Snooping Statistics Settings Window

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

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

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

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

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

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

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

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

MLD Snooping

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

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

MLD Control Messages

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.

- **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.
- **Multicast Listener Report**, **Version 1** - Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
- **Multicast Listener Done** - 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.
- **Multicast Listener Report**, **Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

MLD Snooping Settings

This window is used to configure the MLD snooping settings.

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

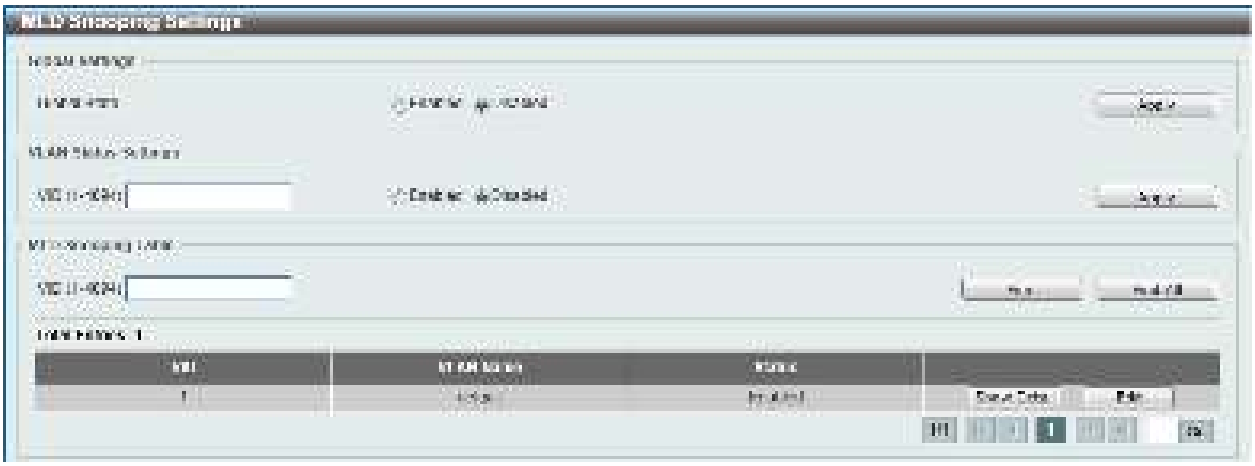


Figure 5-65 MLD Snooping Settings Window

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 **MLD Snooping Table** are described below:

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

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

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

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

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

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

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

Figure 5-66 MLD Snooping VLAN Parameters Window

The window displays the detail information about MLD snooping VLAN. Click the **Modify** button to edit the information in the following window.

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

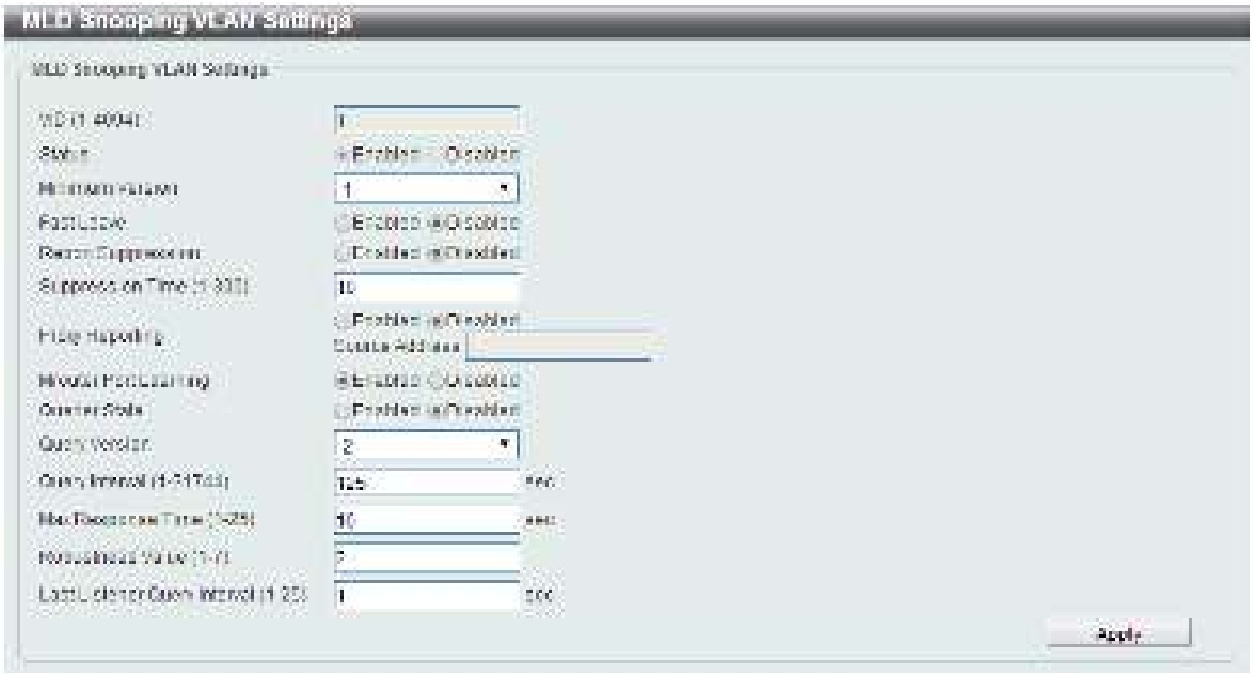


Figure 5-67 MLD Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN.
Fast Leave	Select this option to enable or disable the MLD snooping fast leave function. If enabled, the membership is immediately removed when the system receive the MLD leave message.

Parameter	Description
Report Suppression	Select this option to enable or disable the report suppression.
Suppression Time	Enter the interval of suppressing duplicate MLD reports or leaves. The range is from 1 to 300.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IPv6 of proxy reporting. This is available when **Enabled** is selected in **Proxy Reporting**.
Mrouter Port Learning	Select this option to enable or disable Mrouter port learning.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the MLD snooping querier. Options to choose from are **1**, and **2**.
Query Interval	Enter the interval at which the MLD snooping querier sends MLD general query messages periodically.
Max Response Time	Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is 1 to 25.
Robustness Value	Enter the robustness variable used in MLD snooping.
Last Listener Query Interval	Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages.

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

MLD Snooping Groups Settings

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

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

Figure 5-68 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.

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IP multicast group address.

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

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

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

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

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

The fields that can be configured or displayed for **MLD Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group.
Group Address	Click the radio button and enter an IPv6 multicast group address.
FM	Display the filter mode. The value of the filter mode can be either **IN** or **EX**. • **IN** (Include) - The filter mode is Include. • **EX** (Exclude) - The filter mode is Exclude.
Exp (sec)	Display the time left in seconds before the entry expires.

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

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

MLD Snooping Mrouter Settings

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

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

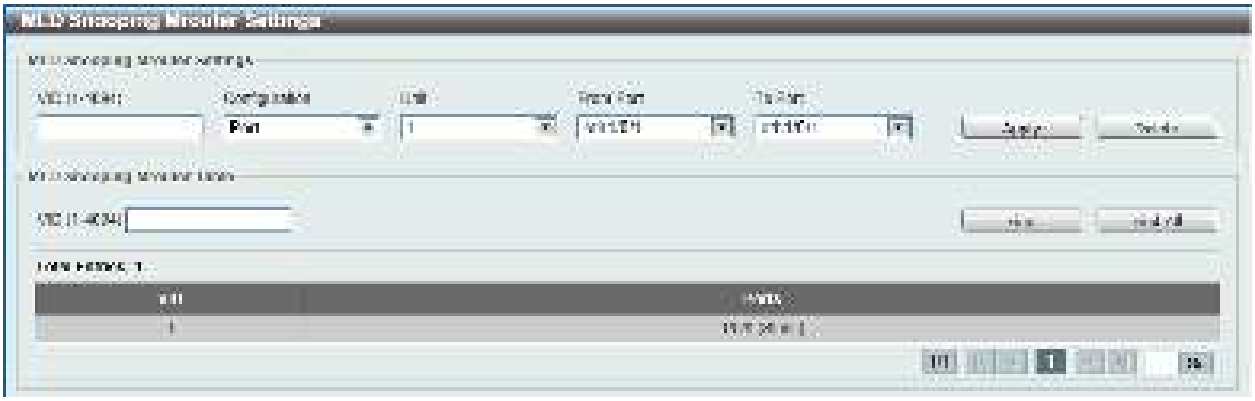


Figure 5-69 MLD Snooping Mrouter Settings Window

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

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are: • **Port** - Select to have the configured ports as being connected to multicast-enabled routers. • **Forbidden Port** - Select to have the configured ports as being not connected to multicast-enabled routers. • **Learn pimv6** - Select to enable dynamic learning of multicast router port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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

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

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

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

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

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

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

MLD Snooping Statistics Settings

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

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

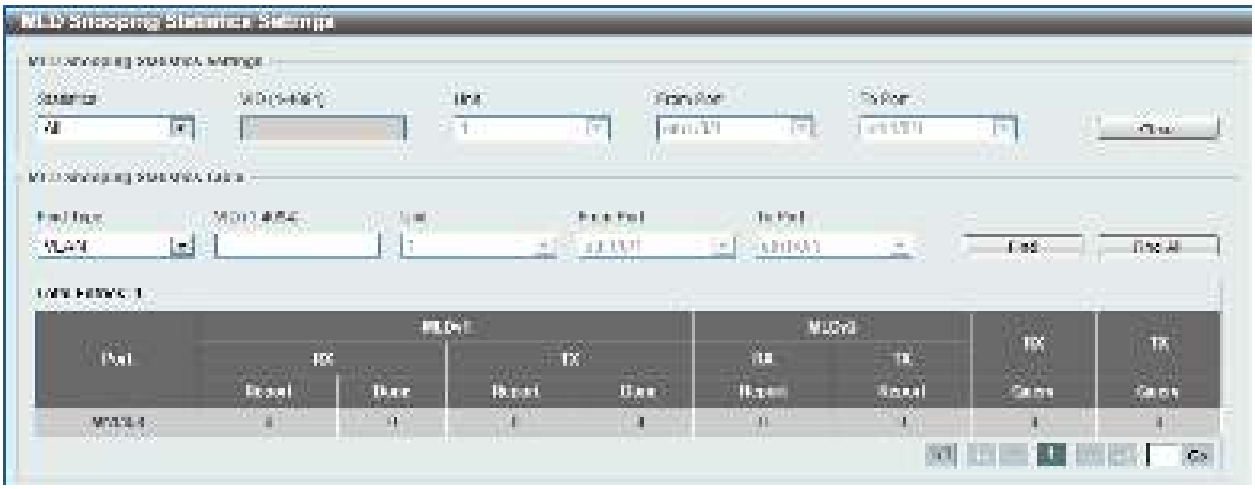


Figure 5-70 MLD Snooping Statistics Settings Window

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

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
Unit	Select the switch unit that will be used for this configuration here. This is available when **Port** is selected in the **Statistics** drop-down list.
From Port / To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** drop-down list.

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

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

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

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

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

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

Multicast Filtering

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

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

Figure 5-71 Multicast Filtering Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are:

Parameter	Description
	• **Forward Unregistered** - Specifies that registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. • **Forward All** - Specifies that all multicast packets will be flooded based on the VLAN domain. • **Filter Unregistered** - Specifies that registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

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

LLDP

LLDP Global Settings

This window is used to configure the LLDP global settings.

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

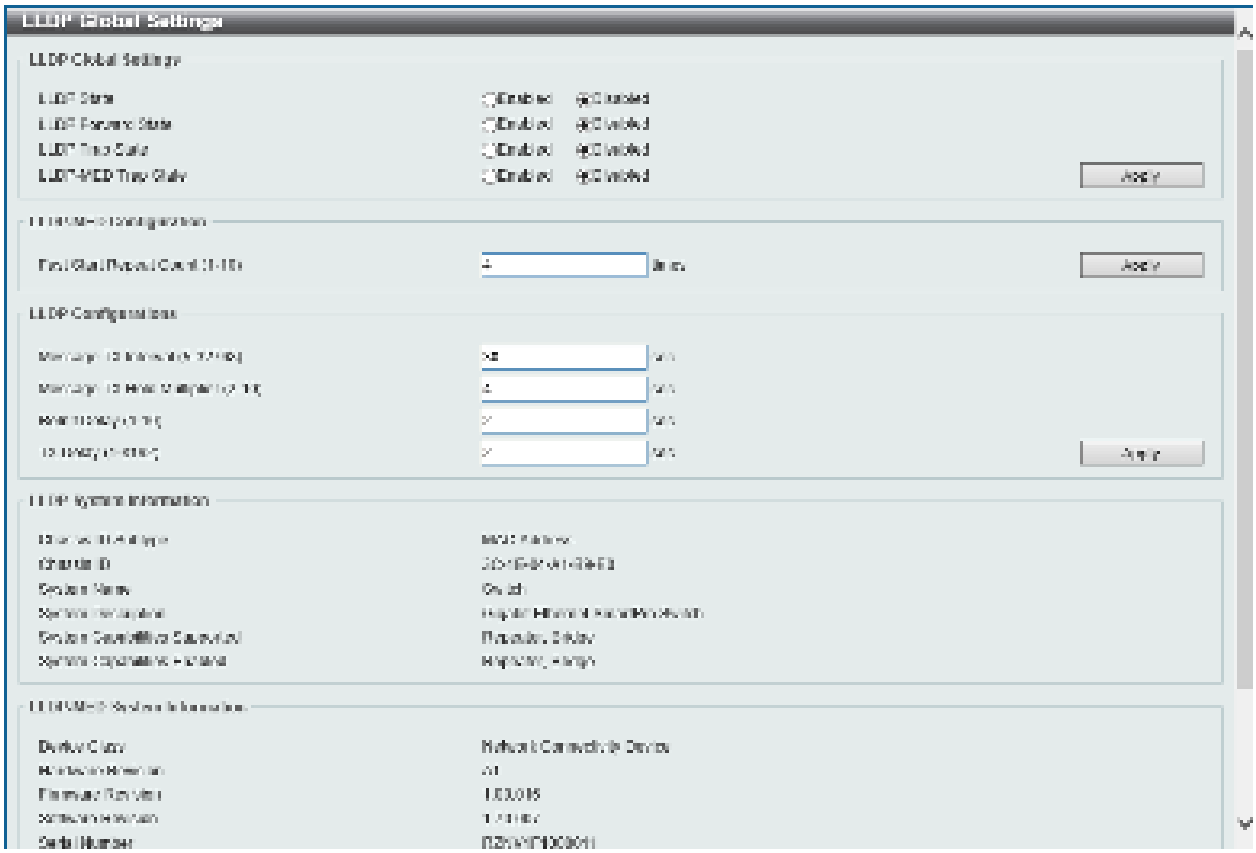


Figure 5-72 LLDP Global Settings Window

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

Parameter	Description
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the **LLDP State** is disabled and **LLDP Forward Sate** is enabled, the received LLDPDU packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the LLDP-MED trap state.

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

The fields that can be configured for **LLDP-MED Configuration** are described below:

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

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

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

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

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

LLDP Port Settings

This window is used to configure the LLDP port settings.

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

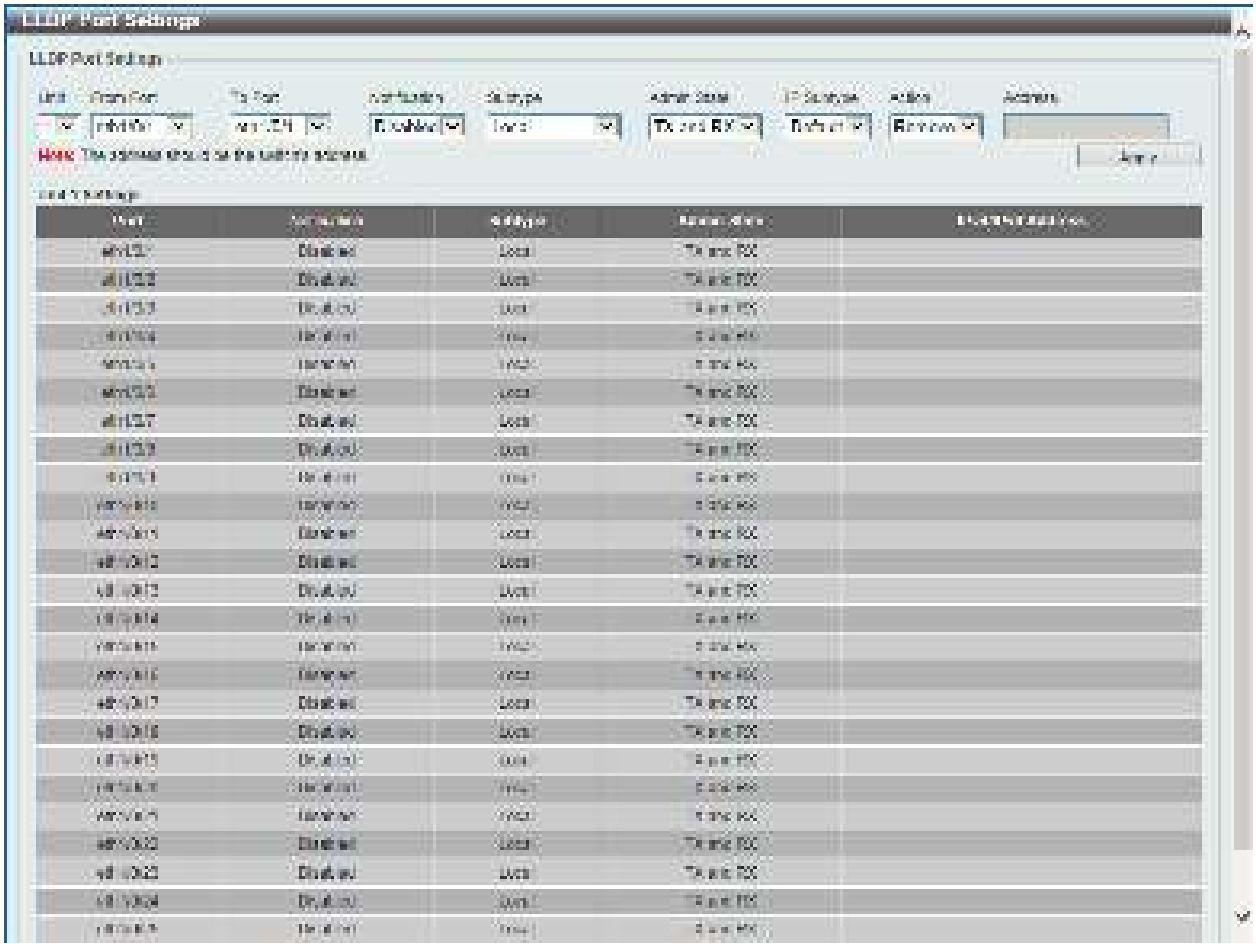


Figure 5-73 LLDP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable the sending of LLDP notifications.
Subtype	Select the subtype of LLDP TLV(s). Options to choose from are **MAC Address**, and **Local**.
Admin State	Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are: • **TX** - The local LLDP agent can only transmit LLDP frames. • **RX** - The local LLDP agent can only receive LLDP frames. • **TX and RX** - The local LLDP agent can both transmit and receive LLDP frames. This is the default option. • **Disabled** - The local LLDP agent can neither transmit nor receive LLDP frames.
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are **Default**, **IPv4**, and **IPv6**.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Remove** and **Add**.
Address	Enter the IP address that will be sent.

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

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

LLDP Management Address List

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

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

Figure 5-74 LLDP Management Address List Window

The fields that can be configured are described below:

Parameter	Description
All/IPv4/IPv6	Select the subtype. Options to choose from are **All**, **IPv4**, and **IPv6**.

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

LLDP Basic TLVs Settings

Type-length-value (TLV) allows the specific sending information as a TLV element within LLDP packets. This window is used to enable the settings for the Basic TLVs Settings. An active LLDP port on the Switch always included mandatory data in its outbound advertisements. There are four optional data types that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The

mandatory data types cannot be disabled. There are also four data types, which can be optionally selected. These include Port Description, System Name, System Description, and System Capability.

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

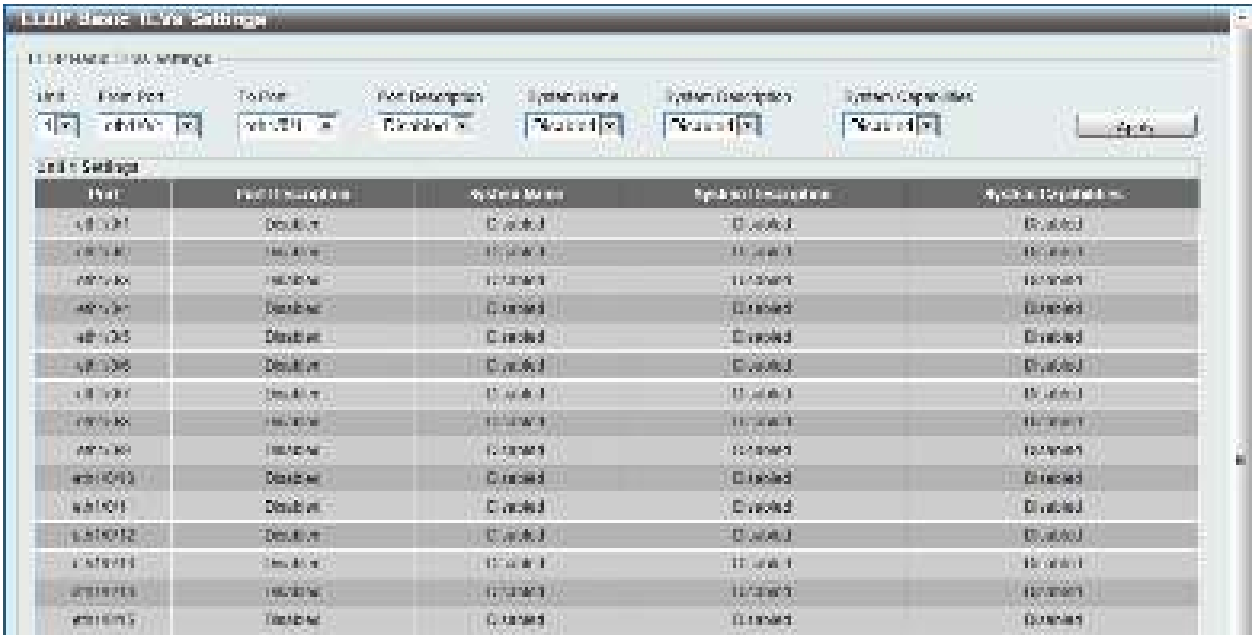


Figure 5-75 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Port Description	Select this option to enable or disable the Port Description option.
System Name	Select this option to enable or disable the System Name option.
System Description	Select this option to enable or disable the System Description option.
System Capabilities	Select this option to enable or disable the System Capabilities option.

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

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs, which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**, as shown below:

Figure 5-76 LLDP Dot1 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Port VLAN	Select this option to enable or disable the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
Protocol VLAN	Select this option to enable or disable Port and Protocol VLAN ID (PPVID) TLV to send, and enter the VLAN ID in PPVID TLV.
VLAN Name	Select this option to enable or disable the VLAN name TLV to send, and enter the ID of the VLAN in the VLAN name TLV.
Protocol Identity	Select this option to enable or disable the Protocol Identity TLV to send, and the protocol name. Options for protocol name to choose from are **None**, **EAPOL**, **LACP**, **GVRP**, **STP**, and **All**.

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

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**, as shown below:

Figure 5-77 LLDP Dot3 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
Link Aggregation	Select this option to enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
Maximum Frame Size	Select this option to enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
Power Via MDI	Select this option to enable or disable the power via MDI TLV to send. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

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

LLDP-MED Port Settings

This window is used to enable or disable transmitting LLDP-MED TLVs.

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

Figure 5-78 LLDP-MED Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable the sending of LLDP-MED notifications.
Capabilities	Select this option to enable or disable transmitting the LLDP-MED capabilities TLV.
Network Policy	Select this option to enable or disable transmitting the LLDP-MED network policy TLV.
PSE	Select this option to enable or disable transmitting the LLDP-MED extended power via MDI TLV, if the local device is PSE device or PD device.
Inventory	Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.

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

LLDP Statistics Information

This window is used to view the neighbor detection activity, LLDP Statistics, and the settings for individual ports on the Switch.

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

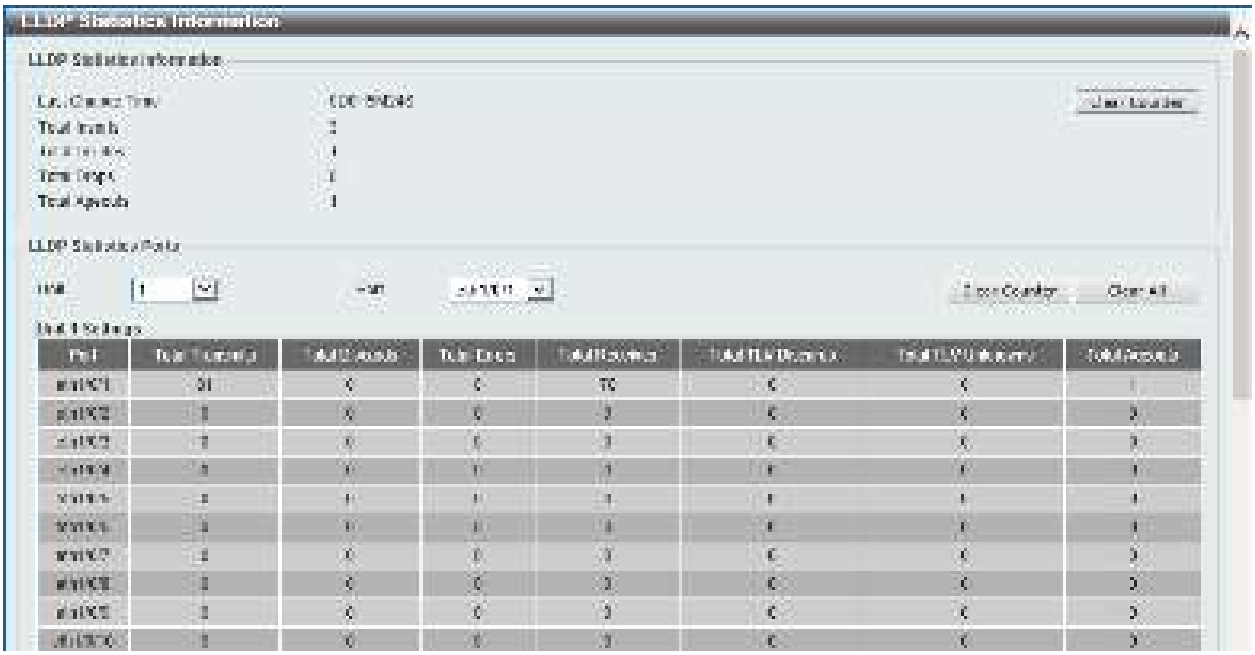


Figure 5-79 LLDP Statistics Information Window

The fields that can be configured are described below:

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

Click the **Clear Counter** button to clear the counter information for the statistics displayed.

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

LLDP Local Port Information

This window is used to display the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

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

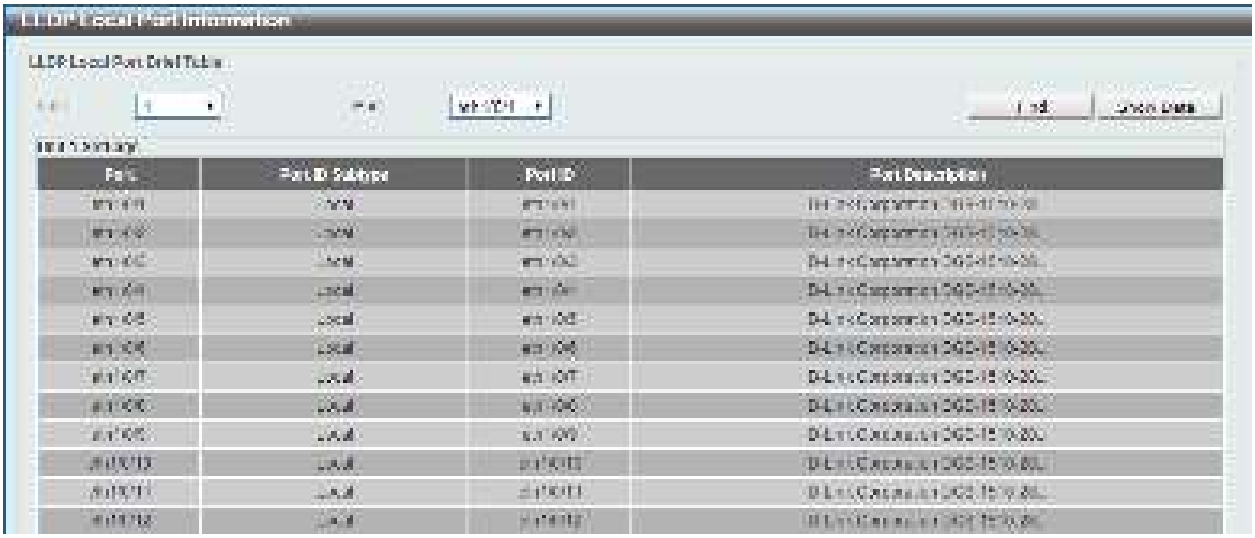


Figure 5-80 LLDP Local Port Information Window

The fields that can be configured are described below:

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

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

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

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

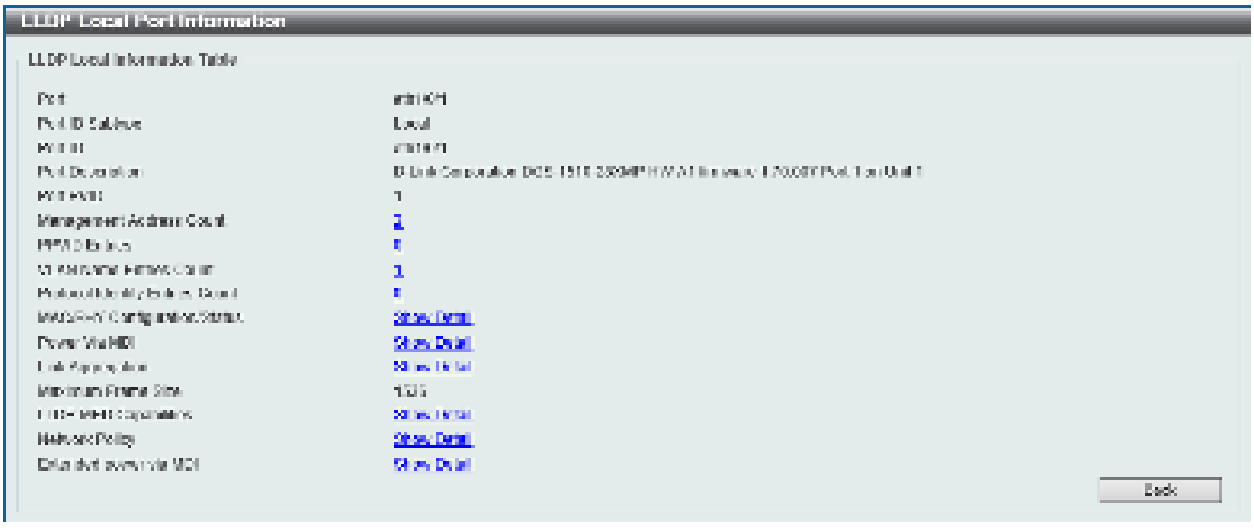


Figure 5-81 LLDP Local Port Information - Show Detail Window

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

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

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.

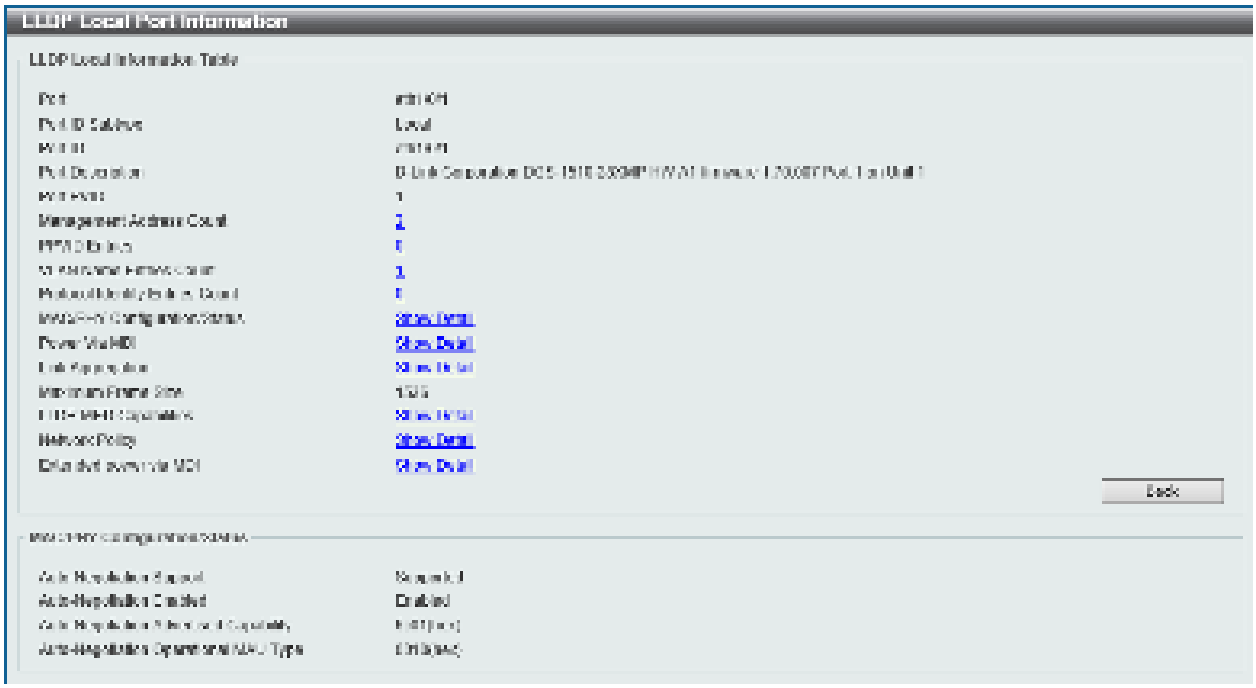


Figure 5-82 LLDP Local Port Information - Show Detail Window

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 shown below:

Figure 5-83 LLDP Neighbor Port Information Window

The fields that can be configured are described below:

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

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

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

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

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

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

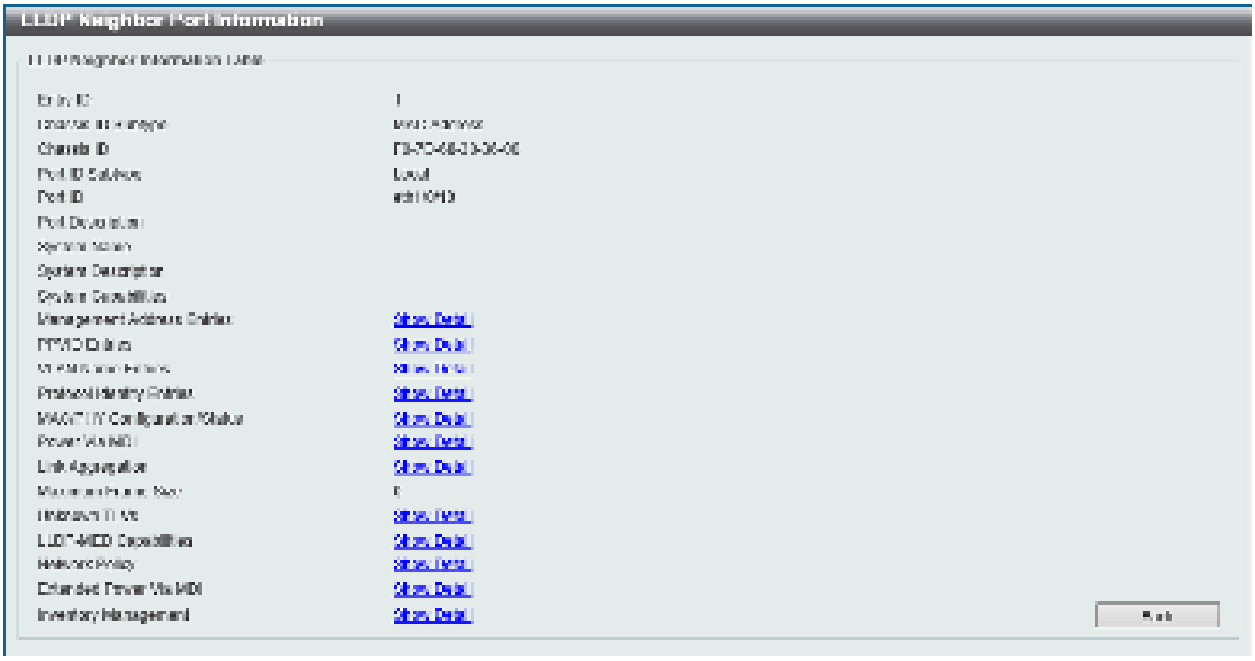


Figure 5-84 LLDP Neighbor Port Information - Show Detail Window

To view more details about, for example, the **LLDP-MED Capabilities**, click the Show Detail hyperlink.

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

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.

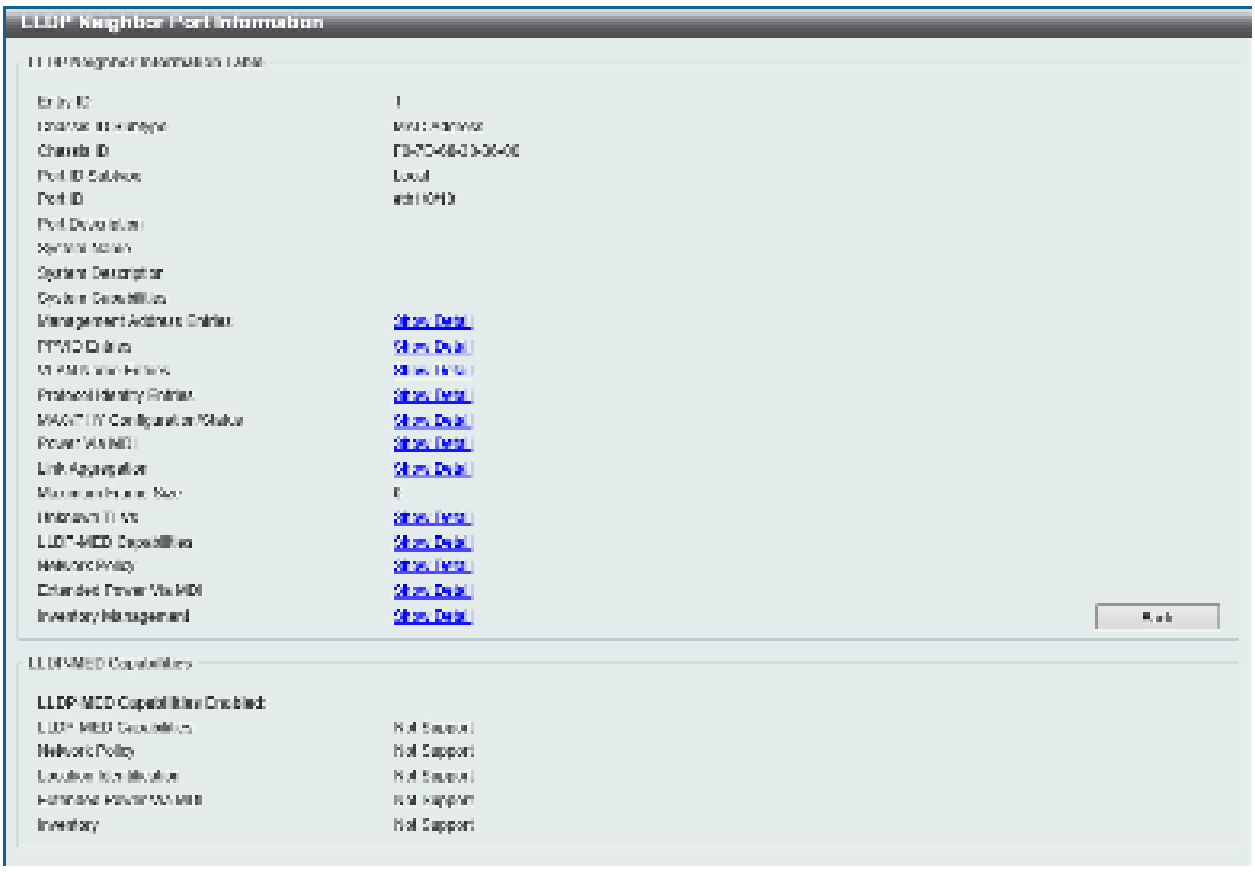


Figure 5-85 LLDP Neighbor Port Information - Show Detail Window

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

6. Layer 3 Features

ARP
Gratuitous ARP
UDP Helper
IPv4 Interface
IPv4 Static/Default Route
IPv4 Route Table
IPv6 Interface
IPv6 Neighbor
IPv6 Static/Default Route
IPv6 Route Table
IPMC

ARP

ARP Aging Time

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

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

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	Enter the ARP aging timeout value here.

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

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

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

Static ARP

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

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

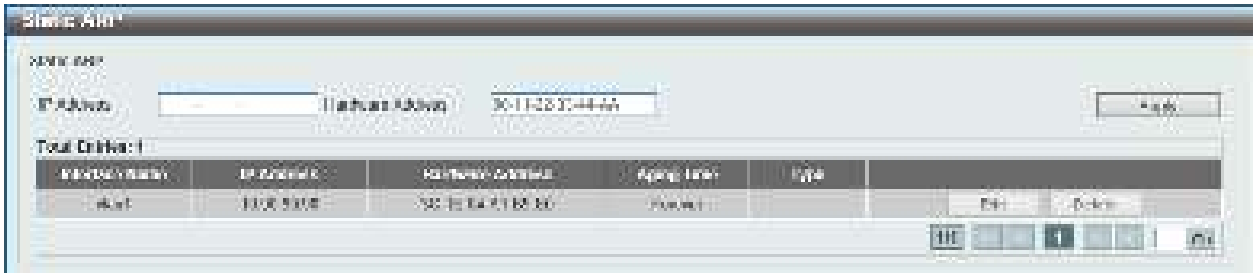


Figure 6-2 Static ARP Window

The fields that can be configured are described below:

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

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

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

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

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

Proxy ARP

This window is used to view and configure the proxy ARP settings. The Proxy ARP feature of the Switch will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP responder. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway. The host, usually a Layer 3 switch, will respond to packets destined for another device.

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

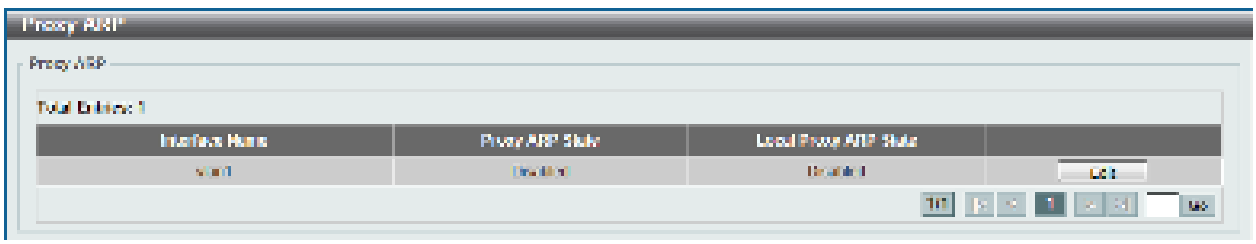


Figure 6-3 Proxy ARP Window

The fields that can be configured are described below:

Parameter	Description
Proxy ARP State	Select to enable or disable the proxy ARP state here.

Parameter	Description
Local Proxy ARP State	Select to enable or disable the local proxy ARP state here. This local proxy ARP function allows the Switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.

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

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

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

ARP Table

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

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

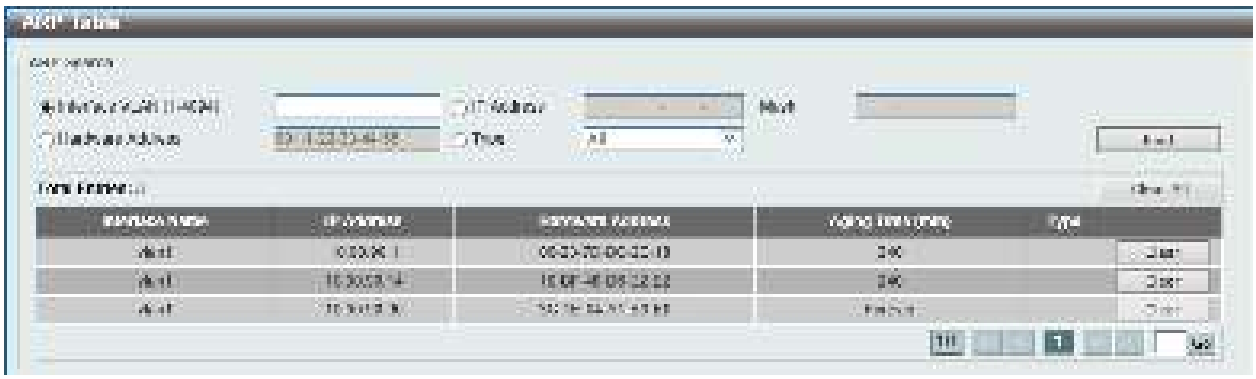


Figure 6-4 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Select and enter the interface's VLAN ID used here. This value must be between **1** and **4094**.
IP Address	Select and enter the IP address to display here.
Mask	After the **IP Address** option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Type	Select the type option here. Options to choose from are **All** and **Dynamic**.

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

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

Click the **Clear** button to clear the specific entry.

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

Gratuitous ARP

This window is used to view and configure the gratuitous ARP settings. A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.

Generally, a device use the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

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

Figure 6-5 Gratuitous ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Gratuitous ARP State	Select option to enable or disable the transmission of gratuitous ARP request packets.
Gratuitous ARP Trap State	Select this option to enable or disable the ARP trap state.
IP Gratuitous ARP Dad-Reply State	Select this option to enable or disable the IP gratuitous ARP Dad-reply state.
Gratuitous ARP Learning State	Select this option to enable or disable the gratuitous ARP learning state. Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. This option used to enable or disable the learning of ARP entries in the ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for.

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

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

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

UDP Helper

IP Forward Protocol

This window is used to display and configure the IP forward protocol settings. This feature is used to enable the forwarding of a specific UDP service type of packets.

To view the following window, click **L3 Features > UDP Helper > IP Forward Protocol**, as shown below:

Figure 6-6 IP Forward Protocol Window

The fields that can be configured are described below:

Parameter	Description
IP Forward Protocol UDP Port	Enter the destination port of the UDP service to be forwarded.

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.

IP Helper Address

This window is used to add or remove a target address for the forwarding of UDP broadcast packets. This feature takes effect only when the received interface has an IP address assigned.

The system only forwards packets that satisfy the following restrictions:

- The destination MAC address must be a broadcast address.
- The destination IP address must be an all-one broadcast.
- The packets are IPv4 UDP packets.
- The IP TTL value must be greater than or equal to 2.

To view the following window, click **L3 Features > UDP Helper > IP Helper Address**, as shown below:

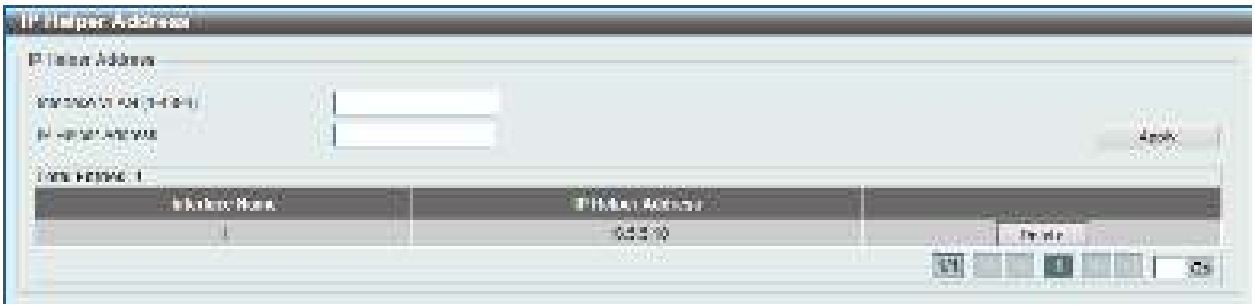


Figure 6-7 IP Helper Address Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
IP Helper Address	Enter the target IPv4 address for the forwarding of the UDP broadcast packet 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.

IPv4 Interface

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

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

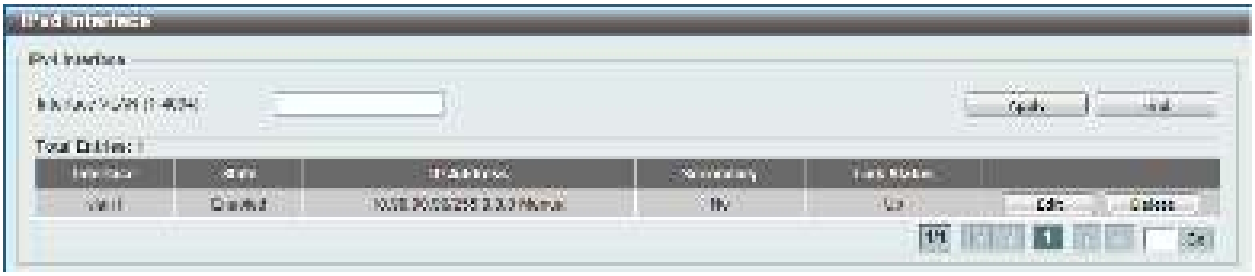


Figure 6-8 IPv4 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface's VLAN ID here. This value must be between 1 and 4094.

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

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

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

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

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

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

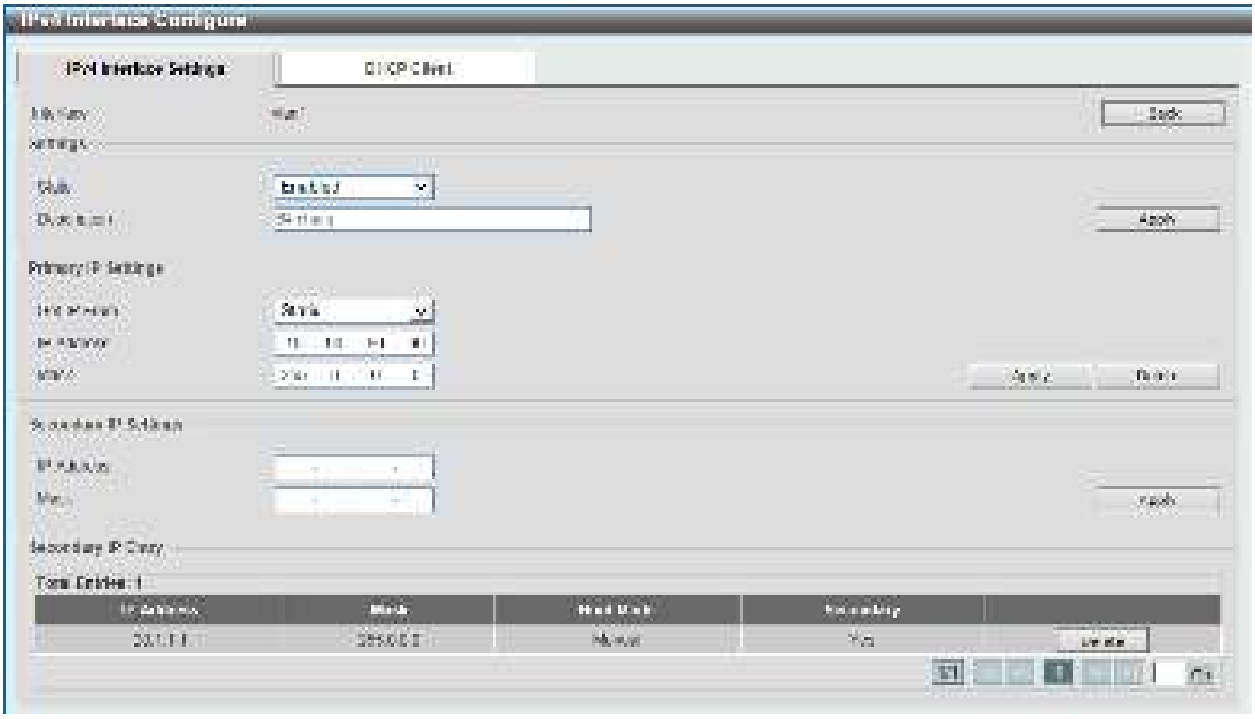


Figure 6-9 IPv4 Interface Configure Window

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

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

Parameter	Description
State	Select this option to enable or disable the IPv4 interface's global state.
Description	Enter the description for the IPv4 interface here. This can be up to 64 characters long.

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

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

Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are: • **Static** - Users can enter the IPv4 address of this interface manually in the fields provided. • **DHCP** - This interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for this interface here.
Mask	Enter the IPv4 subnet mask for this interface here.

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

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

Parameter	Description
IP Address	Enter the IPv4 address as the secondary interface here.
Mask	Enter the IPv4 subnet mask as the secondary interface here.

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

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

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

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

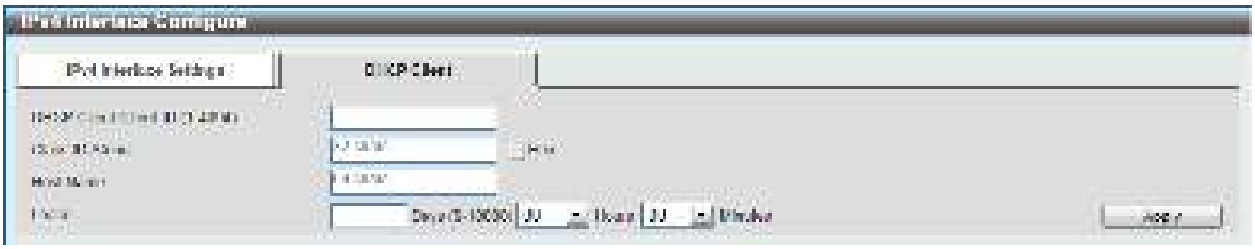


Figure 6-10 DHCP Client Window

The fields that can be configured are described below:

Parameter	Description
DHCP Client Client-ID	Enter the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message.
Class ID String	Enter the vendor class identifier with the maximum of 32 characters. Tick the **Hex** check box to have the class identifier in the hexadecimal form.
Host Name	Enter the host name. The maximum length is 64 characters. The host name must start with a letter, end with a letter or digit, and only with interior characters letters, digits, and hyphens.
Lease	Specify the preferred lease time for the IP address to request from the DHCP server. Enter the day duration of the lease, or select the hour and minute duration of the lease.

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

IPv4 Static/Default Route

This window is used to view and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 formatted addressing. Users can create up to 64 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become active.

Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

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

Figure 6-11 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address for this route here. Tick the **Default Route** check box to use the default route as the IPv4 address.
Mask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.
Backup State	Select the backup state option here. Options to choose from are: • **Primary** - The route is used as the primary route to the destination. • **Backup** - The route is used as the backup route to the destination.

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

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

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

IPv4 Route Table

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

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

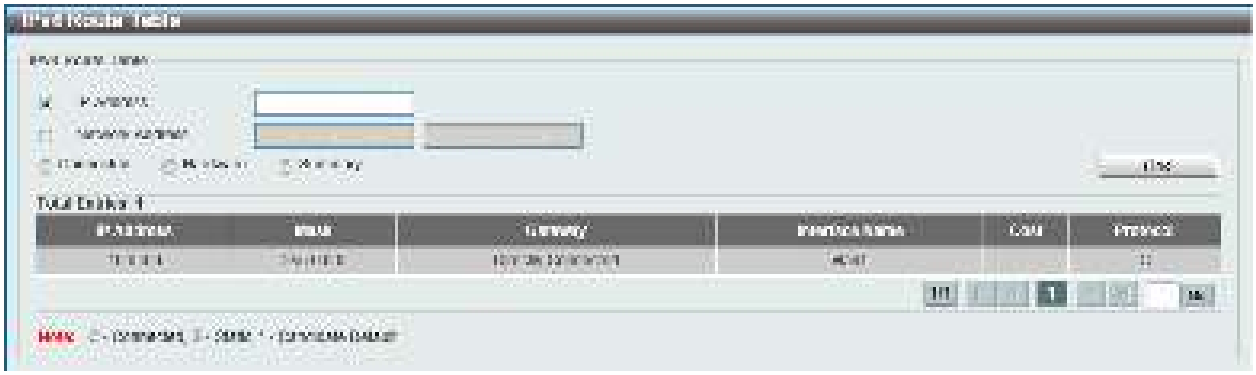


Figure 6-12 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Display the brief information of the active routing entries.

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

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

IPv6 Interface

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

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

Figure 6-13 IPv6 Interface Window

The fields that can be configured are described below:

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

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

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

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

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

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

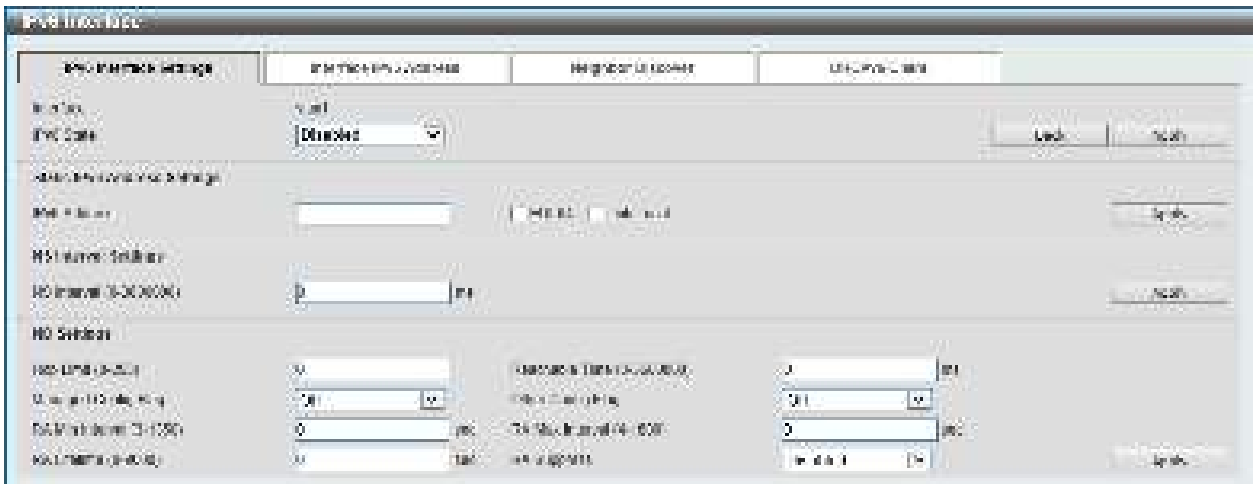


Figure 6-14 IPv6 Interface (Detail, IPv6 Interface Settings) Window

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

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

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

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

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

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

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

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

Parameter	Description
NS Interval	Enter the NS interval between 0 and 3600000 milliseconds.

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

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

Parameter	Description
Hop Limit	Enter the IPv6 hop limit value here. This is used to configure the hop limit to be advertised in RA messages. The IPv6 packet originated at the system will also use this value as the initial hop limit. To use the default value on this interface, configure this value as 0. The range is from 0 to 255.
Reachable Time	Enter the reachable time used in the ND protocol here. The configured time is used by the router on the interface and is also advertised in RA message. If the specified time is 0, the router will use 30 seconds on the interface and advertise 0 (unspecified) in RA message. The reachable time is used by the IPv6 node in

Parameter	Description
	determining the reachability of the neighboring nodes. The range is from 0 to 3600000 milliseconds in multiples of 1000 milliseconds.
Managed Config Flag	Select to turn the managed configure flag **On** or **Off** here. This is used to enable or disable the management configure flag in the advertised RA message. When the neighboring host receives the RA with an enabled flag, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Select to turn the other configure flag **On** or **Off** here. This is used to enable or disable the other configure flag in the advertised RA message. When this feature is enabled, the router will instruct the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than IPv6 address.
RA Min Interval	Enter the minimum value of the interval between retransmission of RA messages here. The range is from 3 to 1350 seconds. This value must be smaller than 75% of the maximum value.
RA Max Interval	Enter the maximum value of the interval between retransmission of RA messages here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA informs the received host of the lifetime for taking the router as the default router.
RA Suppress	Select to enable or disable the sending of RA messages on the interface here. By default, this feature is enabled on a VLAN interface and disabled on a tunnel interface.

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

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

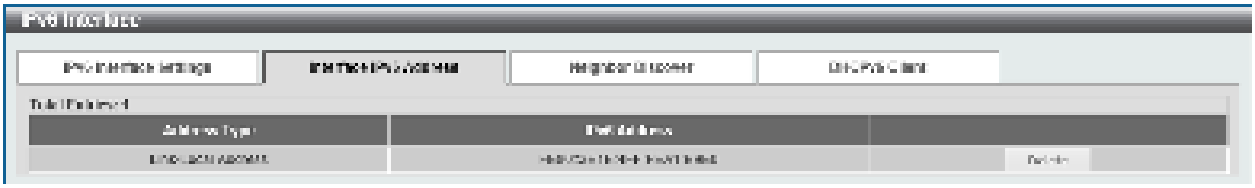


Figure 6-15 IPv6 Interface (Detail, Interface IPv6 Address) Window

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

After clicking the **Neighbor Discover** tab, at the top of the page, the following page will be available.

Figure 6-16 IPv6 Interface (Detail, Neighbor Discover) Window

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

Figure 6-17 IPv6 Interface (Detail, Neighbor Discover, Edit) Window

The fields that can be configured are described below:

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

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

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

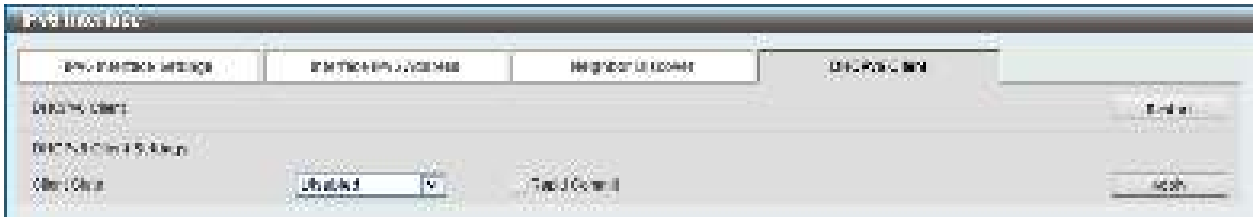


Figure 6-18 IPv6 Interface (Detail, DHCPv6 Client) Window

Click the **Restart** button to restart DHCPv6 client on an interface.

The fields that can be configured for **DHCPv6 Client Settings** are described below:

Parameter	Description
Client State	Select this option to enable or disable the DHCPv6 client state. Tick the **Rapid Commit** check box to proceed with two-message exchange for prefix delegation.

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

IPv6 Neighbor

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

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

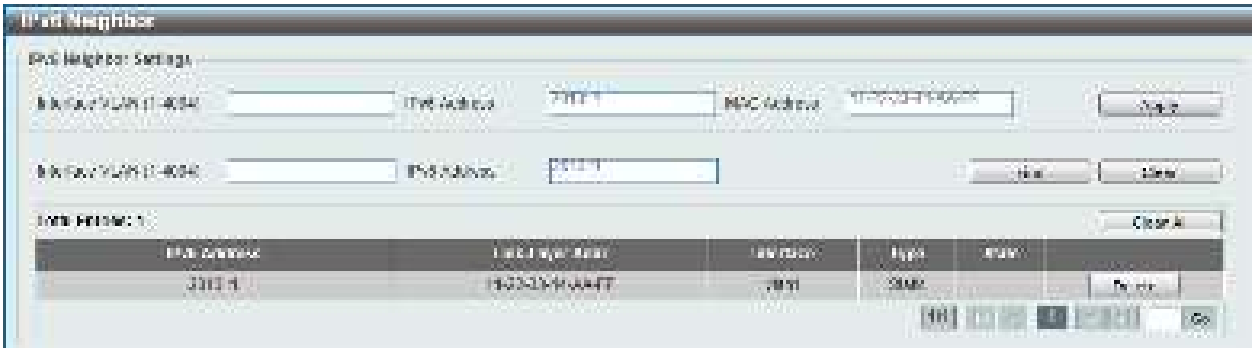


Figure 6-19 IPv6 Neighbor Window

The fields that can be configured are described below:

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

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

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

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

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

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

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

IPv6 Static/Default Route

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

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

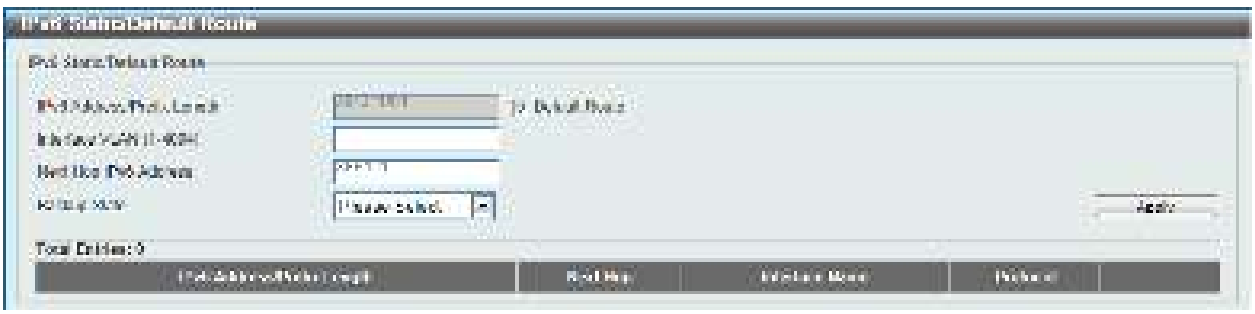


Figure 6-20 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the **Default Route** option to use the default route as the IPv6 address.
Interface VLAN	Enter the interface's VLAN ID that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Backup State	Select the backup state option here. Options to choose from are: • **Primary** - The route is specified as the primary route to the destination. • **Backup** - The route is specified as the backup route to the destination.

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

IPv6 Route Table

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

To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:

Figure 6-21 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address to display here.
IPv6 Address/Prefix Length	Select and enter the IPv6 address and prefix length to display here. Select the **Longer Prefixes** option to display IPv6 routes with prefixes greater than and equal to the prefix length.
Interface VLAN	Select and enter the interface's VLAN ID to display here.
Connected	Select this option to display only connected routes.
Database	Select to view all the related entries in the routing database instead of just the best route.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Display the brief information of the active routing entries.

Click the **Find** button to locate a specific entry based on the information entered.

IPMC

IP Multicast Global Settings

This window is used to display and configure the global IP Multicast (IPMC) settings.

To view the following window, click **L3 Features > IPMC > IP Multicast Global Settings**, as shown below:

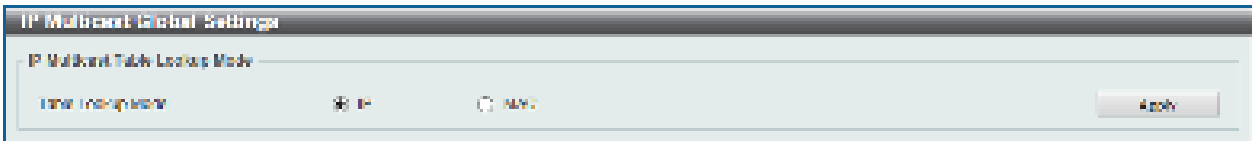


Figure 6-22 IP Multicast Global Settings Window

The fields that can be configured are described below:

Parameter	Description
Table Lookup Mode	Select the IP multicast forwarding lookup mode here. Options to choose from are: • **IP** - Specifies multicast forwarding lookup based on the IP address. • **MAC** - Specifies multicast forwarding lookup based on the MAC address.

Click the **Apply** button to accept the changes made.

IP Multicast Forwarding Cache

This window is used to display the content of the IP multicast routing forwarding cache database.

To view the following window, click **L3 Features > IPMC > IP Multicast Forwarding Cache**, as shown below:

Figure 6-23 IP Multicast Forwarding Cache Window

The fields that can be configured are described below:

Parameter	Description
Group Address	Enter the multicast group IP address here.
Source Address	Enter the source IP address here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

7. Quality of Service (QoS)

Basic Settings
Advanced Settings

Basic Settings

Port Default CoS

This window is used to view and configure the port's default CoS settings.

To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:

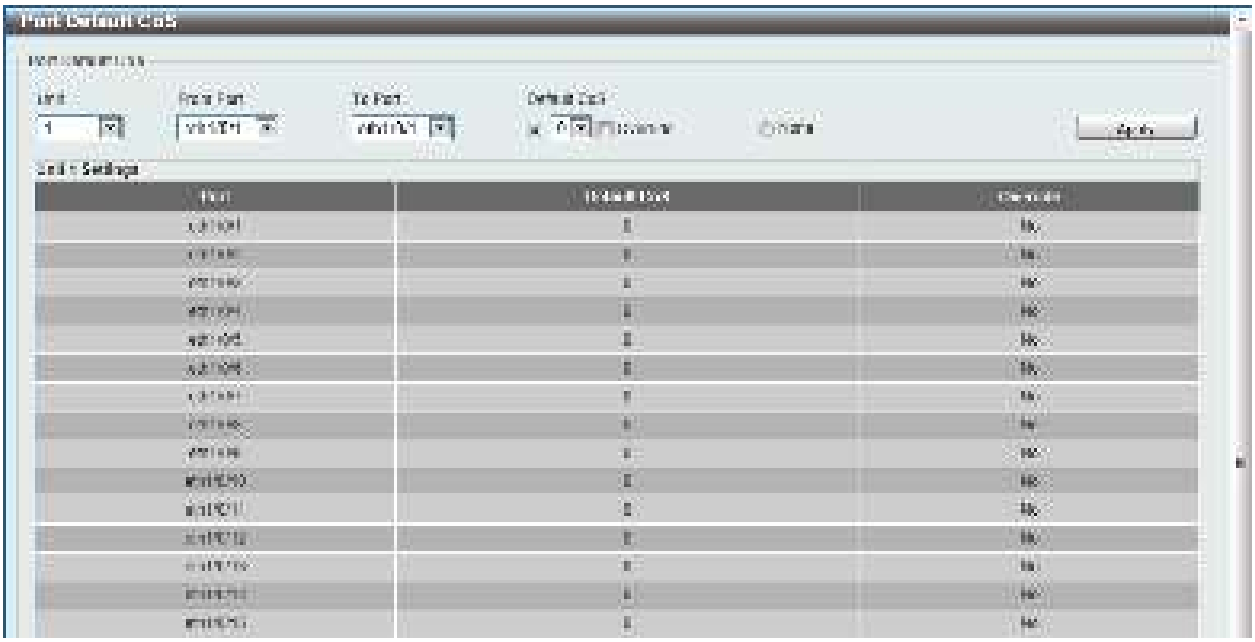


Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are **0** to **7**. Click the **Override** check box to apply the port's default CoS to all packets (tagged or untagged) received by the port. Select the **None** option to use the default settings.

Click the **Apply** button to accept the changes made.

Port Scheduler Method

This window is used to view and configure the port scheduler method settings.

To view the following window, click **QoS > Basic Settings > Port Scheduler Method**, as shown below:

Figure 7-2 Port Scheduler Method Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Scheduler Method	Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (**SP**), Round-Robin (**RR**), Weighted Round-Robin (**WRR**), and Weighted Deficit Round-Robin (**WDRR**). By default, the output queue-scheduling algorithm is **WRR**. **WDRR** operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration. 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

Parameter	Description
	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.

Queue Settings

This window is used to view and configure the queue settings.

To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:

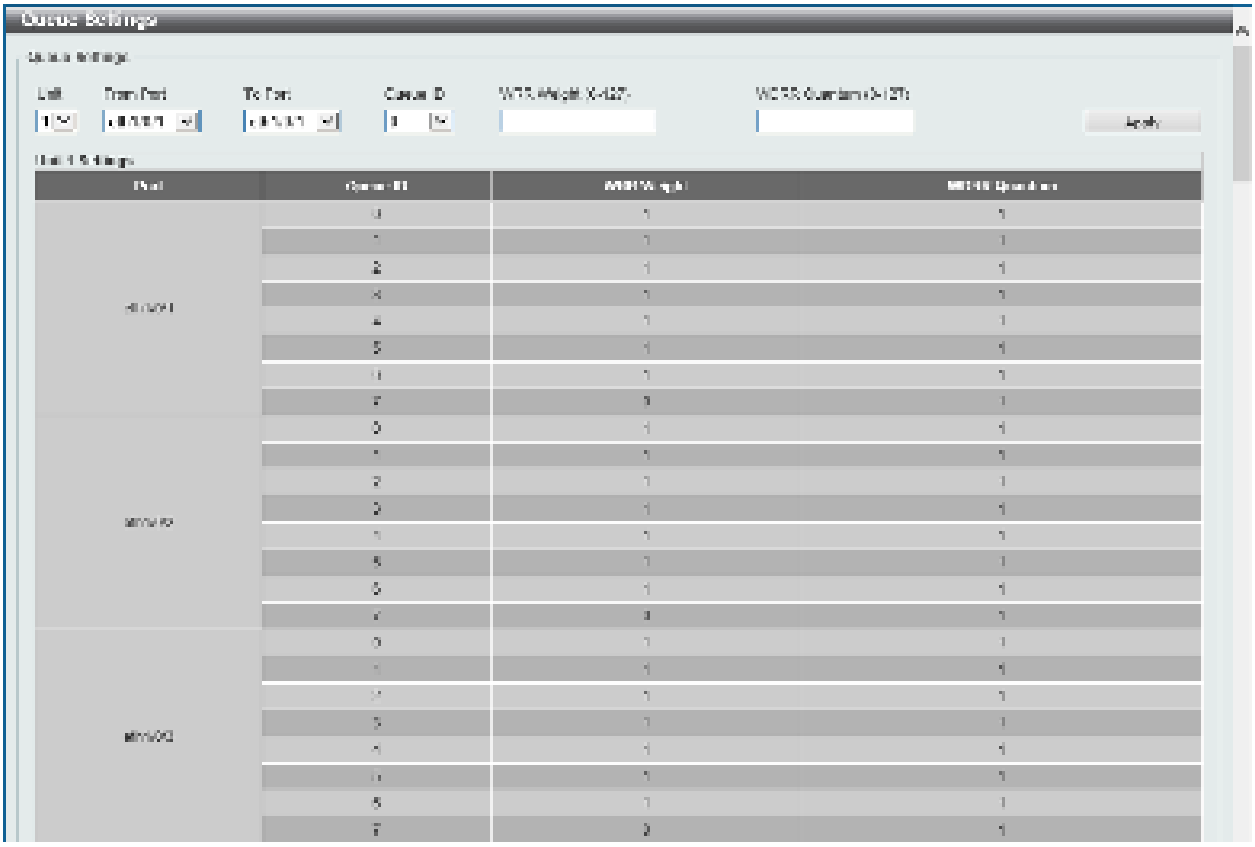


Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Queue ID	Enter the queue ID value here. This value must be between **0** and **7**.
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. The weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0 and 127.

Click the **Apply** button to accept the changes made.

CoS to Queue Mapping

This window is used to view and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:

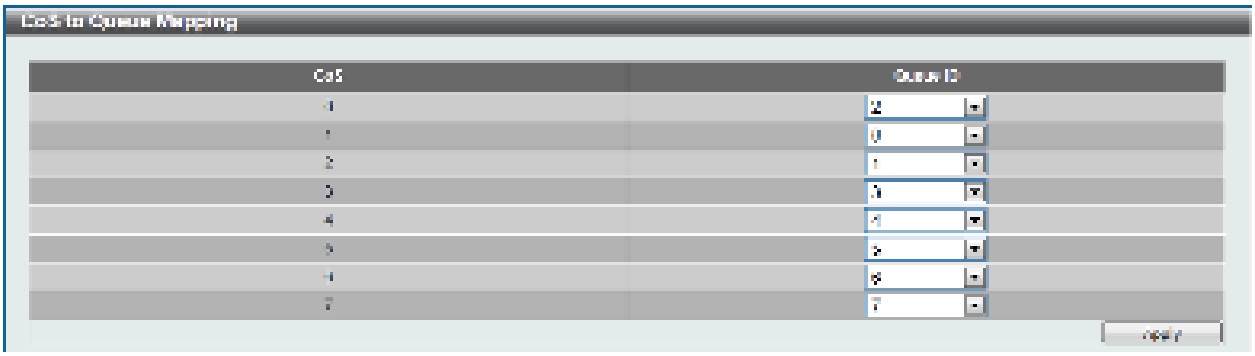


Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are **0** to **7**.

Click the **Apply** button to accept the changes made.

Port Rate Limiting

This window is used to view and configure the port rate limiting settings.

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:

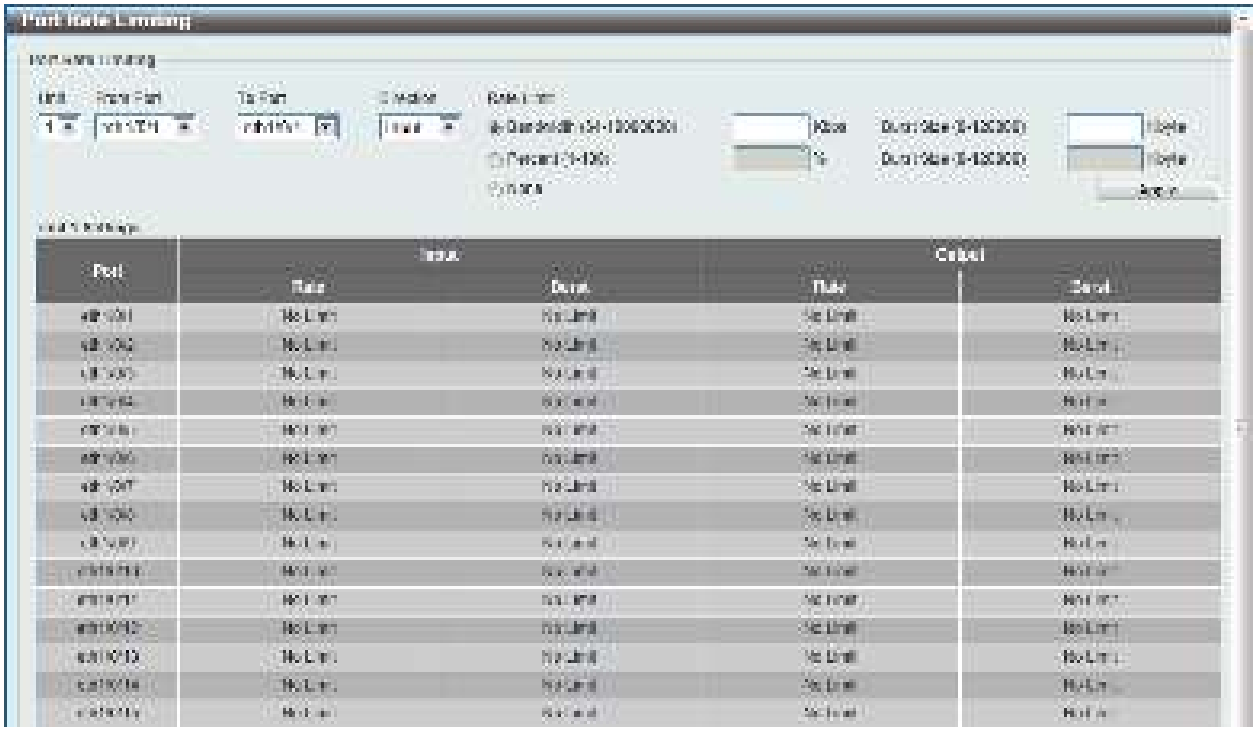


Figure 7-5 Port Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction option here. Options to choose from are: • **Input** - The rate limit for ingress packets is configured. • **Output** - The rate limit for egress packets is configured.
Rate Limit	Select and enter the rate limit value here. When **Bandwidth** is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes. When **Percent** is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes. Select the **None** option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress can trigger a pause frame or a flow control frame when the received traffic exceeds the limitation.

Click the **Apply** button to accept the changes made.

Queue Rate Limiting

This window is used to view and configure the queue rate limiting settings.

To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:

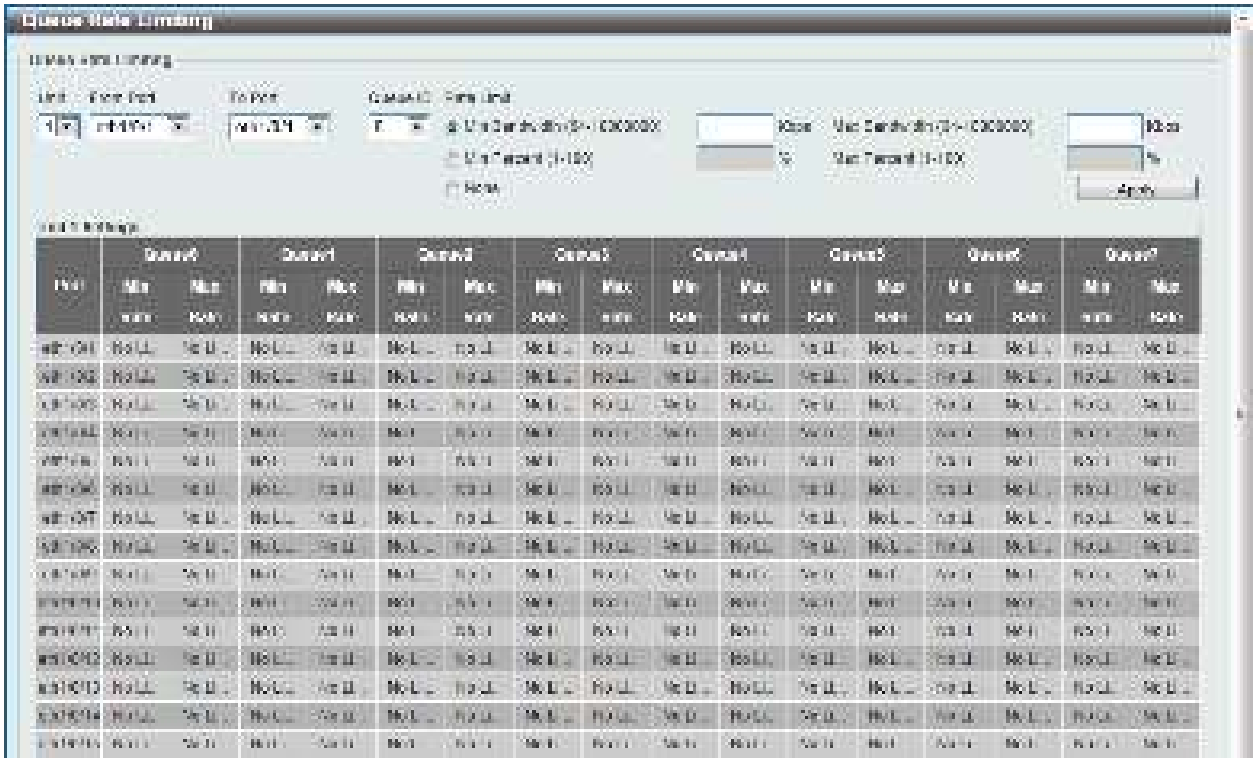


Figure 7-6 Queue Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Queue ID	Select the queue ID that will be configured here. Options to choose from are **0** to **7**.
Rate Limit	Select and enter the queue rate limit settings here. When the **Min Bandwidth** option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the maximum bandwidth (**Max Bandwidth**) rate limit in the space provided. This value must be between 64 and 10000000 kbps. The granularity is 64. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied. The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum

Parameter	Description
	guaranteed bandwidth of one CoS cannot be used across physical ports. When the **Min Percent** option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between **1** and **100** percent (%). Also, enter the maximum percentage value (**Max Percent**) in the space provided. This value must be between **1** and **100** percent (%).

Click the **Apply** button to accept the changes made.

Advanced Settings

DSCP Mutation Map

This window is used to view and configure the Differentiated Services Code Point (DSCP) mutation map settings. When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments. The DSCP-CoS map and DSCP-color map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP.

To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63.
Output DSCP	Enter the output DSCP value here. This value must be between 0 and 63.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Port Trust State and Mutation Binding

This window is used to view and configure port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:

Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Trust State	Select the port trust state option here. Options to choose from are **CoS** and **DSCP**.
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long. Select the **None** option to not allocate a DSCP mutation map to the port(s).

Click the **Apply** button to accept the changes made.

DSCP CoS Mapping

This window is used to view and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:

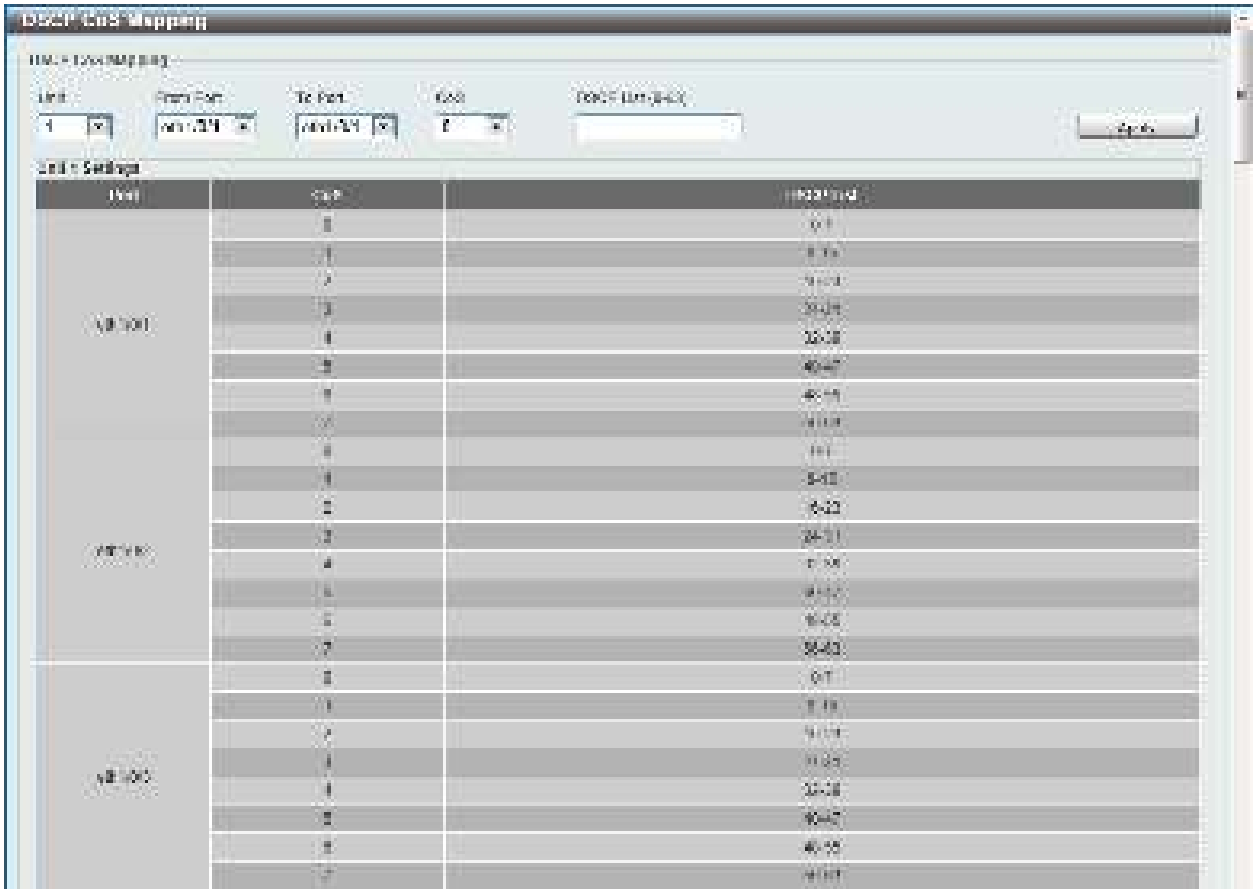


Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
CoS	Select the CoS value. Options to choose from are **0** to **7**.
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63.

Click the **Apply** button to accept the changes made.

CoS Color Mapping

This window is used to view and configure the CoS color mapping settings.

To view the following window, click **QoS > Advanced Settings > CoS Color Mapping**, as shown below:

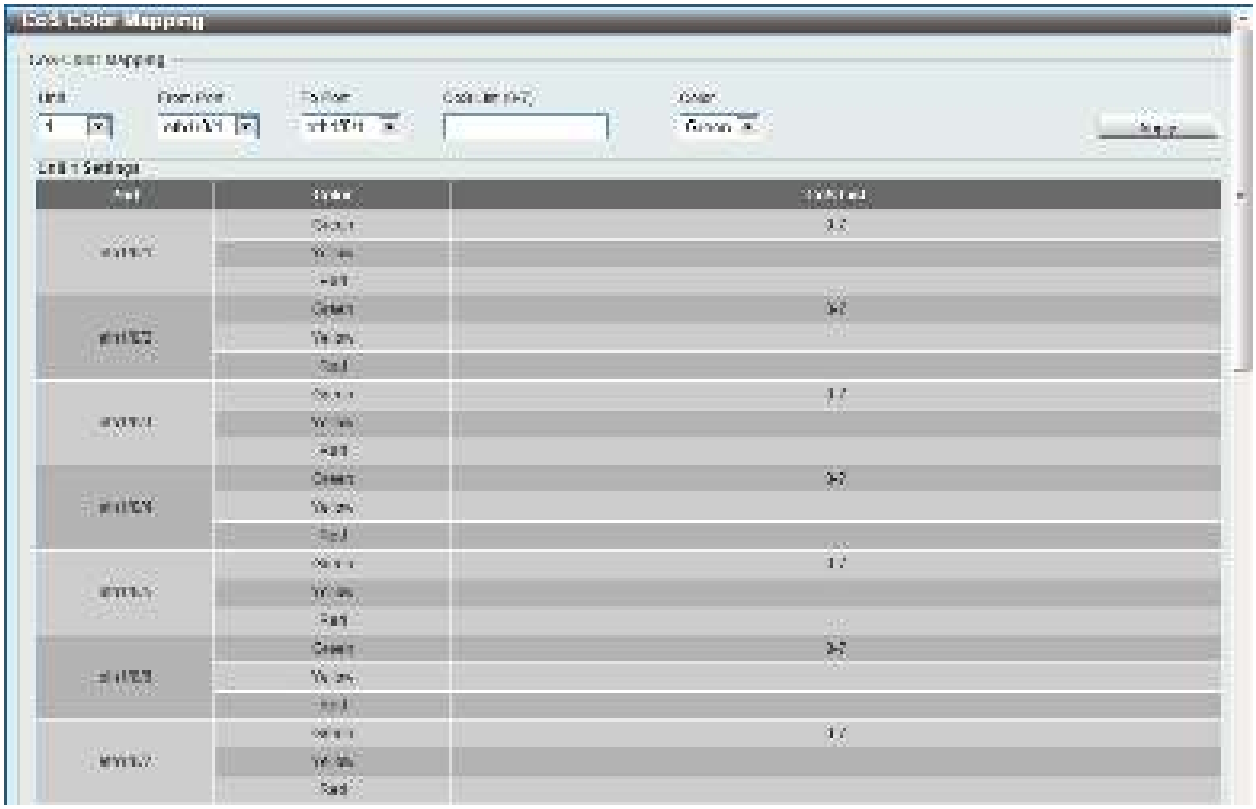


Figure 7-10 CoS Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
CoS List	Enter the CoS value that will be mapped to the color. This value must be between **0** and **7**.
Color	Select the color option. Options to choose from are **Green**, **Yellow**, and **Red**.

Click the **Apply** button to accept the changes made.

DSCP Color Mapping

This window is used to view and configure the DSCP color mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP Color Mapping**, as shown below:

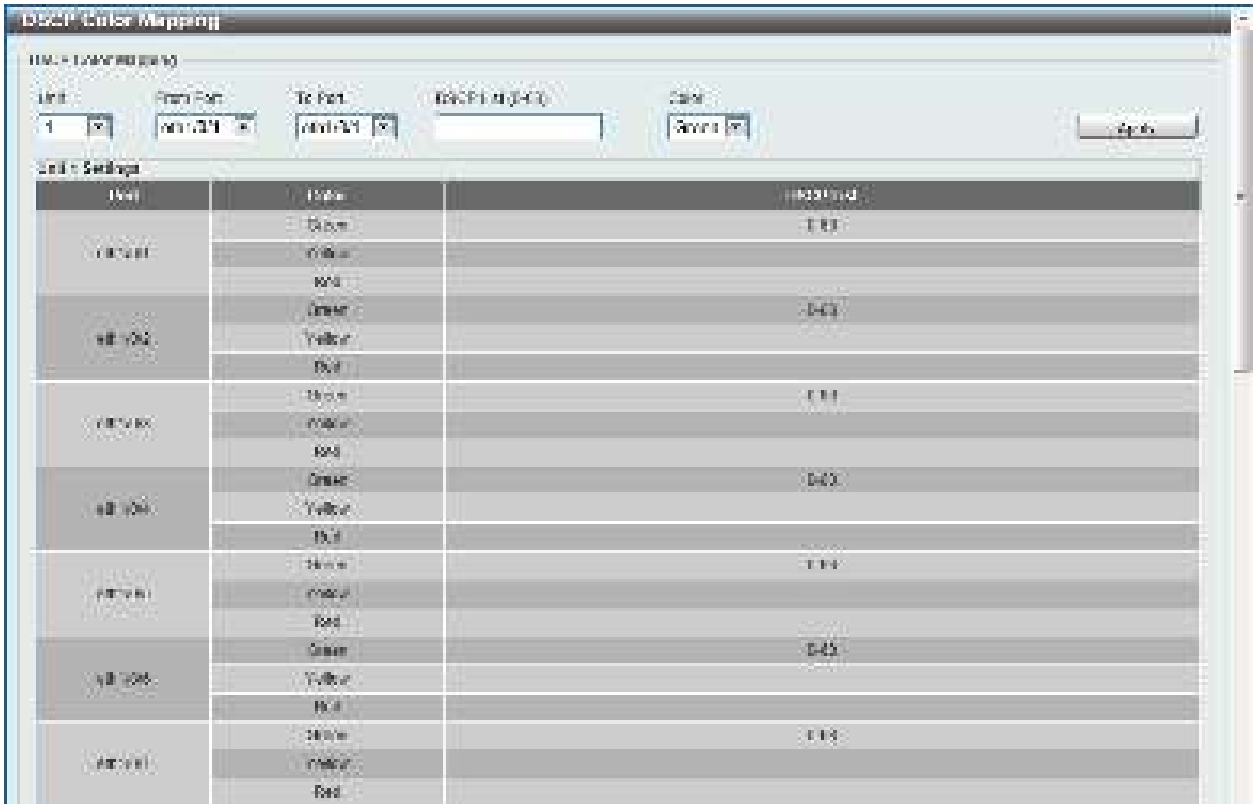


Figure 7-11 DSCP Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
DSCP List	Enter the DSCP list value here that will be mapped to a color. This value must be between 0 and 63.
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are **Green**, **Yellow**, and **Red**.

Click the **Apply** button to accept the changes made.

Class Map

This window is used to view and configure the class map settings.

To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:

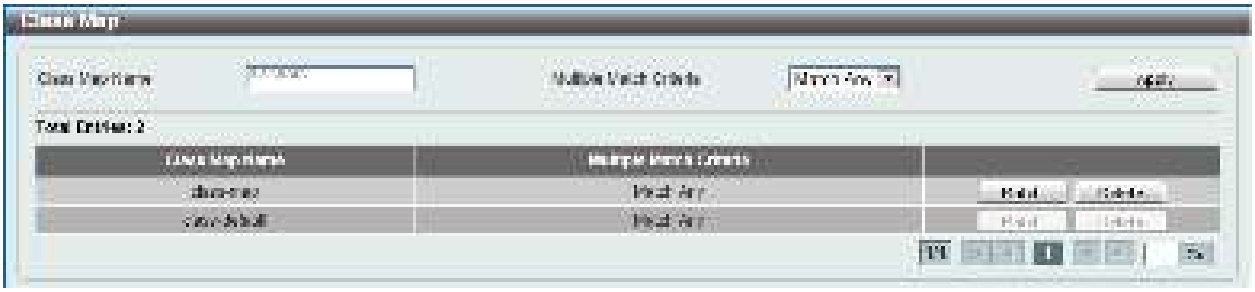


Figure 7-12 Class Map Window

The fields that can be configured are described below:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are **Match All** and **Match Any**.

Click the **Apply** button to accept the changes made.

Click the **Match** button to configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Match** button, the following window will appear.

Figure 7-13 Match Rule Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7.

Parameter	Description
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63. Tick the **IPv4 only** check box to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7. Tick the **IPv4 only** check box to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are **None**, **ARP**, **BGP**, **DHCP**, **DNS**, **EGP**, **FTP**, **IPv4**, **IPv6**, **NetBIOS**, **NFS**, **NTP**, **OSPF**, **PPPOE**, **RIP**, **RTSP**, **SSH**, **Telnet**, and **TFTP**.
VID List	Select and enter the VLAN list value that will be matched with the class map here. 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.

Aggregate Policer

This window is used to view and configure the aggregate policer settings.

To view the following window, click **QoS > Advanced Settings > Aggregate Policer**, as shown below:

Figure 7-14 Aggregate Policer Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer's name here.
Average Rate	Enter the average rate value here. This value must be between **0** and **10000000** kbps.
Normal Burst Size	Enter the normal burst size value here. This value must be between **0** and **16384** Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. This value must be between 0 and **16384** Kbytes.
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to **Transmit**. Options to choose from are:

Parameter	Description
	• **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Enter the IP DSCP value in the space provided. This value sets the IP Differentiated Services Code Point (DSCP) value and transmits the packet with the new IP DSCP value. • **Set-1P-Transmit** - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. • **Set-DSCP-1P** - Enter the IP DSCP and 1P transmit values in the spaces provided. • **Transmit** - Specifies that packets will be transmitted unaltered.
Exceed Action	Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is **Drop**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. • **Set-1P-Transmit** - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. • **Set-DSCP-1P** - Enter the IP DSCP and 1P transmit values in the spaces provided. • **Transmit** - Specifies that packets will be transmitted unaltered.
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. • **Set-1P-Transmit** - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. • **Set-DSCP-1P** - Enter the IP DSCP and 1P transmit values in the spaces provided. • **Transmit** - Specifies that packets will be transmitted unaltered.
Color Aware	Select this option to enable or disable color aware option here. When color aware is not specified, the policer works in the colorblind mode. When color aware is enabled, the policer works in the color aware mode.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

After clicking the **Two Rate Setting** tab, at the top of the page, the following page will be available.

Figure 7-15 Two Rate Settings Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer's name here.
CIR	Enter the Committed Information Rate (CIR) value here. This value must be between 0 and 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. This value must be between 0 and 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.
PIR	Enter the Peak information Rate (PIR) value here. This value must be between 0 and 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. This value must be between 0 and 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to **Transmit**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. • **Set-1P-Transmit** - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. • **Set-DSCP-1P** - Enter the IP DSCP and 1P transmit values in the spaces provided. • **Transmit** - Specifies that packets will be transmitted unaltered.
Exceed Action	Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is **Drop**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. • **Set-1P-Transmit** - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. • **Set-DSCP-1P** - Enter the IP DSCP and 1P transmit values in the spaces provided.

Parameter	Description
	• **Transmit** - Specifies that packets will be transmitted unaltered.
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Enter the IP DSCP value in the space provided. This value sets the IP DSCP value and transmits the packet with the new IP DSCP value. • **Set-1P-Transmit** - Enter the 1P transmit value in the space provided. This value sets the IEEE 802.1p value and transmits the packet with the new value. • **Set-DSCP-1P** - Enter the IP DSCP and 1P transmit values in the spaces provided. • **Transmit** - Specifies that packets will be transmitted unaltered.
Color Aware	Select this option to enable or disable color aware option here. When color aware is not specified, the policer works in the colorblind mode. When color aware is enabled, the policer works in the color aware mode.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Policy Map

This window is used to view and configure the policy map settings.

To view the following window, click **QoS > Advanced Settings > Policy Map**, as shown below:

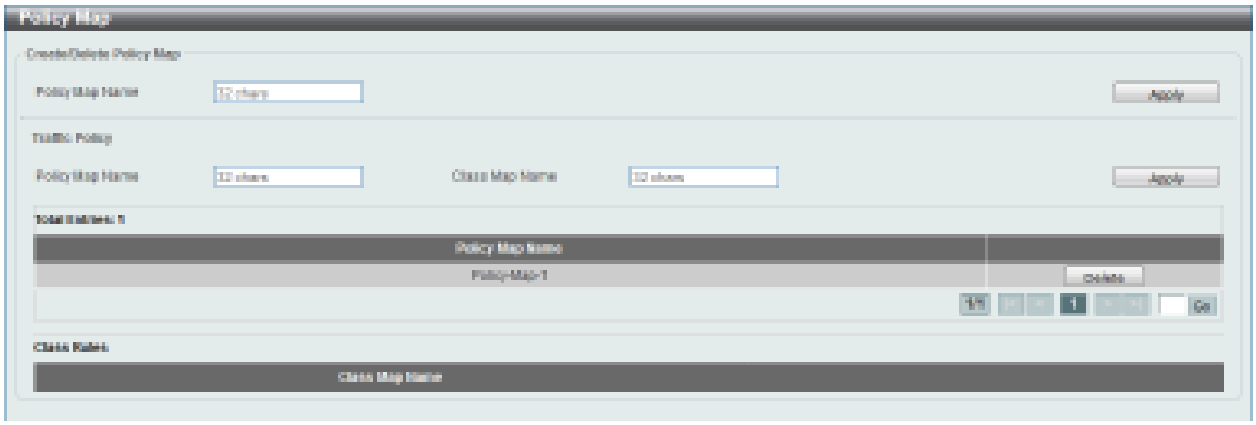


Figure 7-16 Policy Map Window

The fields that can be configured for **Create/Delete Policy Map** are described below:

Parameter	Description
Policy Map Name	Enter the policy map's name here that will be created or deleted. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map's name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map's name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To view the rules of a specific policy map, click the policy map name in the table (the **Policy Map Name** will toggle to the bold font).

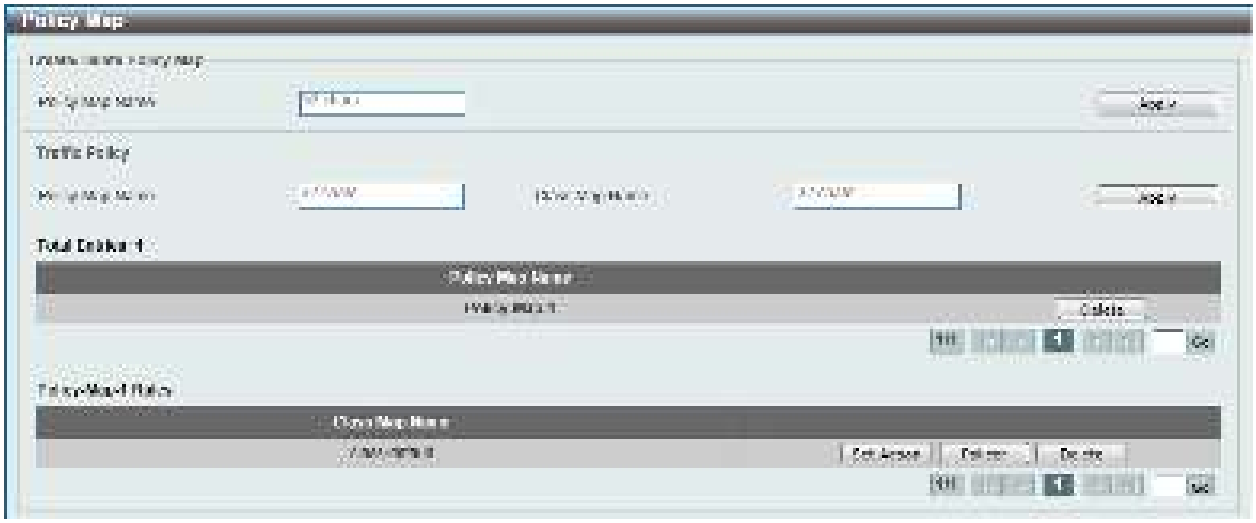


Figure 7-17 Policy Map (View Rules) Window

Click the **Set Action** button to configure the action for the policy map.

Click the **Policer** button to configure the policer action for the policy map.

Click the **Delete** button to remove the specific entry.

After clicking the **Set Action** button, the following window will appear.

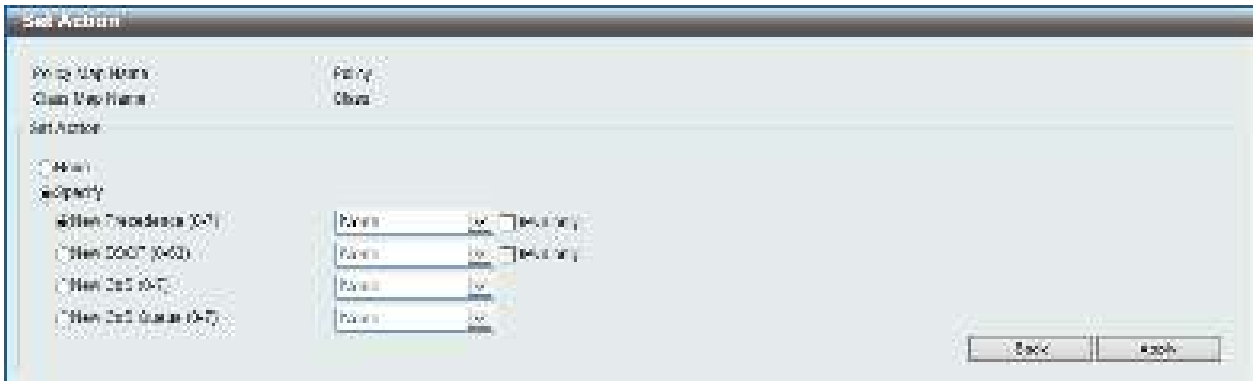


Figure 7-18 Set Action Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this policy map.
Specify	Select the option to match something to this policy map.
New Precedence	Select a new precedence for the packet. This value must be between 0 and 7. Tick the **IPv4 only** to only mark IPv4 precedence. Setting the precedence will not affect the CoS queue selection.
New DSCP	Select a new DSCP for the packet. This value must be between 0 and 63. Tick the **IPv4 only** to only mark IPv4 precedence. Setting DSCP will not affect the CoS queue selection.
New CoS	Select a new CoS value for the packet. This value must be between 0 and 7. Setting CoS will not affect the CoS queue selection.
New CoS Queue	Select a new CoS queue for the packet. This value must be between 0 and 7. This overwrites the original CoS queue selection.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

After clicking the **Policer** button, the following window will appear.

Figure 7-19 Police Action Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this policy map.
Specify	Select the option to match something to this policy map.
Average Rate	Enter the average rate in kilobits per second.
Normal Burst Size	Enter the normal burst size in kilobytes.
Maximum Burst Size	Enter the maximum burst in kilobytes.
Conform Action	Select the action to take on green color packets. Options to choose from are **Drop**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**.

Parameter	Description
Exceed Action	Select the action to take on yellow color packets. Options to choose from are **Drop**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**.
Violate Action	Select the action to take on red color packets. Options to choose from are **None**, **Drop**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**.
Color Aware	Select this option to enable or disable color aware mode.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

Policy Binding

This window is used to view and configure the policy binding settings.

To view the following window, click **QoS > Advanced Settings > Policy Binding**, as shown below:

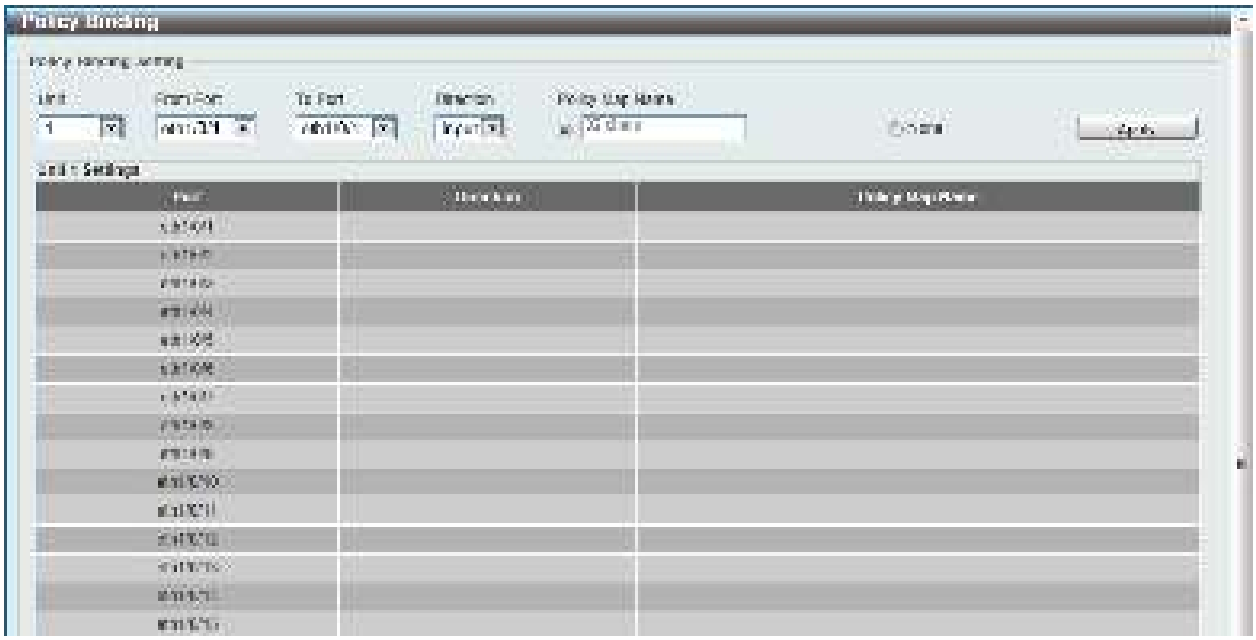


Figure 7-20 Policy Binding Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction option here. Option to choose from is **Input**. **Input** represents Input specified ingress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the **None** option to not tie a policy map to this entry.

Click the **Apply** button to accept the changes made.

8. Access Control List (ACL)

ACL Configuration Wizard
ACL Access List
ACL Interface Access Group
ACL VLAN Access Map
ACL VLAN Filter

ACL Configuration Wizard

This window is used to guide the user to create a new ACL access list or configure an existing ACL access list.

To view the following window, click **ACL > ACL Configuration Wizard**, as shown below:

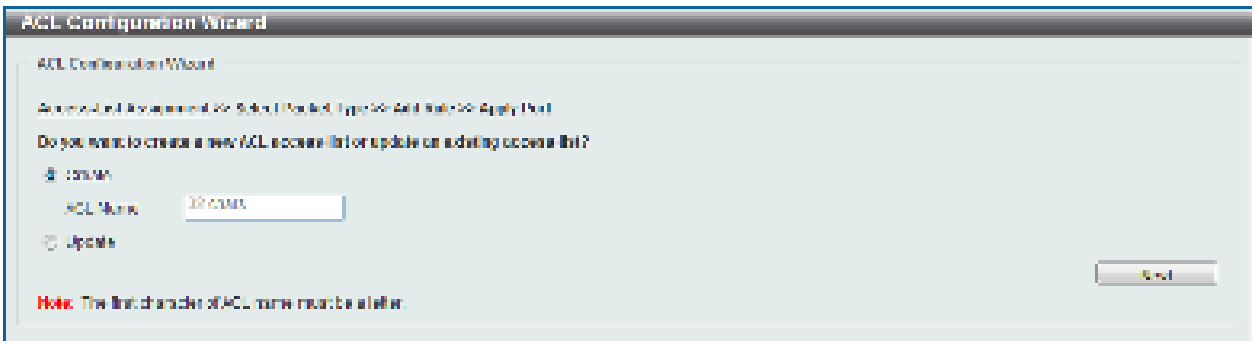


Figure 8-1 ACL Configuration Wizard (Access-List Assignment) - Create Window

Figure 8-2 ACL Configuration Wizard (Access-List Assignment) - Update Window

The fields that can be configured are described below:

Parameter	Description
Create	Select and enter the ACL name with a maximum of 32 characters.
Update	Select to see a table below with the existing ACL access lists. Select the specific re-configure the entry.

Click the **Next** button to continue.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Next** button, the following window will appear.

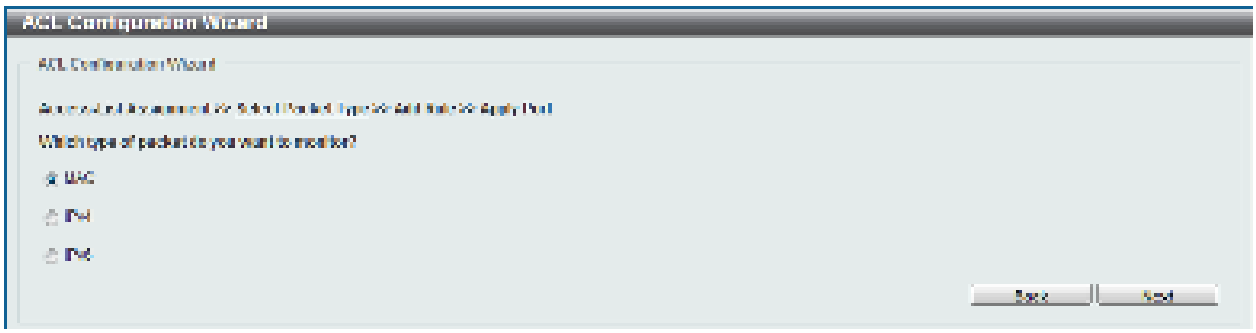


Figure 8-3 ACL Configuration Wizard (Select Packet Type) Window

The fields that can be configured are described below:

Parameter	Description
MAC	Select to be MAC ACL.
IPv4	Select to be IPv4 ACL.
IPv6	Select to be IPv6 ACL.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

After clicking the **MAC** radio button and the **Next** button, the following window will appear.

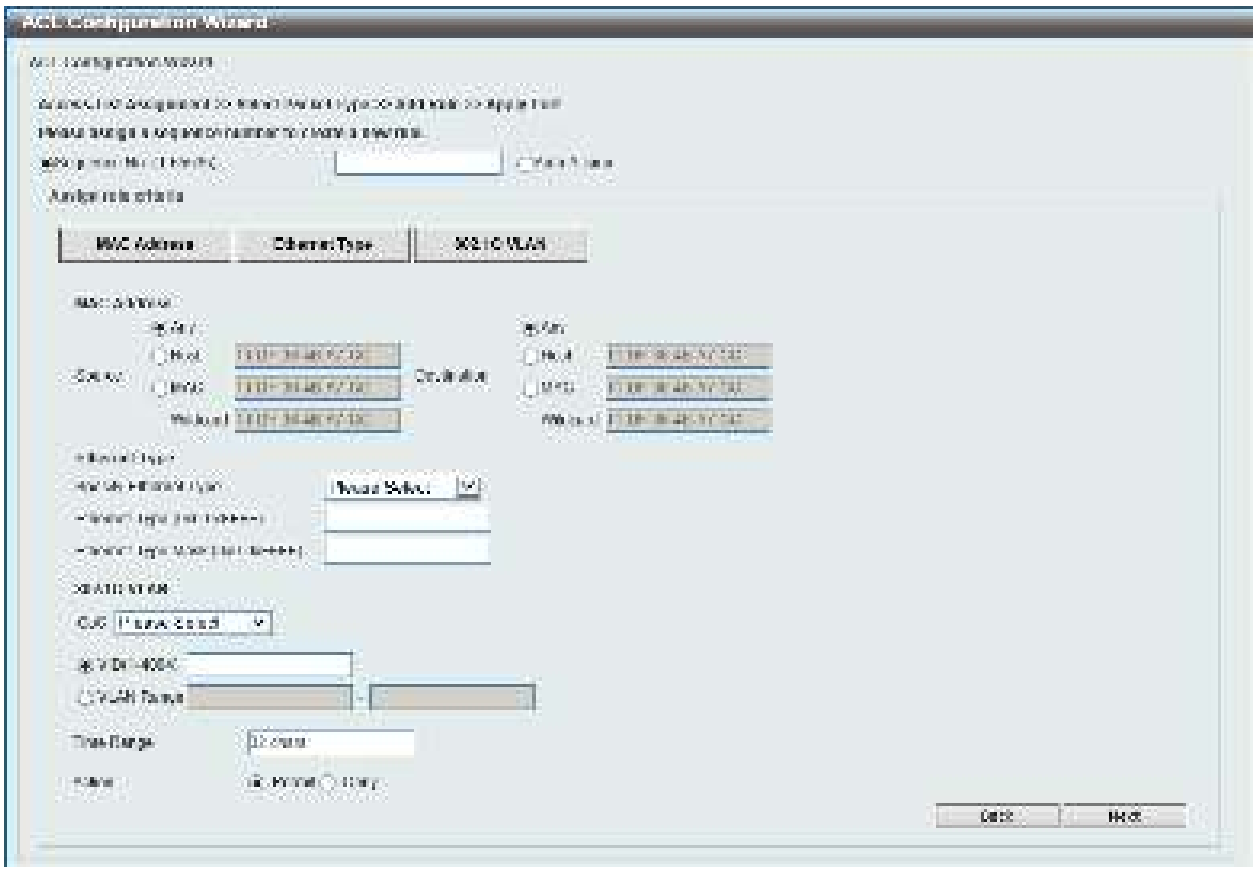


Figure 8-4 ACL Configuration Wizard (Add Rule for MAC ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are **aarp**, **appletalk**, **decent-iv**, **etype-6000**, **etype-8042**, **lat**, **lavc-sca**, **mop-console**, **mop-dump**, **vines-echo**, **vines-ip**, **xns-idp**, and **arp**.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value used here. This value is between **0** and **7**.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

After clicking the **IPv4** radio button and the **Next** button, the following window will appear.

Figure 8-5 ACL Configuration Wizard (Add Rule for IPv4 ACL) Window

This window has a dynamic section. Every selection made in the **Protocol Type** drop-down list will change the bottom part of this window.

The **fixed** fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, and **None**.

After selecting the **TCP** option as the **Protocol Type**, the following section will appear.

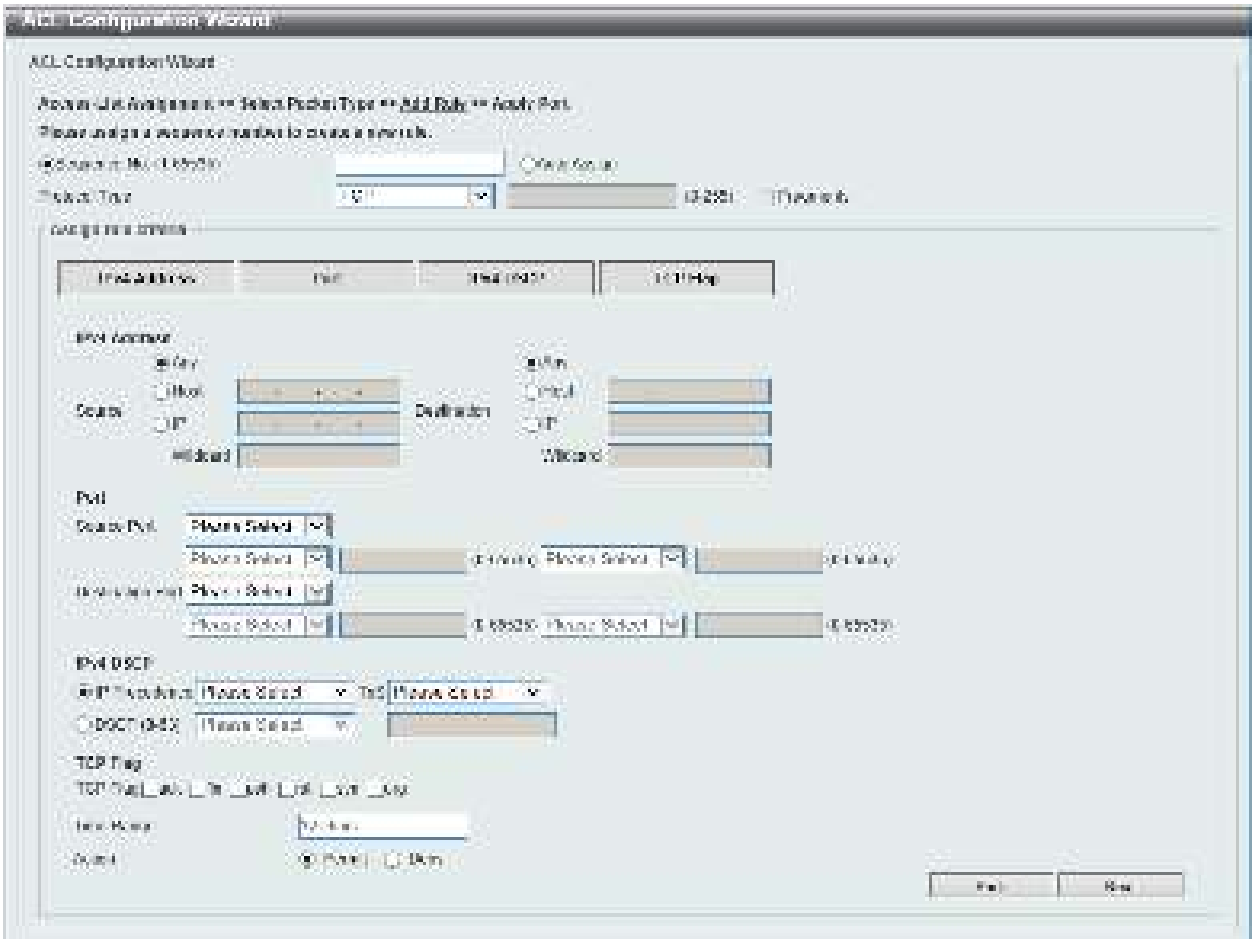


Figure 8-6 ACL Configuration Wizard (Add Rule for IPv4 ACL) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used.

Parameter	Description
	• **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **UDP** option as the **Protocol Type**, the following section will appear.

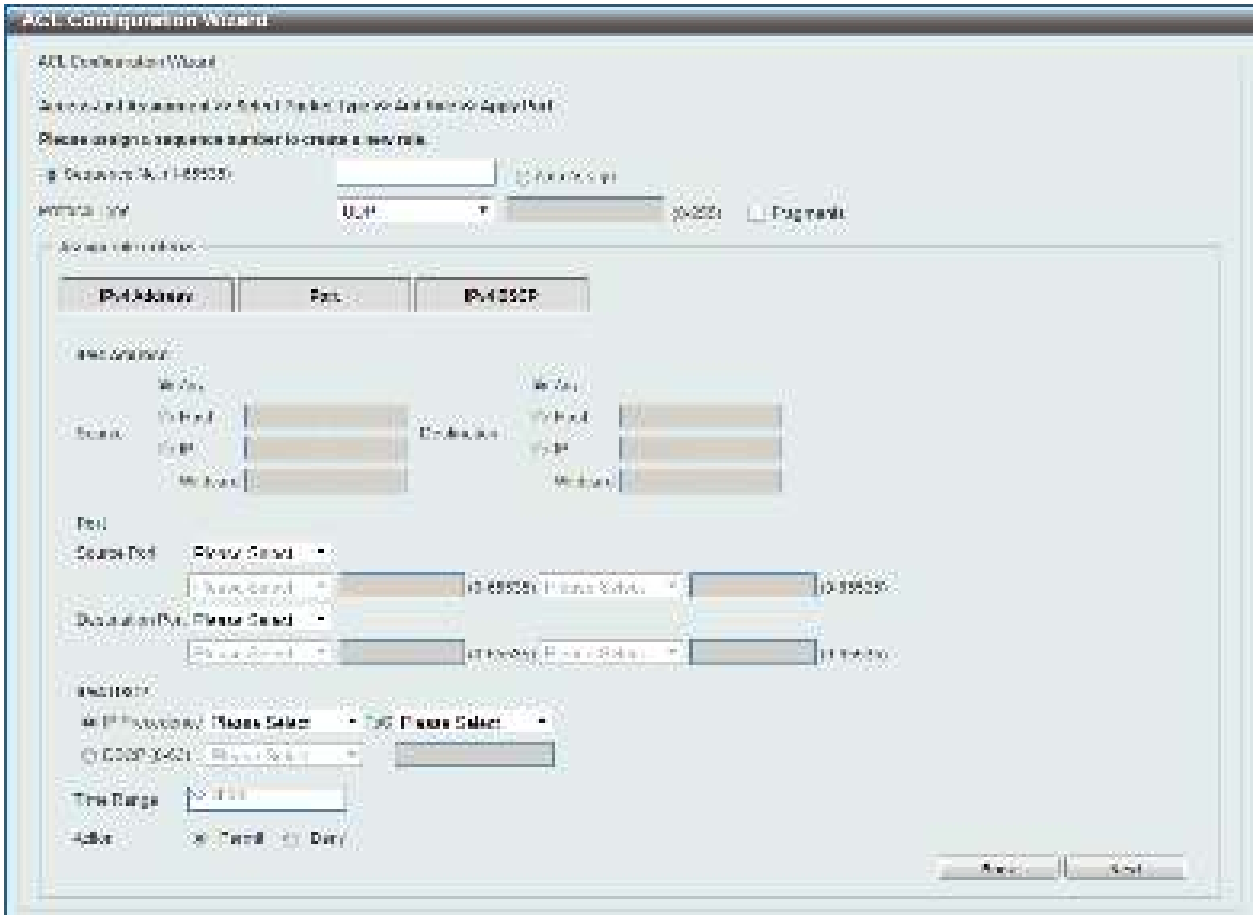


Figure 8-7 ACL Configuration Wizard (Add Rule for IPv4 ACL) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used.

Parameter	Description
	• **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **ICMP** option as the **Protocol Type**, the following section will appear.

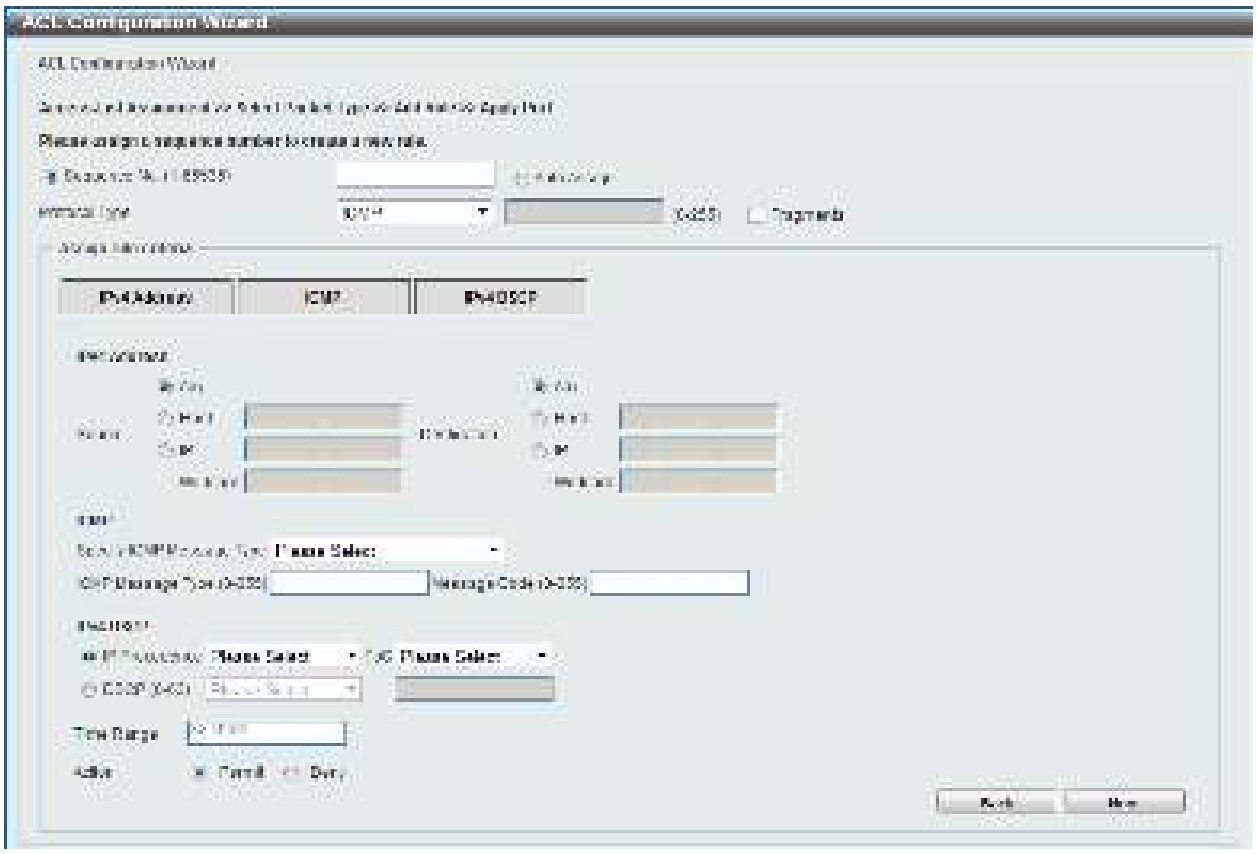


Figure 8-8 ACL Configuration Wizard (Add Rule for IPv4 ACL) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.

Parameter	Description
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, or **Protocol ID** option as the **Protocol Type**, the following section will appear.

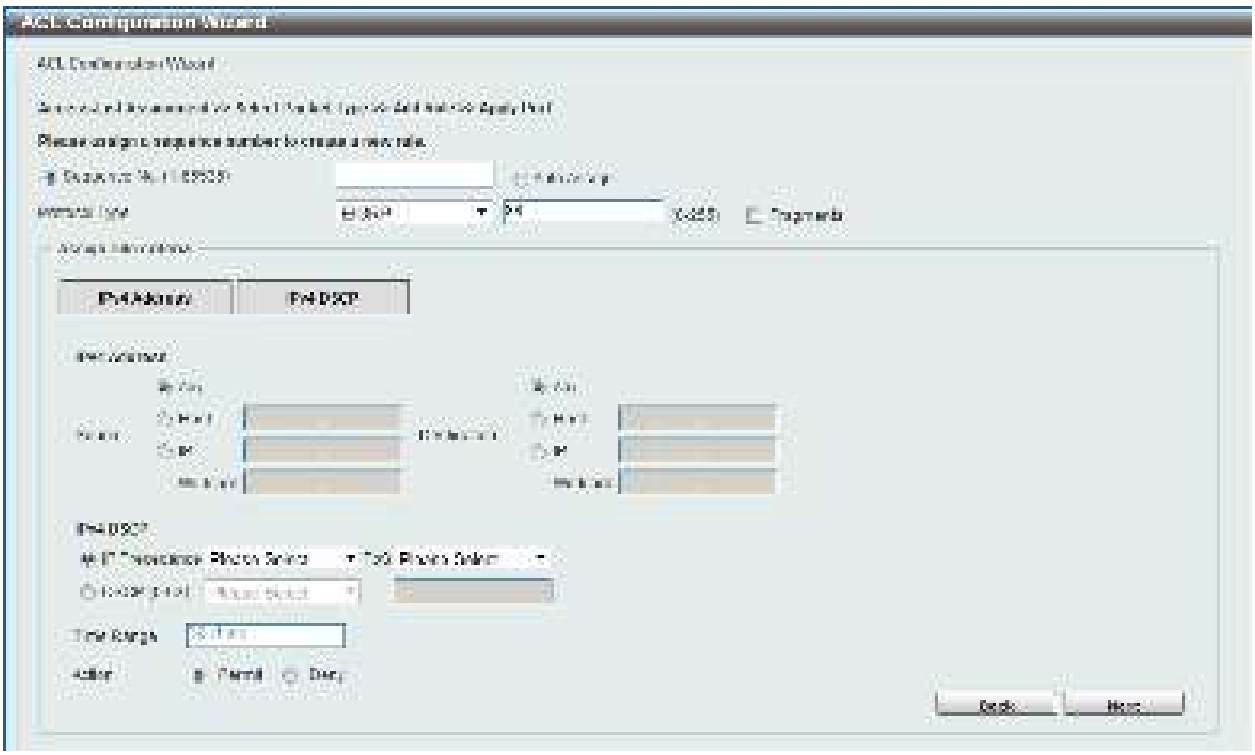


Figure 8-9 ACL Configuration Wizard (Add Rule for IPv4 ACL) EIGRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the **Fragments** option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap.

Parameter	Description
	The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **None** option as the **Protocol Type**, the following section will appear.

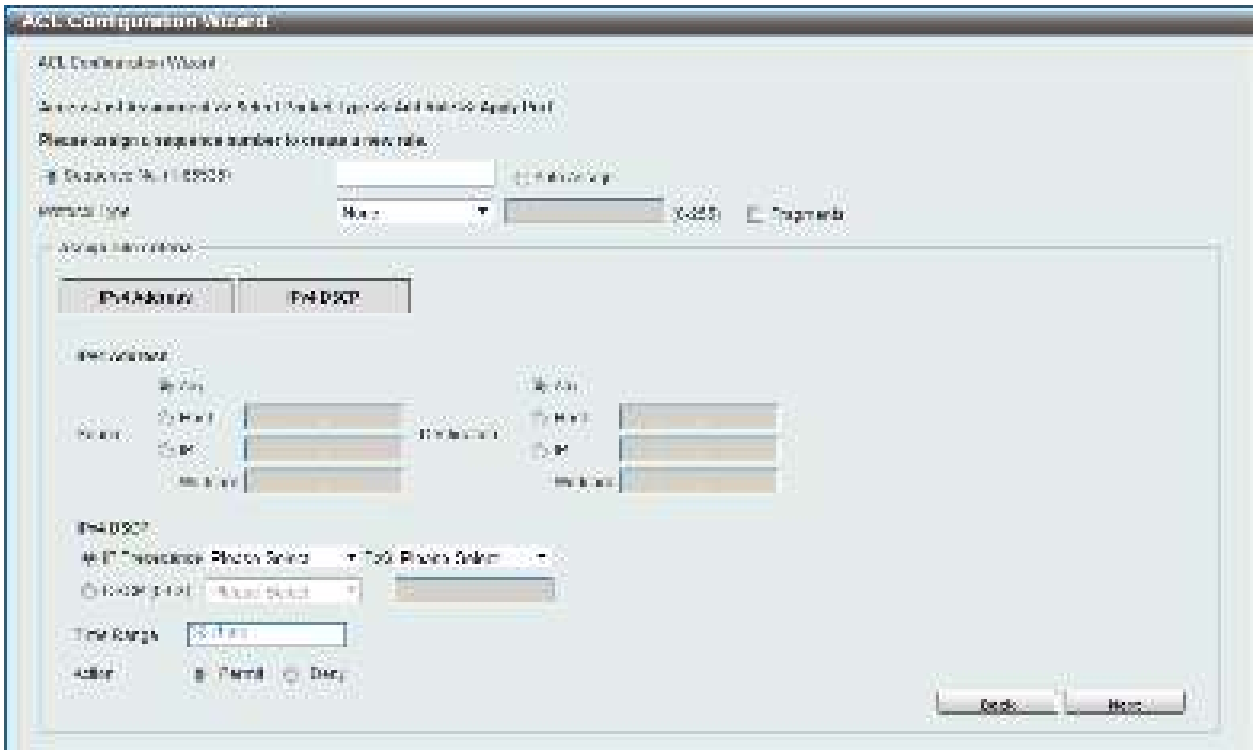


Figure 8-10 ACL Configuration Wizard (Add Rule for IPv4 ACL) None Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the **Fragments** option to include packet fragment filtering.

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

After clicking the **IPv6** radio button and the **Next** button, the following window will appear.

Figure 8-11 ACL Configuration Wizard (Add Rule for IPv6 ACL) Window

This window has a dynamic section. Every selection made in the **Protocol Type** drop-down list will change the bottom part of this window.

The **fixed** fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **Protocol ID**, **ESP**, **PCP**, **SCTP**, and **None**.

After selecting the **TCP** option as the **Protocol Type**, the following section will appear.

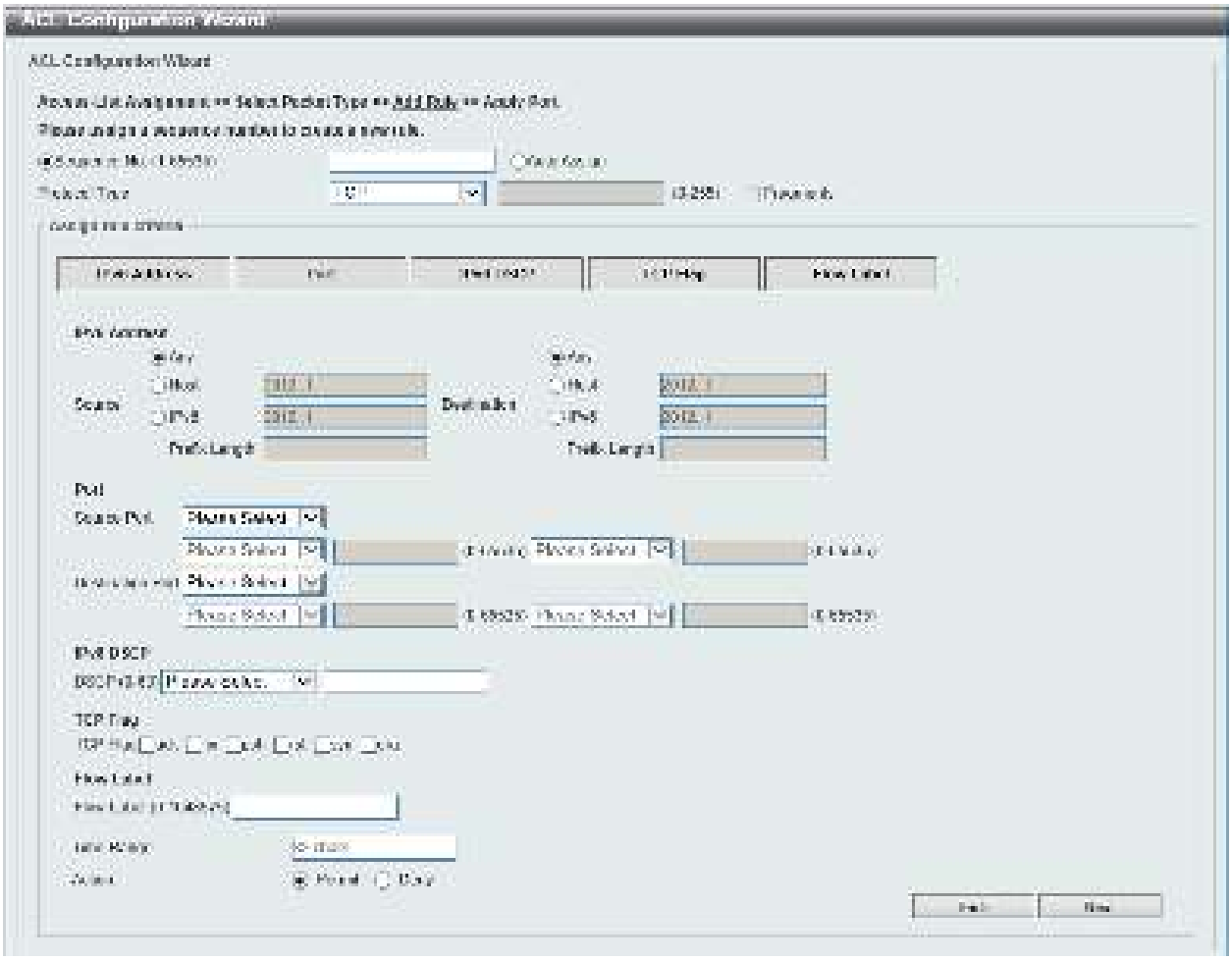


Figure 8-12 ACL Configuration Wizard (Add Rule for IPv6 ACL) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:

Parameter	Description
	• **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **UDP** option as the **Protocol Type**, the following section will appear.

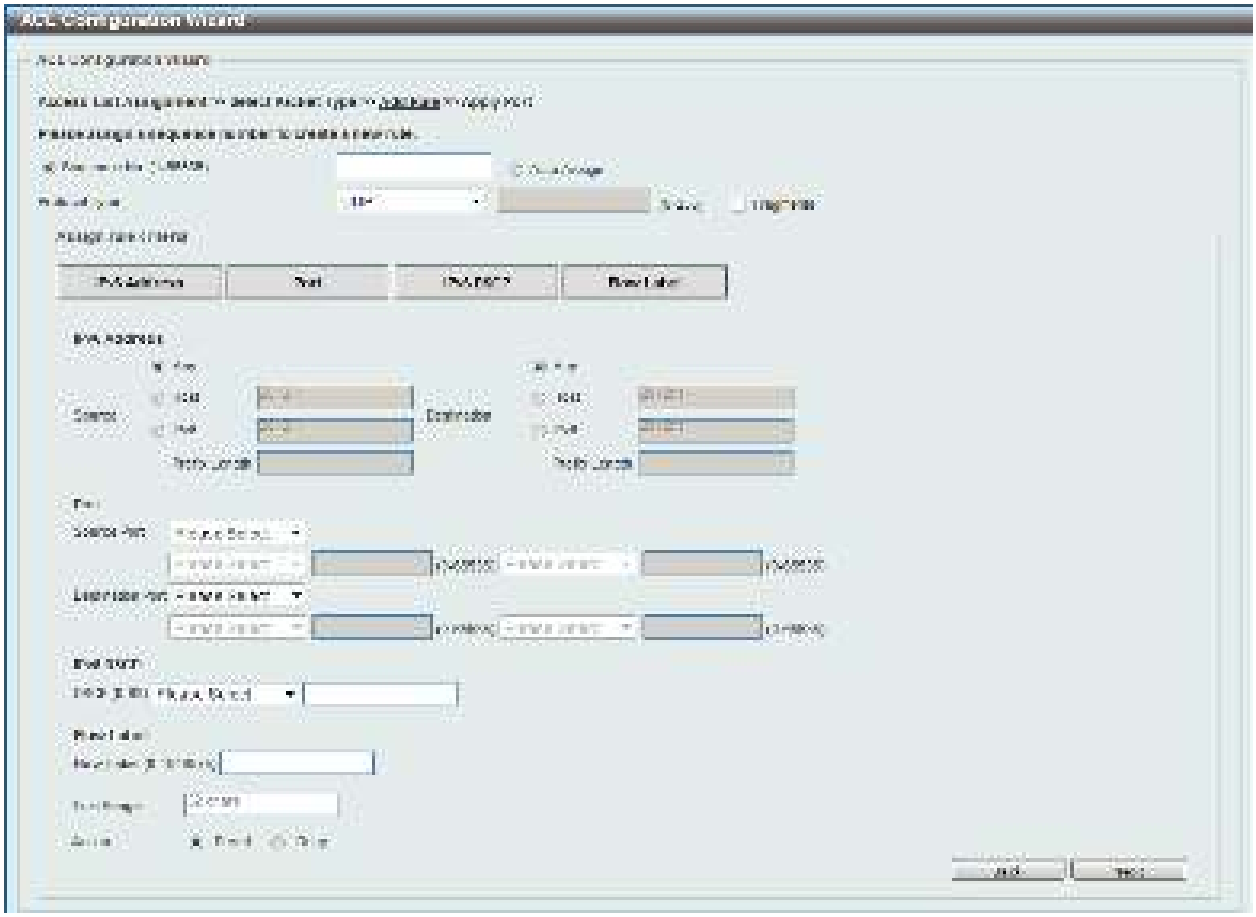


Figure 8-13 ACL Configuration Wizard (Add Rule for IPv6 ACL) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s)

Parameter	Description
	provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **ICMP** option as the **Protocol Type**, the following section will appear.

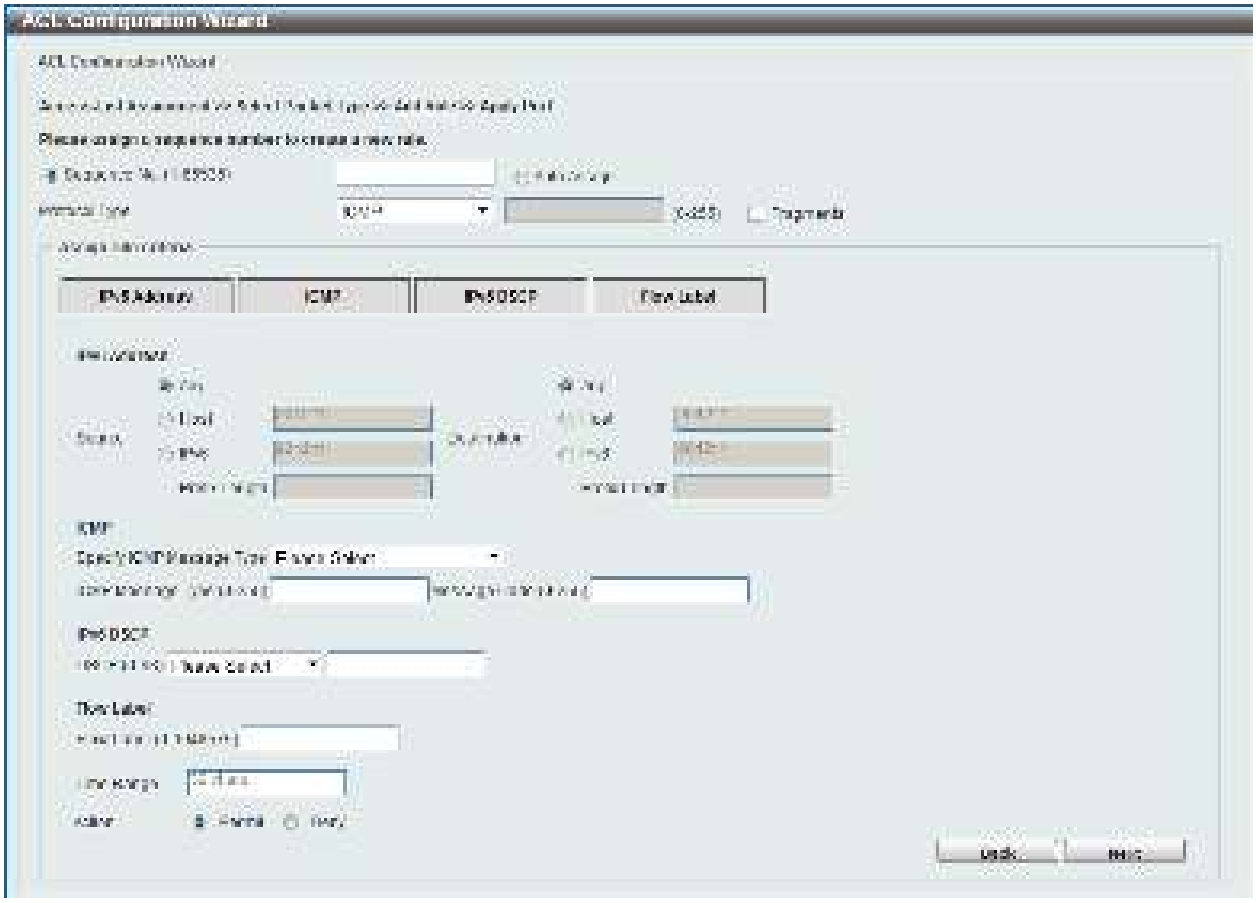


Figure 8-14 ACL Configuration Wizard (Add Rule for IPv6 ACL) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the **ICMP Message Type** is selected, this numerical value will automatically be entered. When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here.
Message Code	When the **ICMP Message Type** is selected, this numerical value will automatically be entered. When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **Protocol ID**, **ESP**, **PCP**, or **SCTP** option as the **Protocol Type**, the following section will appear.

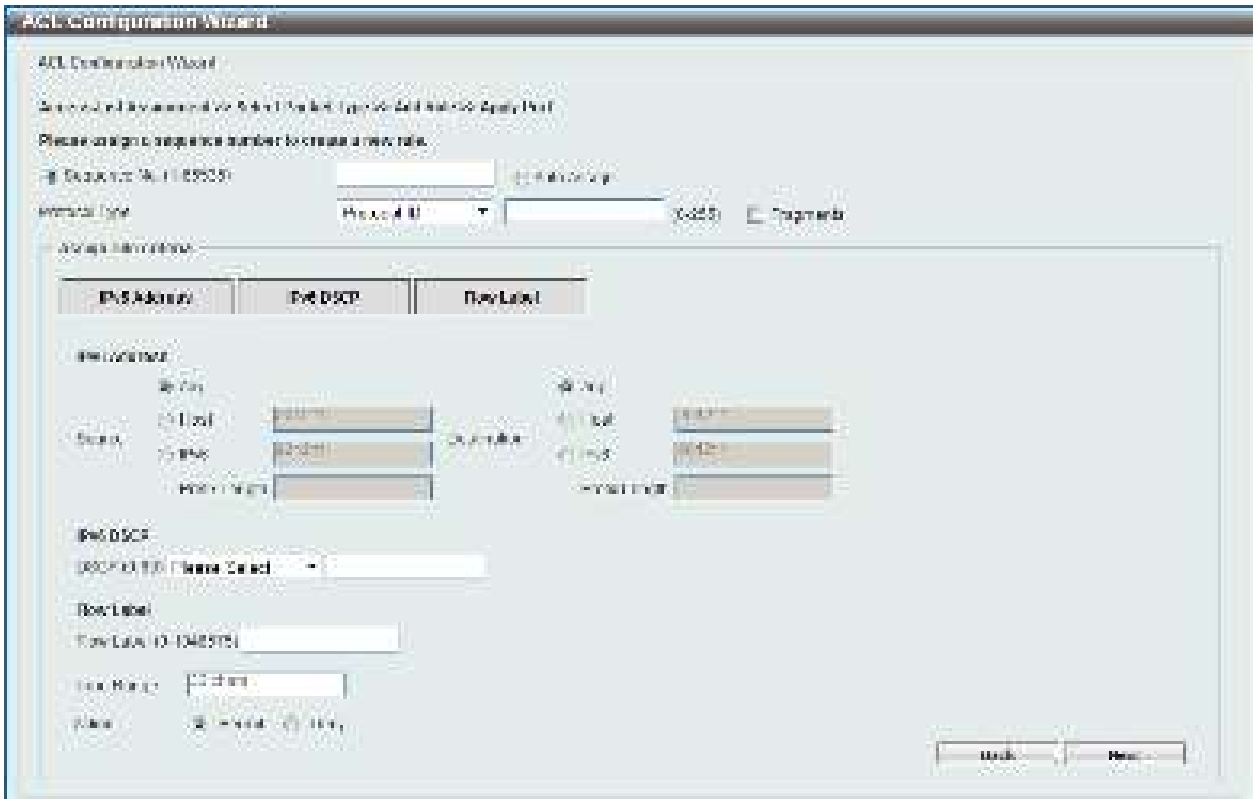


Figure 8-15 ACL Configuration Wizard (Add Rule for IPv6 ACL) Protocol ID Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Protocol	Enter the Protocol ID value used here. This value must be between 0 and 255.
Fragments	Select the **Fragments** option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between **0** and **63**.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

Parameter	Description
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

After selecting the **None** option as the **Protocol Type**, the following section will appear.

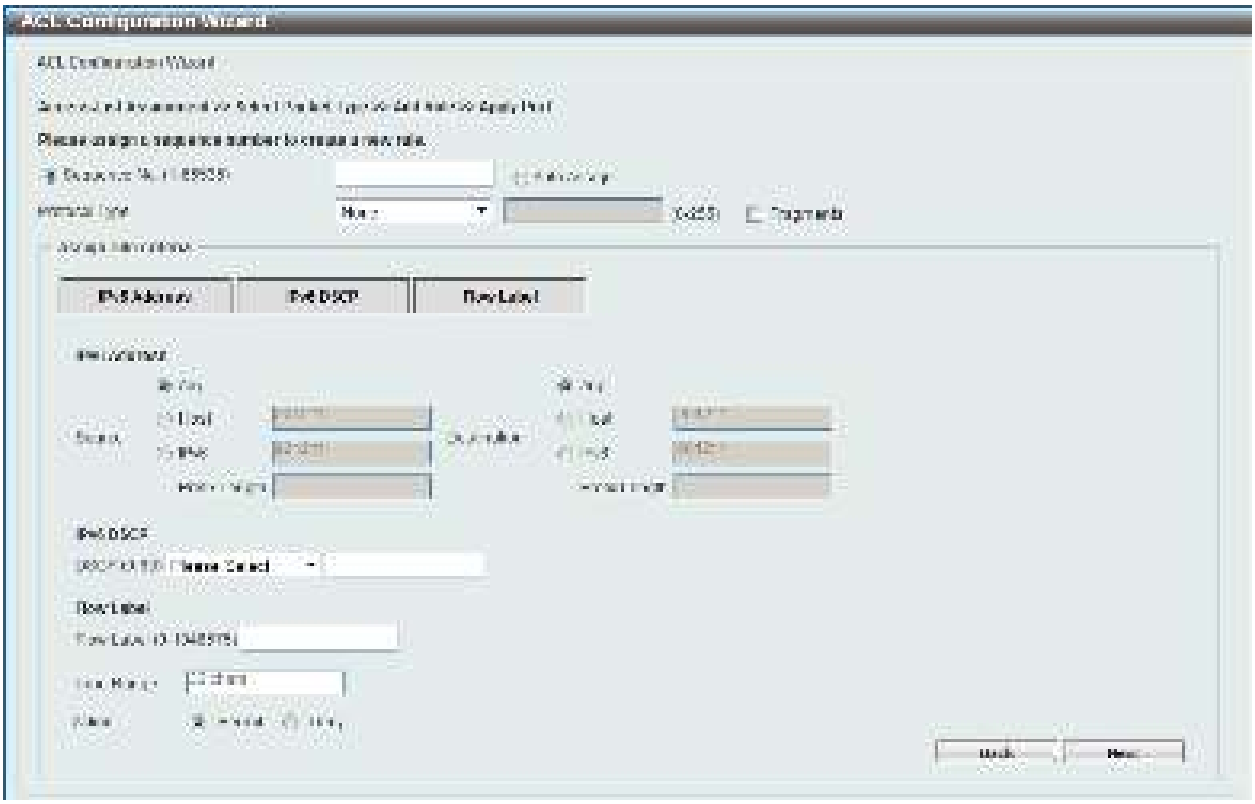


Figure 8-16 ACL Configuration Wizard (Add Rule for IPv6 ACL) None Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the **Fragments** option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.

Parameter	Description
Time Range	Enter the name of the time range to associate with this ACL rule.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

After clicking the **Next** button, the following window will appear.

Figure 8-17 ACL Configuration Wizard (Apply Port) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Option to choose from is **In**.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

ACL Access List

This window is used to view and configure the ACL access list settings.

To view the following window, click **ACL > ACL Access List**, as shown below:

Figure 8-18 ACL Access List Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type to find here. Options to choose from are **All**, **IP ACL**, **IPv6 ACL**, **MAC ACL**, and **Expert ACL**.

Parameter	Description
ID	Enter the ACL ID here. The range is from 1 to 14999.
ACL Name	Enter the ACL name here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add ACL** button to create a new ACL profile.

Click the **Clear All Counter** button to clear all the counter information displayed.

Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the **Add Rule** button to create an ACL rule for the ACL profile selected.

Standard IP ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-19 Standard IP ACL (Add ACL Access List) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ACL ID from 1 to 1999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating a Standard IP ACL profile, the newly created Standard IP ACL profile will be displayed in the ACL profile display table, as shown below:

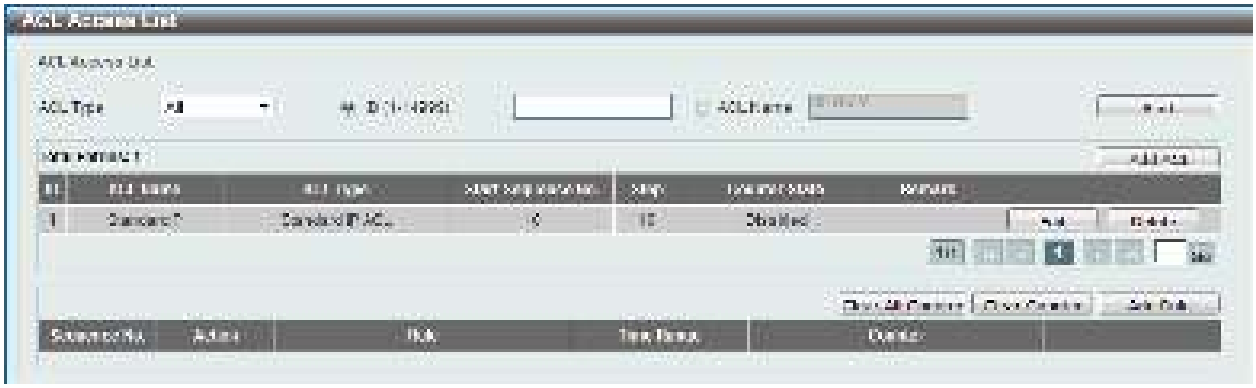


Figure 8-20 Standard IP ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

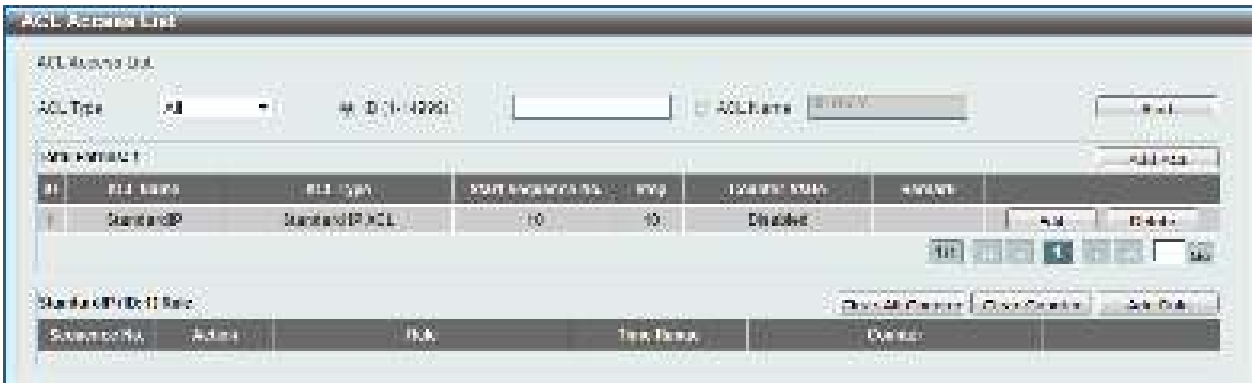


Figure 8-21 Standard IP ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

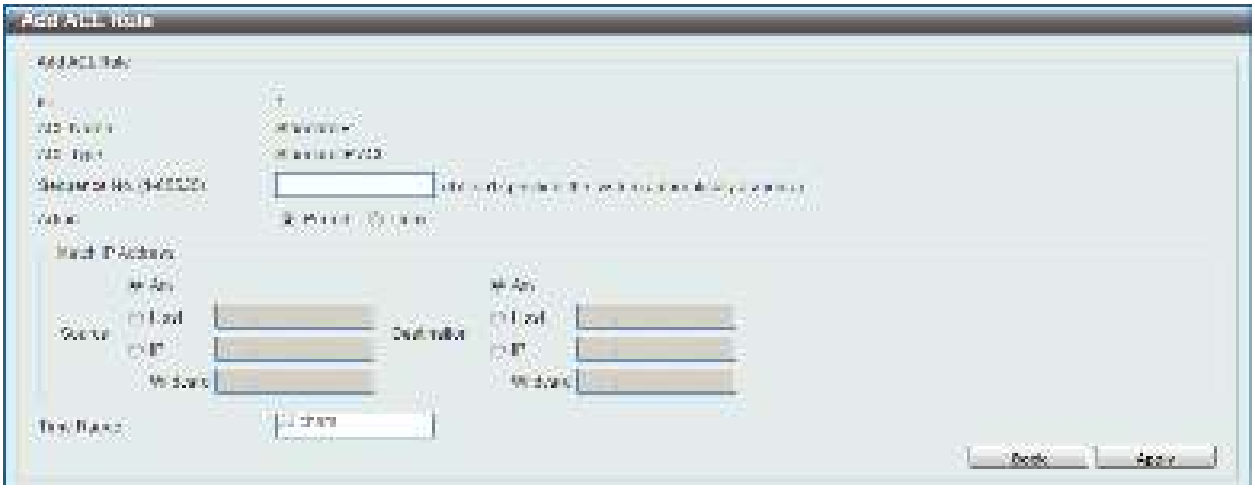


Figure 8-22 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between **1** and **65535**. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap.

Parameter	Description
	The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Time Range	Enter the name of the time range to associate with this ACL rule.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

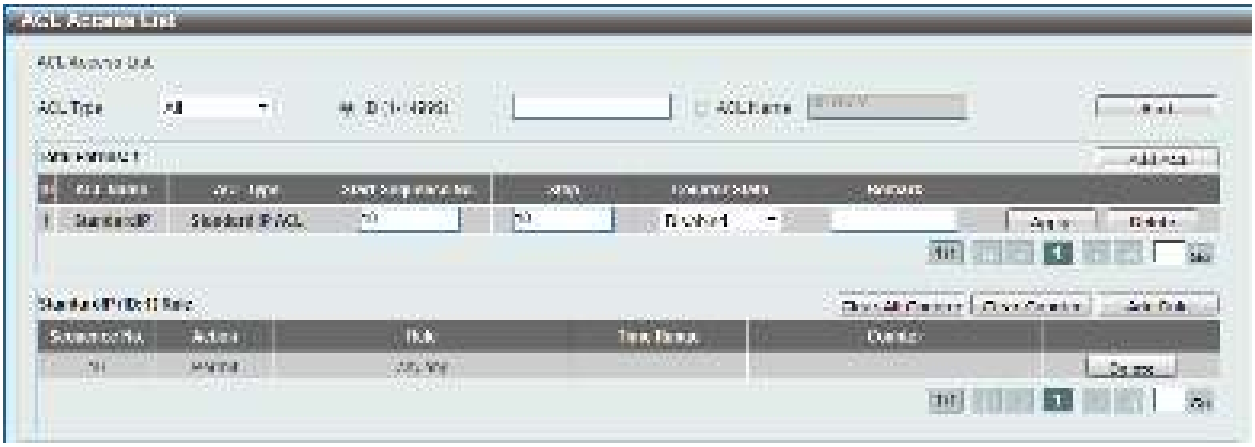


Figure 8-23 Standard IP ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number increment here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

Figure 8-24 Standard IP ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Extended IP ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-25 Extended IP ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ACL ID from 2000 to 3999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Extend IP ACL profile, the newly created Extend IP ACL profile will be displayed in the ACL profile display table, as shown below:

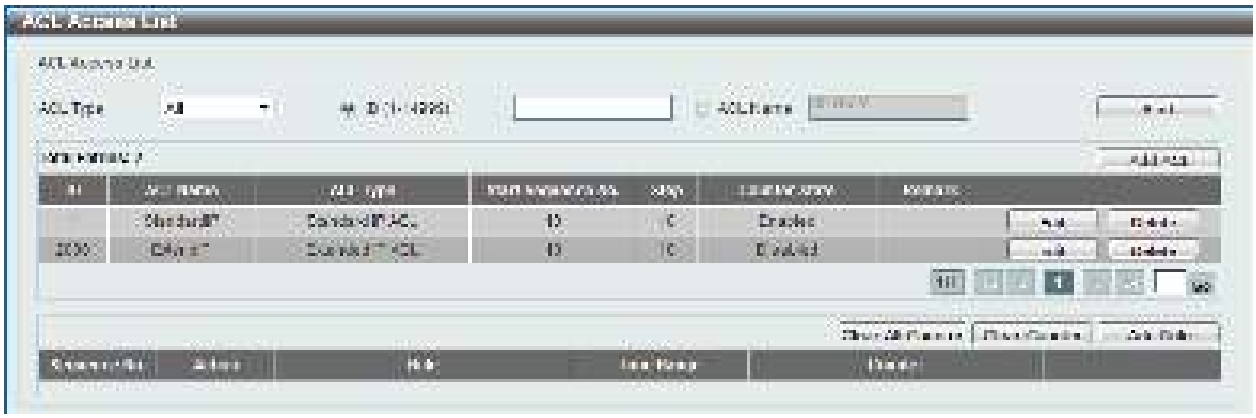


Figure 8-26 Extended IP ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

Figure 8-27 Extended IP ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

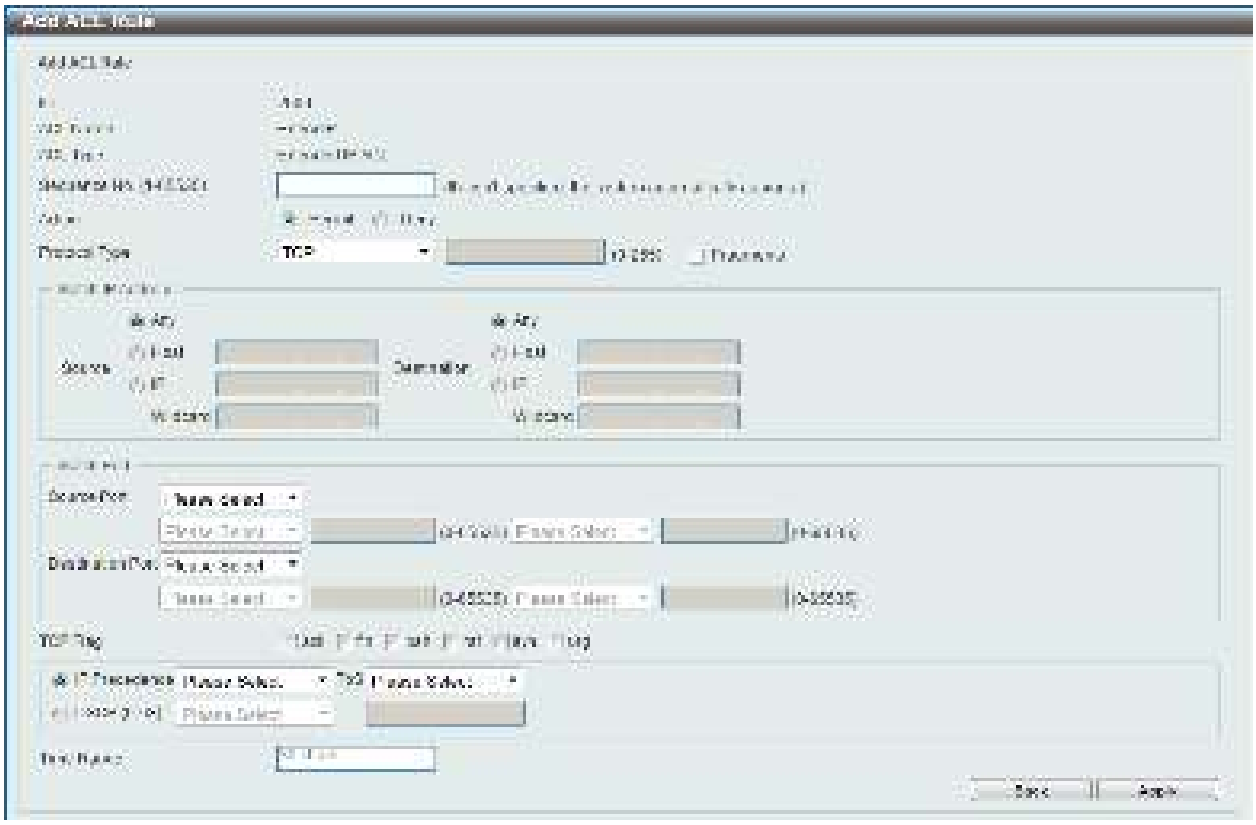


Figure 8-28 Extended IP ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** drop-down list will change the bottom part of this window.

The **fixed** fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, and **None**.

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

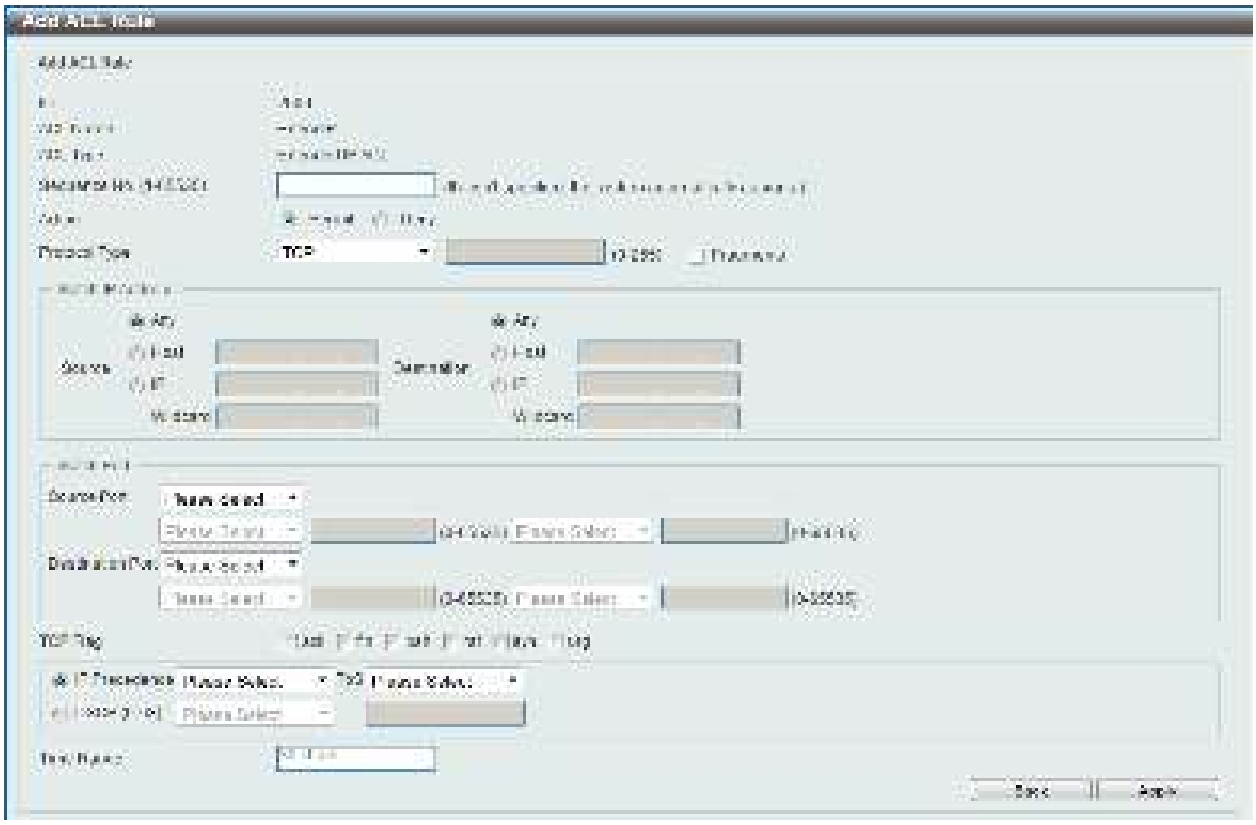


Figure 8-29 Extended IP ACL (Add Rule) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port

Parameter	Description
	number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

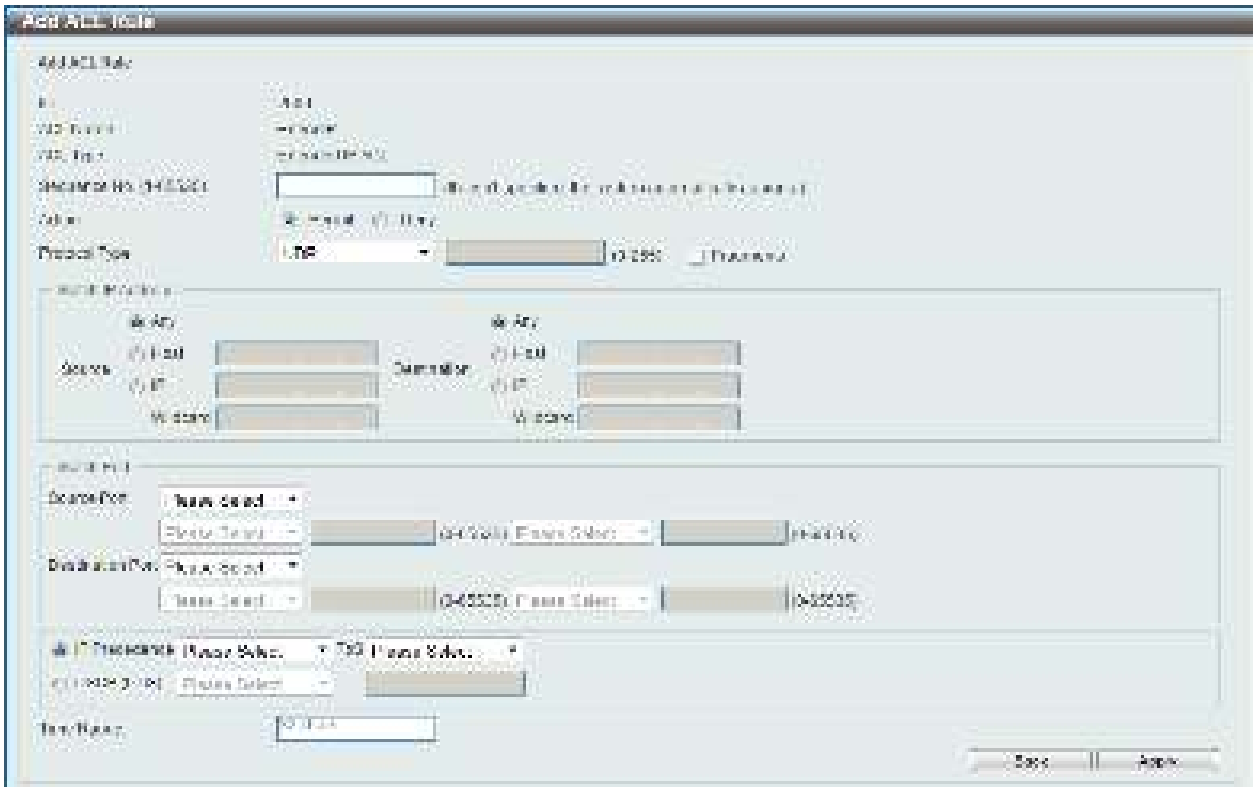


Figure 8-30 Extended IP ACL (Add Rule) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

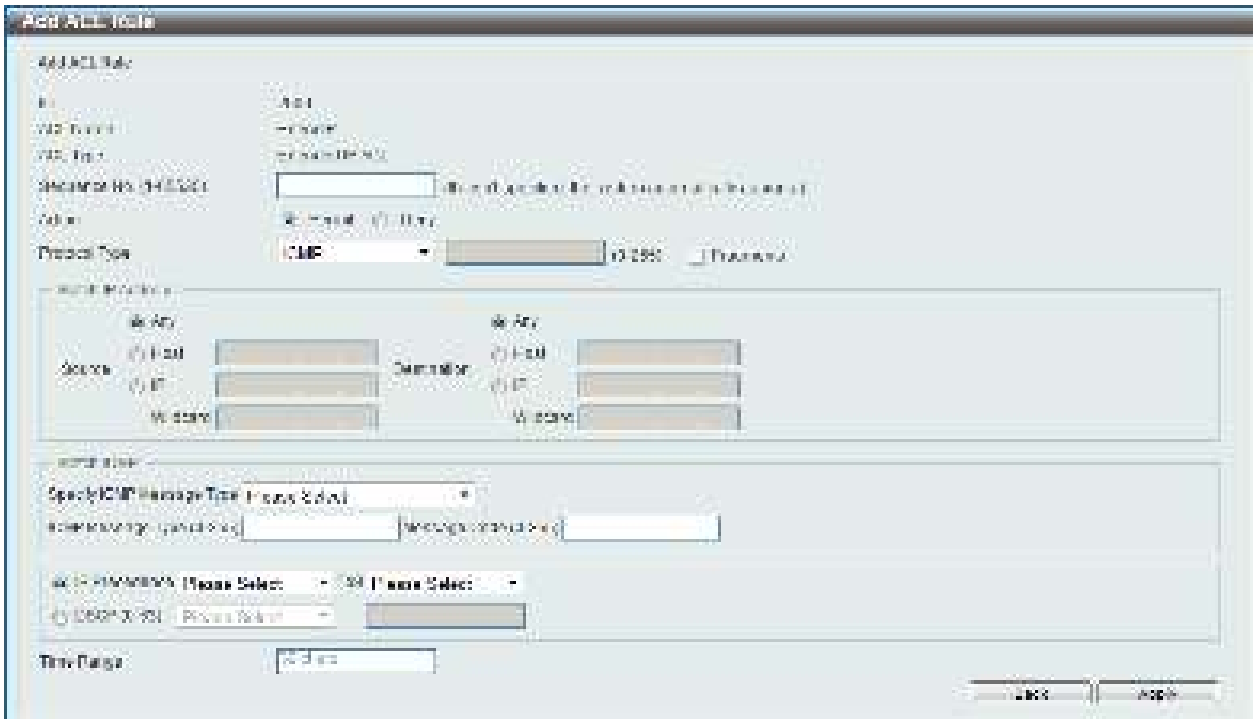


Figure 8-31 Extended IP ACL (Add Rule) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP message type is selected in the **Specify ICMP Message Type** drop-down list, this numerical value will automatically be entered. When the ICMP message type is not selected in the **Specify ICMP Message Type** drop-down list, enter the **ICMP Message Type** numerical value used here.
Message Code	When the ICMP message type is selected in the **Specify ICMP Message Type** drop-down list, this numerical value will automatically be entered.

Parameter	Description
	When the ICMP message type is not selected in the **Specify ICMP Message Type** drop-down list, enter the Message Code numerical value used here.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, or **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

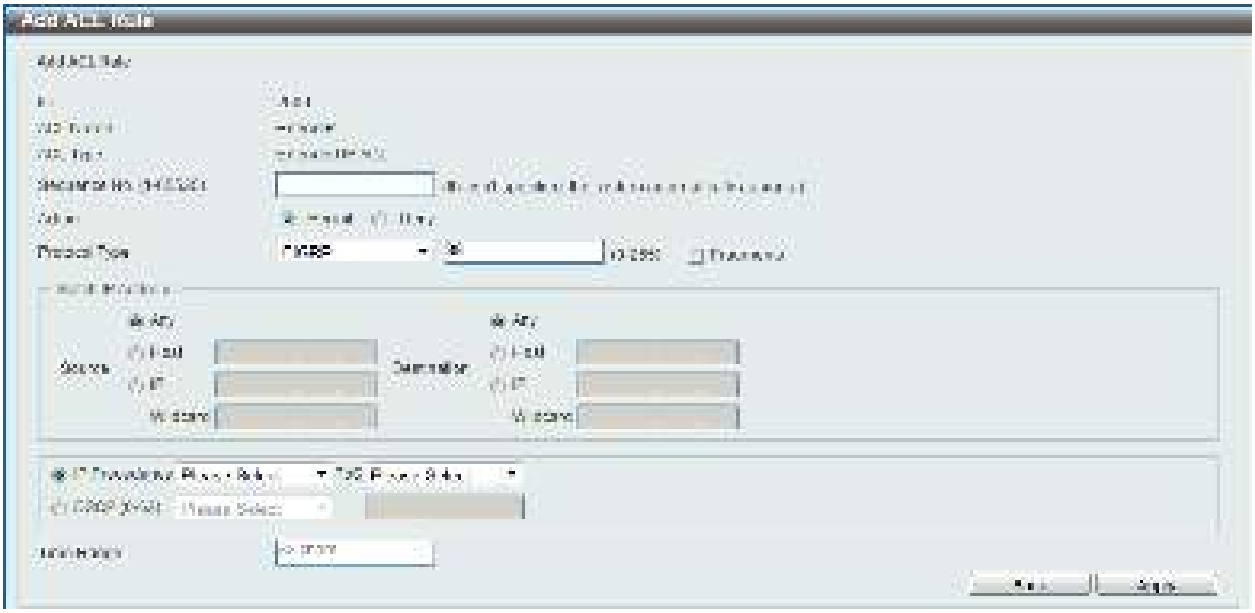


Figure 8-32 Extended IP ACL (Add Rule) EIGRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the **Fragments** option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule.

Parameter	Description
	• **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Time Range	Enter the name of the time range to associate with this ACL rule.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

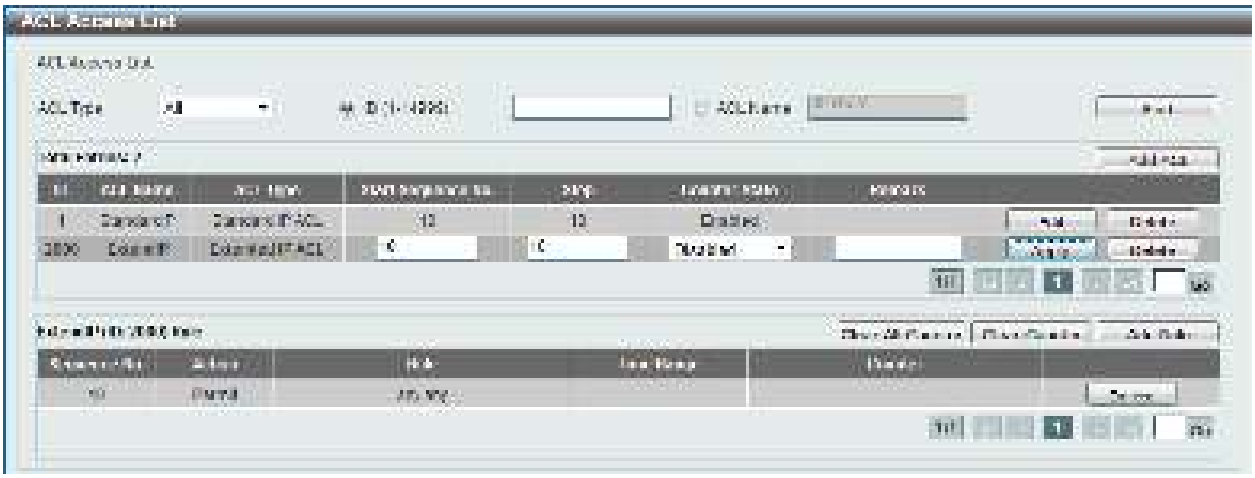


Figure 8-33 Extended IP ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number increment here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

Figure 8-34 Extended IP ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Standard IPv6 ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-35 Standard IPv6 ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ACL ID from 11000 to 12999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating a Standard IPv6 ACL profile, the newly created Standard IPv6 ACL profile will be displayed in the ACL profile display table, as shown below:

Figure 8-36 Standard IPv6 ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

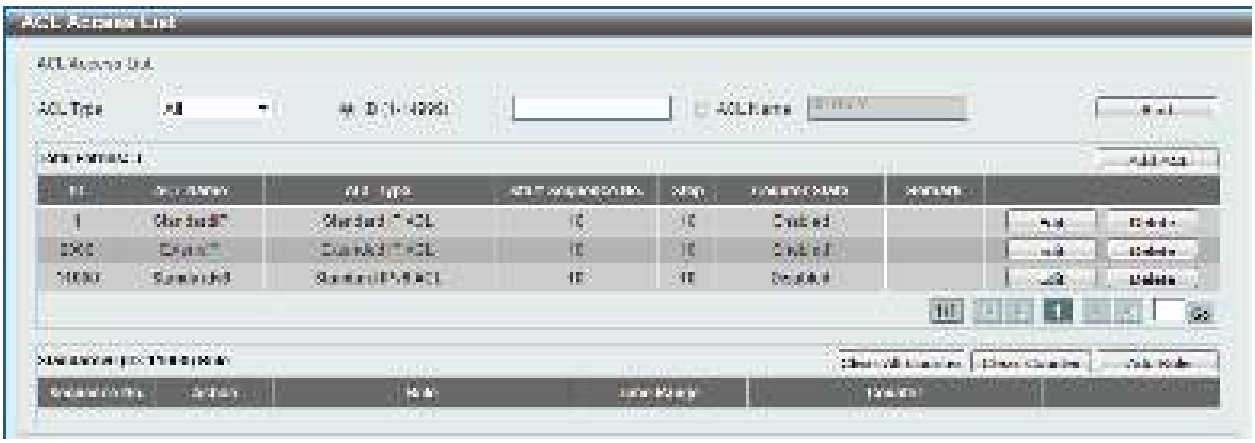


Figure 8-37 Standard IPv6 ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

Figure 8-38 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between **1** and **65535**. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range to associate with this ACL rule.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

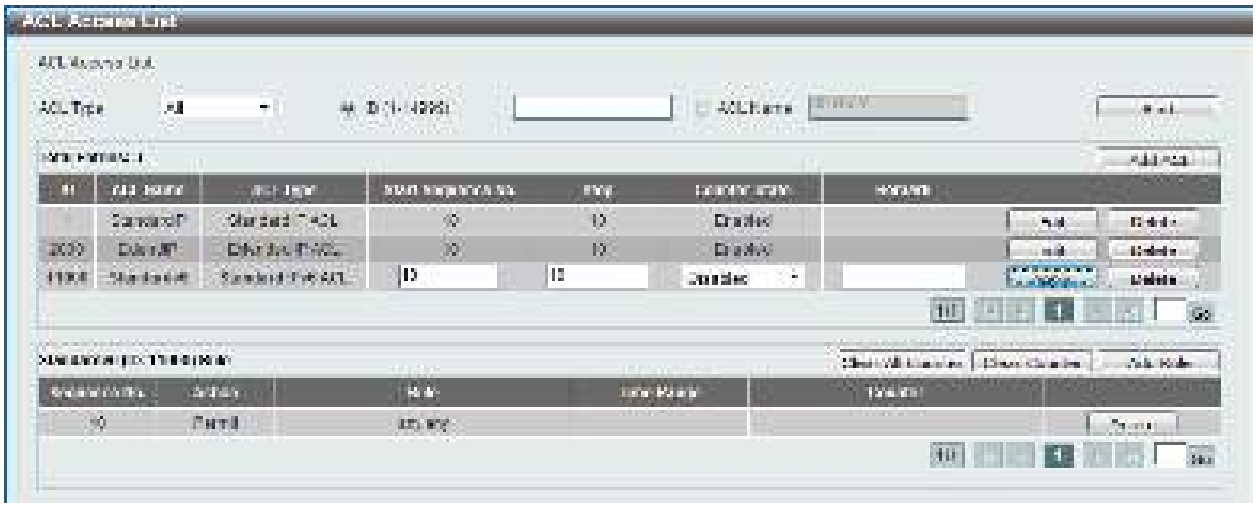


Figure 8-39 Standard IPv6 ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number increment here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

Figure 8-40 Standard IPv6 ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Extended IPv6 ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-41 Extended IPv6 ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ACL ID from 13000 to 14999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Extend IPv6 ACL profile, the newly created Extend IPv6 ACL profile will be displayed in the ACL profile display table, as shown below:

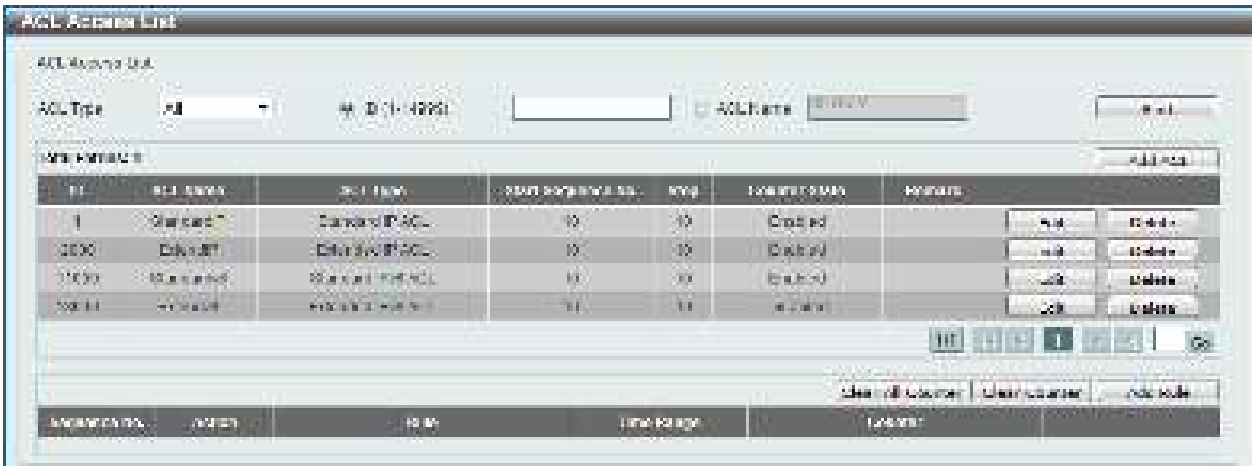


Figure 8-42 Extended IPv6 ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

Figure 8-43 Extended IPv6 ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

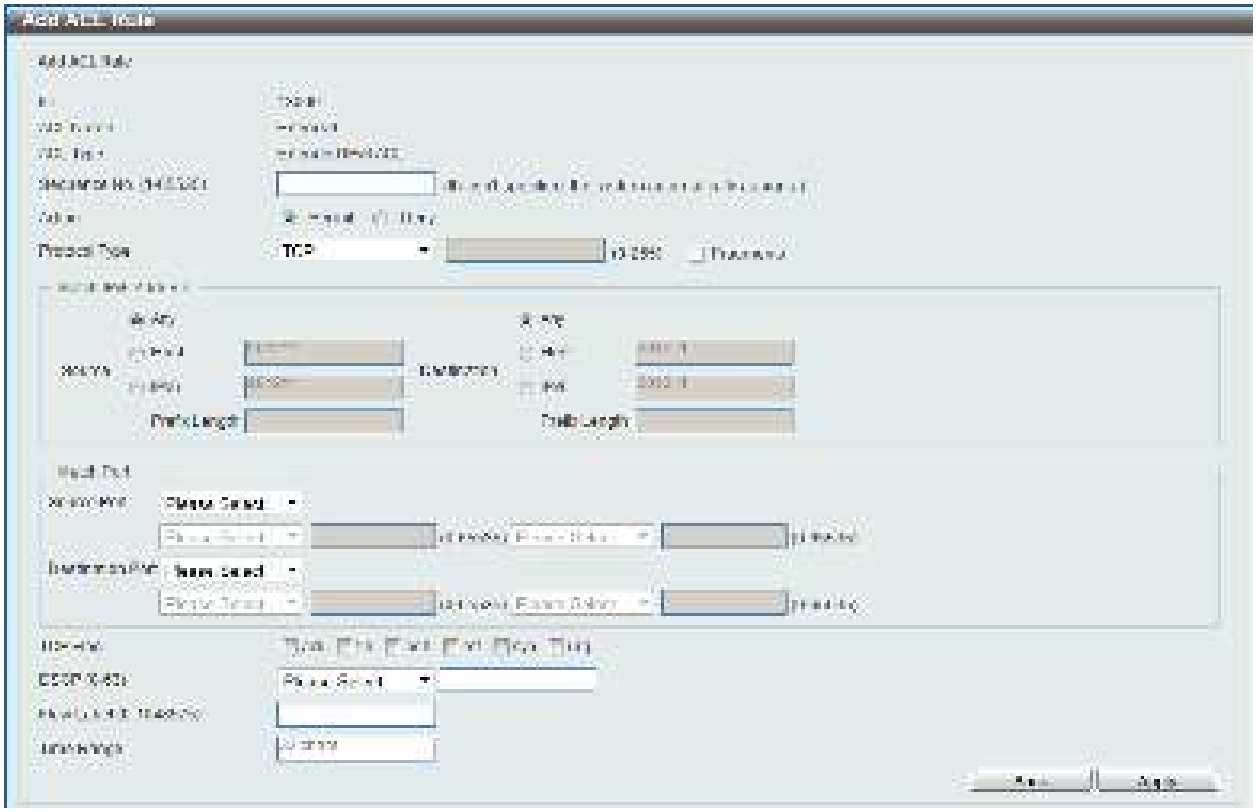


Figure 8-44 Extended IPv6 ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this window.

The **fixed** fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.

Parameter	Description
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **Protocol ID**, **ESP**, **PCP**, **SCTP**, and **None**.

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

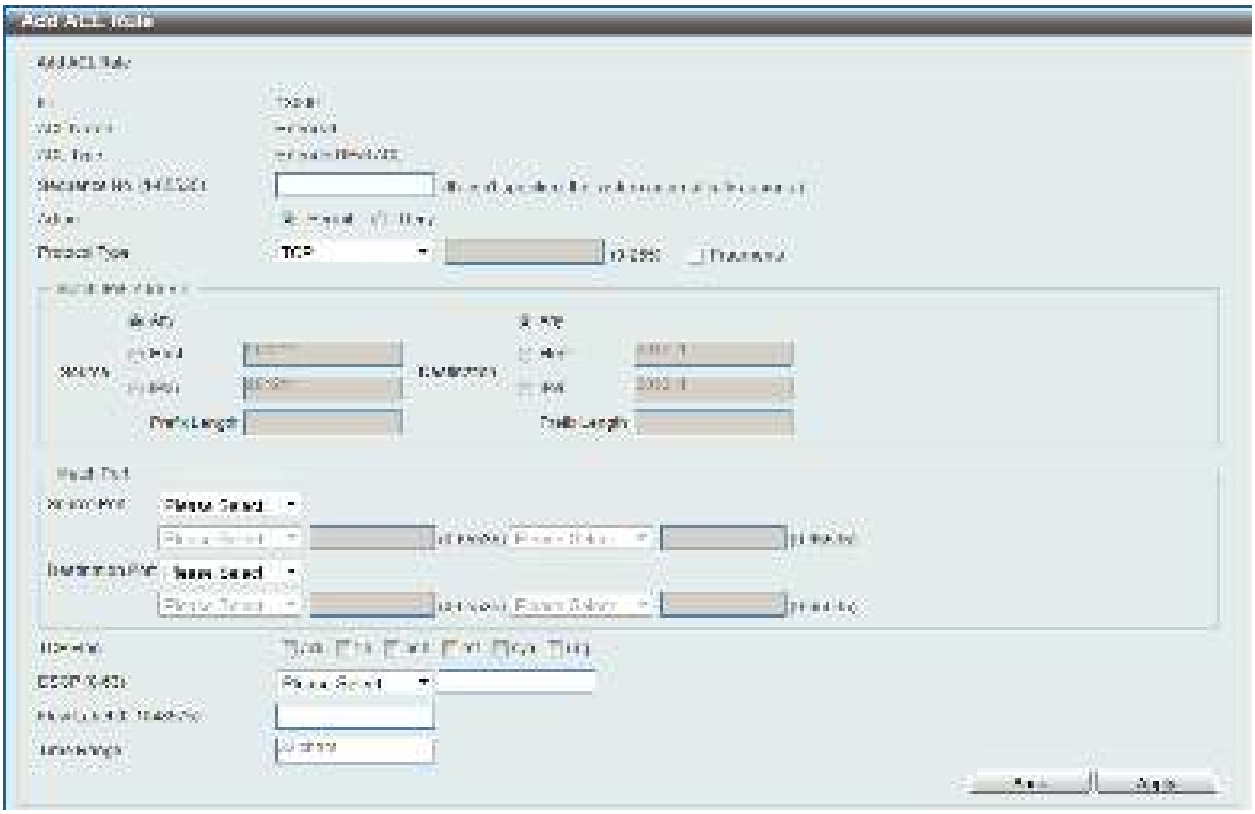


Figure 8-45 Extended IPv6 ACL (Add Rule) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used.

Parameter	Description
	• **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

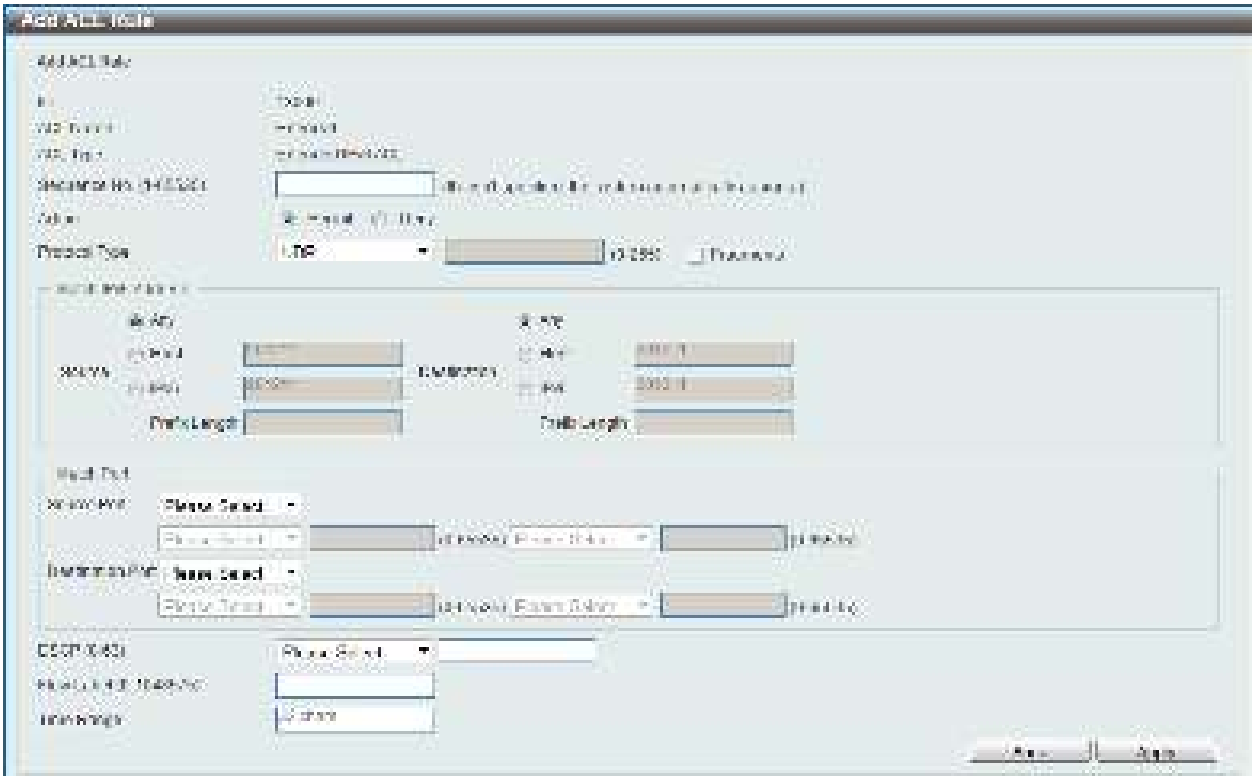


Figure 8-46 Extended IPv6 ACL (Add Rule) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

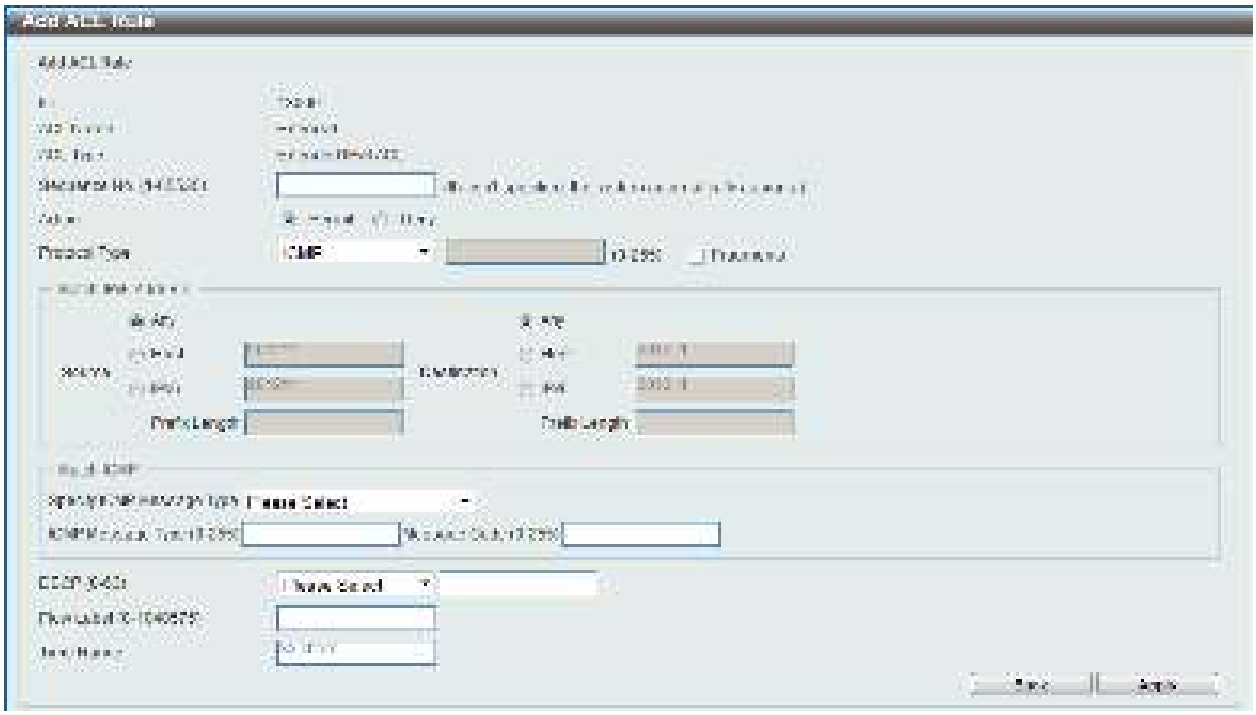


Figure 8-47 Extended IPv6 ACL (Add Rule) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is selected in the **Specify ICMP Message Type** drop-down list, this numerical value will automatically be entered. When the ICMP Message Type is not selected in the **Specify ICMP Message Type** drop-down list, enter the ICMP Message Type numerical value used here.
Message Code	When the ICMP Message Type is selected in the **Specify ICMP Message Type** drop-down list, this numerical value will automatically be entered. When the ICMP Message Type is not selected in the **Specify ICMP Message Type** drop-down list, enter the Message Code numerical value used here.

Parameter	Description
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **Protocol ID**, **ESP**, **PCP**, **SCTP**, or **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

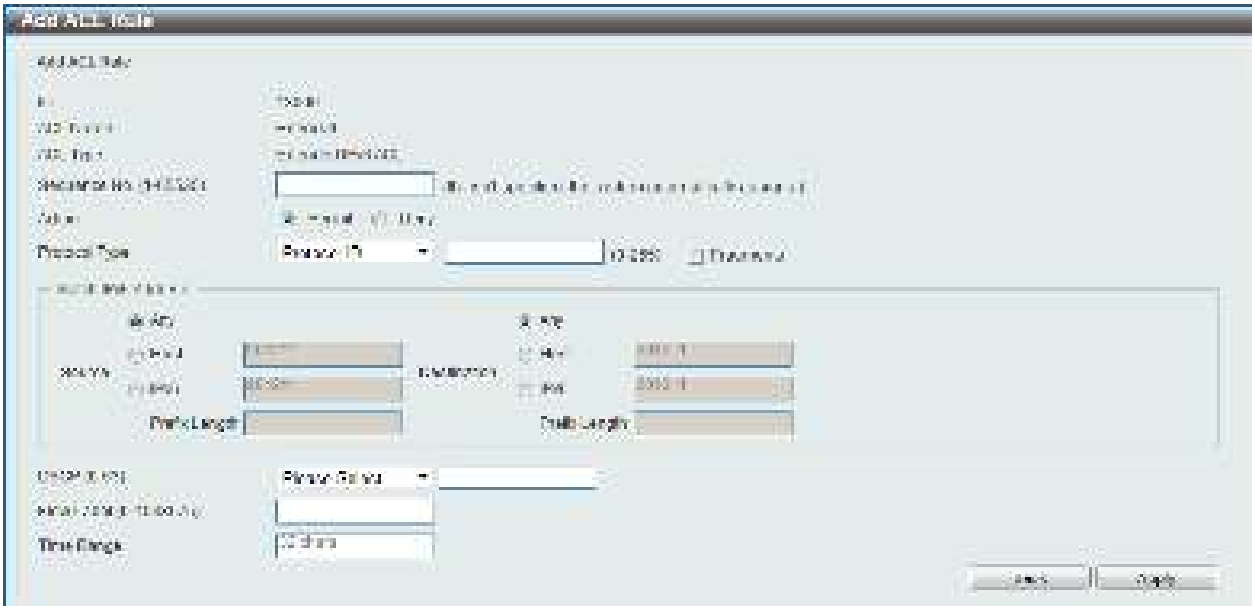


Figure 8-48 Extended IPv6 ACL (Add Rule) Protocol ID Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Protocol	Enter the Protocol ID value used here. This value must be between 0 and 255.
Fragments	Select the **Fragments** option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IPv6 address here. • **IPv6** - The **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.

Parameter	Description
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range to associate with this ACL rule.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

Figure 8-49 Extended IPv6 ACL (Counter State Enabled) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

Figure 8-50 Extended IPv6 ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Extended MAC ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-51 Extended MAC ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ACL ID from 6000 to 7999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Extend MAC ACL profile, the newly created Extend MAC ACL profile will be displayed in the ACL profile display table, as shown below:

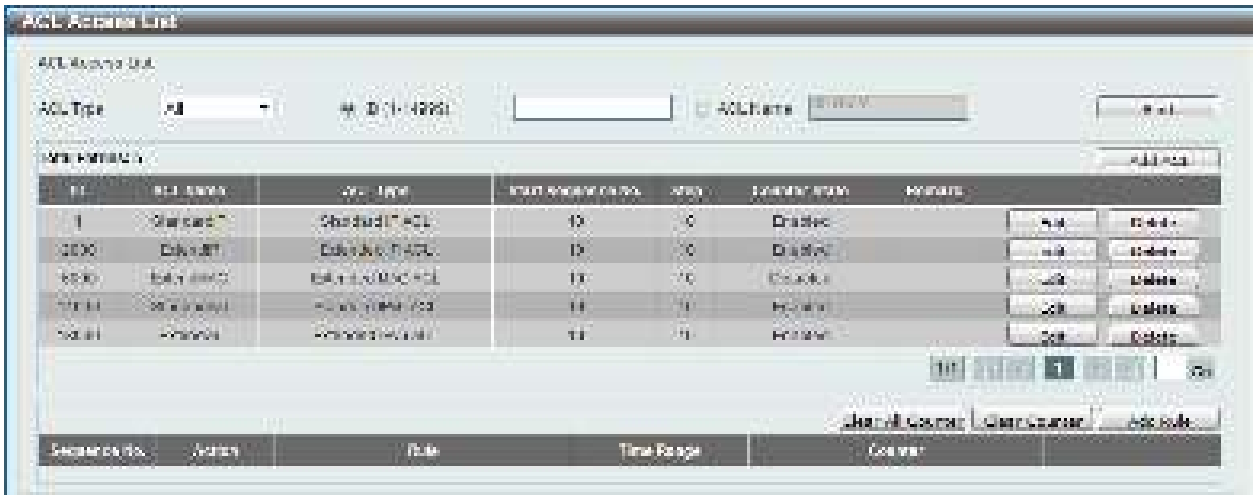


Figure 8-52 Extended MAC ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

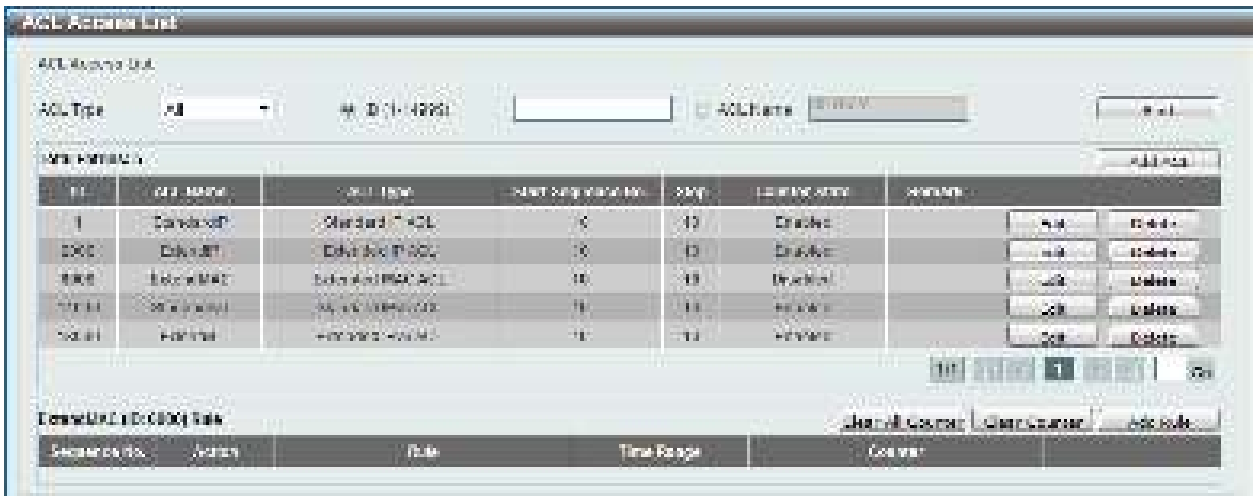


Figure 8-53 Extended MAC ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

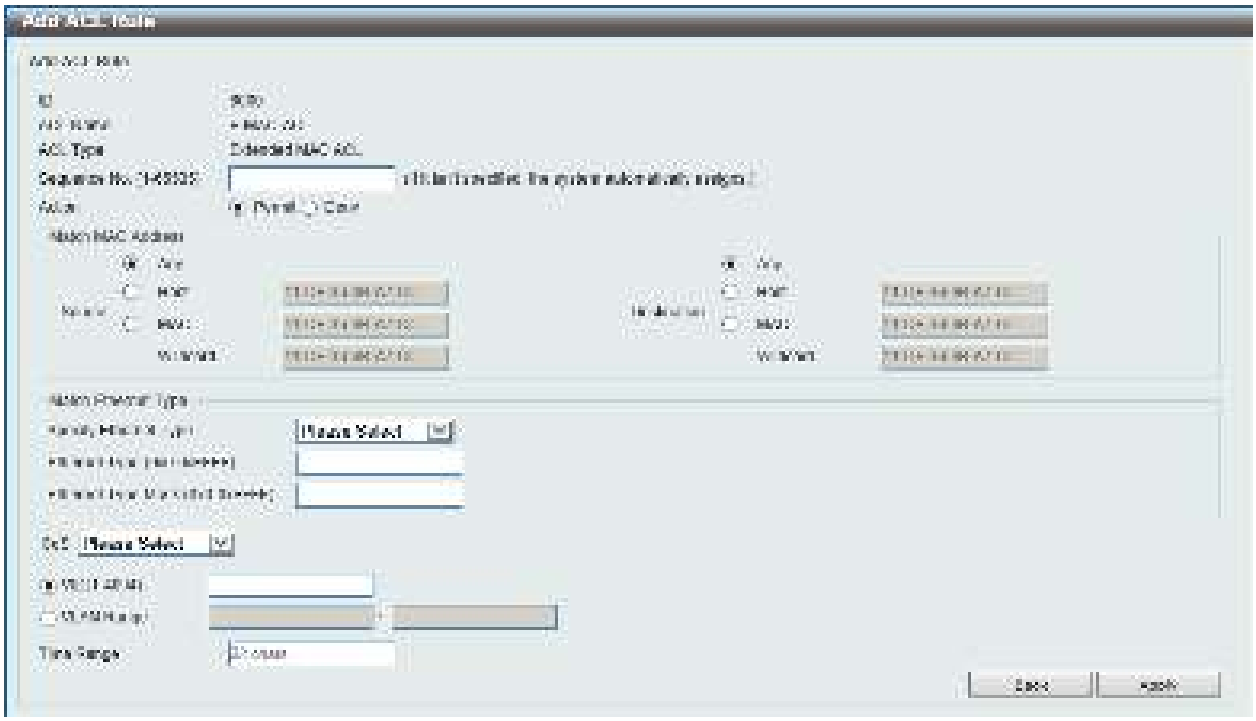


Figure 8-54 Extended MAC ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are **aarp**, **appletalk**, **decent-iv**, **etype-6000**, **etype-8042**, **lat**, **lavc-sca**, **mop-console**, **mop-dump**, **vines-echo**, **vines-ip**, **xns-idp**, and **arp**.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.

Parameter	Description
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value used here. This value is between **0** and **7**.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
Time Range	Enter the name of the time range to associate with this ACL rule.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

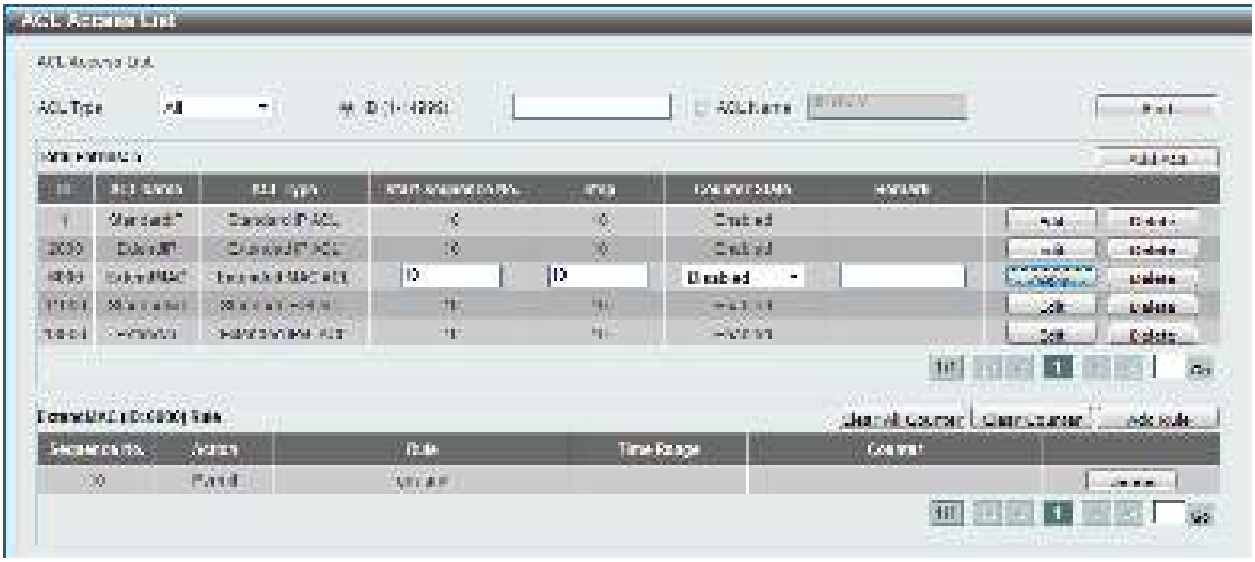


Figure 8-55 Extended MAC ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

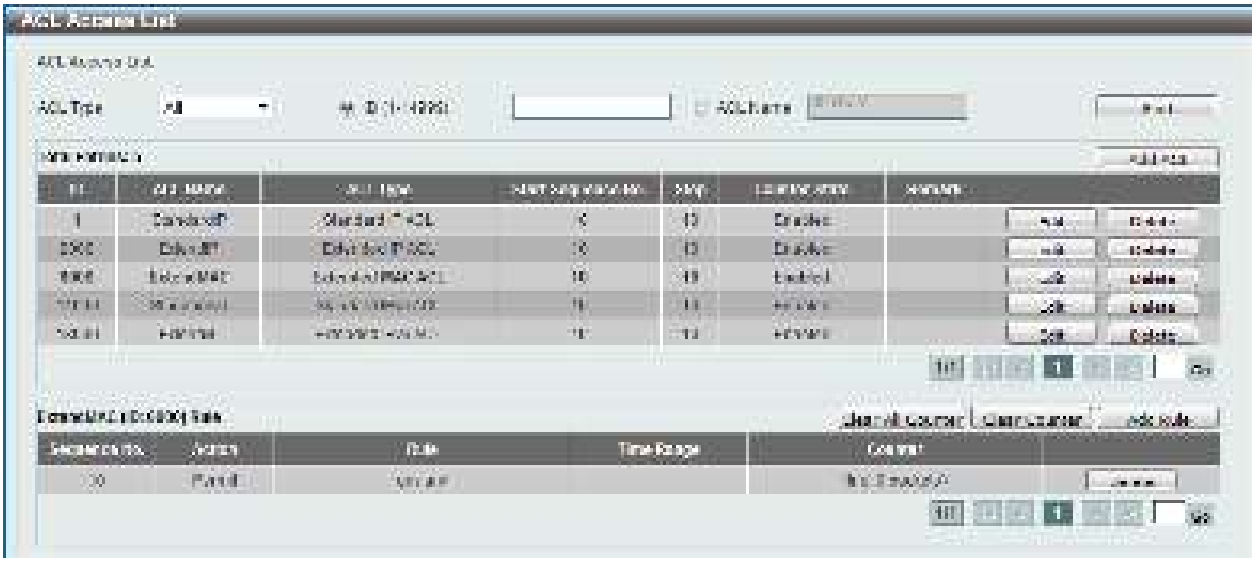


Figure 8-56 Extended MAC ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Extended Expert ACL

After clicking the **Add ACL** button, users can create a new ACL profile, as shown below:

Figure 8-57 Extended Expert ACL (Add Profile) Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL profile type here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ACL ID from 8000 to 9999.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Apply** button to create the new ACL profile.

After creating an Expert ACL profile, the newly created Expert ACL profile will be displayed in the ACL profile display table, as shown below:

Figure 8-58 Extended Expert ACL (Main) Window

Click the **Edit** button to re-configure the specific ACL profile.

Click the **Delete** button to remove the specific ACL profile.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To add an ACL rule in the ACL profile, select it (the ACL profile will toggle to the bold font), and click the **Add Rule** button.

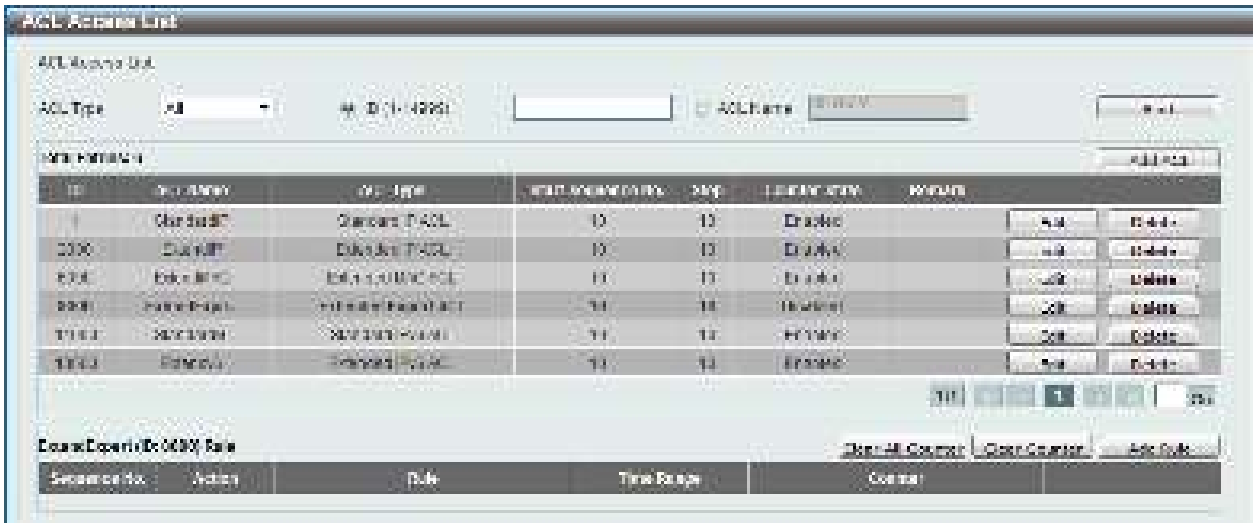


Figure 8-59 Extended Expert ACL (Selected) Window

After selecting the ACL profile and clicking the **Add Rule** button, users can configure the new ACL rule, in the selected ACL profile, as shown below:

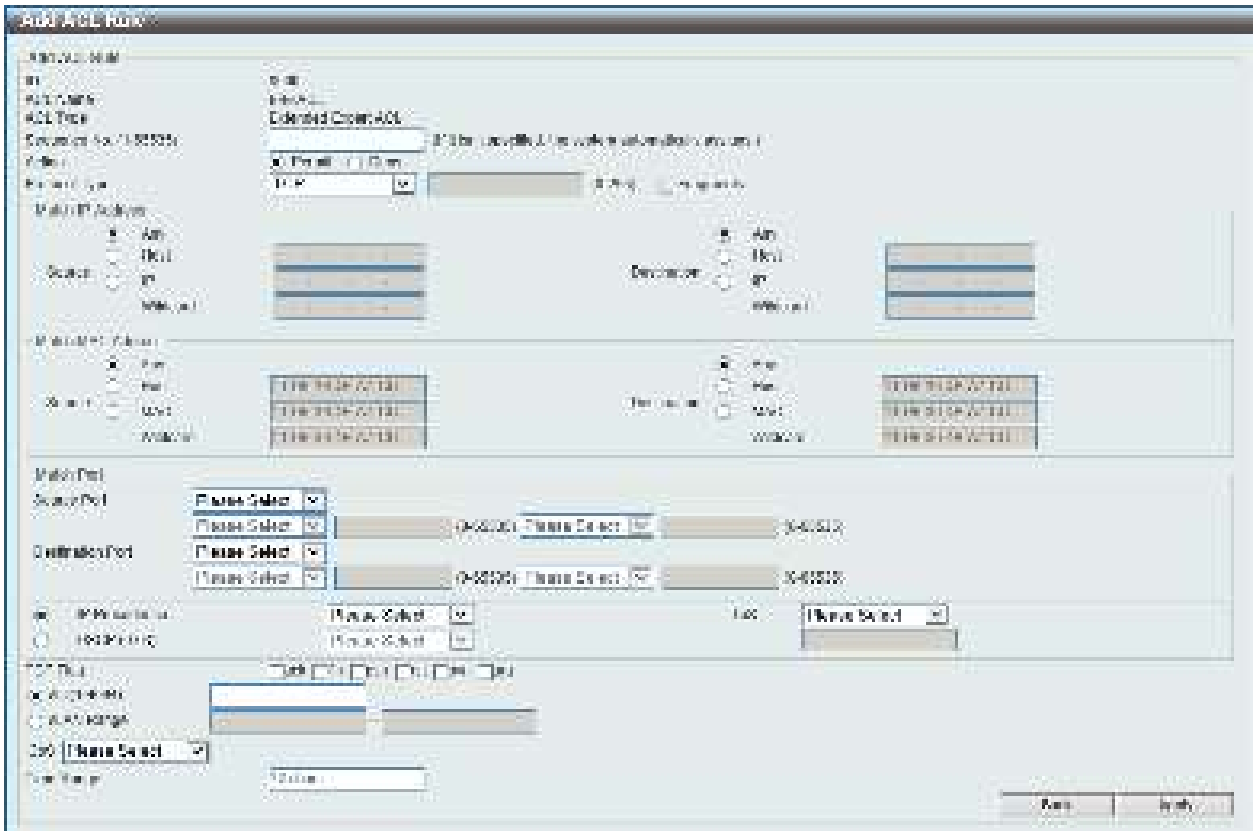


Figure 8-60 Extended Expert ACL (Add Rule) Window

This is a dynamic page. Every selection made in the **Protocol Type** option will change the bottom part of this window.

The **fixed** fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, and **None**.

After selecting the **TCP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

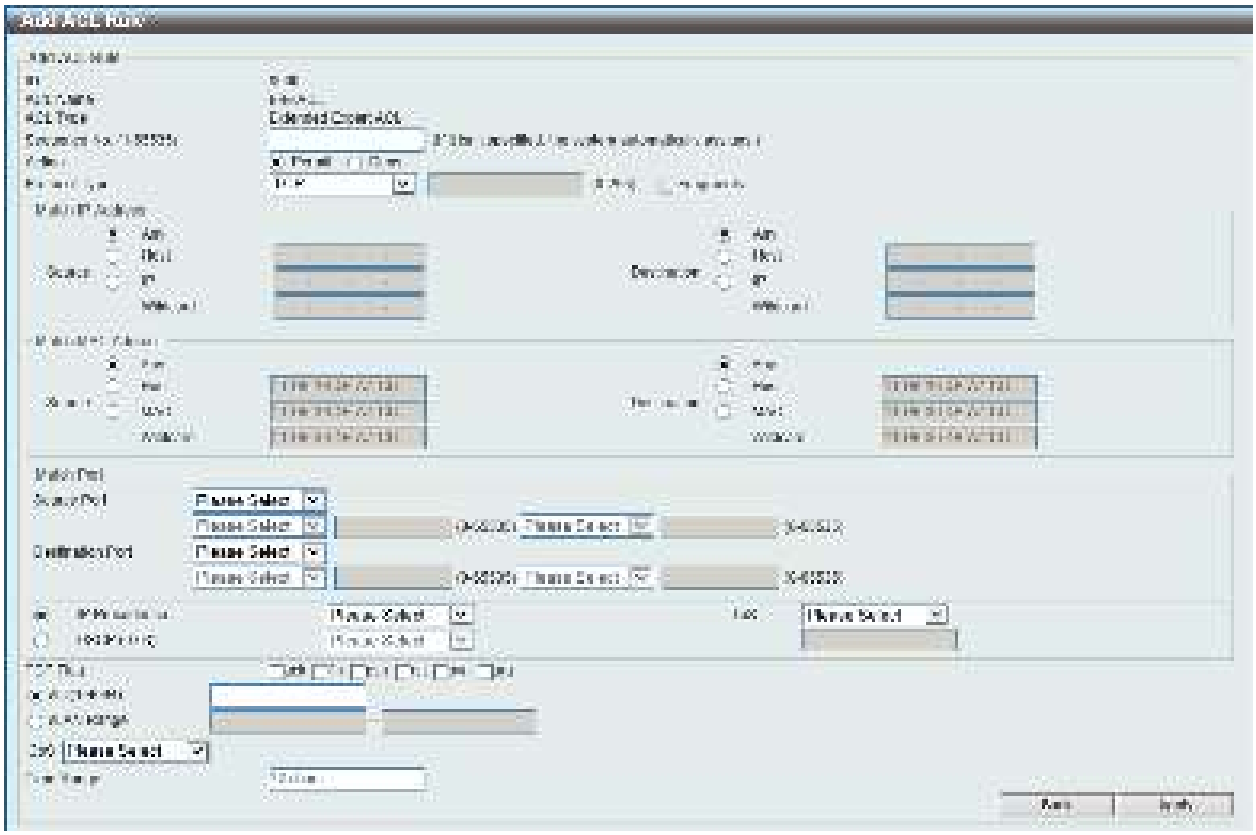


Figure 8-61 Extended Expert ACL (Add Rule) TCP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from **0** to **7**.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **UDP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

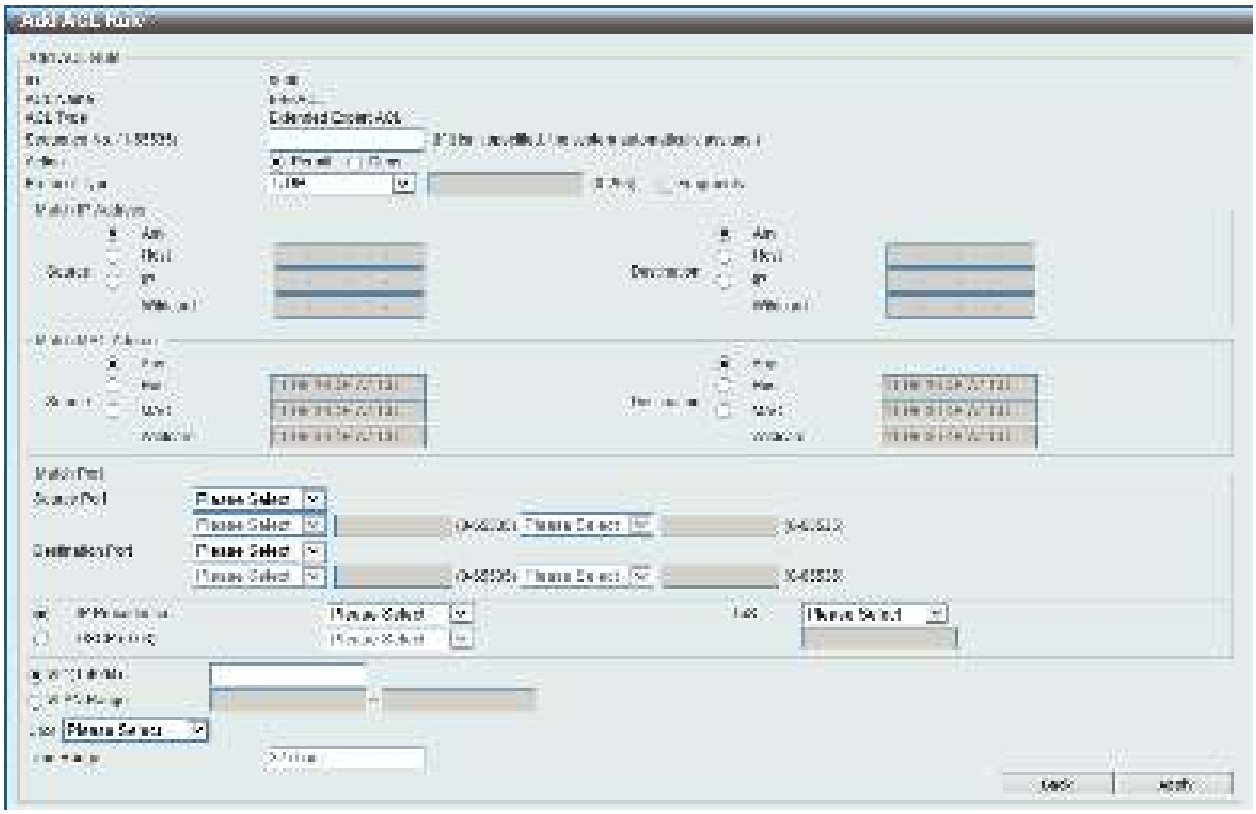


Figure 8-62 Extended Expert ACL (Add Rule) UDP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Range** - The start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from **0** to **7**.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **ICMP** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

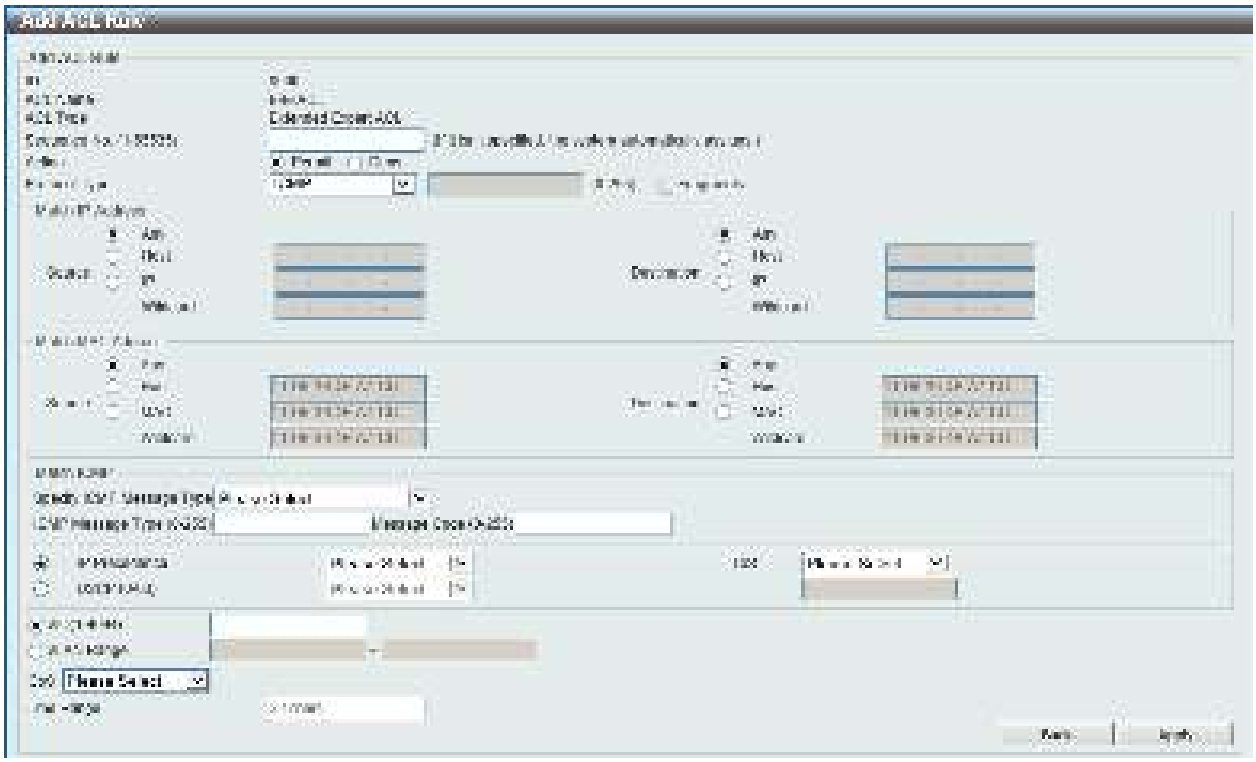


Figure 8-63 Extended Expert ACL (Add Rule) ICMP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Source IP Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify ICMP Message Type	Select the ICMP message type used here.
ICMP Message Type	When the ICMP Message Type is selected in the **Specify ICMP Message Type** drop-down list, this numerical value will automatically be entered. When the ICMP Message Type is not selected in the **Specify ICMP Message Type** drop-down list, enter the ICMP Message Type numerical value used here.
Message Code	When the ICMP Message Type is selected in the **Specify ICMP Message Type** drop-down list, this numerical value will automatically be entered. When the ICMP Message Type is not selected in the **Specify ICMP Message Type** drop-down list, enter the Message Code numerical value used here.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from **0** to **7**.
Time Range	Enter the name of the time range to associate with this ACL rule.

After selecting the **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, or **None** option as the **Protocol Type**, the following page and parameters will be available, as shown below:

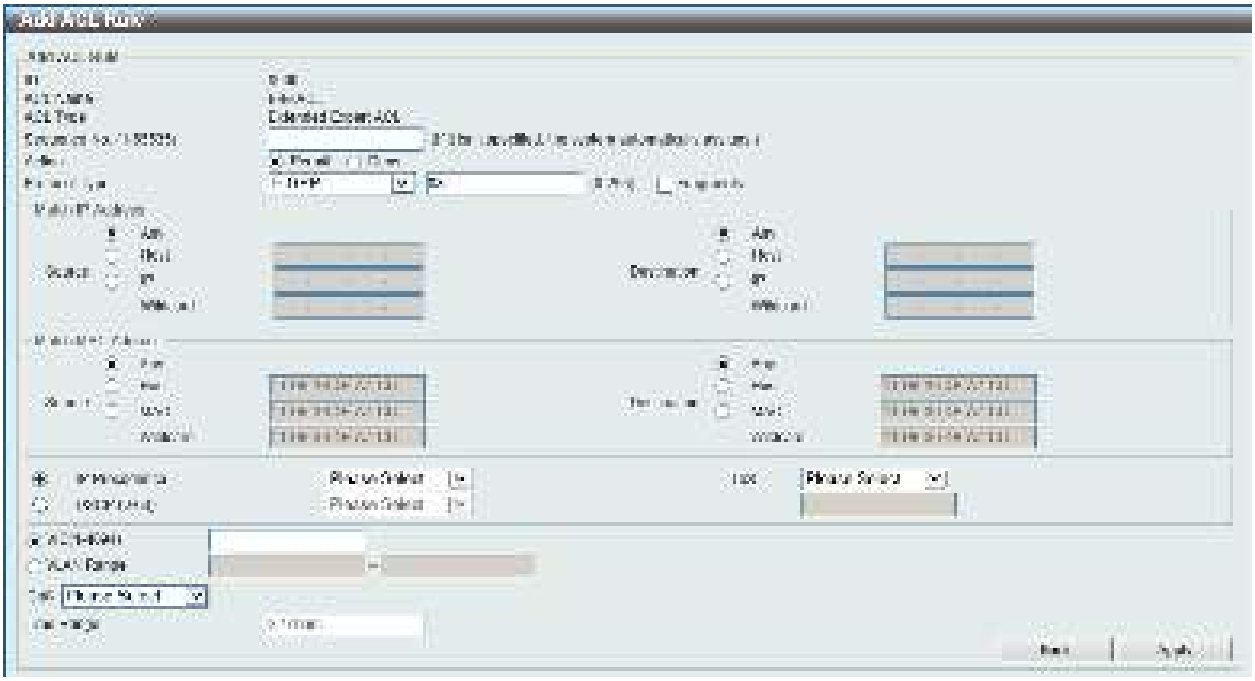


Figure 8-64 Extended Expert ACL (Add Rule) EIGRP Window

The **dynamic** fields that can be configured are described below:

Parameter	Description
Fragments	Select the **Fragments** option to include packet fragment filtering.
Source IP Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination IP Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's IP address here. • **IP** - The **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source MAC Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.

Parameter	Description
Destination MAC Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host's MAC address here. • **MAC** - The **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
IP Precedence	Select the IP precedence value used here. Options to choose from are **0 (routine)**, **1 (priority)**, **2**, **(immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS	After selecting the IP precedence value, select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.
DSCP	Select or enter the DSCP value used here. This value must be between 0 and 63.
VID	Enter the VLAN ID that will be associated with this ACL rule here. This value must be between 1 and 4094.
VLAN Range	Enter the VLAN range here. Enter the minimum and maximum VLAN ID in the range here.
CoS	Select the Class of Service (CoS) value here. Options to choose from are from **0** to **7**.
Time Range	Enter the name of the time range to associate with this ACL rule.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

To enable the **Counter State** option or to enter a **Remark** for the profile, click the **Edit** button, next to the specific ACL profile (found in the ACL profile table).

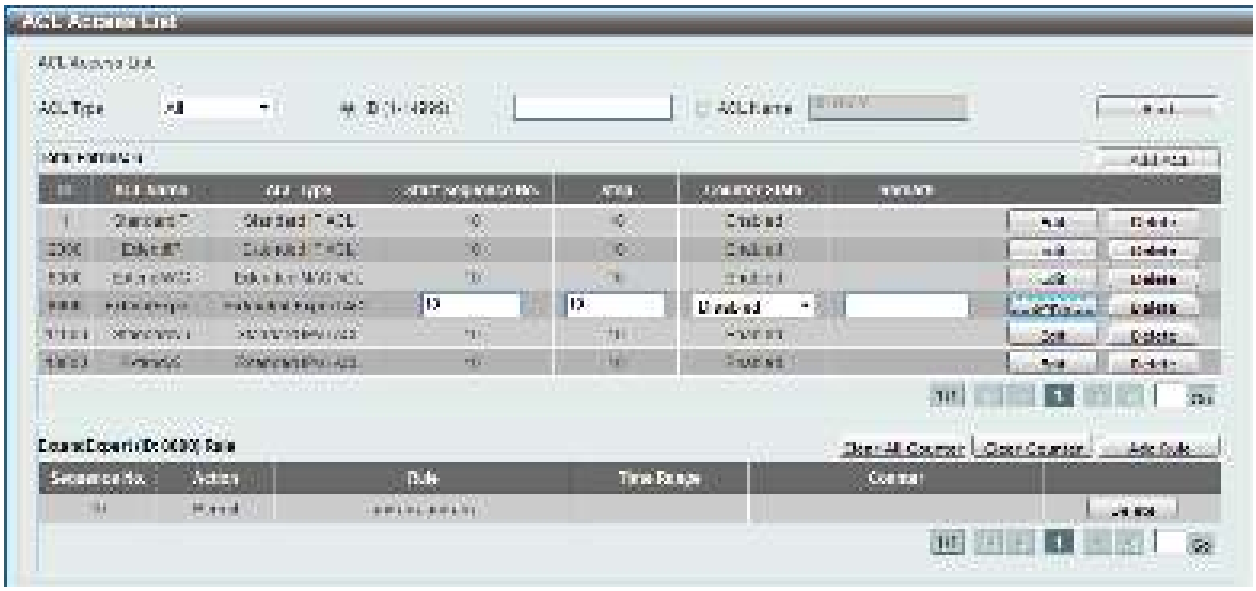


Figure 8-65 Extended Expert ACL (Edit ACL) Window

The fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.

Parameter	Description
Stop	Enter the stop sequence number here.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

To view the list of rules, that are associated with an ACL profile, select the ACL profile (found in the ACL profile table). The rule of ACL rules, connected to the selected ACL profile, will be displayed in the ACL rule table, as shown below:

Figure 8-66 Extended Expert ACL (Rule Display) Window

Click the **Delete** button to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ACL Interface Access Group

This window is used to view and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:

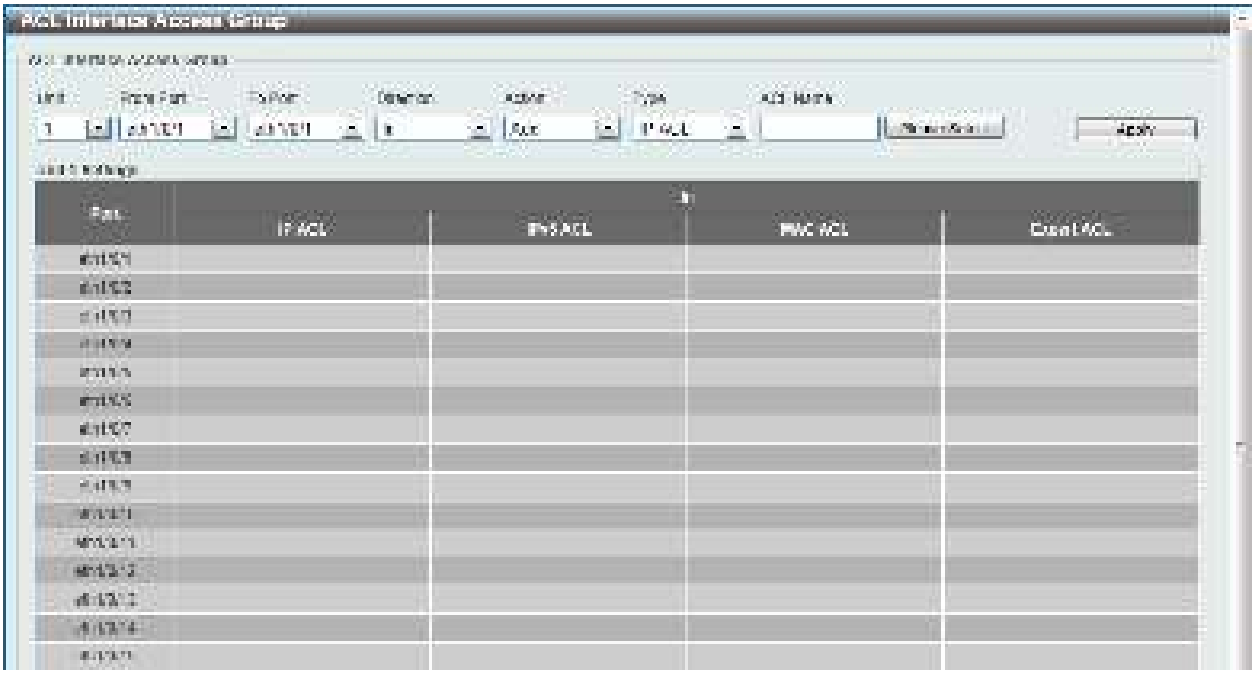


Figure 8-67 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Option to choose from is **In**.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the ACL type here. Options to choose from are **IP ACL**, **IPv6 ACL**, **MAC ACL**, and **Expert ACL**.
ACL Name	Enter the ACL profile's name here. This name can be up to 32 characters long.

Click the **Please Select** button to choose the ACL profile that has been created.

Click the **Apply** button to accept the changes made.

ACL VLAN Access Map

This window is used to view and configure the ACL VLAN access map settings.

To view the following window, click **ACL > ACL VLAN Access Map**, as shown below:

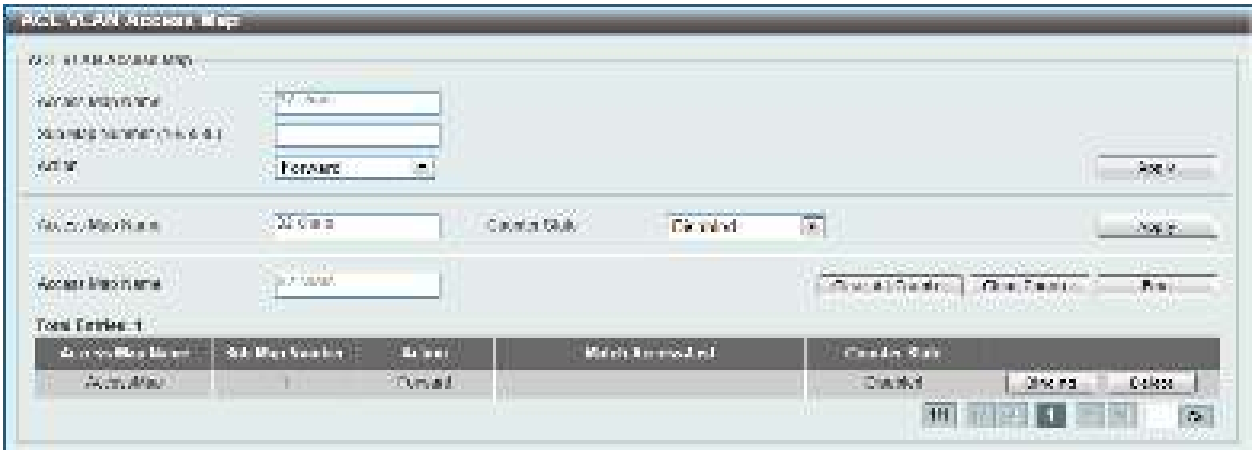


Figure 8-68 ACL VLAN Access Map Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map's name here. This name can be up to 32 characters long.
Sub Map Number	Enter the sub-map's number here. This value must be between 1 and 65535.
Action	Select the action that will be taken here. Options to choose from are **Forward**, **Drop**, and **Redirect**. When the **Redirect** option is selected, select the redirected interface from the drop-down list.
Counter State	Select whether to enable or disable the counter state.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear All Counter** button to clear the counter information for all the access maps.

Click the **Clear Counter** button to the clear the counter information for the specified access map.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Binding** button to configure a new match access list.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Binding** button, the following page will appear.

Figure 8-69 Match Access-List Window

The fields that can be configured are described below:

Parameter	Description
Match IP Access-List	Select the standard or extended IP ACL.
Match IPv6 Access-List	Select the standard or extended IPv6 ACL.
Match MAC Access-List	Select the standard or extended MAC ACL.

Click the **Please Select** button to choose the ACL profile that has been created.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

ACL VLAN Filter

This window is used to view and configure the ACL VLAN filter settings.

To view the following window, click **ACL > ACL VLAN Filter**, as shown below:

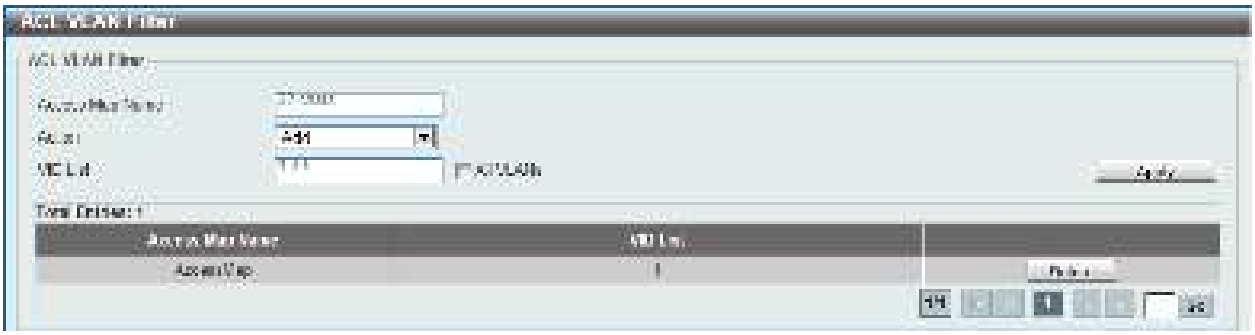


Figure 8-70 ACL VLAN Filter Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map's name here. This name can be up to 32 characters long.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
VID List	Enter the VLAN ID list that will be used here. Select the **All VLANs** option to apply this configuration to all the VLANs configured on this switch.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9. Security

Port Security
802.1X
AAA
RADIUS
TACACS+
IMPB
DHCP Server Screening
ARP Spoofing Prevention
BPDU Attack Protection
MAC Authentication
Web-based Access Control
Japanese Web-based Access Control
Network Access Authentication
Safeguard Engine
Trusted Host
Traffic Segmentation Settings
Storm Control Settings
DoS Attack Prevention Settings
SSH
SSL
Network Protocol Port Protection Settings

Port Security

Port Security Global Settings

This window is used to view and configure the port security global settings. Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view the following window, click **Security > Port Security > Port Security Global Settings**, as shown below:

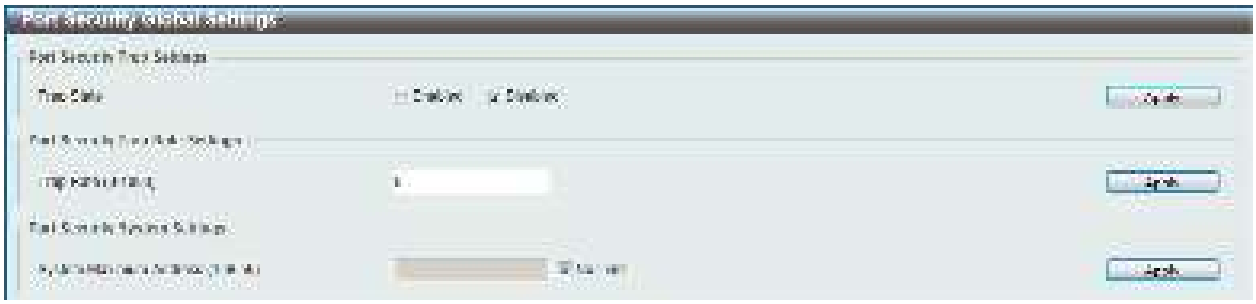


Figure 9-1 Port Security Global Settings Window

The fields that can be configured for **Port Security Trap Settings** are described below:

Parameter	Description
Trap State	Click to enable or disable port security traps on the Switch.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Port Security Trap Rate Settings** are described below:

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 0 indicates an SNMP trap to be generated for every security violation.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Port Security System Settings** are described below:

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit. The valid range is from 1 to 6656. Tick the **No Limit** checkbox to allow the maximum number of secure MAC address.

Click the **Apply** button to accept the changes made.

Port Security Port Settings

This window is used to view and configure the port security port settings.

To view the following window, click **Security > Port Security > Port Security Port Settings**, as shown below:

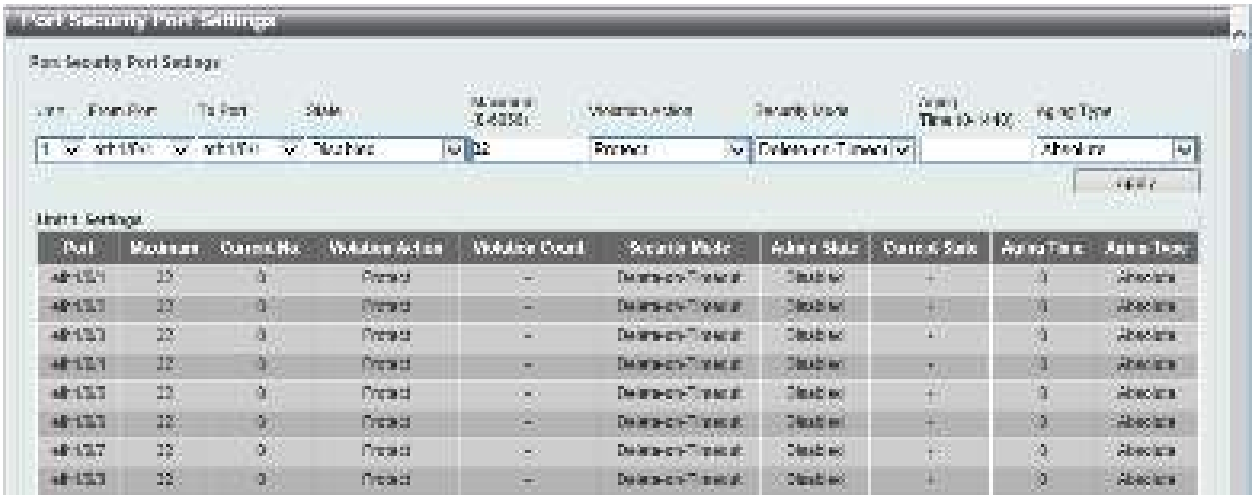


Figure 9-2 Port Security Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 0 and 6656. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are:

Parameter	Description
	• **Protect** - Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. • **Restrict** - Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. • **Shutdown** - Specifies to shut down the port if there is a security violation and record the system log.
Security Mode	Select the security mode option here. Options to choose from are: • **Permanent** - Specifies that all learned MAC addresses are not be purged out unless the user manually deletes those entries. • **Delete-on-Timeout** - Specifies that all learned MAC addresses are purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.
Aging Type	Select the aging type here. Options to choose from are: • **Absolute** - Specifies that all the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type. • **Inactivity** - Specifies that the secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Click the **Apply** button to accept the changes made.

Port Security Address Entries

This window is used to view, clear, and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:

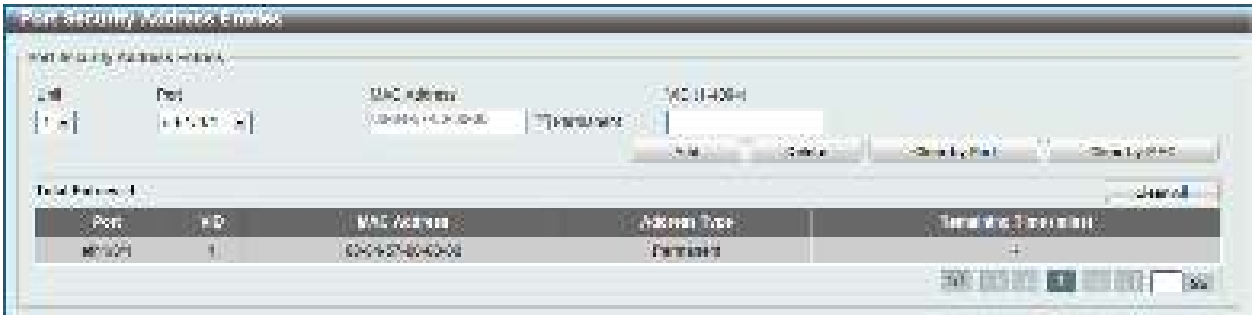


Figure 9-3 Port Security Address Entries Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
MAC Address	Enter the MAC address here. Tick the **Permanent** check box so that all learned MAC addresses would not be purged out unless the user manually deletes those entries.

Parameter	Description
VID	Enter the VLAN ID here. This value must be between 1 and 4094.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove a new entry based on the information entered.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

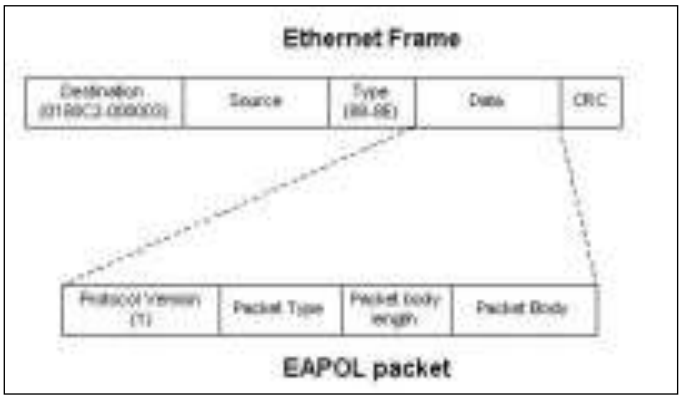


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

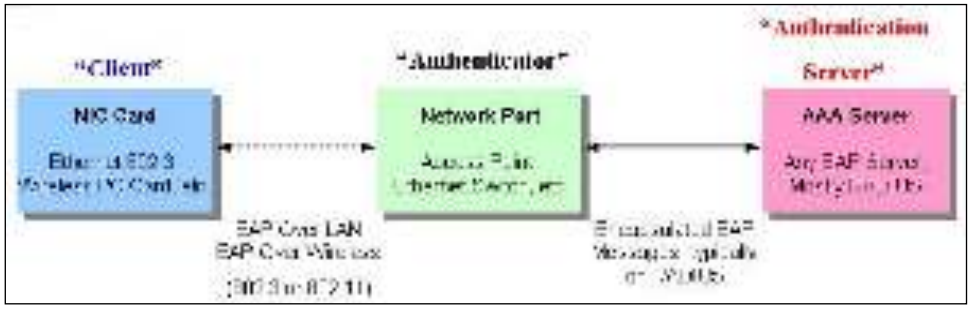


Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

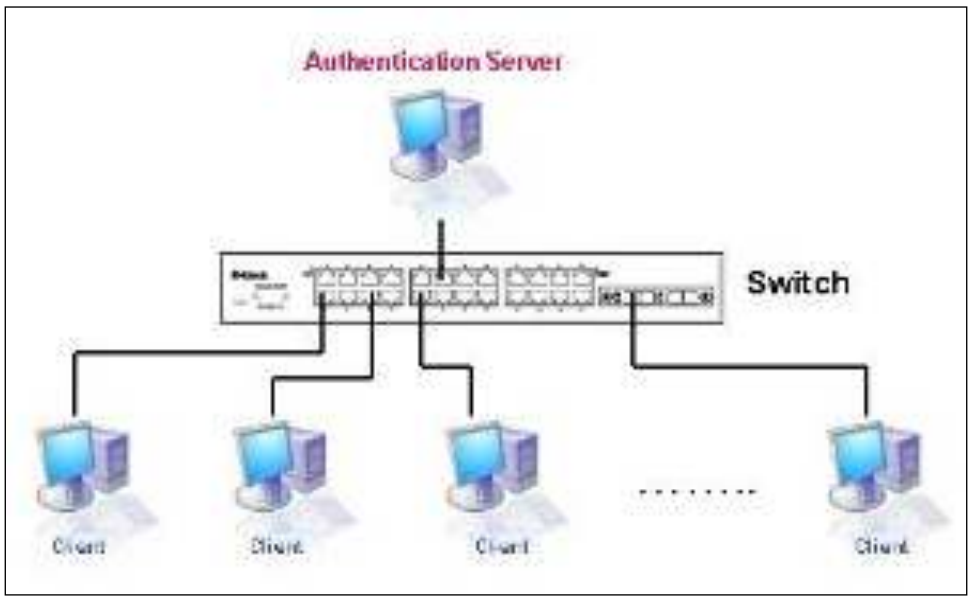


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

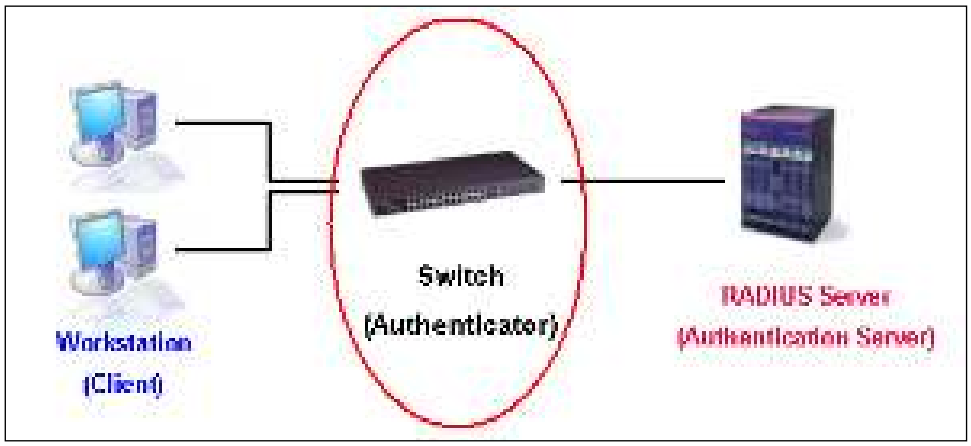


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X state must be enabled. (**Security > 802.1X > 802.1X Global Settings**)

- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running windows XP and windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

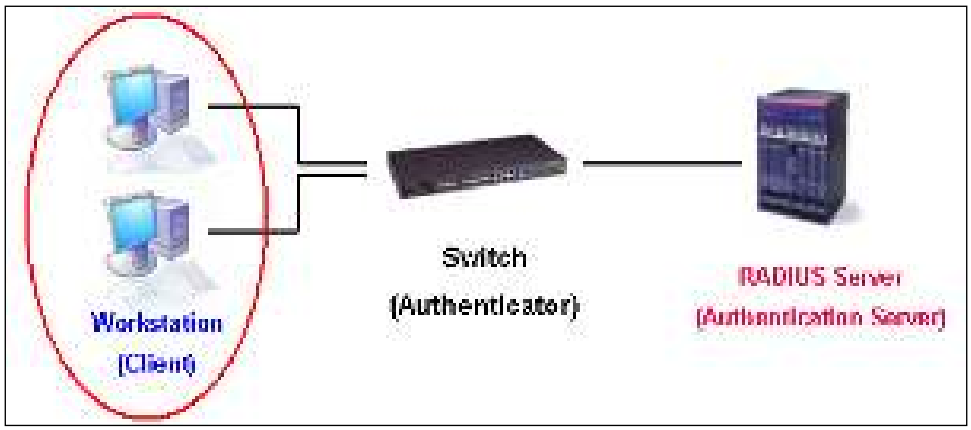


Figure 9-8 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a detailed explanation of how the authentication process is completed between the three roles stated above.

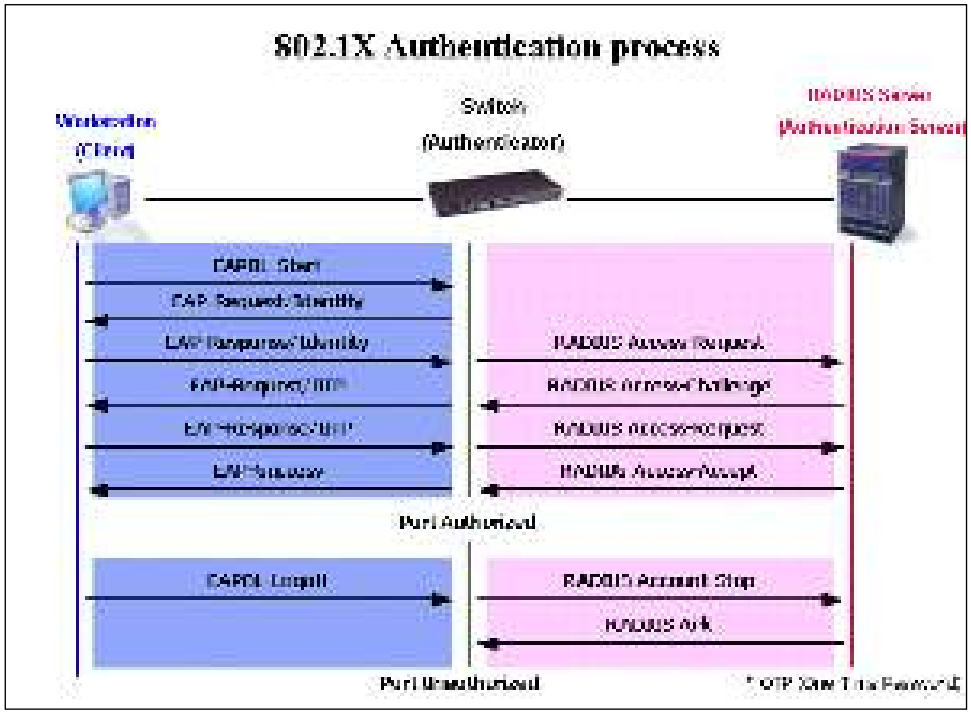


Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **Port-based Access Control** - This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
- **Host-based Access Control** - Using this method, the Switch will automatically learn up to a maximum of 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

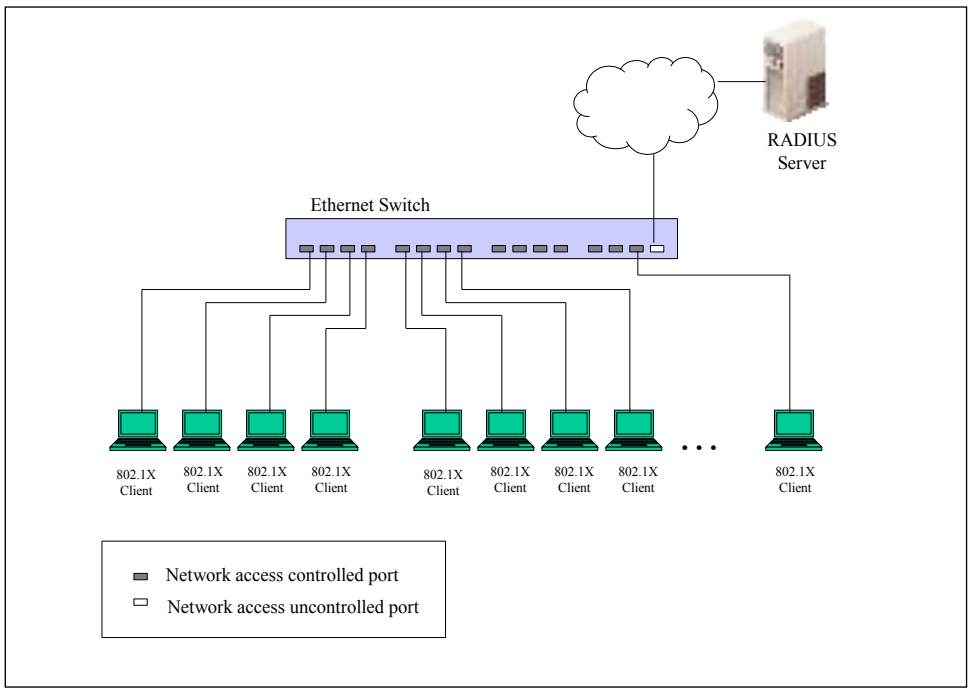


Figure 9-10 Example of Typical Port-based Configuration

Host-based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’

individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

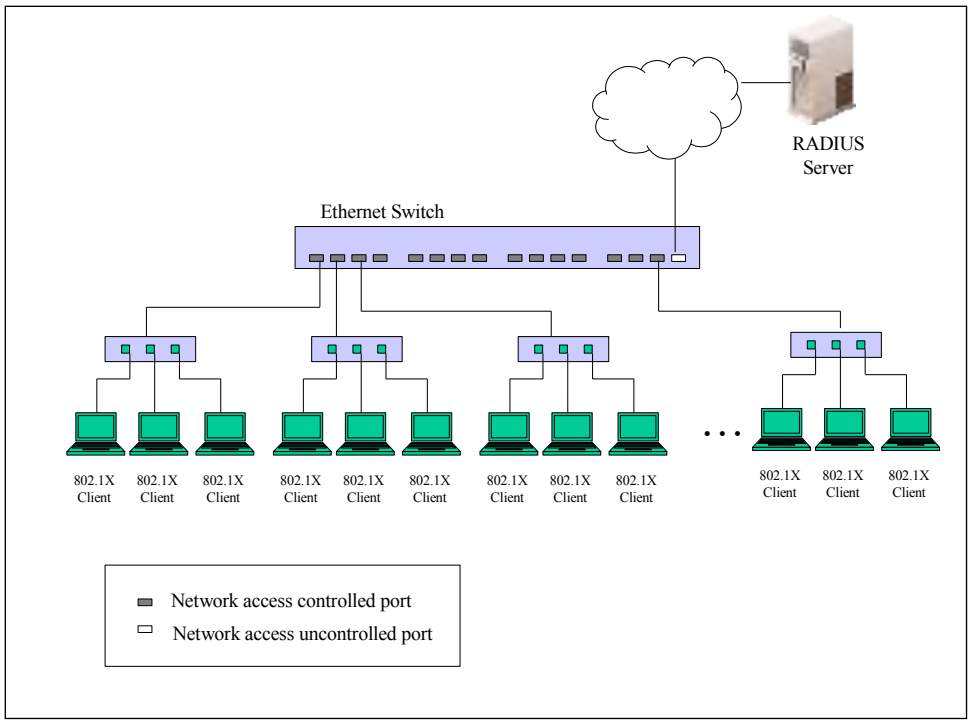


Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to view and configure the 802.1X global settings.

To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:

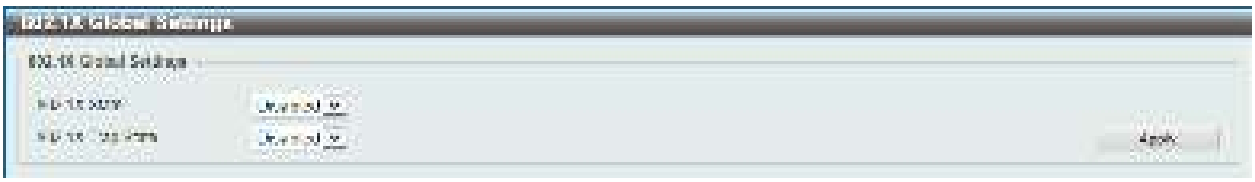


Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

Parameter	Description
802.1X State	Select to enable or disable the 802.1X global state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

Click the **Apply** button to accept the changes made.

802.1X Port Settings

This window is used to view and configure the 802.1X port settings.

To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:

Figure 9-13 802.1X Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are **Both** and **In**. This option configures the direction of the traffic on a controlled port as unidirectional (**In**) or bidirectional (**Both**). The **In** control direction is only valid when the **Host Mode** is configured as **Multi Host** in the Network Access Authentication Port Settings window.
Port Control	Select the port control option here. Options to choose from are: • **ForceAuthorized** - Specifies that the port is not controlled in both directions. • **Auto** - Specifies that access to the port for the controlled direction needs to be authenticated. • **ForceUnauthorized** - Specifies that access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. This value must be between 1 and 10. By default, this option is 2. This option configures the maximum number of times that the backend

Parameter	Description
	authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
Supp Timeout	Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
TX Period	Enter the transmission period value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

Click the **Apply** button to accept the changes made.

Authentication Session Information

This window is used to view and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Session Information**, as shown below:

Figure 9-14 Authentication Session Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Init by Port** button to initiate the session information based on the selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the selections made.

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:

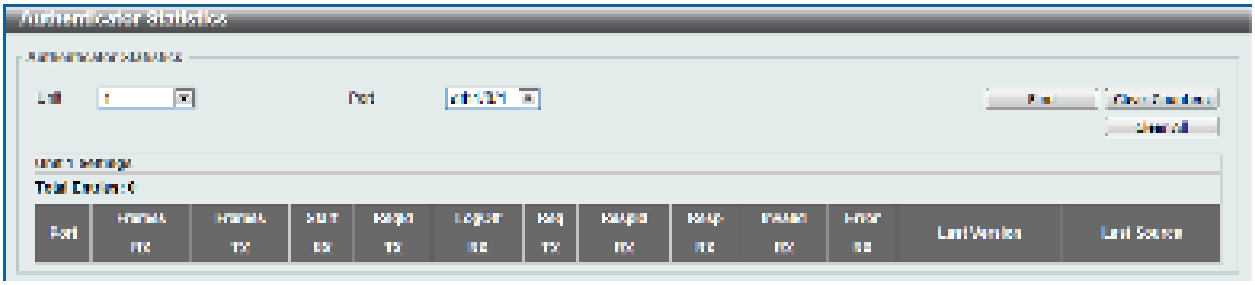


Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Authenticator Session Statistics

This window is used to view and clear the authenticator session statistics.

To view the following window, click **Security > 802.1X > Authenticator Session Statistics**, as shown below:

Figure 9-16 Authenticator Session Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Authenticator Diagnostics

This window is used to view and clear the authenticator diagnostics information.

To view the following window, click **Security > 802.1X > Authenticator Diagnostics**, as shown below:

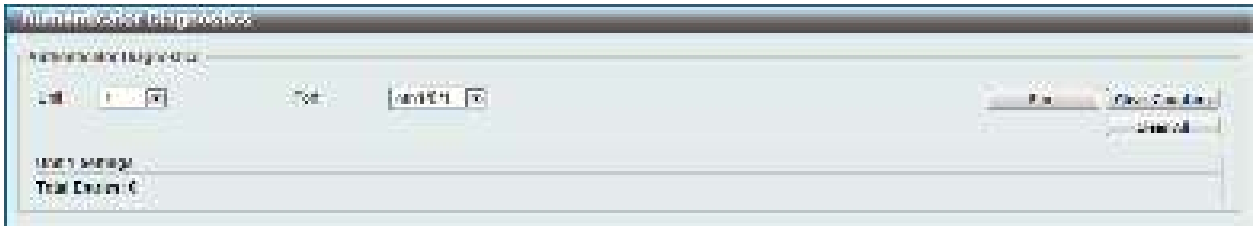


Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

AAA

AAA Global Settings

This window is used to enable or disable the Authentication, Authorization, and Accounting (AAA) global state.

To view the following window, click **Security > AAA > AAA Global Settings**, as shown below:

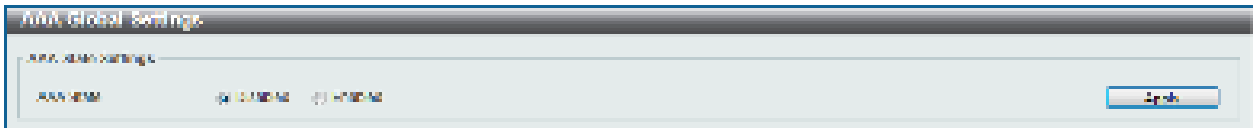


Figure 9-18 AAA Global Settings Window

The fields that can be configured are described below:

Parameter	Description
AAA State	Select to enable or disable the Authentication, Authorization, and Accounting (AAA) global state.

Click the **Apply** button to accept the changes made.

Application Authentication Settings

This window is used to view and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:

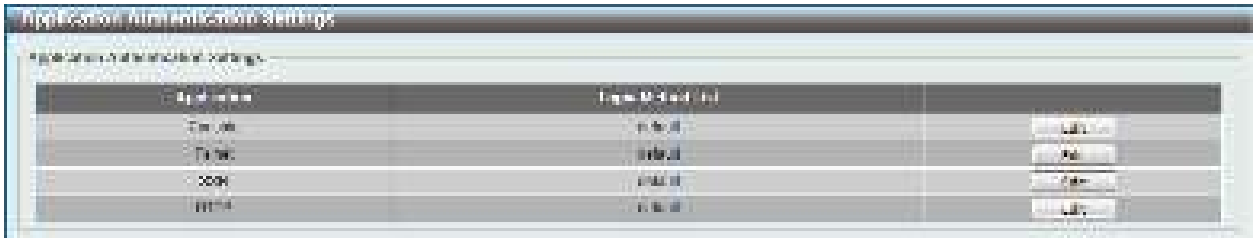


Figure 9-19 Application Authentication Settings Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the **Edit** button for the specific entry, enter the login method list name used here.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Application Accounting Settings

This window is used to view and configure the application accounting settings.

To view the following window, click **Security > AAA > Application Accounting Settings**, as shown below:

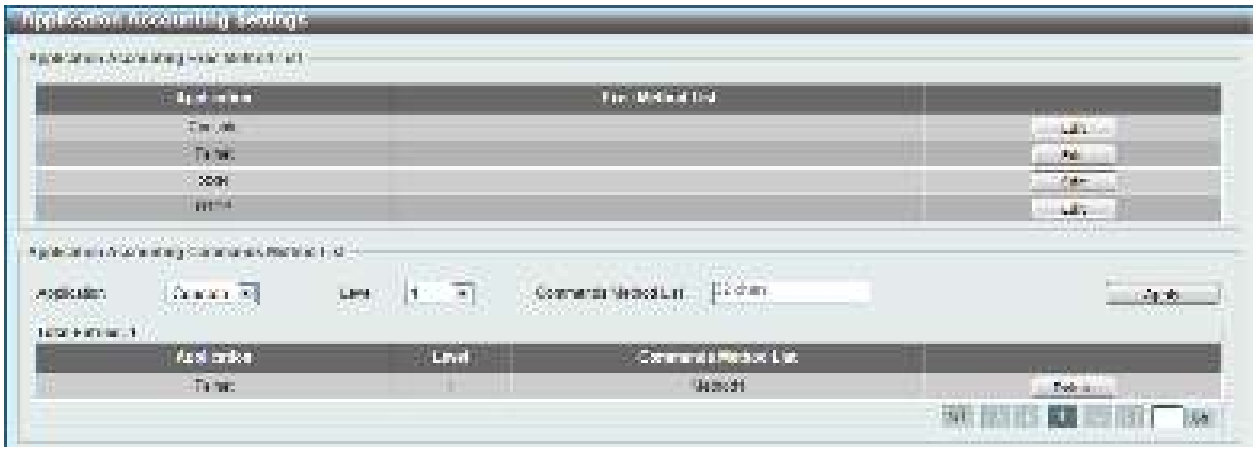


Figure 9-20 Application Accounting Settings Window

The fields that can be configured are described below:

Parameter	Description
Exec Method List	After clicking the **Edit** button for the specific entry, enter the EXEC method list name used here.
Application	Select the application used here. Options to choose from are **Console**, **Telnet**, and **SSH**.

Parameter	Description
Level	Select the privilege level used here. Options to choose from are levels **1** to **15**.
Commands Method List	Enter the commands method list name used here.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authentication Settings

This window is used to view and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:

Figure 9-21 Authentication Settings Window

The fields that can be configured for **AAA Authentication 802.1X** are described below:

Parameter	Description
Status	Select to enable or disable the AAA 802.1X authentication state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **local**, **group** and **radius**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **AAA Authentication JWAC** are described below:

Parameter	Description
Status	Select to enable or disable the AAA JWAC authentication state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **local**, **group** and **radius**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **AAA Authentication MAC-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA MAC authentication state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **local**, **group** and **radius**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **AAA Authentication WEB-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA Web authentication state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **local**, **group** and **radius**.

Click the **Apply** button to accept the changes made.

After clicking the **AAA Authentication Exec** tab, the following page will appear.

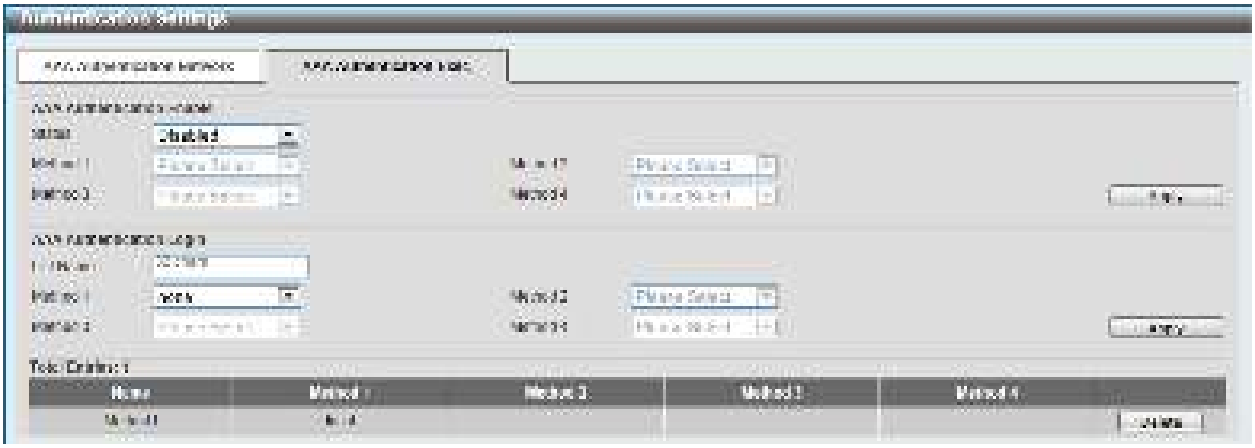


Figure 9-22 AAA Authentication Exec Window

The fields that can be configured for **AAA Authentication Enable** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **enable**, **group**, **radius**, and **tacacs+**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **AAA Authentication Login** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Status	Select to enable or disable the AAA authentication login state here.

Parameter	Description
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **enable**, **group**, **radius**, and **tacacs+**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Accounting Settings

This window is used to view and configure the AAA accounting settings.

To view the following window, click **Security > AAA > Accounting Settings**, as shown below:

Figure 9-23 Accounting Settings Window

The fields that can be configured are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **group**, **radius**, and **tacacs+**.

Click the **Apply** button to accept the changes made.

After clicking the **AAA Accounting System** tab, the following page will appear.

Figure 9-24 AAA Accounting System Window

The fields that can be configured are described below:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **group**, **radius**, and **tacacs+**.

Click the **Apply** button to accept the changes made.

After clicking the **AAA Accounting Exec** tab, the following page will appear.

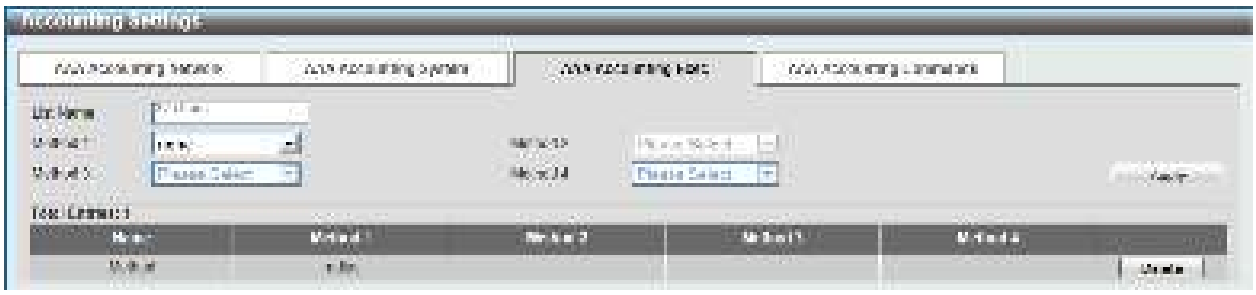


Figure 9-25 AAA Accounting Exec Window

The fields that can be configured are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA accounting EXEC option here.
Method 1 to 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **group**, **radius**, and **tacacs+**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

After clicking the **AAA Accounting Commands** tab, the following page will appear.

Figure 9-26 AAA Accounting Commands Window

The fields that can be configured are described below:

Parameter	Description
Level	Select the privilege level used here. Options to choose from are levels **1** to **15**.
List Name	Enter the method list name that will be used with the AAA accounting commands option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are **none**, **group**, and **tacacs+**. The **none** option is only available for **Method 1**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Server RADIUS Dynamic Author Settings

This window is used to view and configure the dynamic author settings for the RADIUS server.

To view the following window, click **Security > AAA > Server RADIUS Dynamic Author Settings**, as shown below:

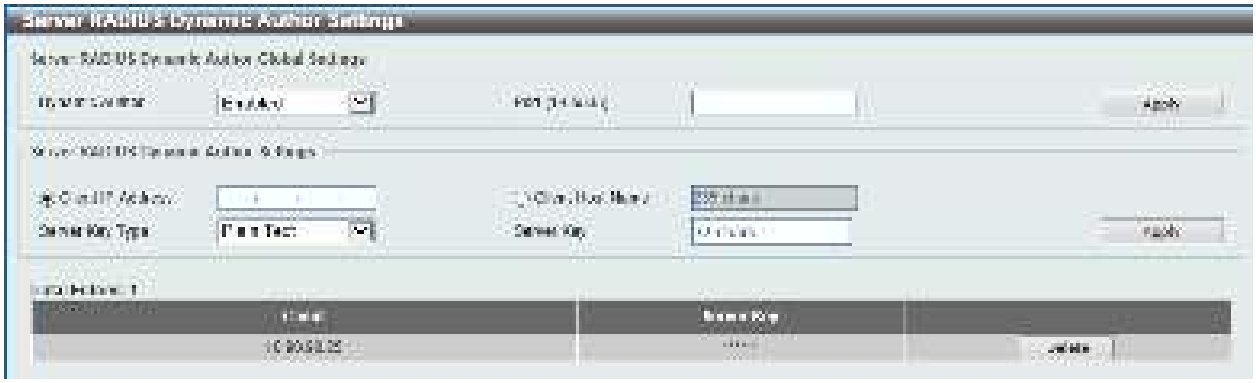


Figure 9-27 Server RADIUS Dynamic Author Settings Window

The fields that can be configured for **Server RADIUS Dynamic Author Global Settings** are described below:

Parameter	Description
Dynamic Author	Select to enable or disable the dynamic author function here. Dynamic authorization allows an external policy server to dynamically send updates to a device.
Port	Enter the port number that is used for the data transmission of the update packets here. The range is from 1 to 65535.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Server RADIUS Dynamic Author Settings** are described below:

Parameter	Description
Client IP Address	Select and enter the IP address of the RADIUS client here.
Client Host Name	Select and enter the hostname of the RADIUS client here.
Server Key Type	Select the RADIUS server key type here. Options to choose from are: • **Plain Text** - Select this option to use the plain text RADIUS server key type. • **Encrypted** - Select this option to use the encrypted RADIUS server key type.
Server Key	When **Plain Text** is selected as the key type, enter the key for the RADIUS server connection in the plain text form here. This key can be up to 32 characters long. When **Encrypted** is selected as the key type, enter the key for the RADIUS server connection in the encrypted form here. This key can be up to 64 characters long.

Click the **Apply** button to add a new entry.

Click the **Delete** button to remove the specified entry.

RADIUS

RADIUS Global Settings

This window is used to view and configure the RADIUS global settings.

To view the following window, click **Security > RADIUS > RADIUS Global Settings**, as shown below:

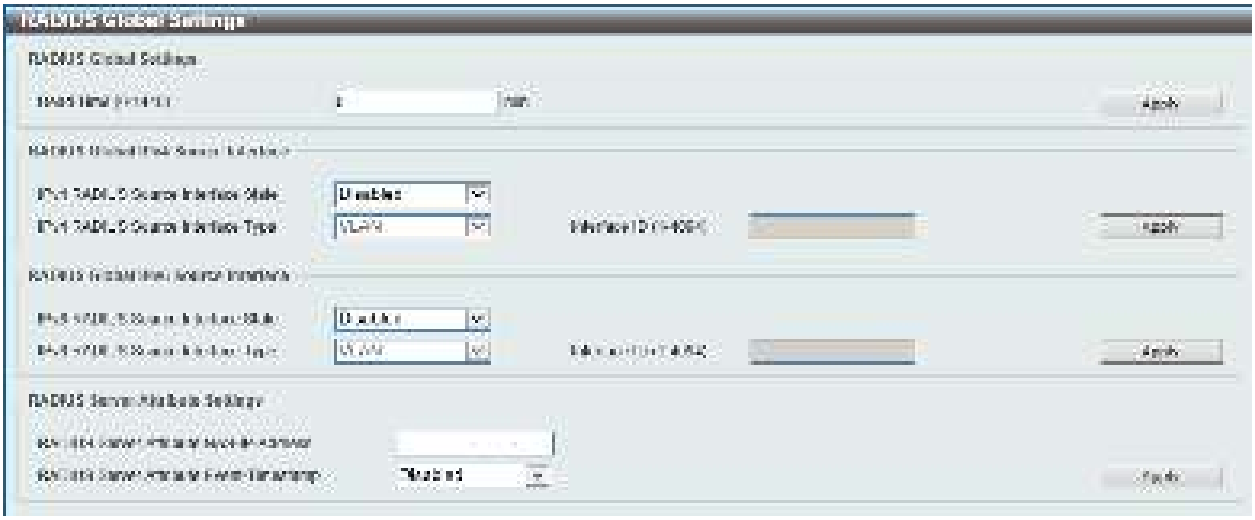


Figure 9-28 RADIUS Global Settings Window

The fields that can be configured for **RADIUS Global Settings** are described below:

Parameter	Description
Dead Time	Enter the dead time value for the RADIUS server connection here. This is used to improve the authentication processing time by setting the dead time to skip unresponsive server host entries. The range is from 0 to 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **RADIUS Global IPv4 Source Interface** are described below:

Parameter	Description
IPv4 RADIUS Source Interface State	Select to enable or disable the state of the IPv4 RADIUS source interface here.
IPv4 RADIUS Source Interface Type	Select the IPv4 RADIUS source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv4 RADIUS source interface type as VLAN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **RADIUS Global IPv6 Source Interface** are described below:

Parameter	Description
IPv6 RADIUS Source Interface State	Select to enable or disable the state of the IPv6 RADIUS source interface here.

Parameter	Description
IPv6 RADIUS Source Interface Type	Select the IPv6 RADIUS source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv6 RADIUS source interface type as VLAN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **RADIUS Server Attribute Settings** are described below:

Parameter	Description
RADIUS Server Attribute NAS-IP-Address	Enter the IPv4 address of the RADIUS server attribute 4 in the RADIUS packet here.
RADIUS Server Attribute Event-Timestamp	Select to enable or disable the RADIUS server attribute event-timestamp function here.

Click the **Apply** button to accept the changes made.

RADIUS Server Settings

This window is used to view and configure the RADIUS server settings.

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:

Figure 9-29 RADIUS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server's IPv4 address here.
IPv6 Address	Enter the RADIUS server's IPv6 address here.
Authentication Port	Enter the authentication port number used here. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. This value must be between 0 and 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 3. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.

Parameter	Description
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

RADIUS Group Server Settings

This window is used to view and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:

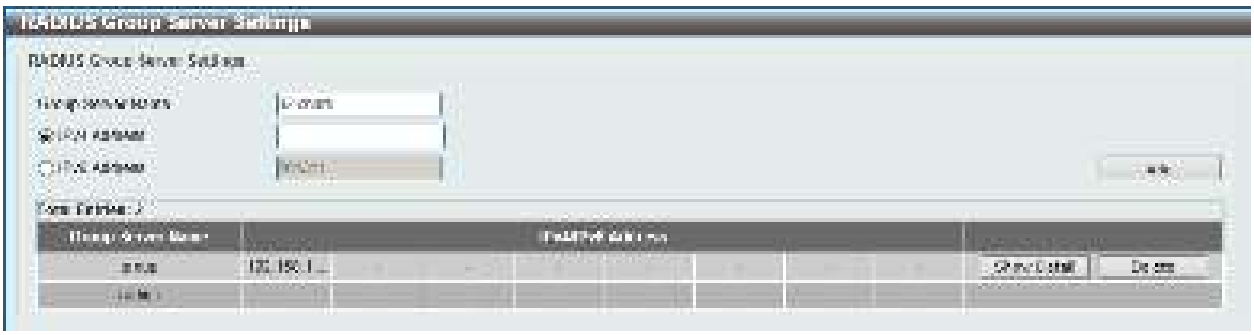


Figure 9-30 RADIUS Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the name of the RADIUS group server here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the RADIUS group server here.
IPv6 Address	Enter the IPv6 address of the RADIUS group server here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure detailed settings for the RADIUS group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.

Figure 9-31 RADIUS Group Server Settings - Detail Window

The fields that can be configured are described below:

Parameter	Description
IPv4 RADIUS Source Interface State	Select to enable or disable the state of the IPv4 RADIUS source interface here.
IPv4 RADIUS Source Interface Type	Select the IPv4 RADIUS source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv4 RADIUS source interface type as VLAN. **Interface ID** - Enter the VLAN interface ID for the IPv4 RADIUS source interface here. The range is from 1 to 4094.
IPv6 RADIUS Source Interface State	Select to enable or disable the state of the IPv6 RADIUS source interface here.
IPv6 RADIUS Source Interface Type	Select the IPv6 RADIUS source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv6 RADIUS source interface type as VLAN. **Interface ID** - Enter the VLAN interface ID for the IPv6 RADIUS source interface here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:

Figure 9-32 RADIUS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

TACACS+

TACACS+ Global Settings

This window is used to display and configure the global TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Global Settings**, as shown below:

Figure 9-33 TACACS+ Global Settings Window

The fields that can be configured in **TACACS+ Global IPv4 Source Interface** are described below:

Parameter	Description
IPv4 TACACS+ Source Interface State	Select to enable or disable the state of the IPv4 TACACS+ source interface here.
IPv4 TACACS+ Source Interface Type	Select the IPv4 TACACS+ source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv4 TACACS+ source interface type as VLAN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **TACACS+ Global IPv6 Source Interface** are described below:

Parameter	Description
IPv6 TACACS+ Source Interface State	Select to enable or disable the state of the IPv6 TACACS+ source interface here.
IPv6 TACACS+ Source Interface Type	Select the IPv6 TACACS+ source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv6 TACACS+ source interface type as VLAN.
Interface ID	Enter the VLAN interface ID here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

TACACS+ Server Settings

This window is used to view and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Server Settings**, as shown below:

Figure 9-34 TACACS+ Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server's IPv4 address here.
IPv6 Address	Enter the TACACS+ server's IPv6 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

TACACS+ Group Server Settings

This window is used to view and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Group Server Settings**, as shown below:

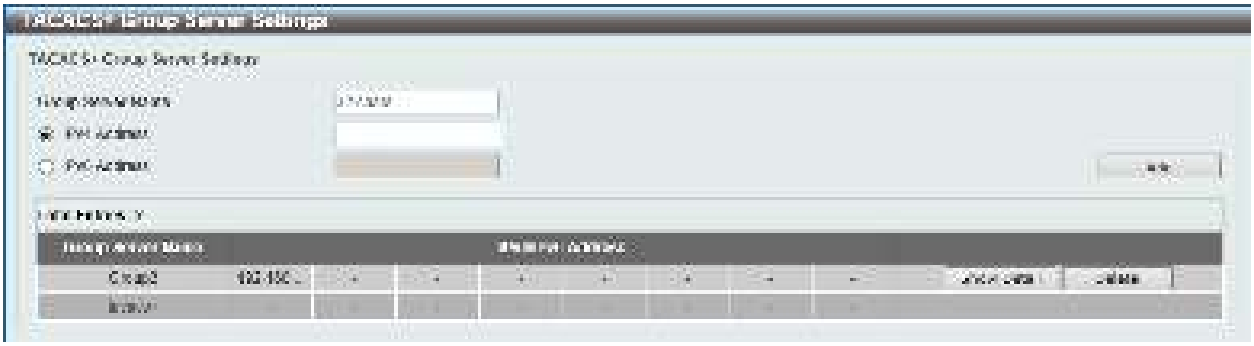


Figure 9-35 TACACS+ Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the name of the TACACS+ group server here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the TACACS+ group server here.
IPv6 Address	Enter the IPv6 address of the TACACS+ group server here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure detailed settings for the TACACS+ group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.

Figure 9-36 TACACS+ Group Server Settings - Detail Window

The fields that can be configured are described below:

Parameter	Description
IPv4 TACACS+ Source Interface State	Select to enable or disable the state of the IPv4 TACACS+ source interface here.
IPv4 TACACS+ Source Interface Type	Select the IPv4 TACACS+ source interface type here. Options to choose from are:

Parameter	Description
	• **VLAN** - Specifies the IPv4 TACACS+ source interface type as VLAN. **Interface ID** - Enter the VLAN interface ID for the IPv4 TACACS+ source interface here. The range is from 1 to 4094.
IPv6 TACACS+ Source Interface State	Select to enable or disable the state of the IPv6 TACACS+ source interface here.
IPv6 TACACS+ Source Interface Type	Select the IPv6 TACACS+ source interface type here. Options to choose from are: • **VLAN** - Specifies the IPv6 TACACS+ source interface type as VLAN. **Interface ID** - Enter the VLAN interface ID for the IPv6 TACACS+ source interface here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

TACACS+ Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click **Security > TACACS+ > TACACS+ Statistic**, as shown below:

Figure 9-37 TACACS+ Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the **Clear** button to clear the information based on the group selected.

Click the **Clear All** button to clear all the information in this table.

Click the **Clear** button to clear all the information for the specific port.

IMPB

The IP network layer uses a four-byte address. The Ethernet link-layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port Binding (IMPB) is to restrict the access to a switch to a number of authorized users. Authorized clients can access a switch's port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system

will block the access by dropping its packet. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

This window is used to view and configure the DHCP snooping global settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:

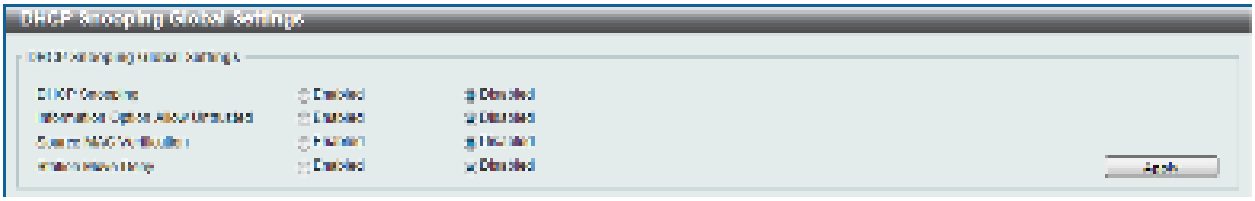


Figure 9-38 DHCP Snooping Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Snooping	Select to enable or disable the DHCP snooping global status.
Information Option Allow Untrusted	Select to enable or disable the option to globally allow DHCP packets with the relay Option 82 on the untrusted interface.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address.
Station Move Deny	Select to enable or disable the DHCP snooping station move state. When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

Click the **Apply** button to accept the changes made.

DHCP Snooping Port Settings

This window is used to view and configure the DHCP snooping port settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings**, as shown below:

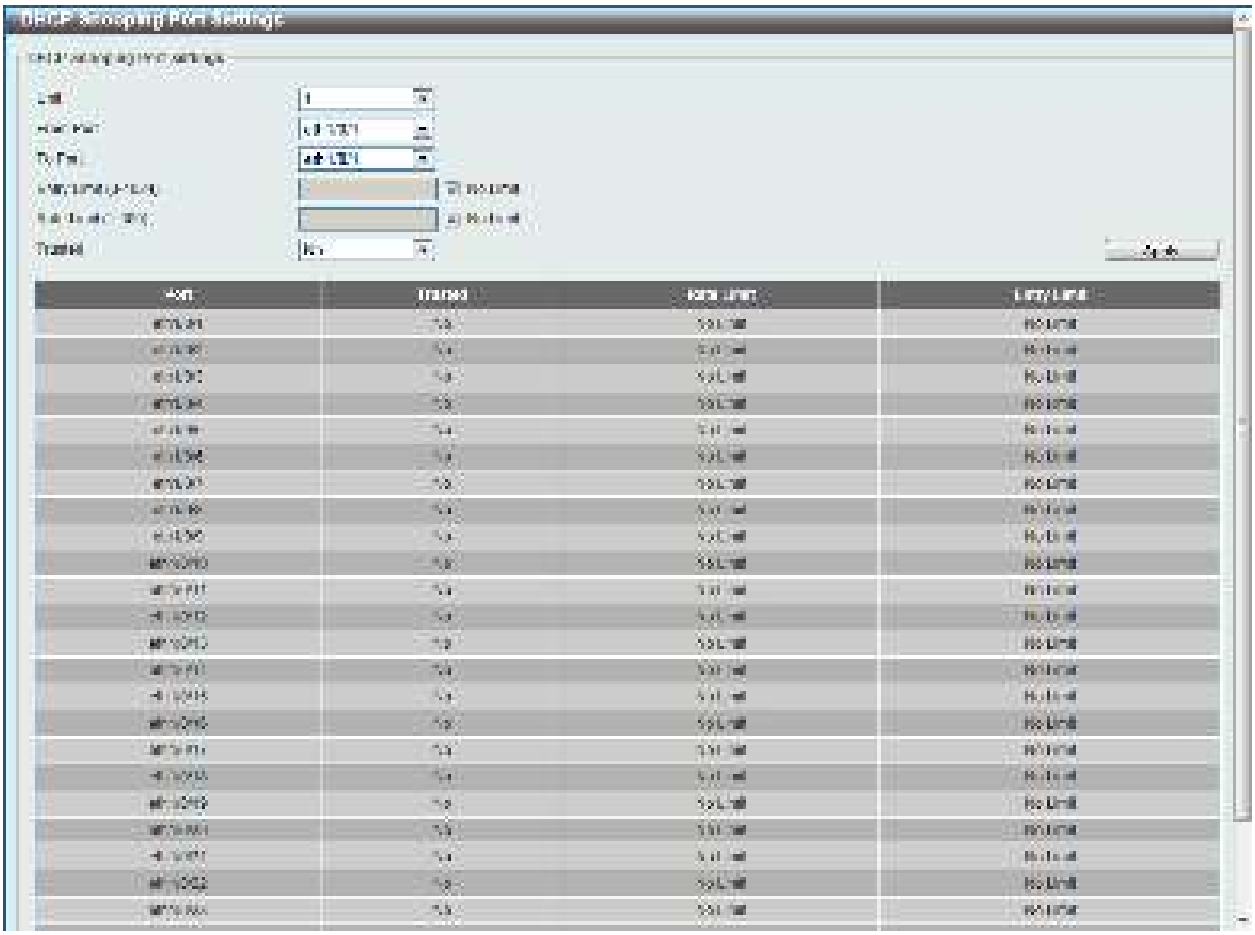


Figure 9-39 DHCP Snooping Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. This value must be between 0 and 1024. Tick the **No Limit** option to disable the function.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 300. Tick the **No Limit** option to disable the function.
Trusted	Select the trusted option here. Options to choose from are **No** and **Yes**. Ports connected to the DHCP server or to other switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

Click the **Apply** button to accept the changes made.

DHCP Snooping VLAN Settings

This window is used to view and configure the DHCP snooping VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:

Figure 9-40 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the DHCP snooping VLAN setting here.

Click the **Apply** button to accept the changes made.

DHCP Snooping Database

This window is used to view and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:

Figure 9-41 DHCP Snooping Database Window

The fields that can be configured for **DHCP Snooping Database** are described below:

Parameter	Description
Write Delay	Enter the write delay time value here. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds. Select the **Default** option to use the default value.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be stored to here. Location to choose from is **TFTP**.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear the stored DHCP snooping database.

The fields that can be configured for **Load DHCP Snooping Database** are described below:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be loaded from here. Location to choose from is **TFTP**.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear all the counter information.

DHCP Snooping Binding Entry

This window is used to view and configure the DHCP snooping binding entries.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry**, as shown below:

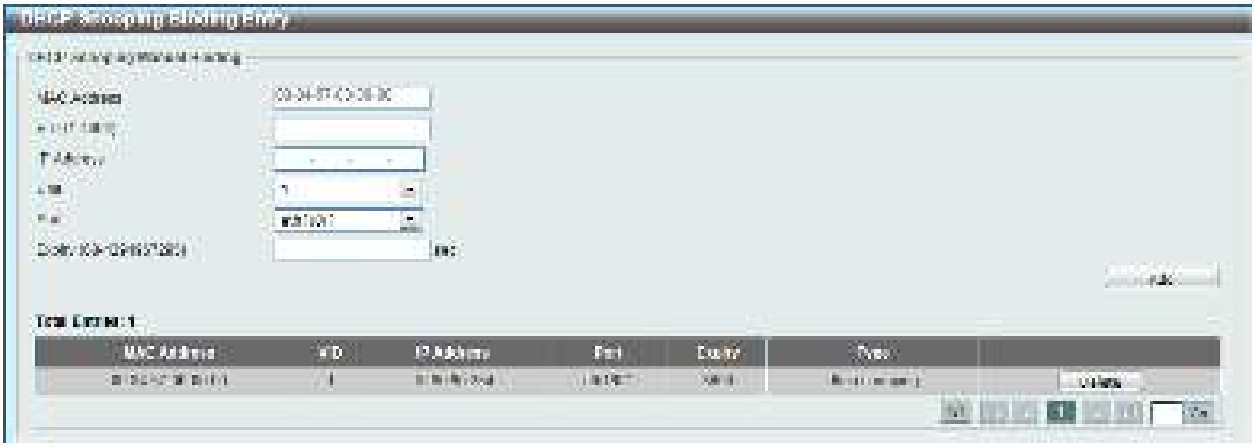


Figure 9-42 DHCP Snooping Binding Entry Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID of the DHCP snooping binding entry here. This value must be between 1 and 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Dynamic ARP Inspection

ARP Access List

This window is used to view and configure the dynamic ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:

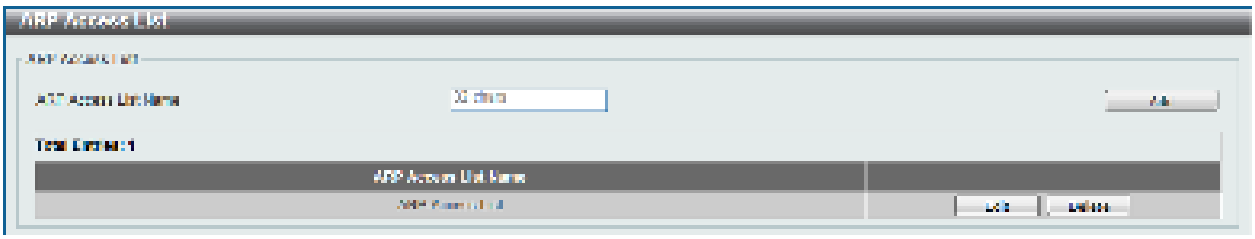


Figure 9-43 ARP Access List Window

The fields that can be configured are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

Click the **Add** button to add a new entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Edit** button, the following window will appear.

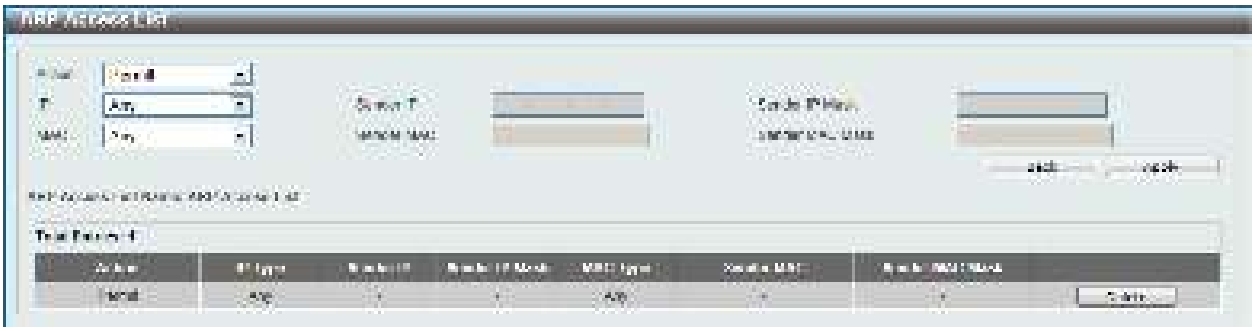


Figure 9-44 ARP Access List - Edit Window

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Permit** and **Deny**.
IP	Select the type of sender IP address that will be used here. Options to choose from are **Any**, **Host**, and **IP with Mask**.
Sender IP	After selecting the **Host** or **IP with Mask** options as the type of **IP**, enter the sender IP address used here.

Parameter	Description
Sender IP Mask	After selecting the **IP with Mask** option as the type of **IP**, enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are **Any**, **Host**, and **MAC with Mask**.
Sender MAC	After selecting the **Host** or **MAC with Mask** options as the type of **MAC**, enter the sender MAC address used here.
Sender MAC Mask	After selecting the **MAC with Mask** option as the type of **MAC**, enter the sender MAC mask used here.

Click the **Back** button to return to the previous page.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Inspection Settings

This window is used to view and configure the ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings**, as shown below:

Figure 9-45 ARP Inspection Settings Window

The fields that can be configured for **ARP Inspection Validation** are described below:

Parameter	Description
Src-MAC	Select to enable of disable the source MAC option here. This option specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
Dst-MAC	Select to enable of disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
IP	Select to enable of disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It

Parameter	Description
	also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to configure the ARP inspection VLAN logging settings.

After clicking the **Edit** button, the following fields can be configured:

Parameter	Description
ACL Logging	Select the ACL logging action here. This specifies the logging criteria for packets that are dropped or permitted based on ACL matches. Options to choose from are: • **Deny** - Specifies logging when denied by the configured ACL. • **Permit** - Specifies logging when permitted by the configured ACL. • **All** - Specifies logging when permitted or denied by the configured ACL. • **None** - Specifies that ACL-matched packets are not logged.
DHCP Logging	Select the DHCP logging action here. This specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings. Options to choose from are: • **Deny** - Specifies logging when denied by DHCP bindings. • **Permit** - Specifies logging when permitted by DHCP bindings. • **All** - Specifies logging when permitted or denied by DHCP bindings. • **None** - Specifies to prevent the logging of all packets permitted or denied by DHCP bindings.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting **Yes** or **No**.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Port Settings

This window is used to view and configure the ARP inspection port settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:

Figure 9-46 ARP Inspection Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 150 packets per seconds.
Burst Interval	Enter the burst interval value here. This value must be between 1 and 15. Tick the **None** option to disable the option.
Trust State	Select to enable or disable the trust state here.

Click the **Apply** button to accept the changes made.

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

This window is used to view and configure the ARP inspection VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:

Figure 9-47 ARP Inspection VLAN Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the ARP inspection option's state for the specified VLAN here.

Click the **Apply** button to accept the changes made.

ARP Inspection Statistics

This window is used to view and clear the ARP inspection statistics information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics**, as shown below:

Figure 9-48 ARP Inspection Statistics Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Click the **Clear by VLAN** button to clear the information based on the VLAN ID(s) entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Log

This window is used to view, configure, and clear the ARP inspection log information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log**, as shown below:

Figure 9-49 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
Log Buffer	Enter the log's buffer value used here. This value must be between 1 and 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to view and configure the IP source guard port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:

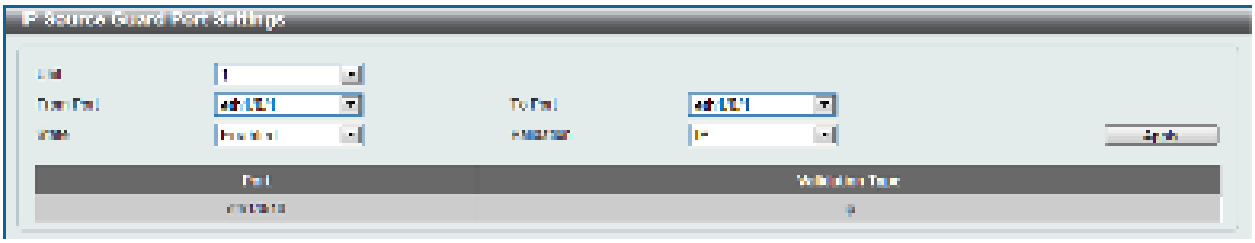


Figure 9-50 IP Source Guard Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IP source guard's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are **IP** and **IP-MAC**. Selecting **IP** means that the IP address of the received packets will be checked. Selecting **IP-MAC** means that the IP address and the MAC address of the received packets will be checked.

Click the **Apply** button to accept the changes made.

IP Source Guard Binding

This window is used to view and configure the IP source guard binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:

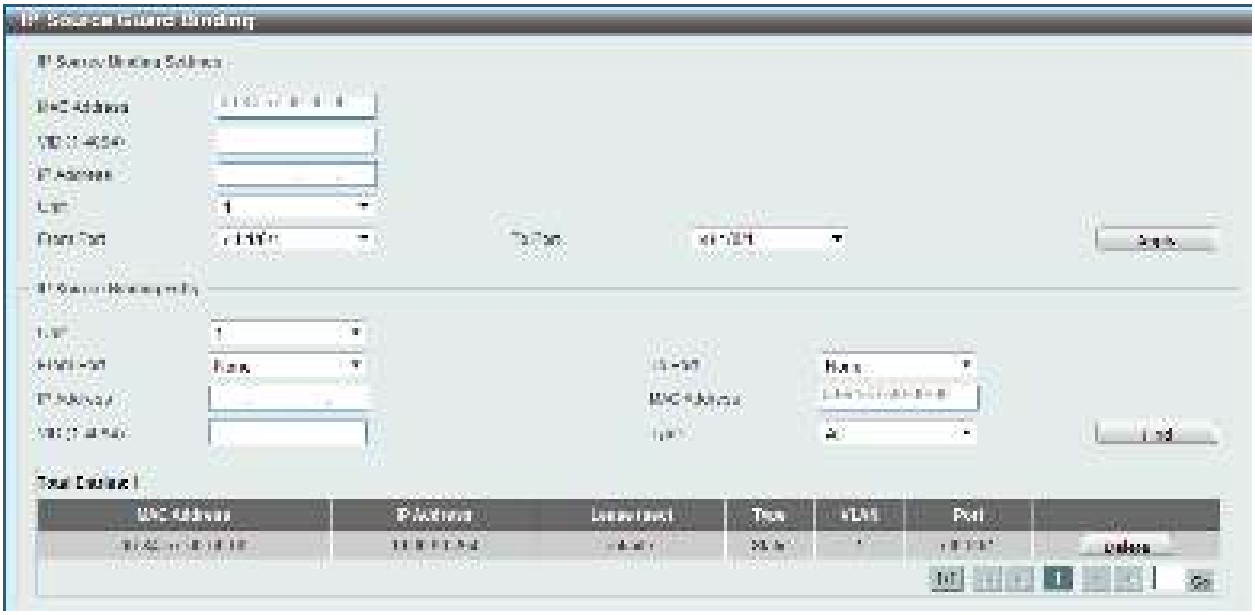


Figure 9-51 IP Source Guard Binding Window

The fields that can be configured for **IP Source Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
IP Address	Enter the IP address of the binding entry here.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **IP Source Binding Entry** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
From Port / To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	Select the type of binding entry to find here. Options to choose from are: • **All** - Specifies that all the DHCP binding entries will be displayed. • **DHCP Snooping** - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping.

Parameter	Description
	• **Static** - Specifies to display the IP-source guard binding entry that is manually configured.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IP Source Guard HW Entry

This window is used to view the IP source guard hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:

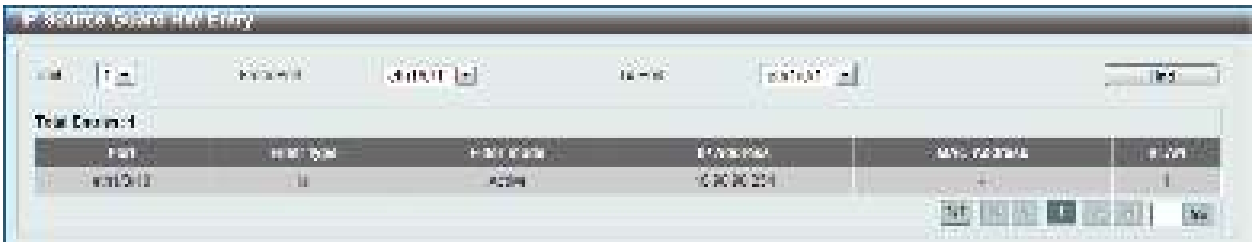


Figure 9-52 IP Source Guard HW Entry Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this query here.
From Port / To Port	Select the appropriate port range used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Advanced Settings

IP-MAC-Port Binding Settings

This window is used to view and configure the IP-MAC-Port binding settings.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings**, as shown below:

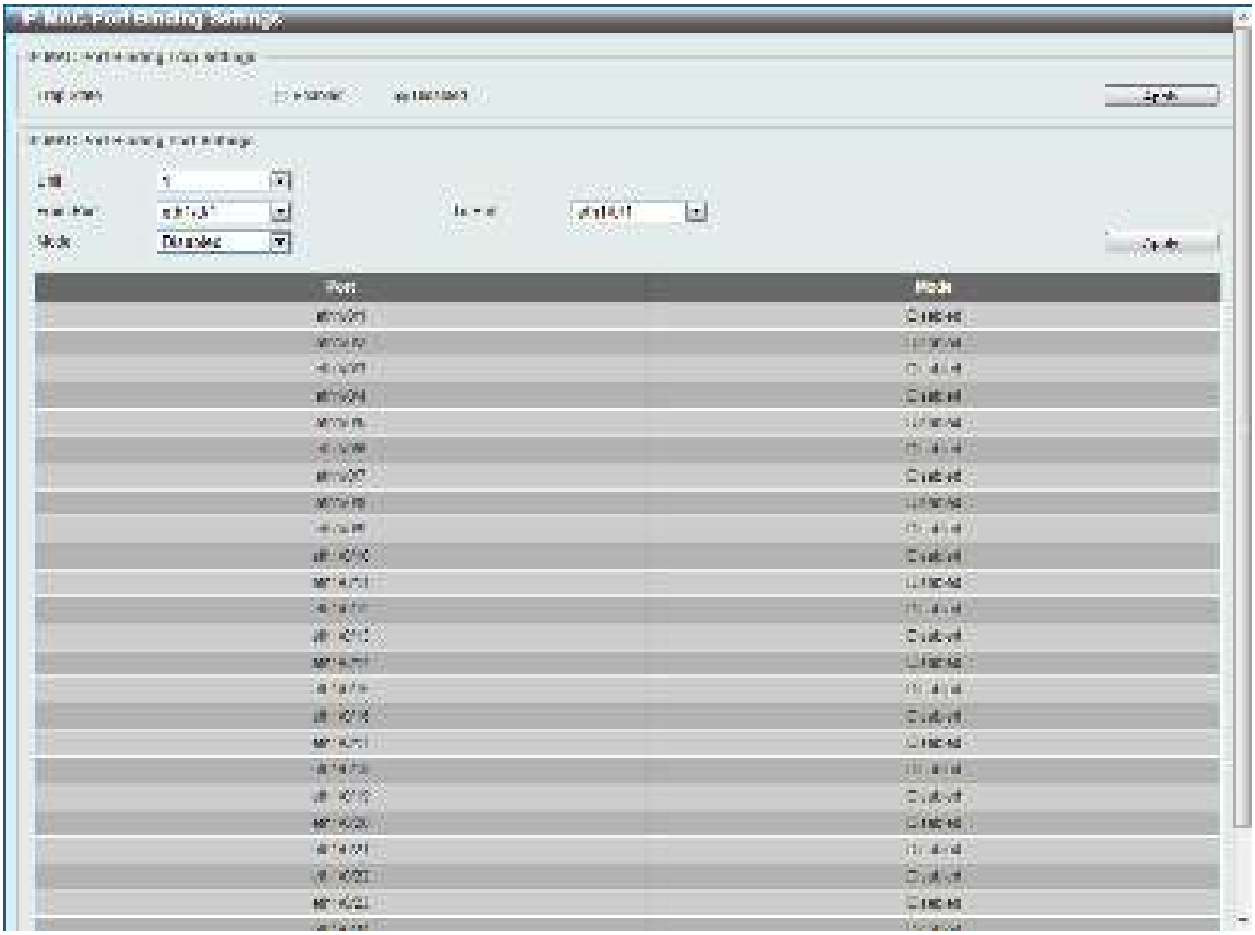


Figure 9-53 IP-MAC-Port Binding Settings Window

The fields that can be configured for **IP-MAC-Port Binding Trap Settings** are described below:

Parameter	Description
Trap State	Select the enable or disable the IP-MAC-Port binding option's trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **IP-MAC-Port Binding Port Settings** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are **Disabled**, **Strict**, and **Loose**. When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source

Parameter	Description
	MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

Click the **Apply** button to accept the changes made.

IP-MAC-Port Binding Blocked Entry

This window is used to view and clear the IP-MAC-Port binding blocked entry table.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry**, as shown below:

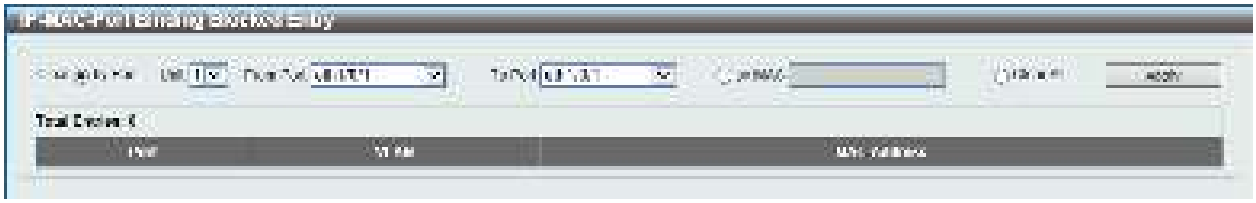


Figure 9-54 IP-MAC-Port Binding Blocked Entry Window

The fields that can be configured are described below:

Parameter	Description
Clear All	Leave all fields unselected and click the **Apply** button to clear all IMPB blocked entry information.
Clear by Port	Select this option to clear the entry table based on the port(s) selected.
Unit	Select the switch unit that will be clear here.
From Port / To Port	Select the appropriate port range that will be cleared here.
Clear by MAC	Select this option to clear the entry table based on the MAC address entered. Enter the MAC address that will be cleared in the space provided.
Clear All	Select this option to clear all entries that contain MAC addresses.

Click the **Apply** button to accept the changes made.

IPv6

IPv6 Snooping

This window is used to view and configure the IPv6 snooping settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Snooping**, as shown below:

Figure 9-55 IPv6 Snooping Window

The fields that can be configured for **Station Move Setting** are described below:

Parameter	Description
Station Move	Select the station move options here. Options to choose from are **Permit** and **Deny**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **IPv6 Snooping Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 511. Tick the **No Limit** option to disable this option.
Protocol	Select the protocol that will be associated with this policy here. Options to choose from are **Disabled**, **DHCP**, **NDP**, and **All**. DHCPv6 Snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database. ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD NS and DAD NA) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.
VID List	Enter the VLAN ID list used here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 ND Inspection

This window is used to view and configure the IPv6 ND inspection settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 ND Inspection**, as shown below:

Figure 9-56 IPv6 ND Inspection Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name used here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.
Validate Source-MAC	Select to enable or disable the validation of the source MAC address option here. When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 RA Guard

This window is used to view and configure the IPv6 Router Advertisement (RA) guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 RA Guard**, as shown below:

Figure 9-57 IPv6 RA Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is **Host**, which will block all the RA packets. If the device's role is **Router**, RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 DHCP Guard

This window is used to view and configure the IPv6 DHCP guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:

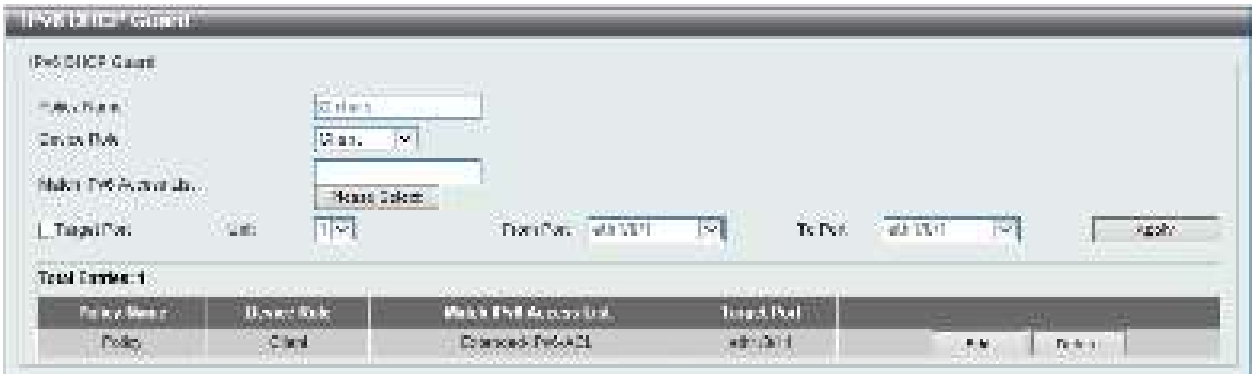


Figure 9-58 IPv6 DHCP Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Client** and **Server**. By default, the device's role is set as **Client**, which will block all the DHCPv6 packets from the DHCPv6 Server. If the device's role is set as **Server**, DHCPv6 Server packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 Source Guard

IPv6 Source Guard Settings

This window is used to view and configure the IPv6 source guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:

Figure 9-59 IPv6 Source Guard Settings Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to permit of deny data traffic from the auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the administrator that wants to block hosts with self-configured addresses from sending traffic.
Link Local Traffic	Select to permit of deny hardware permitted data traffic send by the link-local address.
Target Port	Tick this option to specify the target port.
Unit	Select the switch unit that will be used for this configuration here.

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 Neighbor Binding

This window is used to view and configure the IPv6 neighbor binding settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding**, as shown below:

Figure 9-60 IPv6 Neighbor Binding Window

The fields that can be configured for **IPv6 Neighbor Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address used here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.
IPv6 Address	Enter the IPv6 address used here.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **IPv6 Neighbor Binding Entry** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this search here.
From Port / To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

DHCP Server Screening

This function allows users to not only to restrict all DHCP server packets but also to receive any specified DHCP server packet by any specified DHCP client. It is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

The first time the DHCP filter is enabled it will create both an access profile entry and an access rule per port entry, it will also create other access rules. These rules are used to block all DHCP server packets. In addition to a permit DHCP entry it will also create one access profile and one access rule entry the first time the DHCP client MAC address is used as the client MAC address. The Source IP address is the same as the DHCP server's IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fields, which the user has configured.

When DHCP server filter function is enabled all DHCP server packets will be filtered from a specific port.

DHCP Server Screening Global Settings

This window is used to view and configure the DHCP server screening global settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Global Settings**, as shown below:

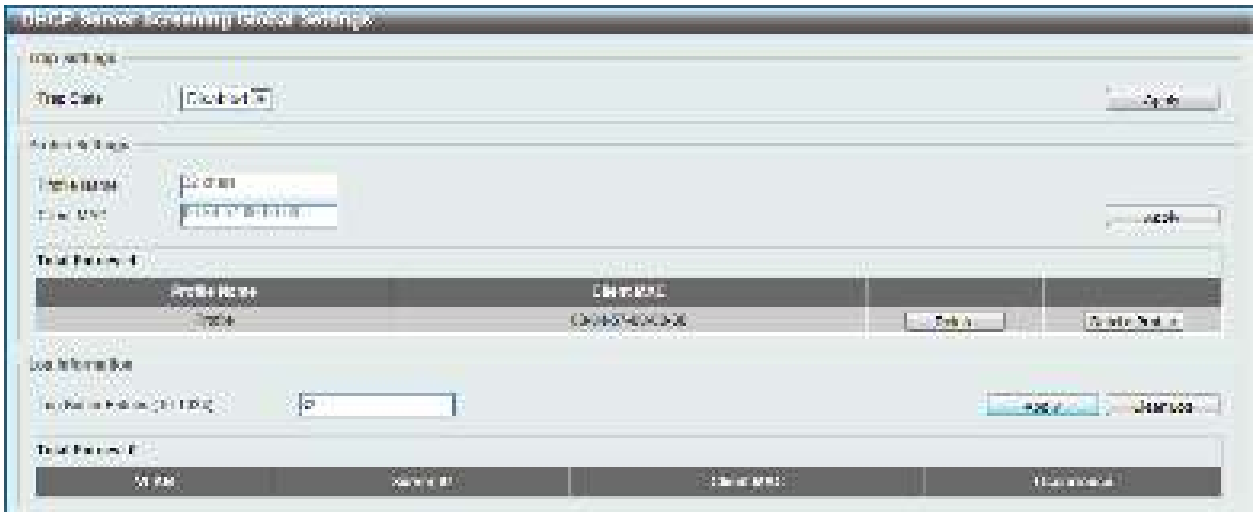


Figure 9-61 DHCP Server Screening Global Settings Window

The fields that can be configured for **Trap Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DHCP server screening trap here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.
Client MAC	Enter the MAC address used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Delete Profile** button to remove the specified profile.

The fields that can be configured for **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. This value must be between 10 and 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

Click the **Clear Log** button to clear the log.

DHCP Server Screening Port Settings

This window is used to view and configure the DHCP server screening port settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:

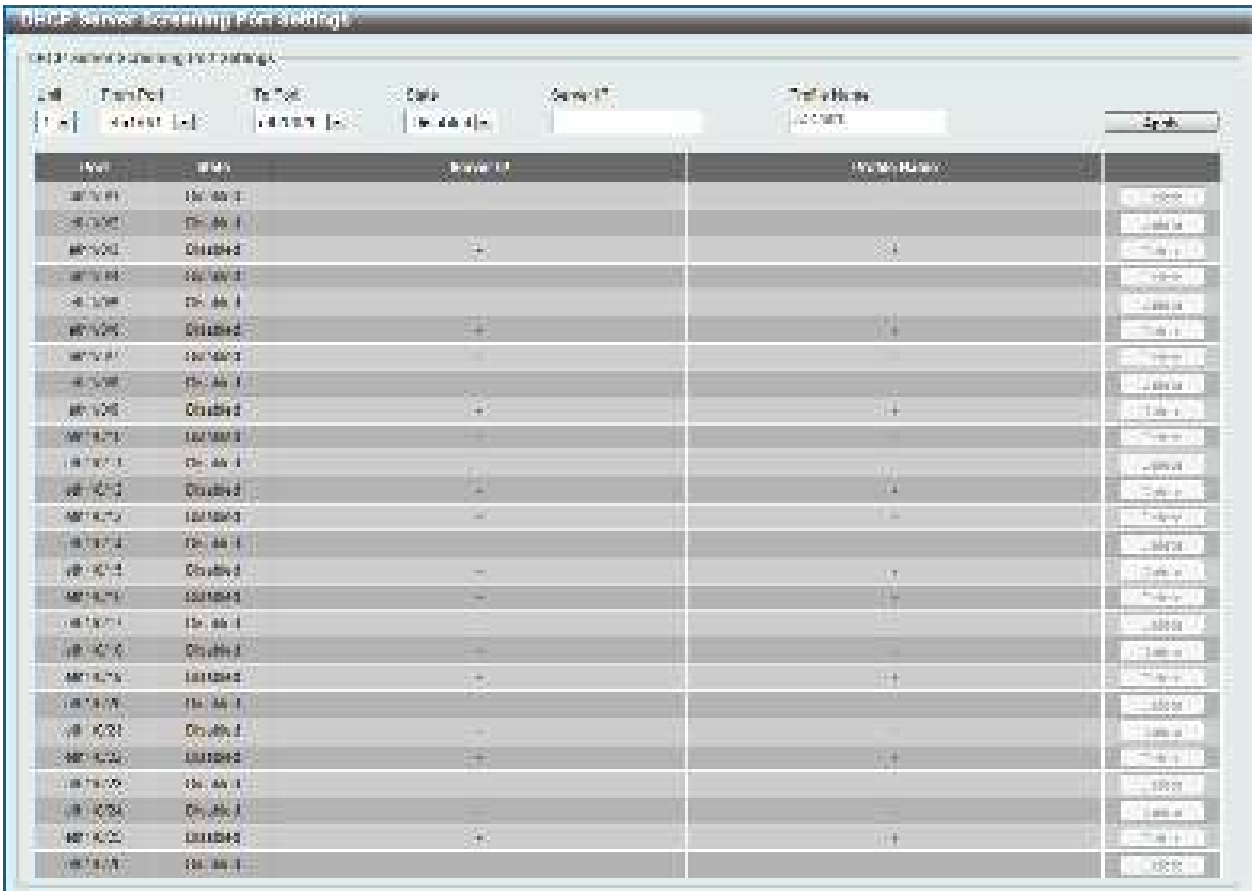


Figure 9-62 DHCP Server Screening Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Parameter	Description
State	Select to enable or disable the DHCP server screening function on the port(s) specified.
Server IP	Enter the DHCP server's IP address here.
Profile Name	Enter the DHCP server screening profile that will be used for the port(s) specified here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Spoofing Prevention

This window is used to view and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

To view the following window, click **Security > ARP Spoofing Prevention**, as shown below:

Figure 9-63 ARP Spoofing Prevention Window

The fields that can be configured for **ARP Spoofing Prevention Logging State** are described below:

Parameter	Description
ARP Spoofing Prevention Logging State	Select to enable or disable the ARP spoofing logging state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **ARP Spoofing Prevention** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway's IP address used here.
Gateway MAC	Enter the gateway's MAC address used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

BPDU Attack Protection

This window is used to view and configure the BPDU attack protection settings. In generally, there are two states in the BPDU attack protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet and it will take action based on the configuration. Thus, BPDU protection can only be enabled on the STP-disabled port.

BPDU protection has a higher priority than the FBPDU setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the BPDU tunnel port setting in determination of BPDU handling. When a port is configured as a BPDU tunnel port for STP, it will forward STP BPDU but if the port is BPDU protection enabled, the port will not forward STP BPDUs.

To view the following window, click **Security > BPDU Attack Protection**, as shown below:

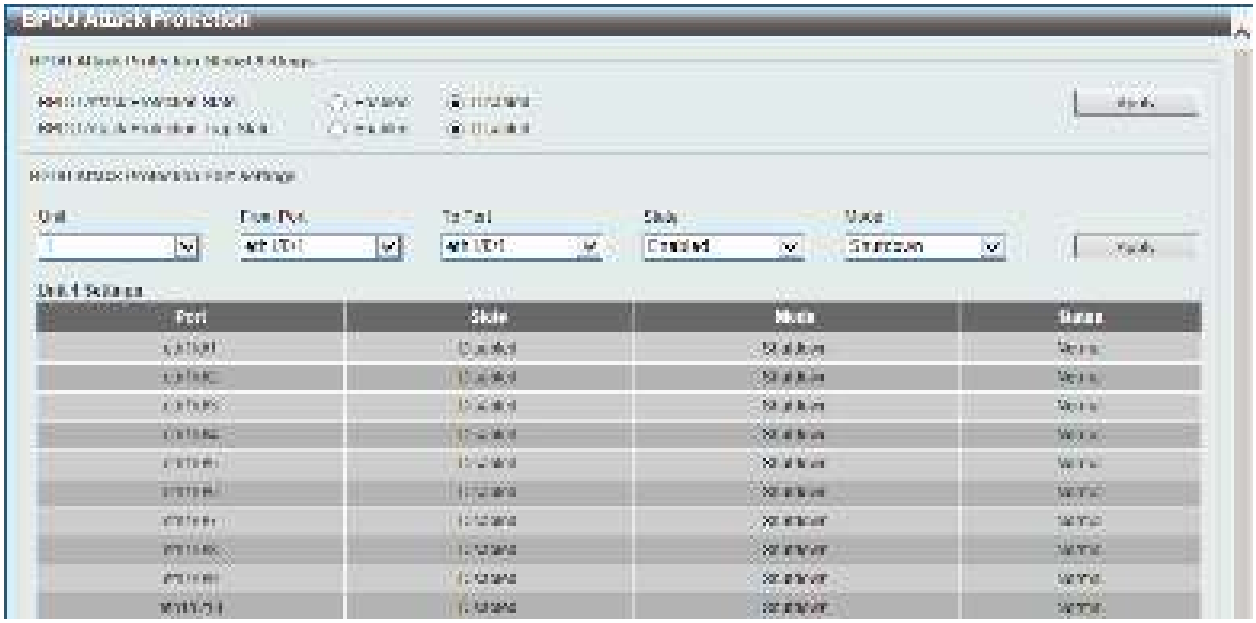


Figure 9-64 BPDU Attack Protection Window

The fields that can be configured are described below:

Parameter	Description
BPDU Attack Protection State	Select to enable or disable the BPDU attack protection feature's global state here.
BPDU Attack Protection Trap State	Select to enable or disable the BPDU attack protection feature's trap state here.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the BPDU attack protection feature's state on the port(s) specified.
Mode	Select the BPDU attack protection feature's mode that will be applied to the port(s) specified. Options to choose from are:

Parameter	Description
	• **Drop** - Drop all received BPDU packets when the port enters under attack state. • **Block** - Drop all packets (include BPDU and normal packets) when the port enters under attack state. • **Shutdown** - Shut down the port when the port enters under attack state.

Click the **Apply** button to accept the changes made.

MAC Authentication

This window is used to view and configure the MAC authentication settings. MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

To view the following window, click **Security > MAC Authentication**, as shown below:

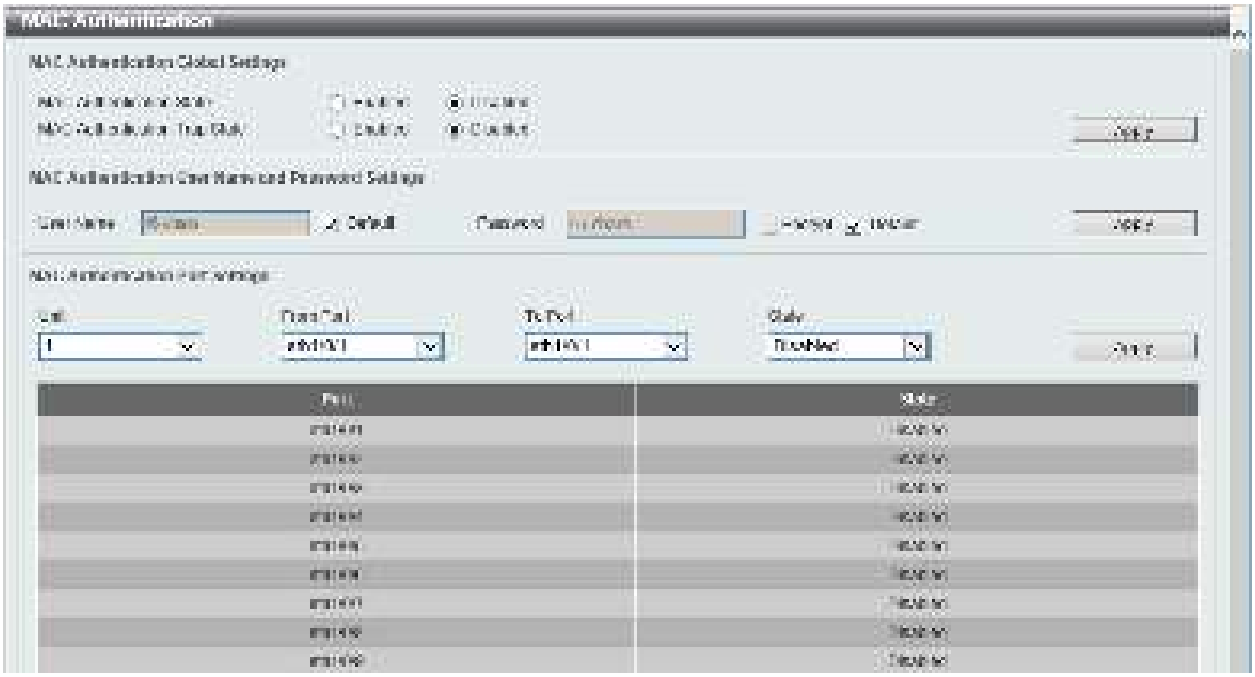


Figure 9-65 Port Security Global Settings Window

The fields that can be configured for **MAC Authentication Global Settings** are described below:

Parameter	Description
MAC Authentication State	Select to enable or disable the MAC authentication feature's global state.
MAC Authentication Trap State	Select to enable or disable the MAC authentication feature's trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **MAC Authentication User Name and Password Settings** are described below:

Parameter	Description
User Name	Enter the username used for MAC authentication here. This name can be up to 16 characters long. Tick the **Default** option to restore the username to the client's MAC address here.
Password	Enter the password used for MAC authentication here. Tick the **Encrypt** option save this password in the encrypted form. Tick the **Default** option to restore the password to the client's MAC address here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **MAC Authentication Port Settings** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

Click the **Apply** button to accept the changes made.

Web-based Access Control

Web-based Access Control (WAC) is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages (e.g., http://www.dlink.com) through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is unauthenticated, the Switch will launch a pop-up user name and password window to query users. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

D-Link's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC, which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration. Whether or not a virtual IP is specified, users can access the WAC pages through the Switch's system IP. When a virtual IP is not specified, the authenticating Web request will be redirected to the Switch's system IP.

The Switch's implementation of WAC features a user-defined port number that allows the configuration of the TCP port for either the HTTP or HTTPS protocols. This TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for

authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80 and the default port number for HTTPS is 443. If no protocol is specified, the default protocol is HTTP.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:

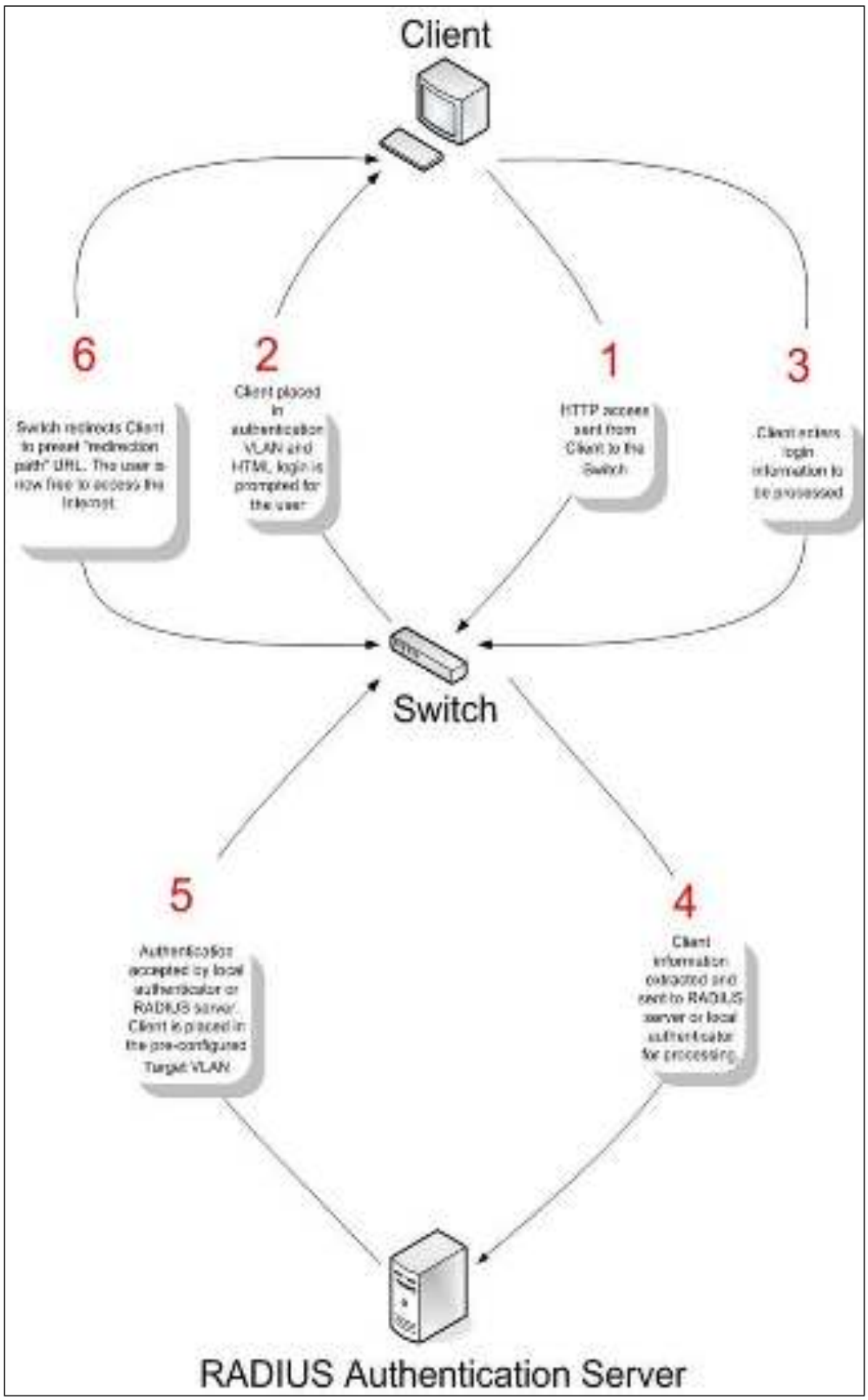


Figure 9-66 RADIUS Authentication Server

Conditions and Limitations

- If the client is utilizing DHCP to attain an IP address, the authenticating VLAN must provide a DHCP server or a DHCP relay functions so that client may obtain an IP address.
- Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
- If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

Web Authentication

This window is used to view and configure the Web authentication settings.

To view the following window, click **Security > Web-based Access Control > Web Authentication**, as shown below:

Figure 9-67 Port Security Global Settings Window

The fields that can be configured are described below:

Parameter	Description
Web Authentication State	Select to enable or disable the Web authentication feature's global state.
Trap State	Select to enable or disable the Web authentication feature's trap state.
Virtual IPv4	Enter the virtual IPv4 address used here. The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. Therefore, it's not allowed to configure virtual IP in the same subnet as the Switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly. The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command. If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication.
Virtual IPv6	Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.
Virtual URL	Enter the virtual URL used here. This URL can be up to 128 characters long.
Redirection Path	Enter the redirection path here. This path can be up to 128 characters long.

Click the **Apply** button to accept the changes made.

WAC Port Settings

This window is used to view and configure the WAC port settings.

To view the following window, click **Security > Web-based Access Control > WAC Port Settings**, as shown below:

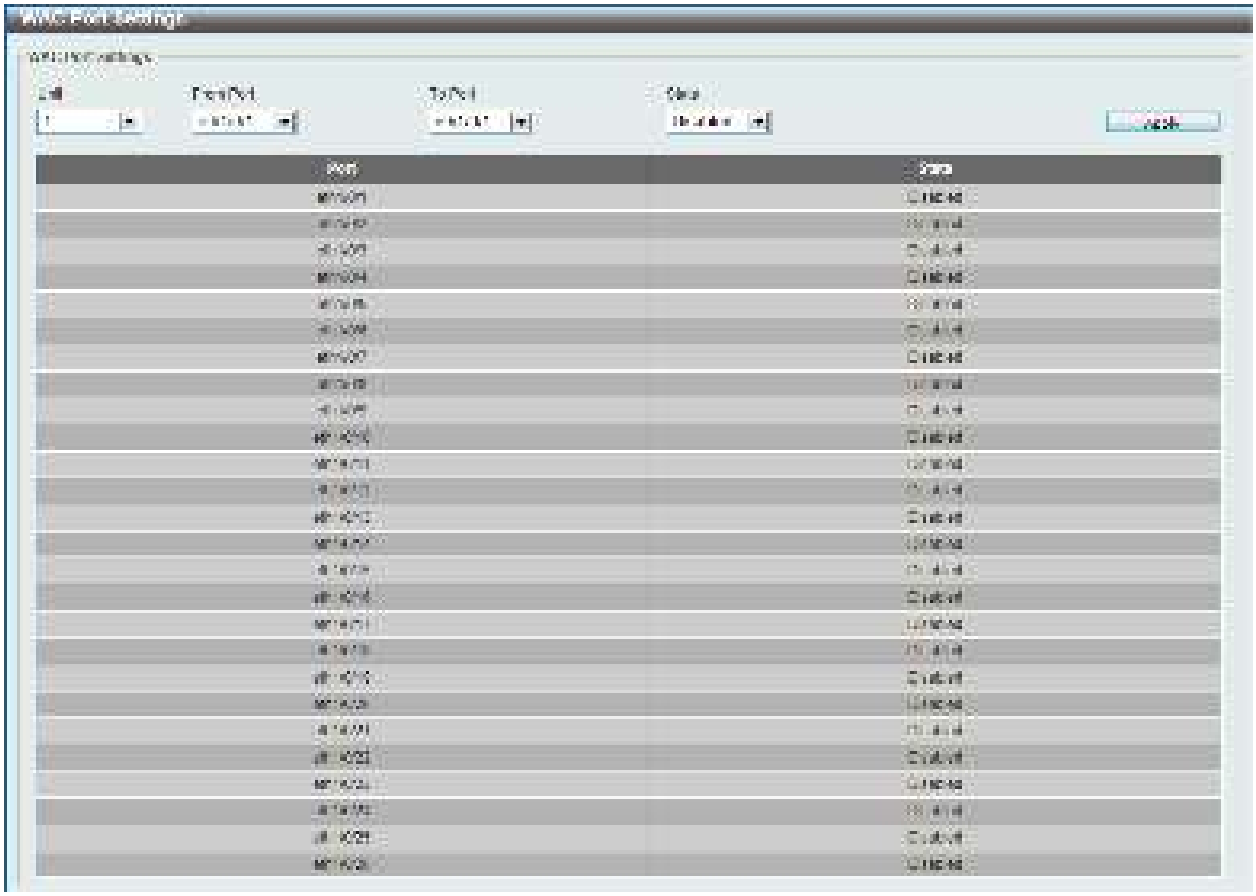


Figure 9-68 WAC Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the WAC feature on the port(s) specified.

Click the **Apply** button to accept the changes made.

WAC Customize Page

This window is used to view and configure the WAC customized login page.

To view the following window, click **Security > Web-based Access Control > WAC Customize Page**, as shown below:

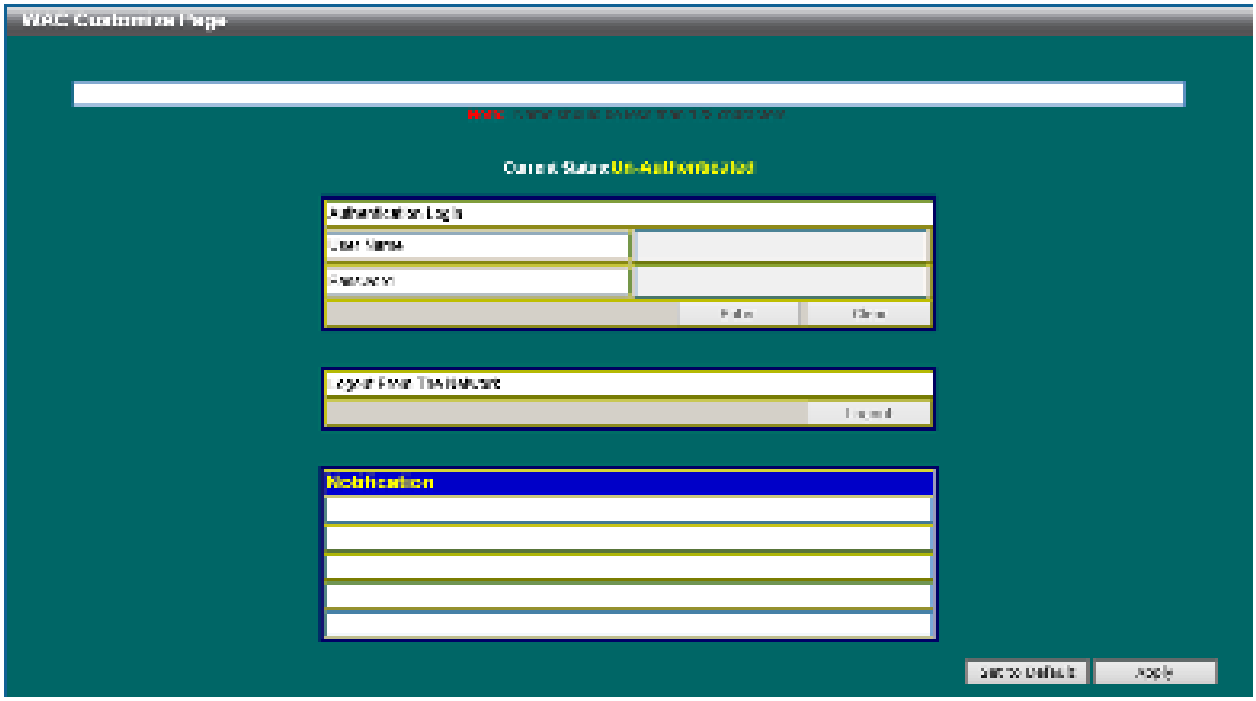


Figure 9-69 WAC Customize Page Window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There a 5 lines available for additional information.

Click the **Set to Default** button to replace the information with the default information.

Click the **Apply** button to accept the changes made.

Japanese Web-based Access Control

JWAC Global Settings

This window is used to view and configure the Japanese Web-based Access Control (JWAC) global settings.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Global Settings**, as shown below:

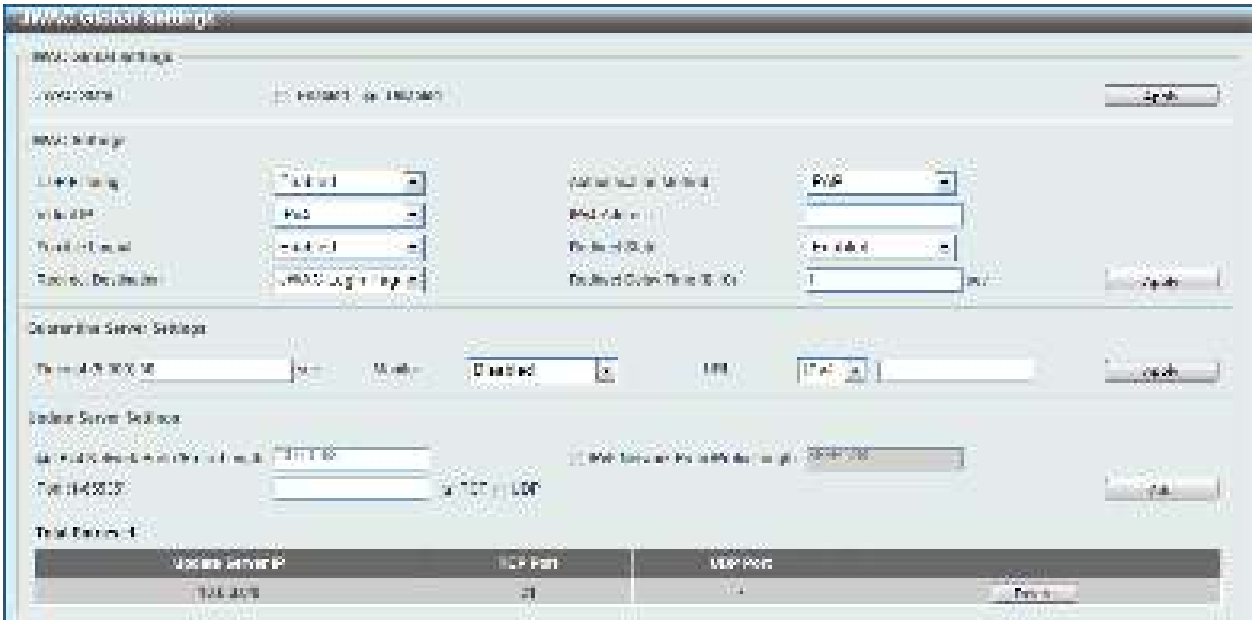


Figure 9-70 JWAC Global Settings Window

The fields that can be configured for **JWAC Global Settings** are described below:

Parameter	Description
JWAC State	Select to enable or disable the JWAC feature's global state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **JWAC Settings** are described below:

Parameter	Description
UDP Filtering	Select to enable or disable UDP filtering here.
Authentication Method	Select the authentication method used here. Options to choose from are **MD5**, **CHAP**, **PAP**, **MS-CHAP**, and **MS-CHAP-v2**.
Virtual IP	Select the virtual IP option used here. Options to choose from are **IPv4**, **IPv6**, and **URL**.
IPv4 Address	After selecting **IPv4** as the **Virtual IP**, the following field will be available. Enter the virtual IPv4 address used here. All JWAC authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packets or ARP requests. Therefore, it's not allowed to configure virtual IP in the same subnet as the switch's IP interface or the same subnet as the host PCs' subnet, otherwise JWAC authentication cannot operate correctly. The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS

Parameter	Description
	server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command. If the IPv4 virtual IP is not configured, the IPv4 access cannot start JWAC authentication.
IPv6 Address	After selecting **IPv6** as the **Virtual IP**, the following field will be available. Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a JWAC authentication.
Virtual URL	After selecting **URL** as the **Virtual IP**, the following field will be available. Enter the virtual URL used here.
Forcible Logout	Select to enable or disable the forcible logout option here. When the forcible logout feature is enabled, a ping packet from an authenticated host to the JWAC switch with a TTL of 1 and a destination IP the same as virtual IP will be regarded as a logout request and the host will be moved back to unauthenticated state.
Redirect State	Select to enable or disable the redirection state here. When redirect is enabled, all Web access is redirected to the quarantine server or JWAC login page.
Redirect Destination	Select the redirect destination here. Options to choose from are **Quarantine Server** and **JWAC Login Page**. When redirecting to the quarantine server, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When redirecting to the JWAC login page, the unauthenticated host will be redirected to the JWAC login page in the switch to finish authentication. When redirecting to the quarantine server is specified, a quarantine server must be configured first before enabling the JWAC function globally. When redirect is disabled, all Web access is denied except for access to the quarantine server or JWAC login page.
Redirect Delay Time	Enter the redirect delay time value here. This value must be between 0 and 10 seconds. By default, this value 1 second.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Quarantine Server Settings** are described below:

Parameter	Description
Timeout	Enter the quarantine server's timeout value here. This value must be between 5 and 300 seconds. By default, this value is 30 seconds.
Monitor	Select to enable or disable the monitor option here. When the JWAC quarantine server monitor feature is enabled, the JWAC switch will monitor the quarantine server to ensure the server is okay. If the switch detects no quarantine server, it will redirect all unauthenticated HTTP accesses to the JWAC Login Page if the redirect option is enabled and the redirect destination is configured to be quarantine server.
URL	Select the whether the quarantine server uses an **IPv4** or **IPv6** address and enter the respective IP address in the space provided.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Update Server Settings** are described below:

Parameter	Description
IPv4 Network Prefix/Prefix Length	Enter the update server's IPv4 address and prefix length here. Any servers (like update.microsoft.com or some sites of Antivirus software companies, which ActiveX needs to access to accomplish the authentication before the client passes the authentication) should be added with its IP address or with the network address. By adding the network address, an entry can serve multiple update servers on the same network. Multiple update server addresses or network addresses can be configured.
IPv6 Network Prefix/Prefix Length	Enter the update server's IPv6 address and prefix length here.
Port	Enter the update server's port used here. This value must be between 1 and 65535. Also, select whether this port is a **TCP** or **UDP** port.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

JWAC Port Settings

This window is used to view and configure the JWAC port settings.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Port Settings**, as shown below:

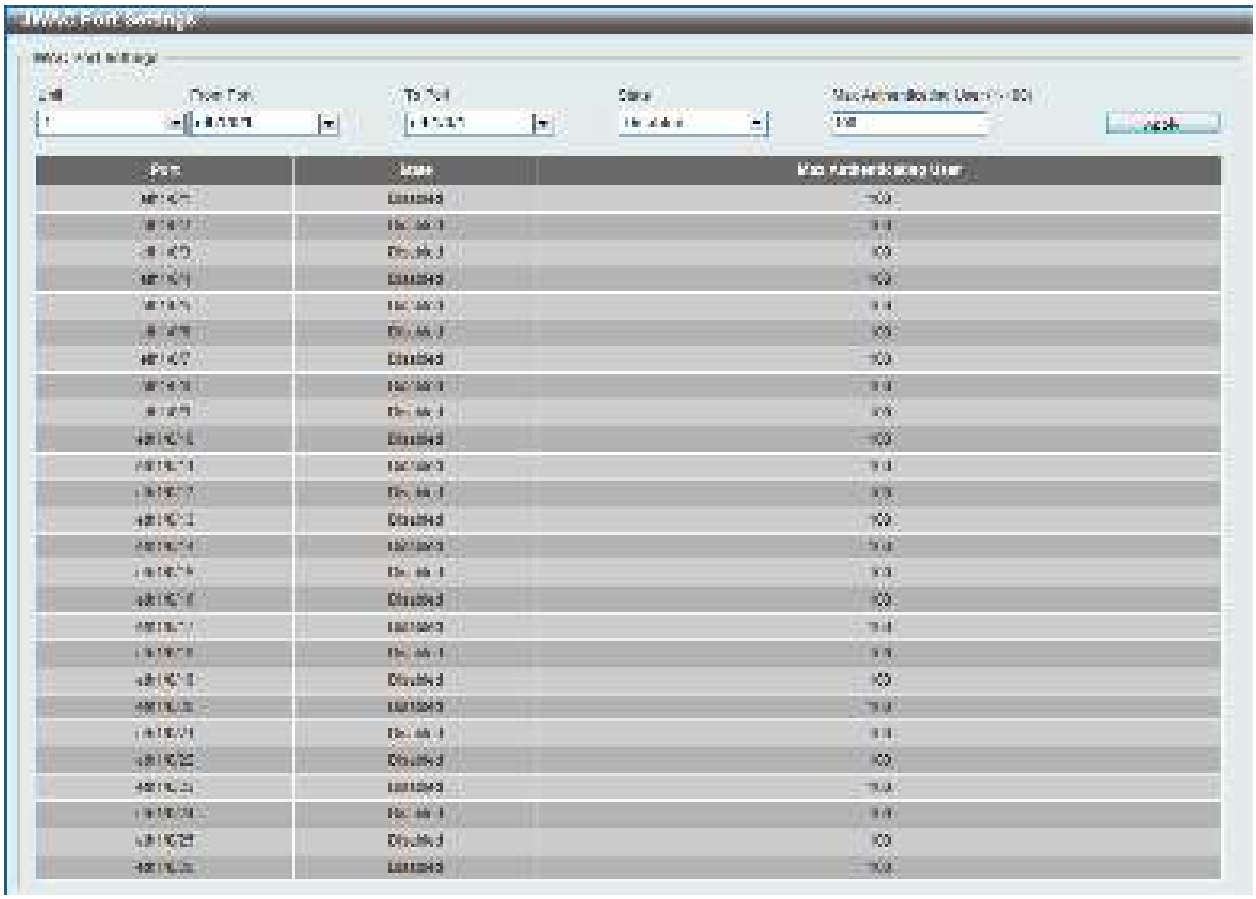


Figure 9-71 JWAC Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select whether JWAC is enabled or disabled on the port(s) specified.
Max Authenticating User	Enter the maximum number of authentication users allowed here. This value must be between 1 and 100.

Click the **Apply** button to accept the changes made.

JWAC Customize Page Language

This window is used to view and configure the JWAC customize page's language.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Customize Page Language**, as shown below:

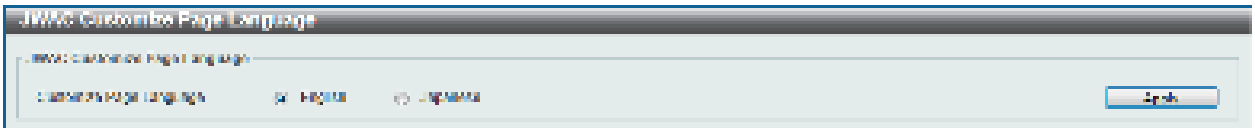


Figure 9-72 JWAC Customize Page Language Window

The fields that can be configured are described below:

Parameter	Description
Customize Page Language	Select the language option that will be used when the JWAC login page is displayed.

Click the **Apply** button to accept the changes made.

JWAC Customize Page

This window is used to view and configure the JWAC customize page settings.

To view the following window, click **Security > Japanese Web-based Access Control > JWAC Customize Page**, as shown below:

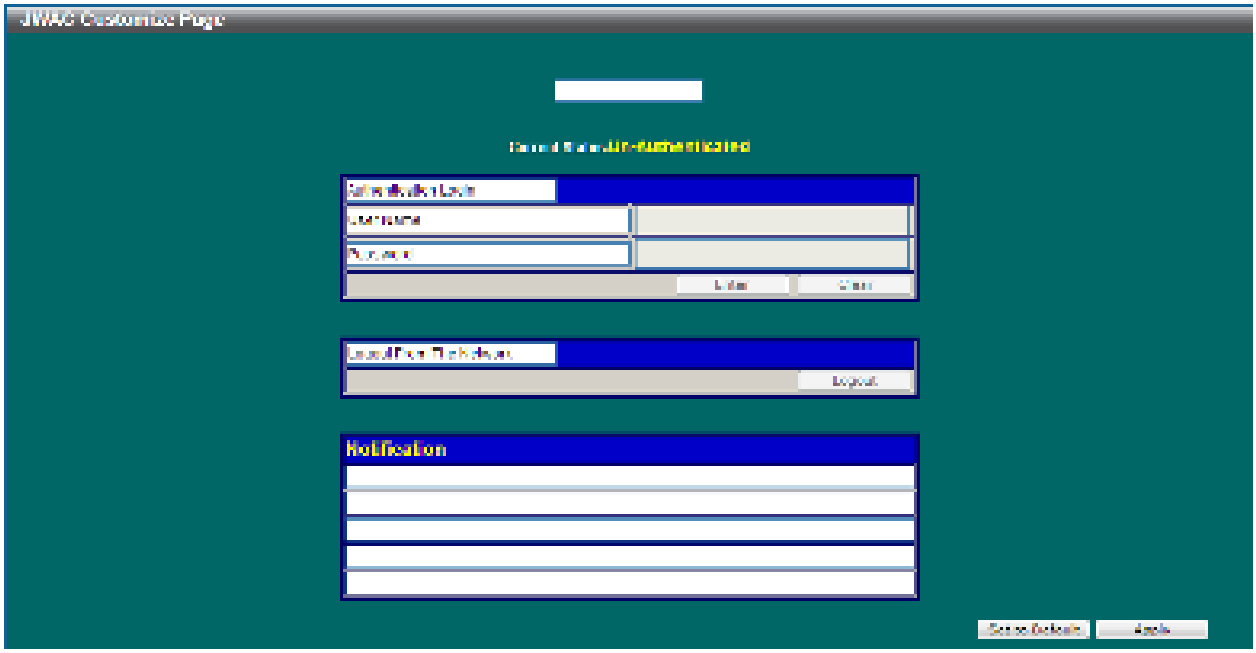


Figure 9-73 JWAC Customize Page (English) Window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There a 5 lines available for additional information.

Click the **Set to Default** button to replace the information with the default information.

Click the **Apply** button to accept the changes made.

After changing the language to **Japanese** the JWAC customize page will look like this.

Figure 9-74 JWAC Customize Page (Japanese) Window

Click the **Set to Default** button to replace the information with the default information.

Click the **Apply** button to accept the changes made.

Network Access Authentication

Guest VLAN

This window is used to view and configure the network access authentication guest VLAN settings.

To view the following window, click **Security > Network Access Authentication > Guest VLAN**, as shown below:

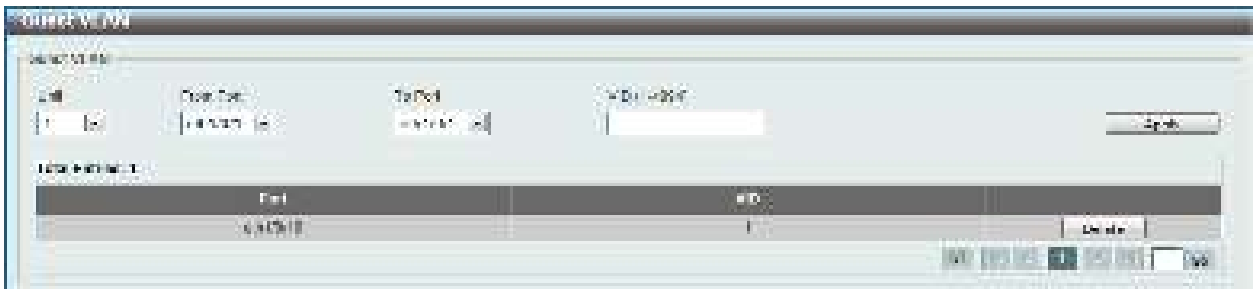


Figure 9-75 Guest VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Network Access Authentication Global Settings

This window is used to view and configure the network access authentication global settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:

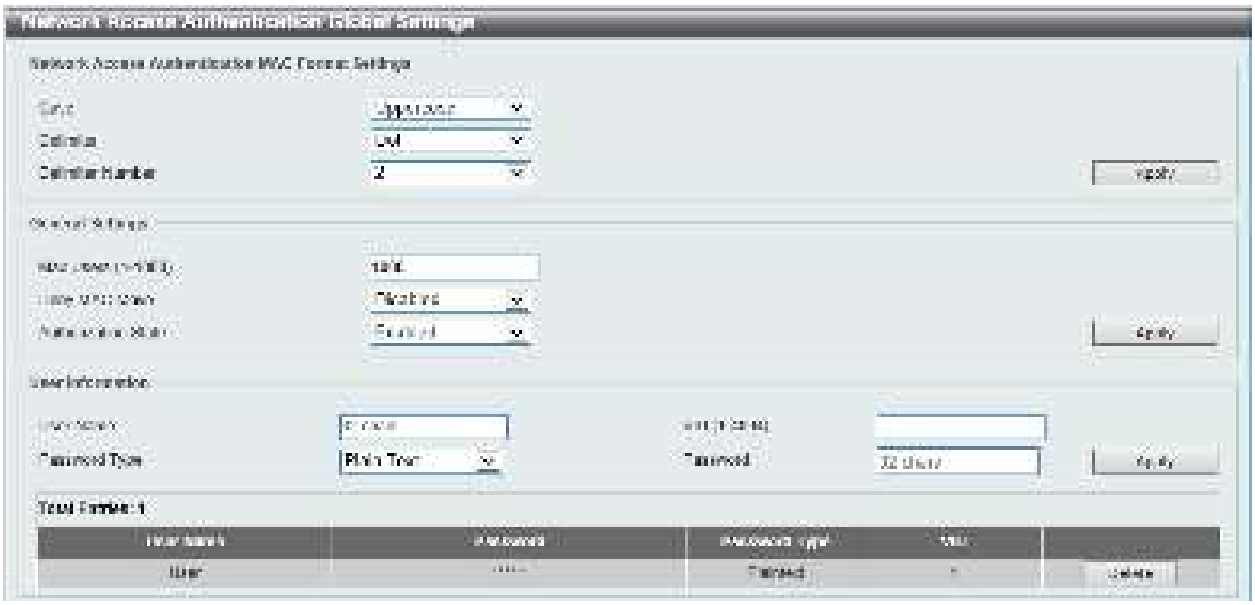


Figure 9-76 Network Access Authentication Global Settings Window

The fields that can be configured for **Network Access Authentication MAC Format Settings** are described below:

Parameter	Description
Case	Select the case format that will be used for the network access authentication MAC address here. Options to choose from are **Lowercase** and **Uppercase**.
Delimiter	Select the delimiter that will be used for the network access authentication MAC address here. Options to choose from are **Hyphen**, **Colon**, **Dot**, and **None**.
Delimiter Number	Select the delimiter number option here. Options to choose from are **1**, **2**, and **5**.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **General Settings** are described below:

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. This value must be between 1 and 1000. By default, this option is 1000.
Deny MAC-Move	Select to enable or disable the deny MAC-move feature here. This option controls whether to allow authenticated hosts to do roaming across different switch ports and only controls whether a host, which is authenticated at a port set to the multi-authenticate mode is allowed to move to another port.

Parameter	Description
	If a station is allowed to move, there are two situations. It may need to be re-authenticated or directly moved to the new port without re-authentication based on the following rule. If the new port has the same authentication configuration as the original port, then re-authentication is not needed. The host will inherit the same authorization attributes with new port. The authenticated host can do roaming from port 1 to port 2, and inherit the authorization attributes without re-authentication. If the new port has the different authentication configuration as the original port, then re-authentication is needed. The authenticated host on port 1 can move and re-authenticated by port 2. If the new port has no authentication method enabled, then the station is directly moved to the new port. The session with the original port is removed. The authenticated host on port 1 can be moved to port 2. If this feature is disabled and an authenticated host moves to another port, then this is treated as a violation error.
Authorization State	Select to enable or disable the authorized state here. The option is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example VLAN, 802.1p default priority, bandwidth, and ACL) assigned by the RADIUS server will be accepted if the authorization status is enabled. Bandwidth and ACL are assigned on a per-port basis. If in the multi-authenticated mode, VLAN and 802.1p are assigned on a per-host basis. Otherwise, Bandwidth and ACL are assigned on a per-port basis.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **User Information** are described below:

Parameter	Description
User Name	Enter the user name used here. This name can be up to 32 characters long.
VID	Enter the VLAN ID used here.
Password Type	Select the password type option here. Options to choose from are **Plain Text** and **Encrypted**.
Password	Enter the password used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Network Access Authentication Port Settings

This window is used to view and configure the network access authentication port settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Port Settings**, as shown below:

Figure 9-77 Network Access Authentication Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are **Multi Host** and **Multi Auth**. If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. If the port is operated in the multi-authenticated mode, then each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.
VID List	After selecting the **Multi Auth** option as the **Host Mode**, the following parameter is available. Enter the VLAN ID used here. This is useful when different VLANs on the Switch have different authentication requirements. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. This option is useful for trunk ports to do per-VLAN authentication control. When a port's authentication mode is changed to multi-host, the previous authentication VLAN(s) on this port will be cleared.
CompAuth Mode	Select the compound authentication mode option here. Options to choose from are:

Parameter	Description
	• **Any** - Specifies that if any of the authentication method (802.1X, MAC-based Access Control, WAC, or JWAC) to passes, then passes. • **MAC-JWAC** - Specifies to verify MAC-based authentication first. If the client passes, JWAC will be verified next. Both authentication methods need to be passed. • **MAC-WAC** - Specifies to verify MAC-based authentication first. If the client passes, WAC will be verified next. Both authentication methods need to be passed.
Max Users	Enter the maximum users value used here. This value must be between 1 and 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol.
ReAuth Timer	Enter the re-authentication timer value here. This value must be between 1 and 65535 seconds. By default, this value is 3600 seconds.
Inactivity State	Select to enable or disable the inactivity state here.
Inactivity Timer	When the **Inactivity State** is enabled, enter the inactivity timer value here. This value must be between 120 and 65535 seconds. This parameter only affects the WAC and JWAC authentication protocols.
Restart	Enter the restart time value used here. This value must be between 1 and 65535 seconds.

Click the **Apply** button to accept the changes made.

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:

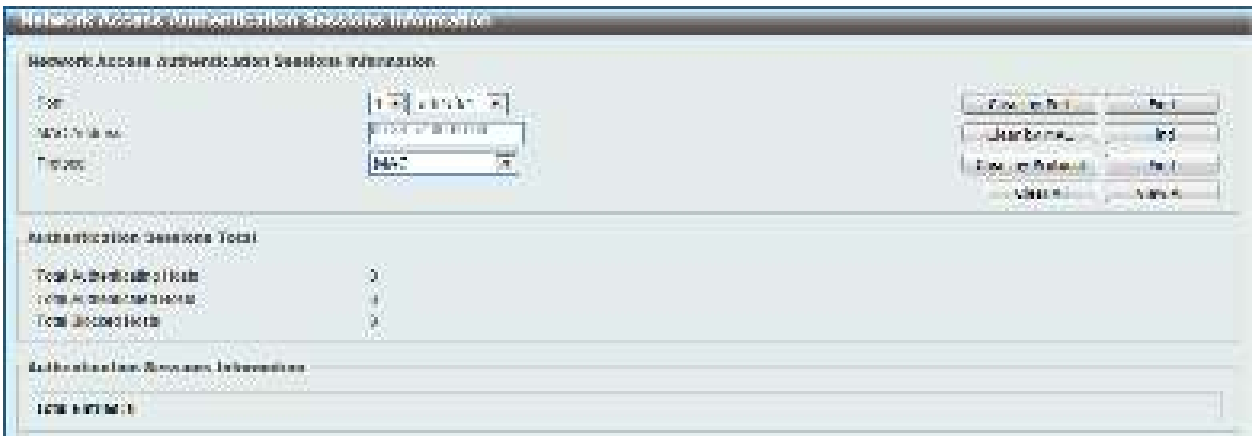


Figure 9-78 Network Access Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate switch unit and port used for the query here.
MAC Address	Enter the MAC address used here.

Parameter	Description
Protocol	Select the protocol option used here. Options to choose from are **MAC**, **WAC**, **JWAC**, and **DOT1X**.

Click the **Apply** button to accept the changes made.

Click the **Clear by Port** button to the clear the information based on the port selected.

Click the **Clear by MAC** button to the clear the information based on the MAC address entered.

Click the **Clear by Protocol** button to the clear the information based on the protocol selected.

Click the **Clear All** button to clear all the information in this table.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to locate and display all the entries.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Packets that are destined to the CPU can be classified into three groups. These groups, otherwise known as sub-interfaces, are logical interfaces that the CPU will use to identify certain types of traffic. The three groups are **Protocol**, **Manage**, and **Route**. Generally, the **Protocol** group should receive the highest priority when the Switch's CPU processes received packets and the **Route** group should receive the lowest priority as the Switch's CPU usually does get involved in the processing of routing packets. In the **Protocol** group, packets are protocol control packets identified by the router. In the **Manage** group, packets are destined to any router or system network management interface by means of interactive access protocols, like Telnet and SSH. In the **Route** group, packets are identified as traversing routing packets that is generally processed by the router CPU.

In the following table a list of supported protocols are displayed with their respective sub-interfaces (groups):

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol (ARP)
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
GVRP	Protocol	GARP VLAN Registration Protocol
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol

Protocol Name	Sub-interface (Group)	Description
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's sub-interfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.

NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to view and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:

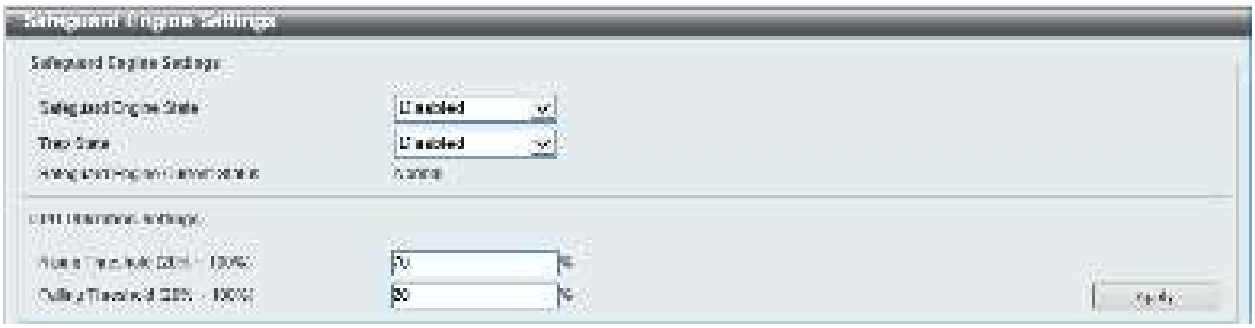


Figure 9-79 Safeguard Engine Settings Window

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.
Trap State	Select to enable or disable the safeguard engine trap state here.

The fields that can be configured for **CPU Utilization Settings** are described below:

Parameter	Description
Rising Threshold	Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level,

Parameter	Description
	the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

Click the **Apply** button to accept the changes made.

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:

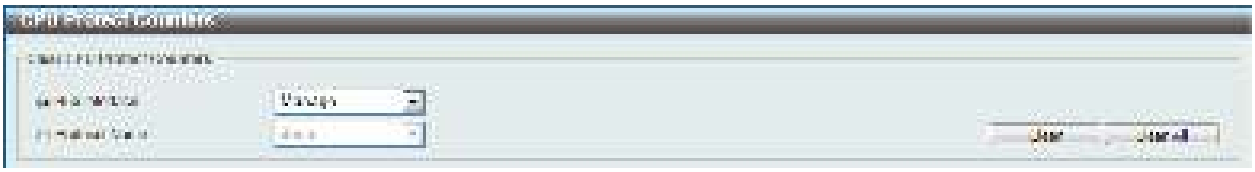


Figure 9-80 CPU Protect Counters Window

The fields that can be configured are described below:

Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, **Route**, and **All**. This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here. Options to choose from are DHCP, ARP, DNS, GVRP, ICMPv4, ICMPv6-Neighbor, ICMPv6-Other, IGMP, LACP, SNMP, SSH, STP, Telnet, TFTP, Web, 802.1X, and All.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

CPU Protect Sub-Interface

This window is used to view and configure the CPU protection sub-interface settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Sub-Interface**, as shown below:

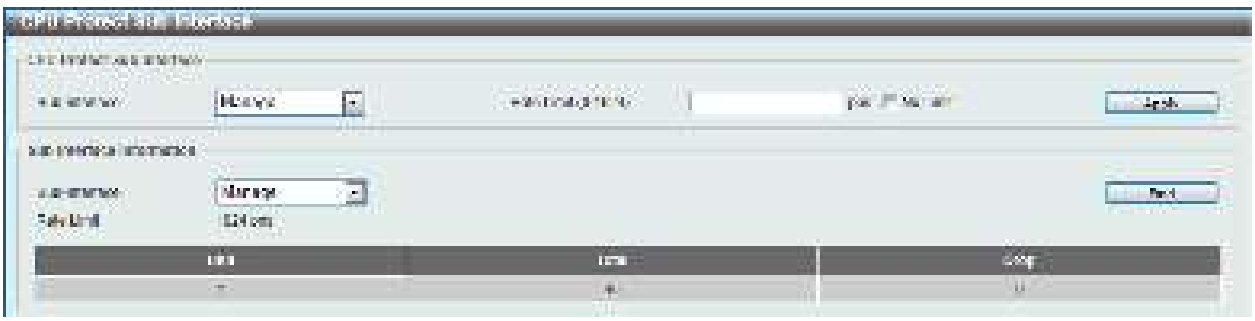


Figure 9-81 CPU Protect Sub-Interface Window

The fields that can be configured for **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Sub-Interface Information** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.

Click the **Find** button to locate a specific entry based on the information entered.

CPU Protect Type

This window is used to view and configure the CPU protection type settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Type**, as shown below:

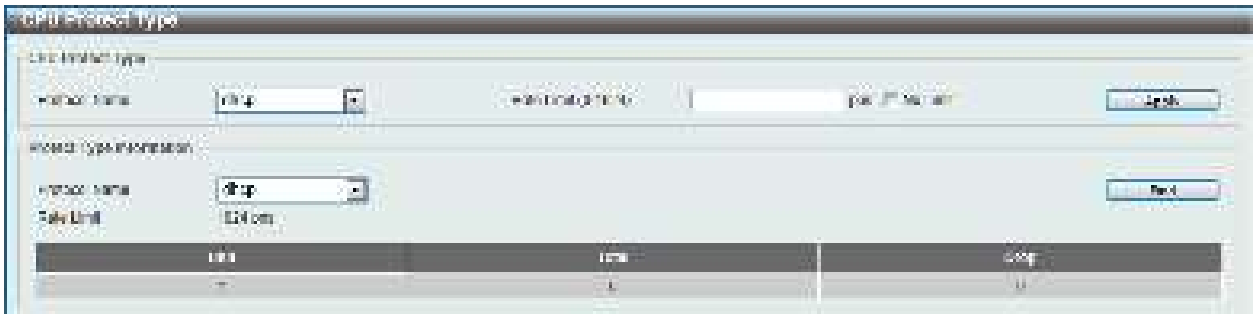


Figure 9-82 CPU Protect Type Window

The fields that can be configured for **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here. Options to choose from are DHCP, ARP, DNS, GVRP, ICMPv4, ICMPv6-Neighbor, ICMPv6-Other, IGMP, LACP, SNMP, SSH, STP, Telnet, TFTP, Web, and 802.1X.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Protect Type Information** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here. Options to choose from are DHCP, ARP, DNS, GVRP, ICMPv4, ICMPv6-Neighbor, ICMPv6-

Parameter	Description
	Other, IGMP, LACP, SNMP, SSH, STP, Telnet, TFTP, Web, and 802.1X.

Click the **Find** button to locate a specific entry based on the information entered.

Trusted Host

This window is used to view and configure the trusted host settings.

To view the following window, click **Security > Trusted Host**, as shown below:

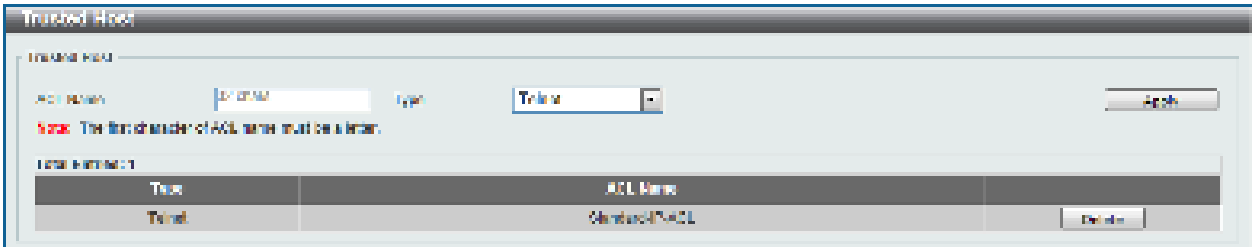


Figure 9-83 Trusted Host Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the ACL name used here. This name can be up to 32 characters long.
Type	Select the trusted host type here. Options to choose from are **Telnet**, **SSH**, **Ping**, **HTTP**, and **HTTPS**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Traffic Segmentation Settings

This window is used to 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:

Figure 9-84 Traffic Segmentation Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the receiving switch unit that will be used for this configuration here.
From Port / To Port	Select the receiving port range used for the configuration here.
Forward Unit	Select the forward switch unit that will be used for this configuration here.
From Forward Port / To Forward Port	Select the forward port range used for the configuration here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Storm Control Settings

This window is used to view and configure the storm control settings.

To view the following window, click **Security > Storm Control Settings**, as shown below:

Figure 9-85 Storm Control Settings Window

The fields that can be configured for **Storm Control Trap Settings** are described below:

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are: • **None** - No traps are sent. • **Storm Occur** - A trap notification is sent when a storm event is detected. • **Storm Clear** - A trap notification is sent when a storm event is cleared. • **Both** - A trap notification is sent when a storm event is detected or cleared.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Storm Control Polling Settings** are described below:

Parameter	Description
Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.
Retries	Enter the retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the **Infinite** option to disable this feature.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Storm Control Port Settings** are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **Unicast**. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Action	Select the action that will be taken here. Options to choose from are: • **None** - Specifies not to filter the storm packets. • **Shutdown** - Specifies to shut down the port when the value specified for rise threshold is reached. • **Drop** - Specifies to discard packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are **PPS**, **Kbps**, and **Level**.
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 0 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 0 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

Click the **Apply** button to accept the changes made.

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.

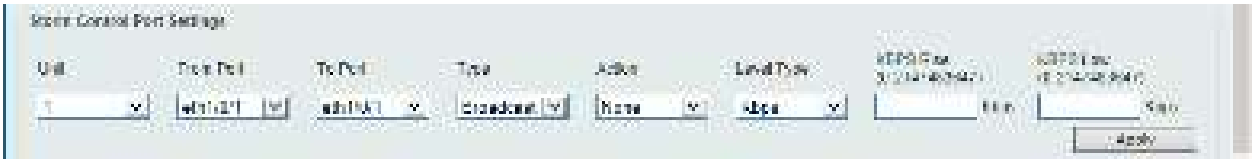


Figure 9-86 Storm Control (Kbps) Window

The fields that can be configured are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps.
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

Click the **Apply** button to accept the changes made.

After selecting the **Level** option as the **Level Type**, the following parameters are available.

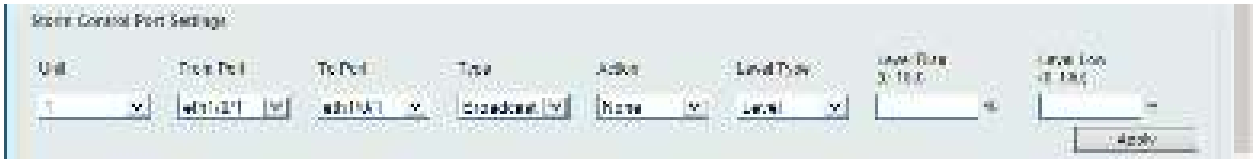


Figure 9-87 Storm Control (Level) Window

The fields that can be configured are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%.
Level Low	Enter the low-level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%. If the low level is not specified, the default value is 80% of the specified risen level.

Click the **Apply** button to accept the changes made.

DoS Attack Prevention Settings

This window is used to 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 of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size) which is 65535 bytes. The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

Figure 9-88 DoS Attack Prevention Settings Window

The fields that can be configured for **SNMP Server Enable Traps DoS Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DoS attack prevention trap state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured 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.

SSH

Secure Shell (SSH) is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.

- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

This window is used to view and configure the SSH global settings.

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

Figure 9-89 SSH Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IP SSH Server State	Select to enable or disable the SSH server's global state.
IP SSH Service Port	Enter the SSH service port number used here. This value must be between 1 and 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

Click the **Apply** button to accept the changes made.

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:

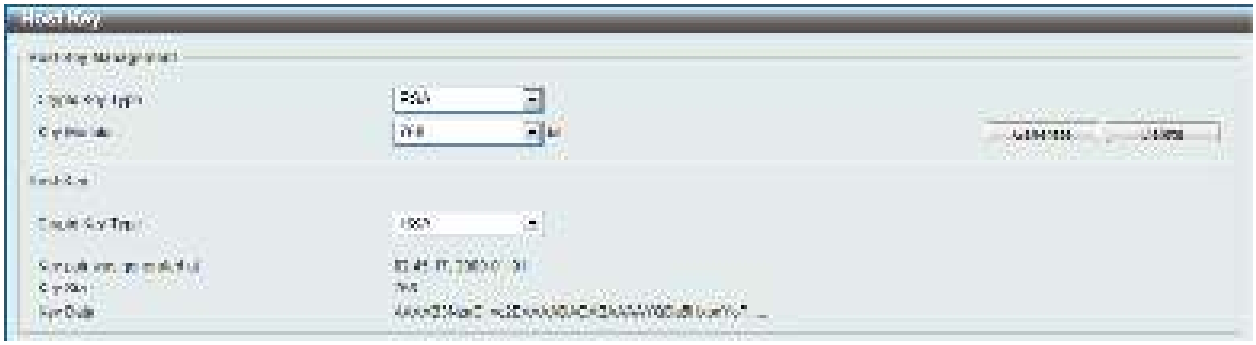


Figure 9-90 Host Key Window

The fields that can be configured for **Host Key Management** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.
Key Modulus	Select the key modulus value here. Options to choose from are **360**, **512**, **768**, **1024**, and **2048** bit.

Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured for **Host Key** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.

SSH Server Connection

This window is used to view the SSH server connections table.

To view the following window, click **Security > SSH > SSH Server Connection**, as shown below:

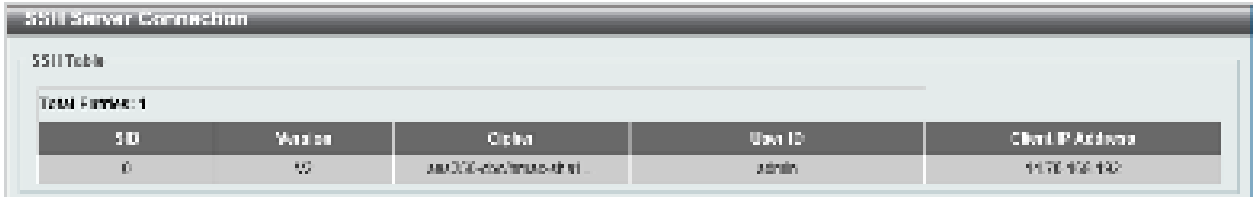


Figure 9-91 SSH Server Connection Window

SSH User Settings

This window is used to view and configure the SSH user settings.

To view the following window, click **Security > SSH > SSH User Settings**, as shown below:

Figure 9-92 SSH User Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the SSH user's username used here. This name can be up to 32 characters long.
Authentication Method	Select the authentication methods used here. Options to choose from are **Password**, **Public Key**, and **Host-based**.
Key File	After selecting the **Public Key** or **Host-based** option as the **Authentication Method**, enter the public key here.
Host Name	After selecting the **Host-based** option as the **Authentication Method**, enter the host name here.
IPv4 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv4 address here.
IPv6 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv6 address here.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a server and client through the use of authentication, digital signatures, and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms, and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and server as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

- **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys, and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
- **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) to create the encrypted text.

- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function, which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA256.

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the client. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server or the Switch file system. The Switch supports TLS 1.0, TLS 1.1, and TLS 1.2. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to server.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web-based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https:// (Ex. https://xx.xx.xx.xx). Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

This window is used to view and configure the SSL feature's global settings.

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:

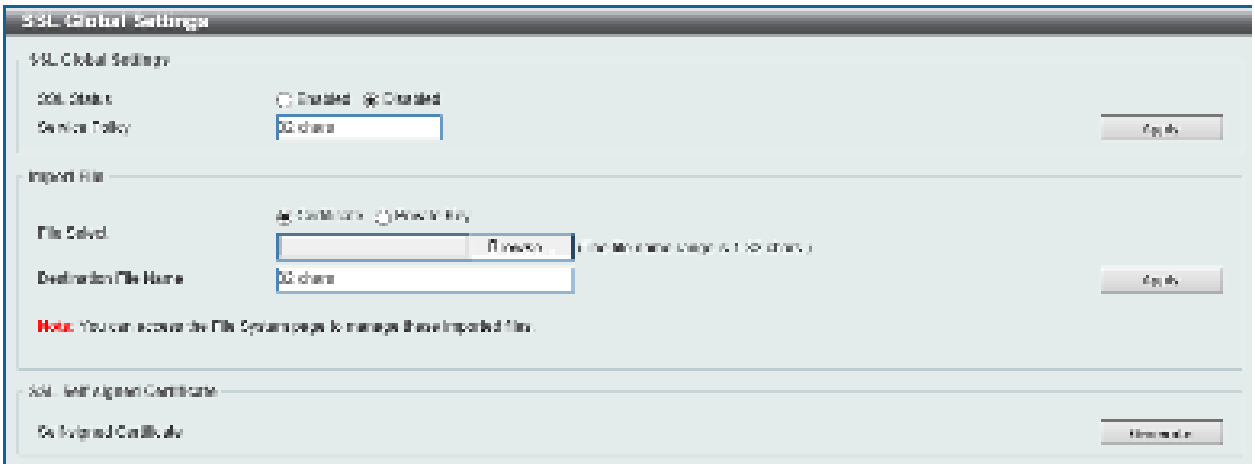


Figure 9-93 SSL Global Settings Window

The fields that can be configured for **SSL Global Settings** are described below:

Parameter	Description
SSL Status	Select to enable or disable the SSL feature's global status here.

Parameter	Description
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Import File** are described below:

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are **Certificate** and **Private Key**. After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the **Browse** button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Generate** button in the **SSL-Self-signed Certificate** section to generate a new self-signed certificate, regardless if there is a built-in self-signed certificate or not. The certificate generated does not affect the user-downloaded certificates.

NOTE: The SSL self-signed certificate only supports self-signature RSA certificates with a key length of 2048 bits.

Crypto PKI Trustpoint

This window is used to view and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:

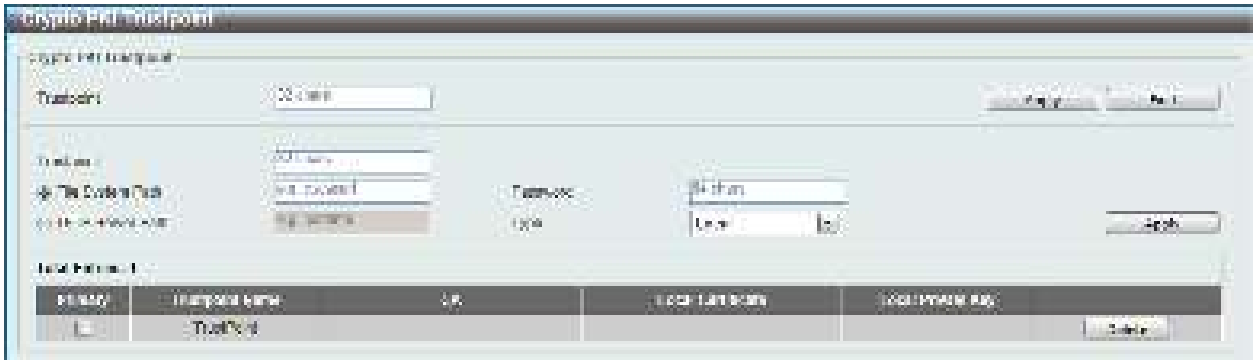


Figure 9-94 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password

Parameter	Description
	phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server's path here.
Type	Select the type of certificate that will be imported here. Options to choose from are: • **Both** - Specifies to import the CA certificate, local certificate, and key pairs. • **CA** - Specifies to import the CA certificate only. • **Local** - Specifies to import local certificate and key pairs only.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SSL Service Policy

This window is used to view and configure the SSL service policy settings.

To view the following window, click **Security > SSL > SSL Service Policy**, as shown below:

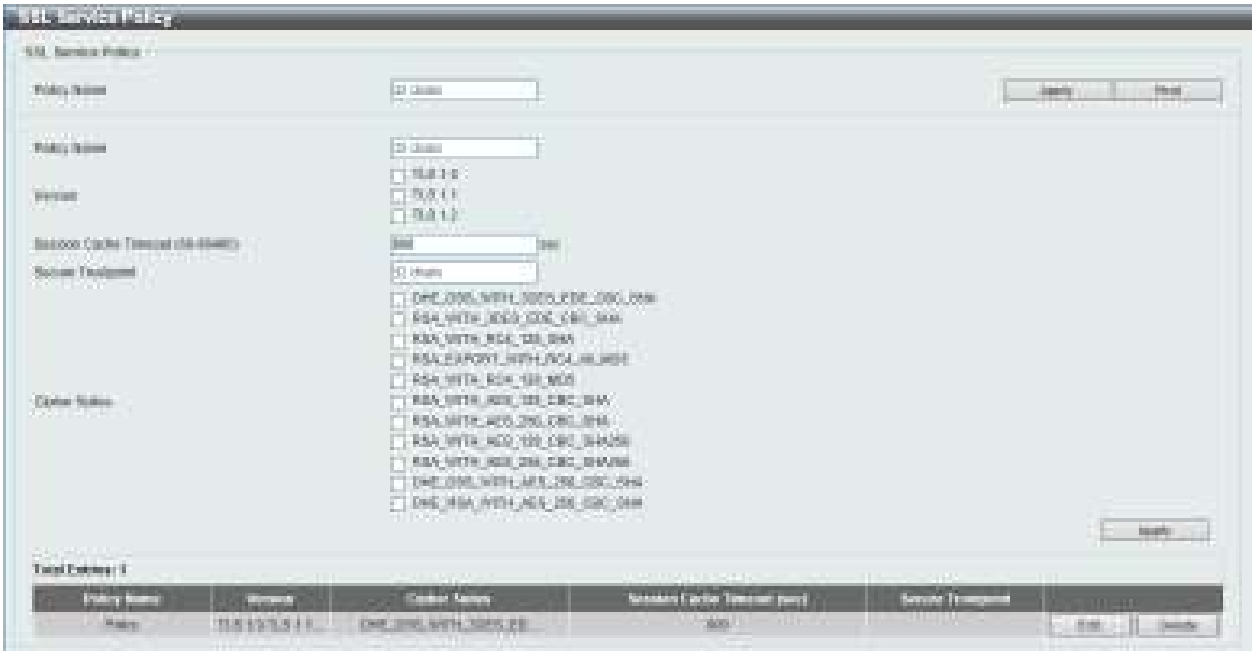


Figure 9-95 SSL Service Policy Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the service policy name here. This name can be up to 32 characters long.
Version	Select the TLS version that will be used here. Options to choose from are **TLS 1.0**, **TLS 1.1**, and **TLS1.2**.
Session Cache Timeout	Enter the session cache timeout value used here. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.

Parameter	Description
Secure Trustpoint	Enter the secure trust point's name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

Network Protocol Port Protection Settings

This window is used to display and configure the network protocol port protection settings.

To view the following window, click **Security > Network Protocol Port Protection Settings**, as shown below:

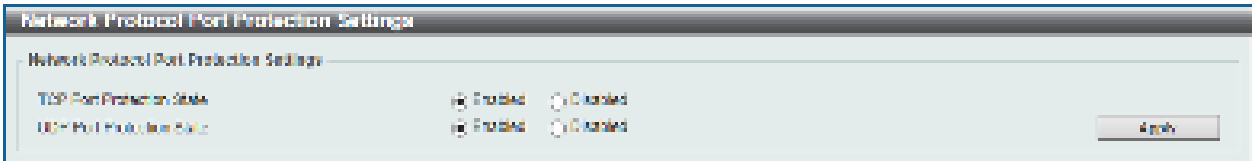


Figure 9-96 Network Protocol Port Protect Settings Window

The fields that can be configured are described below:

Parameter	Description
TCP Port Protect State	Select to enable or disable the TCP port network protocol protection function here.
UDP Port Protect State	Select to enable or disable the UDP port network protocol protection function here.

Click the **Apply** button to accept the changes made.

10. OAM

Cable Diagnostics
DDM

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

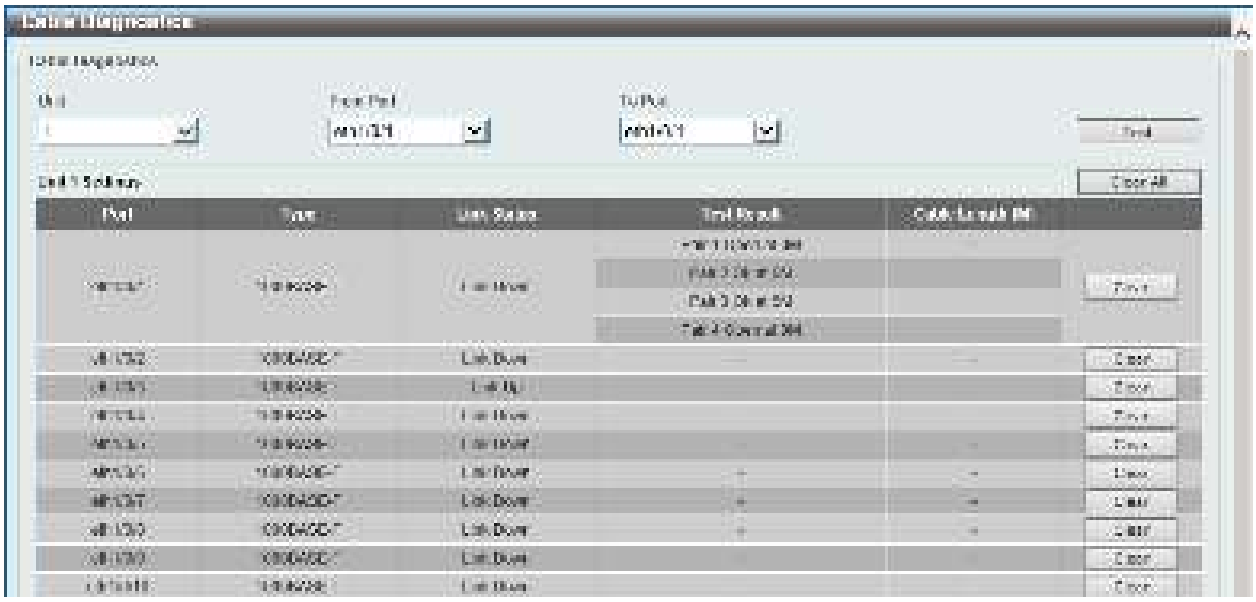


Figure 10-1 Cable Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Test** button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP modules inserting to the Switch and to configure alarm settings, warning settings, temperature

threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:

Figure 10-2 DDM Settings Window

The fields that can be configured are described below:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select this option to enable or disable sending alarm level trap.
Transceiver Monitoring Traps Warning	Select this option to enable or disable sending warning level trap.
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the Alarm or Warning threshold. • **Alarm** - Shutdown the port when the configured alarm threshold range is exceeded. • **Warning** - Shutdown the port when the configured warning threshold range is exceeded. • **None** - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

Click the **Apply** button to accept the changes made for each individual section.

DDM Temperature Threshold Settings

This window is used to configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:

Figure 10-3 DDM Temperature Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of temperature threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between -128 and 127.996 °C.

Click the **Apply** button to accept the changes made.

DDM Voltage Threshold Settings

This window is used to configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Voltage Threshold Settings**, as shown below:

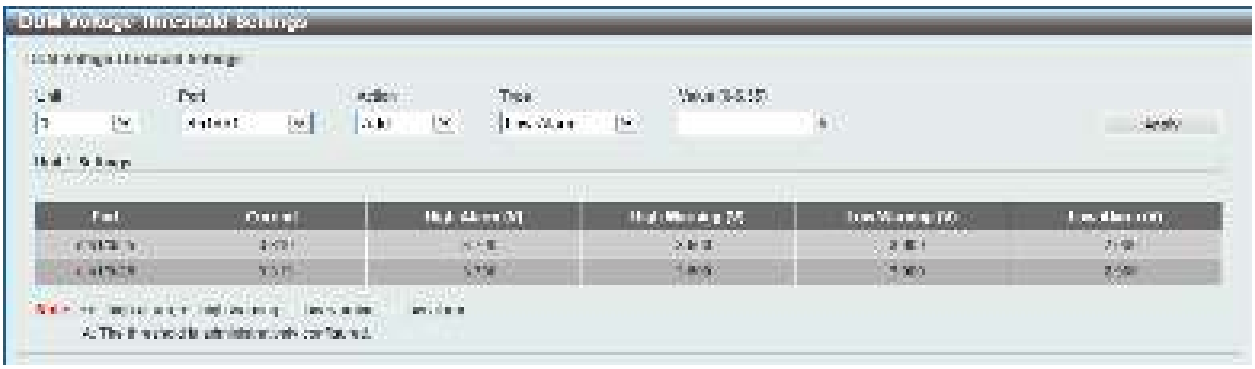


Figure 10-4 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of voltage threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between 0 and 6.55 Volt.

Click the **Apply** button to accept the changes made.

DDM Bias Current Threshold Settings

This window is used to configure the threshold of the bias current for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Bias Current Threshold Settings**, as shown below:

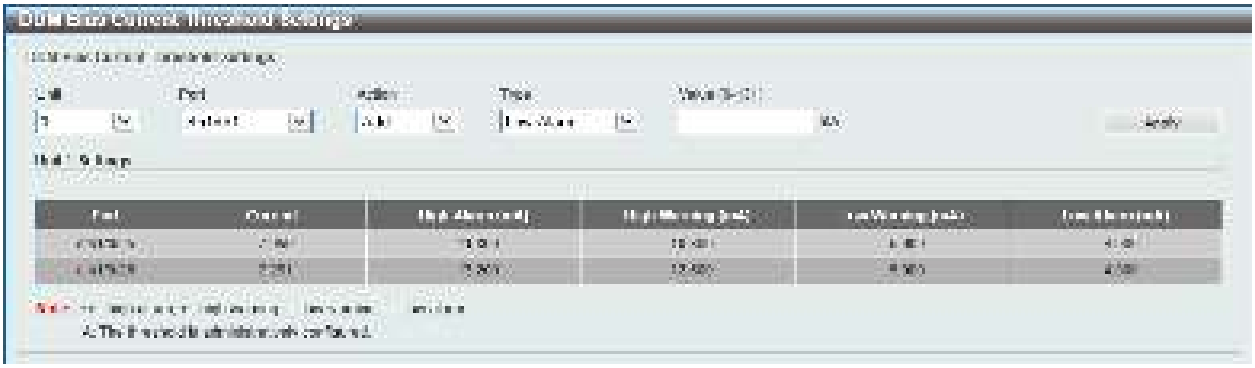


Figure 10-5 DDM Bias Current Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of bias current threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between 0 and 131 mA.

Click the **Apply** button to accept the changes made.

DDM TX Power Threshold Settings

This window is used to configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:

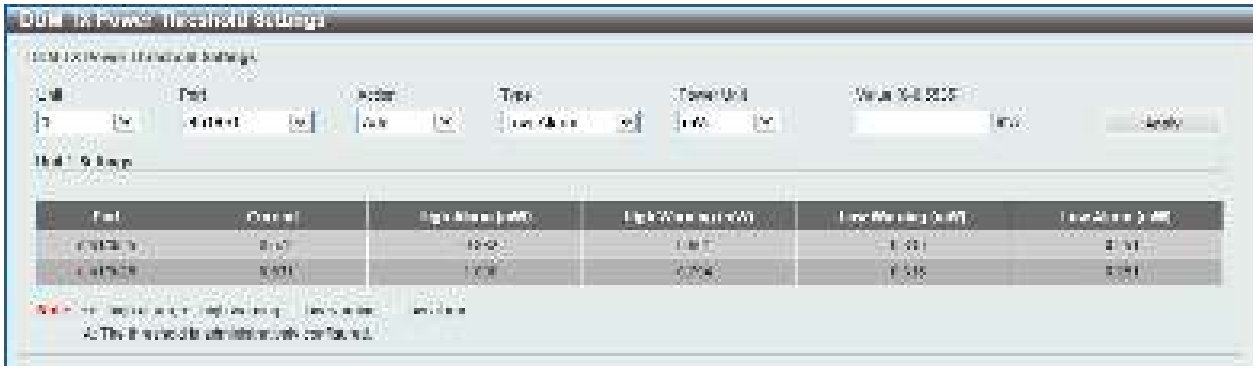


Figure 10-6 DDM TX Power Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of TX power threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value. When selecting **mW** in the **Power Unit** drop-down list, this value must be between 0 and 6.5535. When selecting **dBm** in the **Power Unit** drop-down list, this value must be between -40 and 8.1647.

Click the **Apply** button to accept the changes made.

DDM RX Power Threshold Settings

This window is used to configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:

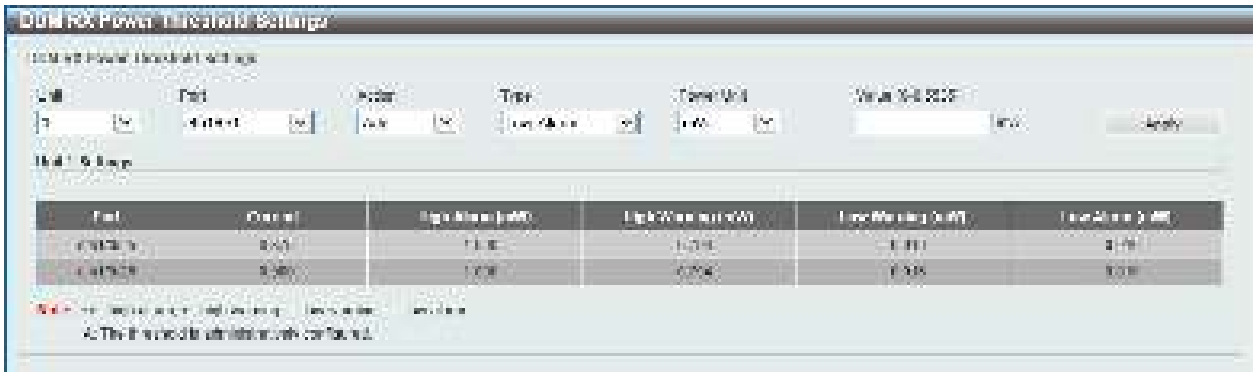


Figure 10-7 DDM RX Power Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of RX power threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value. When selecting **mW** in the **Power Unit** drop-down list, this value must be between 0 and 6.5535. When selecting **dBm** in the **Power Unit** drop-down list, this value must be between -40 and 8.1647.

Click the **Apply** button to accept the changes made.

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:

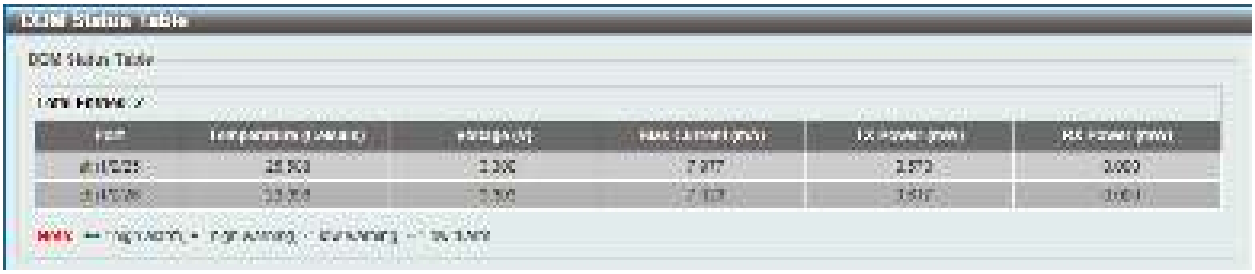


Figure 10-8 DDM Status Table Window

11. Monitoring

Utilization
Statistics
Mirror Settings
sFlow
Device Environment

Utilization

Port Utilization

This window is used to display the percentage of the total available bandwidth being used on the port.

To view the following window, click **Monitoring > Utilization > Port Utilization**, as shown below:

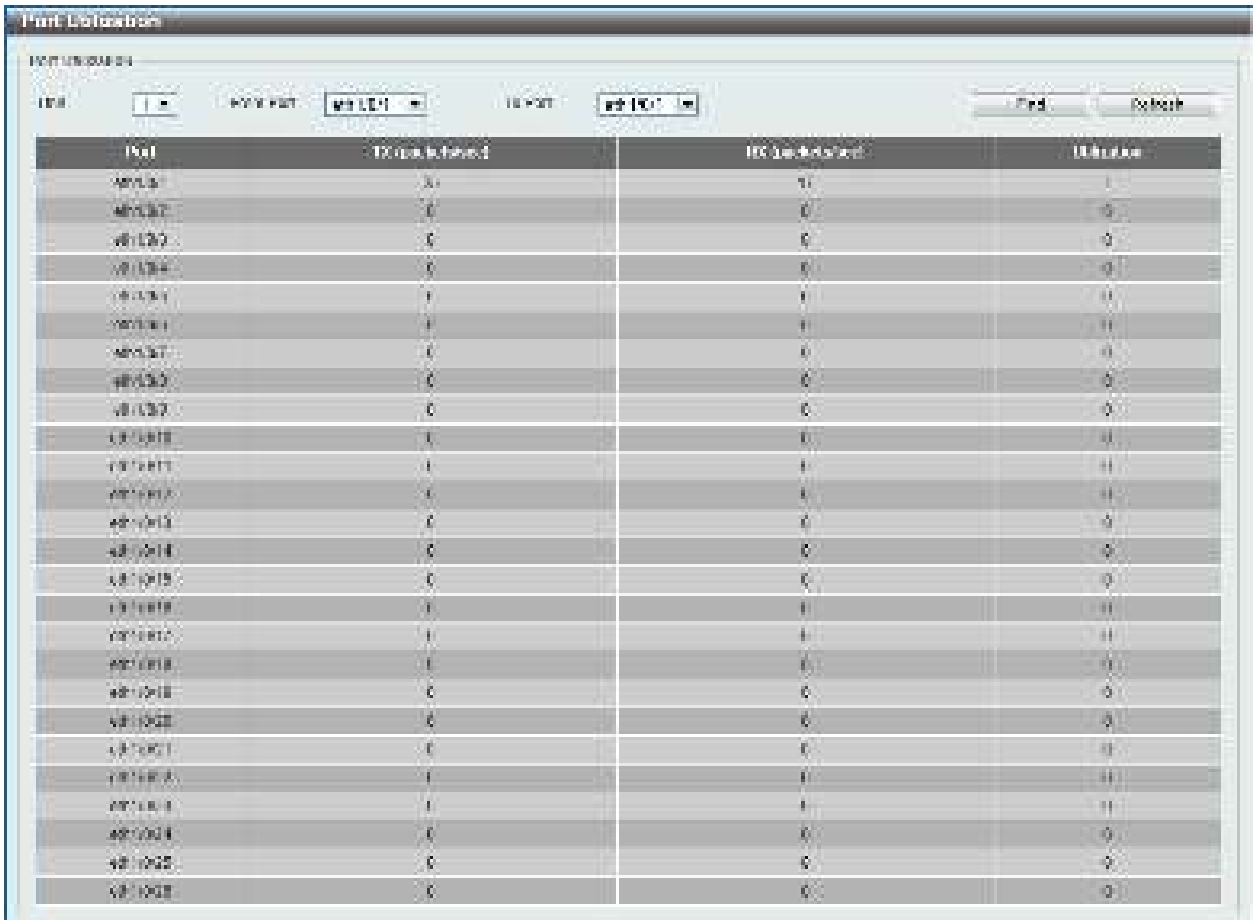


Figure 11-1 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Refresh** button to refresh the display table.

Statistics

Port

This window is used to display the packet statistics of ports.

To view the following window, click **Monitoring > Statistics > Port**, as shown below:

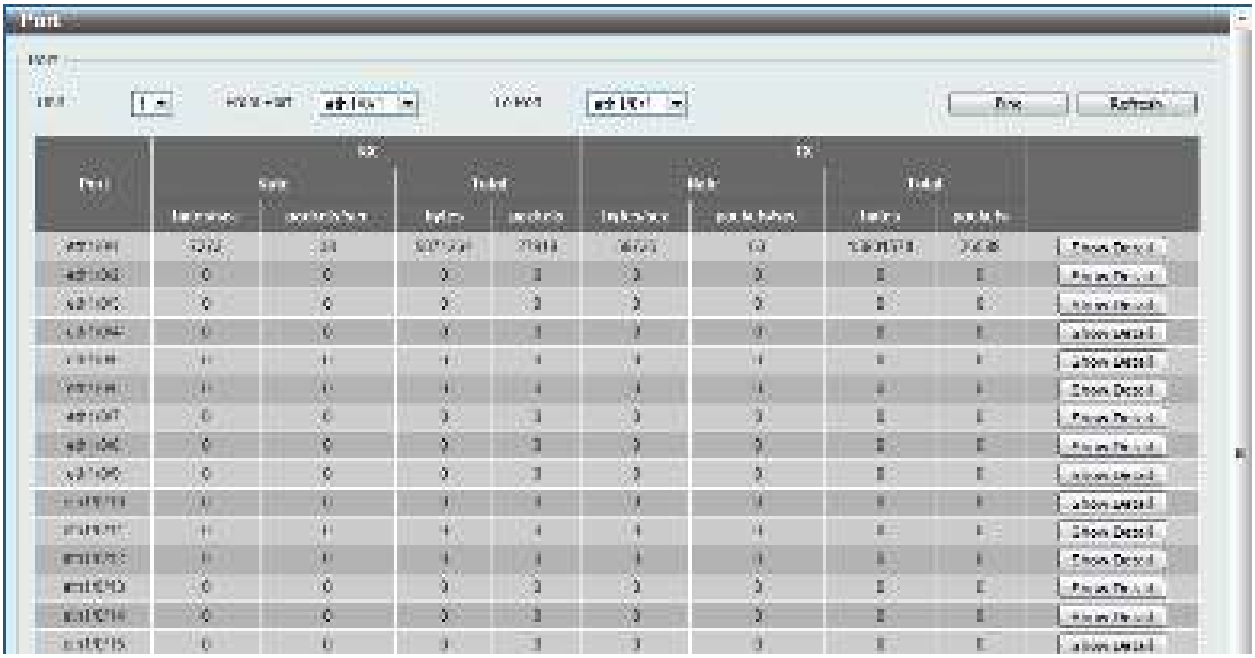


Figure 11-2 Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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 **Show Detail** button to see the detail information of the specific port.

After clicking the **Show Detail** button, the following page will appear.

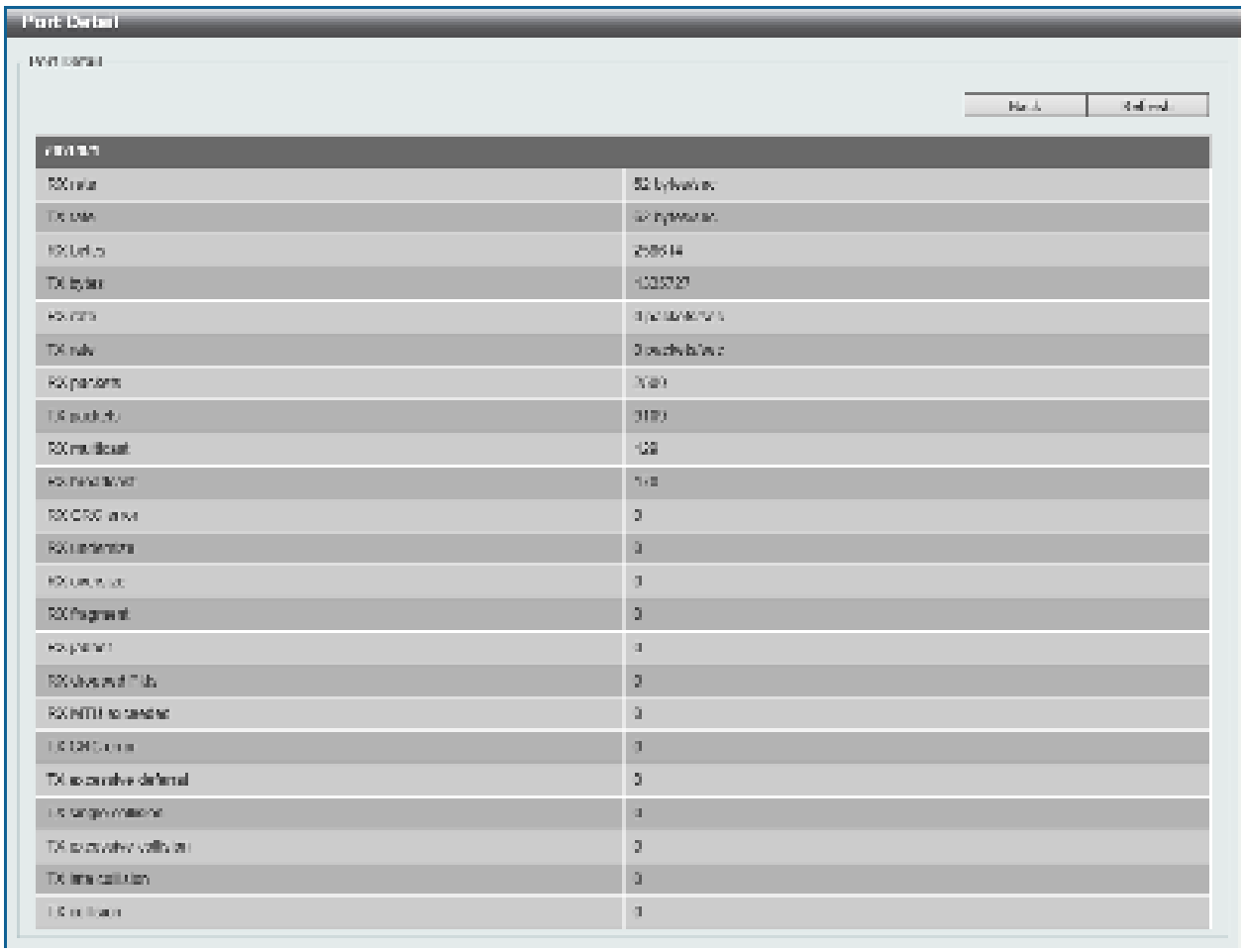


Figure 11-3 Port Detail Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the display table.

Port Counters

This window is used to display port counter statistics.

To view the following window, click **Monitoring > Statistics > Port Counters**, as shown below:

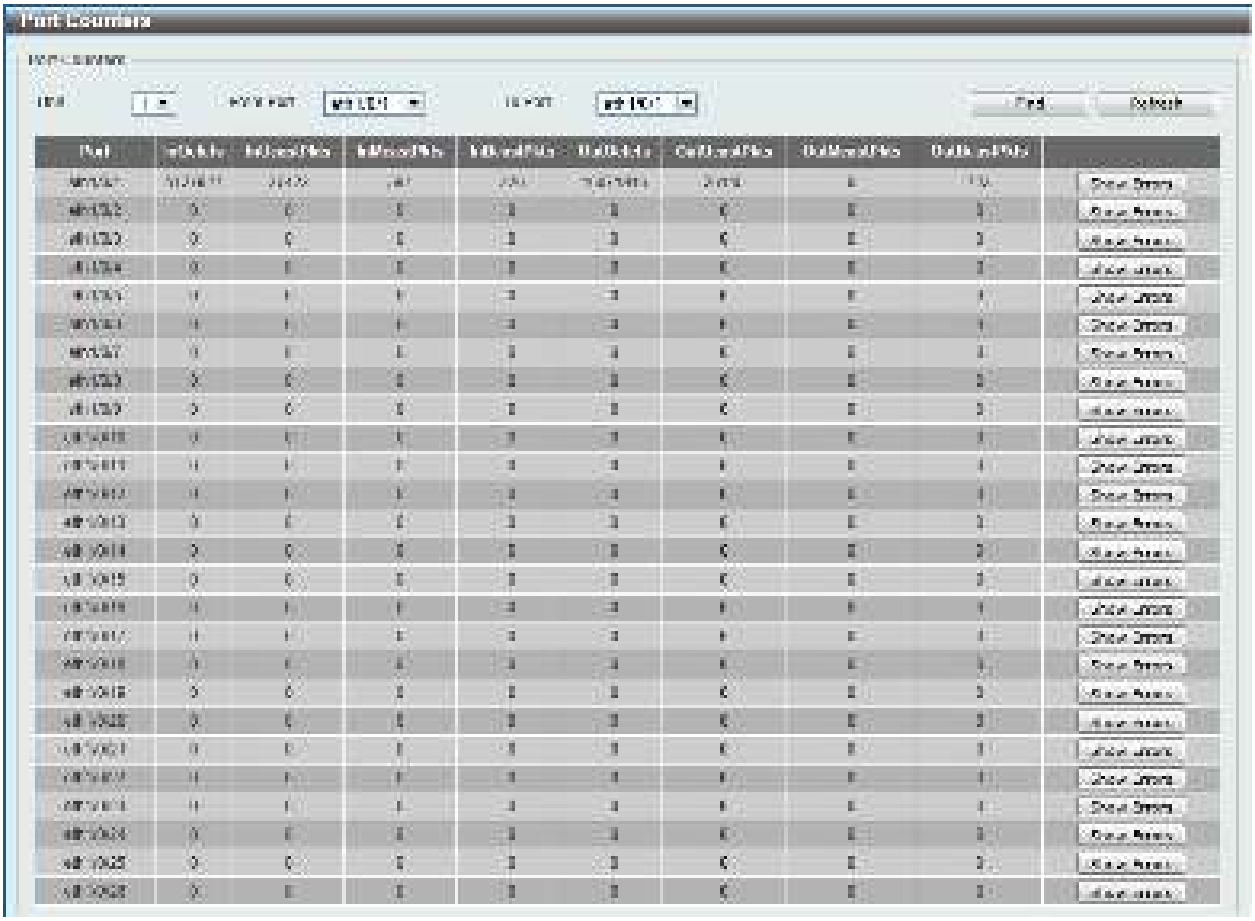


Figure 11-4 Port Counters Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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 **Show Errors** button to see all error counters of the specific port.

After clicking the **Show Errors** button, the following page will appear.

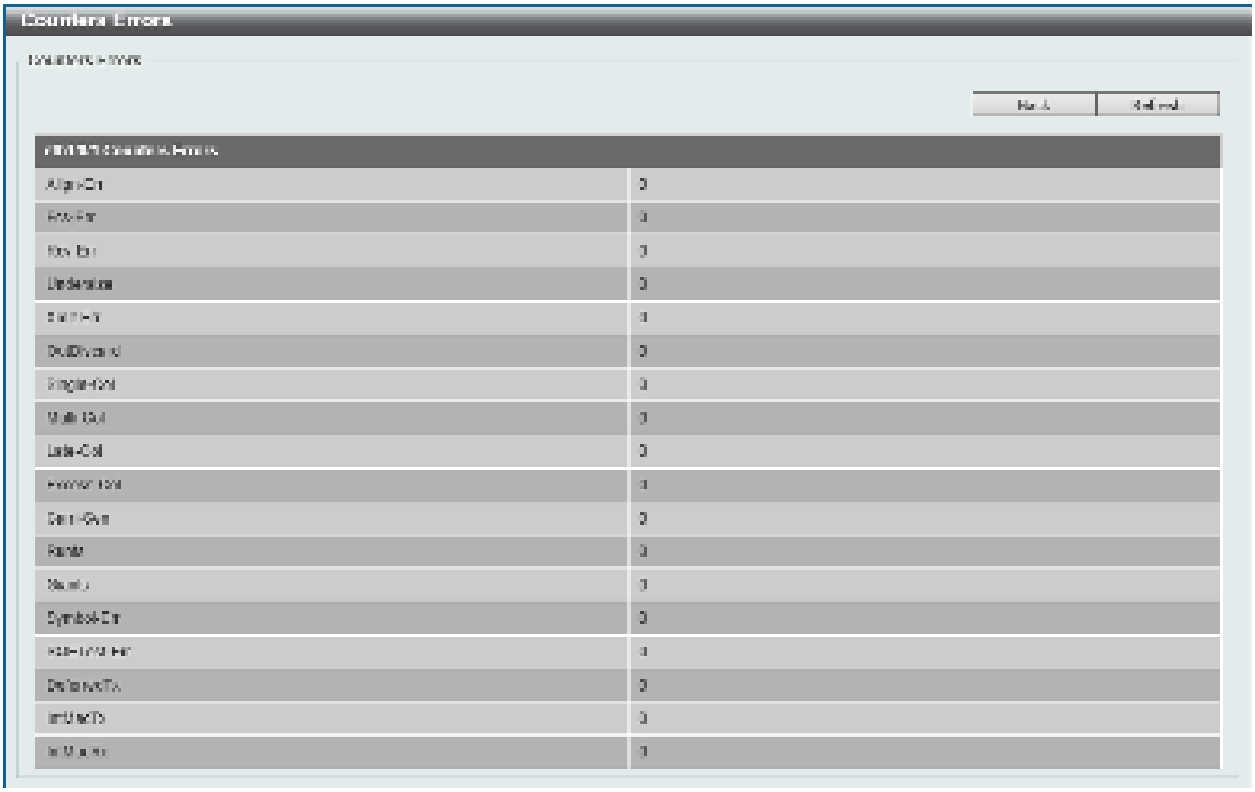


Figure 11-5 Counters Errors Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the display table.

Counters

This window is used to display all port counters, and clear the port counters of the specified or all ports.

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:

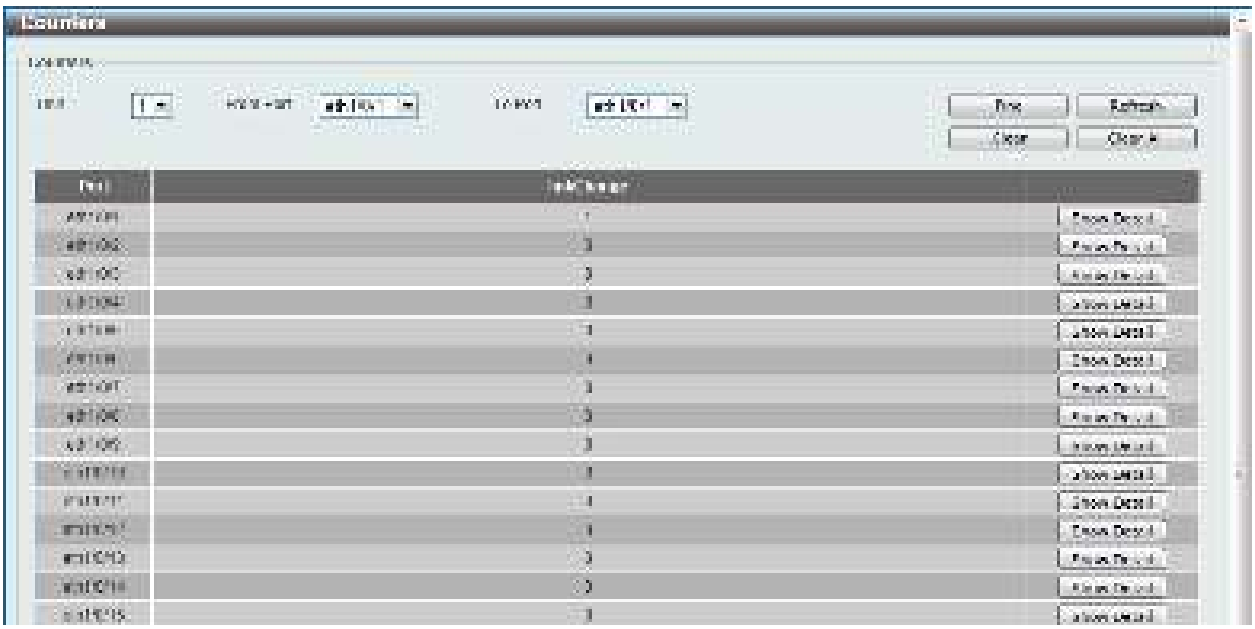


Figure 11-6 Counters Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.

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 the information for the specific ports.

Click the **Clear All** button to clear all the information in this table.

Click the **Show Detail** button to see the detail information of the specific port.

After clicking the **Show Detail** button, the following page will appear.

Figure 11-7 Port Counters Detail Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the display table.

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:

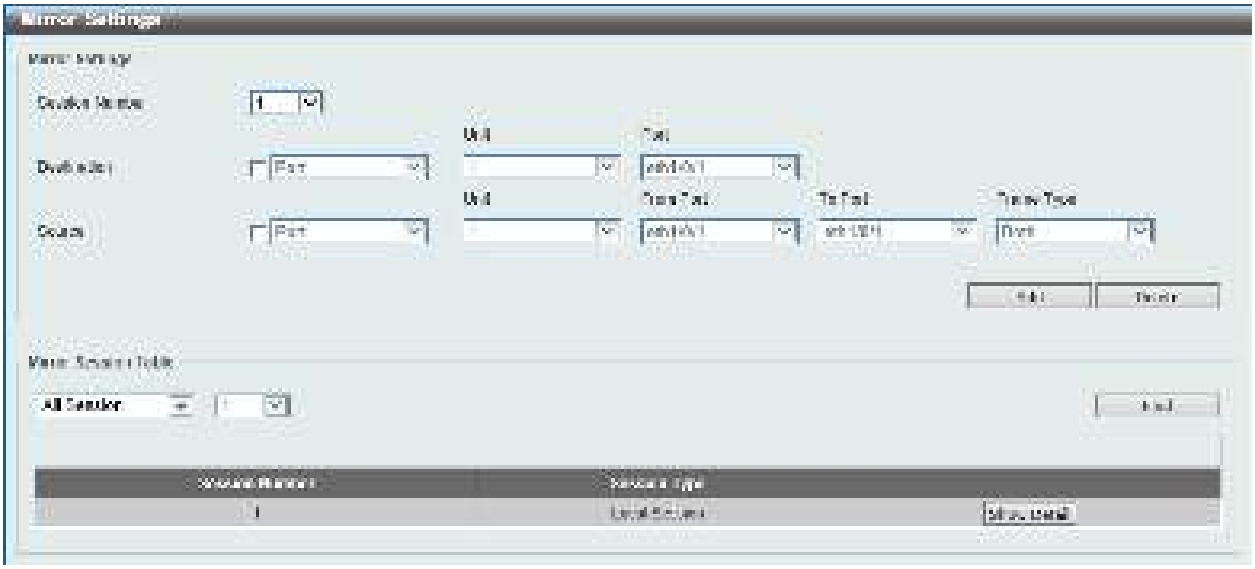


Figure 11-8 Mirror Settings Window

The fields that can be configured for **Mirror Settings** are described below:

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	Tick the checkbox, next to the **Destination** option, to configure the destination for this port mirror entry. In the first drop-down menu, select the **Port** option. In the second drop-down menu, select the destination switch's Unit ID. In the third drop-down menu, select the destination switch's port number.
Source	Tick the checkbox, next to the **Source** option, to configure the source for this port mirror entry. In the first drop-down menu, we can select the source type. Options to choose from are: • **Port** - In the first drop-down menu, select the source switch's Unit ID. 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 fifth drop-down menu. Options to choose from as the **Frame Type** are **Both**, **RX**, **TX**, and **TX Forwarding**. 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. When selecting **TX Forwarding**, traffic in the outgoing direction will be mirrored only when the port(s) is/are in the STG forwarding state. • **ACL** - Enter the ACL profile name in the space provided.

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

The fields that can be configured for **Mirror Session Table** are described below:

Parameter	Description
Mirror Session Type	Select the mirror session type of information that will be displayed from the drop-down menu. Options to choose from are **All Session**, and **Session Number**. After selecting the **Session Number** option, select the session number from the second drop-down menu. This number is from 1 to 4.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to see the detail information of the specific session.

After clicking the **Show Detail** button, the following window will appear.

Figure 11-9 Mirror Session Detail Window

Click the **Back** button to return to the previous window.

sFlow

sFlow (RFC3176) is a technology for monitoring traffic in data networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The architecture and sampling techniques used in the sFlow monitoring system were designed for providing continuous site-wide (and enterprise-wide) traffic monitoring of high speed switched and routed networks.

sFlow Agent Information

This window is used to view the sFlow agent information.

To view the following window, click **Monitoring > sFlow > sFlow Agent Information**, as shown below:

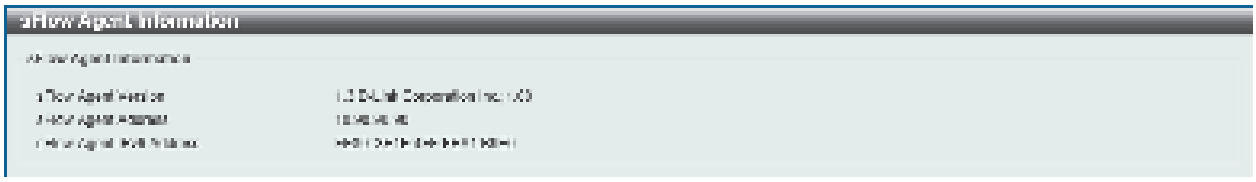


Figure 11-10 sFlow Agent Information Window

sFlow Receiver Settings

This window is used to view and configure receivers for the sFlow agents. Receivers cannot be added to or removed from the sFlow agent.

To view the following window, click **Monitoring > sFlow > sFlow Receiver Settings**, as shown below:

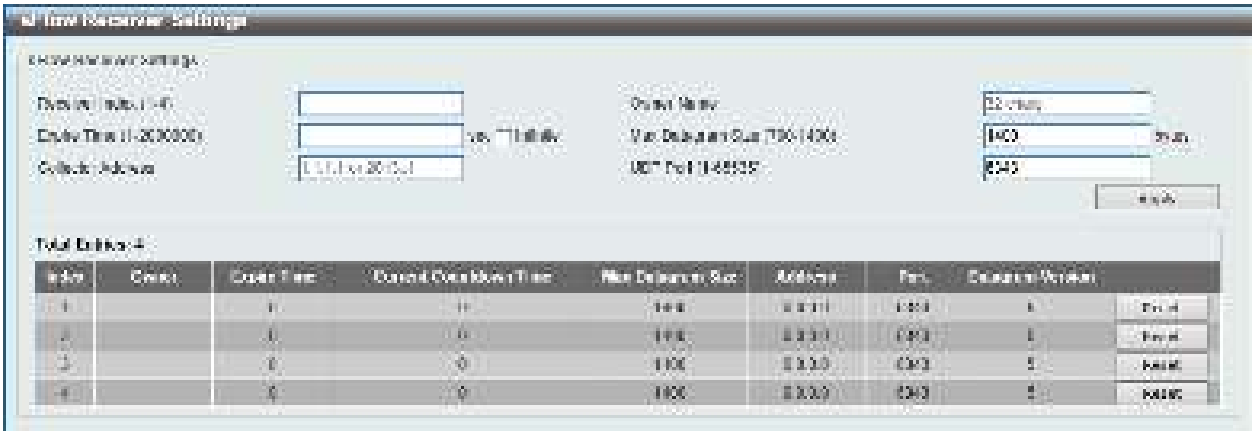


Figure 11-11 sFlow Receiver Settings Window

The fields that can be configured are described below:

Parameter	Description
Receiver Index	Enter the index number of the receiver here. This number must be between 1 and 4.
Owner Name	Enter the owner name of the receiver here. This name can be up to 32 characters long.
Expire Time	Enter the expiration time for the entry here. The parameters of the entry will reset when the timer expired. The range is from 1 to 2000000 seconds. Selecting **Infinite** specifies that the entry will not expire.
Max Datagram Size	Enter the maximum number of data bytes of a single sFlow datagram here. The range is from 700 to 1400 bytes. By default, this value is 1400 bytes.
Collector Address	Enter the remote sFlow collector's IPv4 or IPv6 address here.
UDP Port	Enter the remote sFlow collector's UDP port number here. This number must be between 1 and 65535. By default, this value is 6343.

Click the **Apply** button to accept the changes made.

Click the **Reset** button to reset the specified entry's settings to the default settings.

sFlow Sampler Settings

This window is used to view and configure sFlow Sampler settings.

To view the following window, click **Monitoring > sFlow > sFlow Sampler Settings**, as shown below:

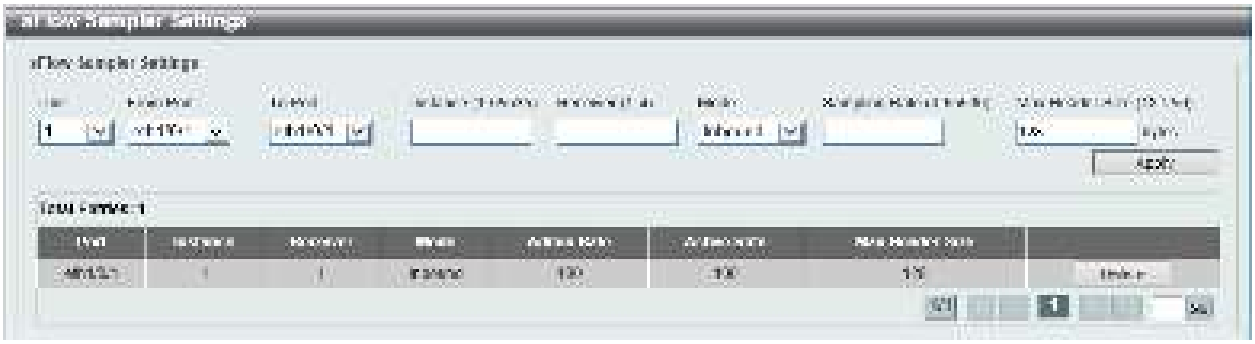


Figure 11-12 sFlow Sampler Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance's index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver's index for this sampler. If not specified, the value is 0. This value must be between 1 and 4.
Mode	Select the mode here. Options to choose from are: • **Inbound** - Specifies to sample ingress packets. This is the default direction of a sampler. • **Outbound** - Specifies to sample egress packets.
Sampling Rate	Enter the packet-sampling rate here. This value must be between 0 and 65536. Entering 0 will disable this function. If not specified, the default value is 0.
Max Header Size	Enter the maximum number of bytes that should be copied from sampled packets. This value must be between 18 and 256 bytes. By default, this value is 128 bytes.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

sFlow Poller Settings

This window is used to view and configure the sFlow Poller settings.

To view the following window, click **Monitoring > sFlow > sFlow Poller Settings**, as shown below:

Figure 11-13 sFlow Poller Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance's index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver's index value for this poller here. This value must be between 1 and 4.
Interval	Enter the maximum number of seconds between successive polling samples. This value must be between 0 and 120 seconds. Entering 0 will disable this feature. By default, this value is 0.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Device Environment

The device environment feature displays the Switch internal temperature status.

To view the following window, click **Monitoring > Device Environment**, as shown below:

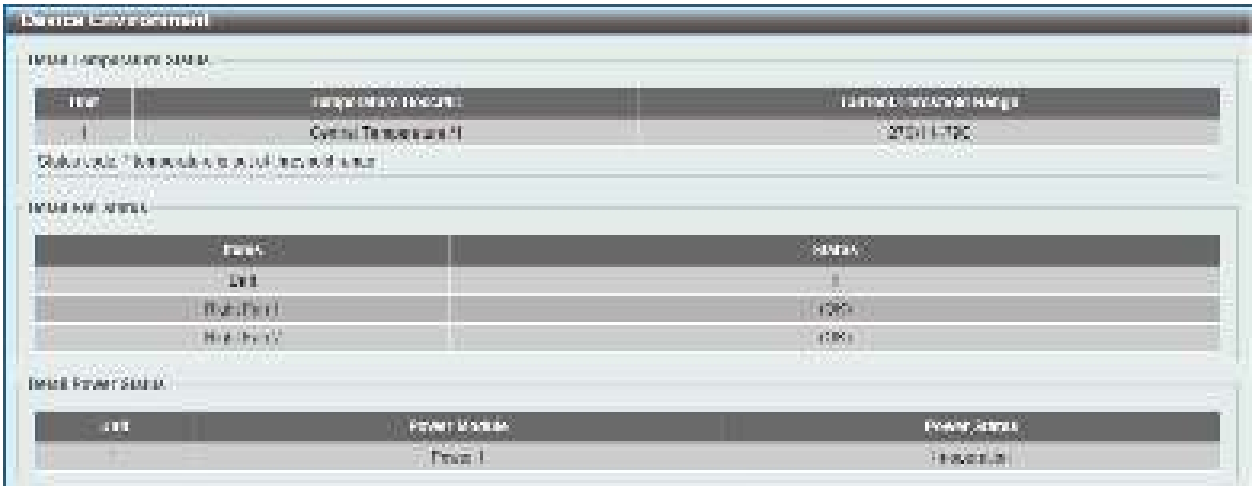


Figure 11-14 Device Environment Window

12. Green

Power Saving
EEE

Power Saving

This window is used to configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:

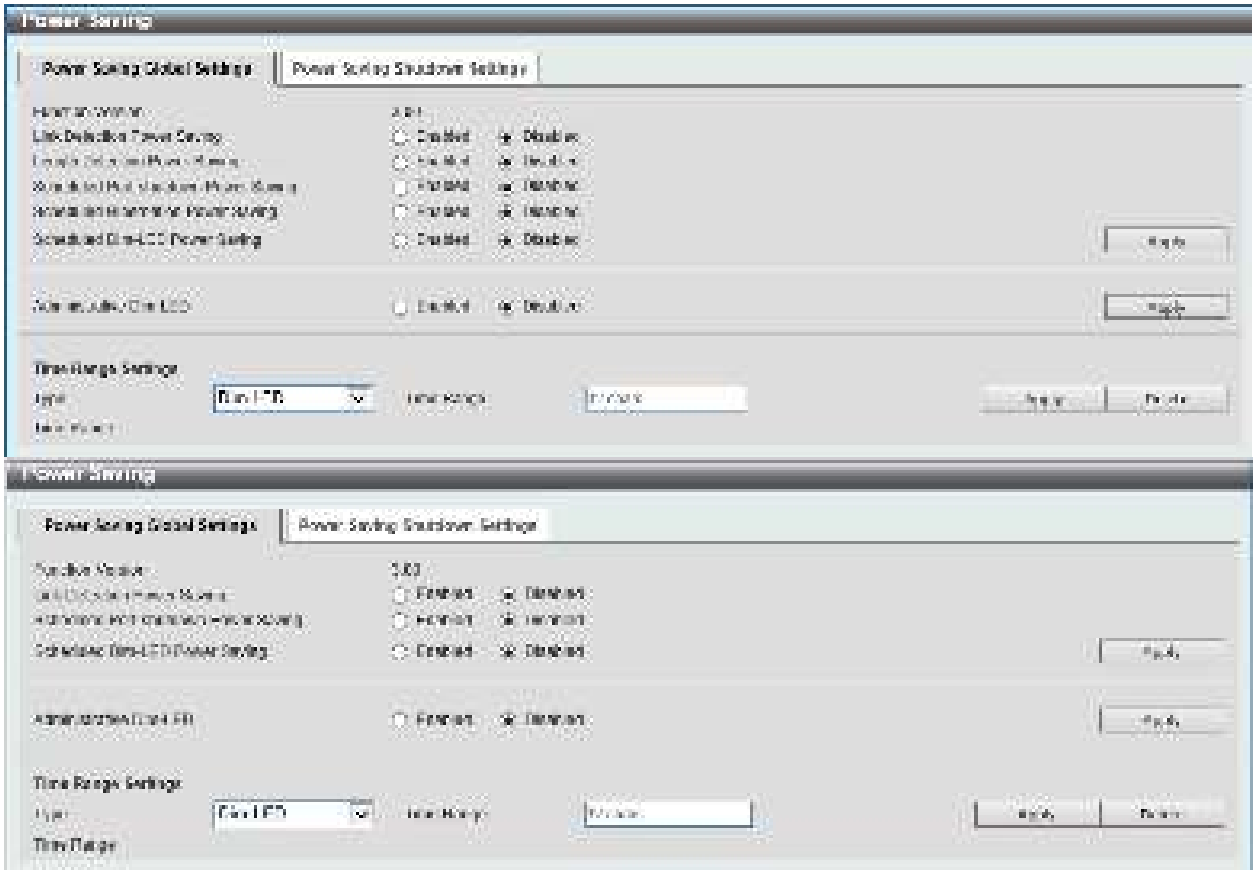


Figure 12-1 Power Saving Window

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.
Length Detection Power Saving	Select this option to enable or disable the cable length detection power saving feature. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power.
Scheduled Port-shutdown Power Saving	Select this option to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Hibernation Power Saving	Select to enable or disable the scheduled hibernation power saving function here.

Parameter	Description
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	Enter the name of the time range to associate with the power saving type.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

NOTE: The **hibernation** feature can only be configured when physical stacking is disabled on this switch.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

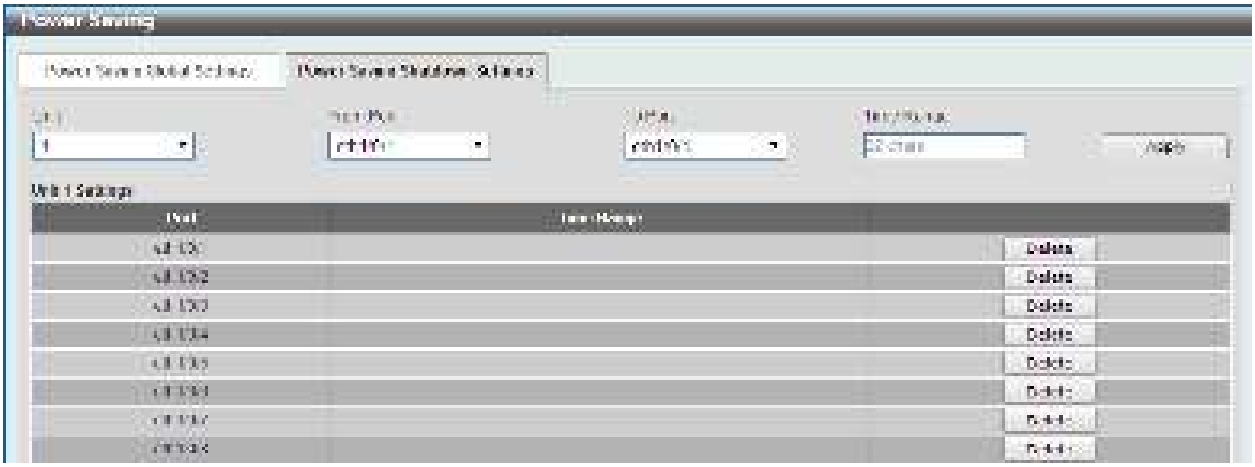


Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
Time Range	Enter the name of the time range to associate with the ports.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:

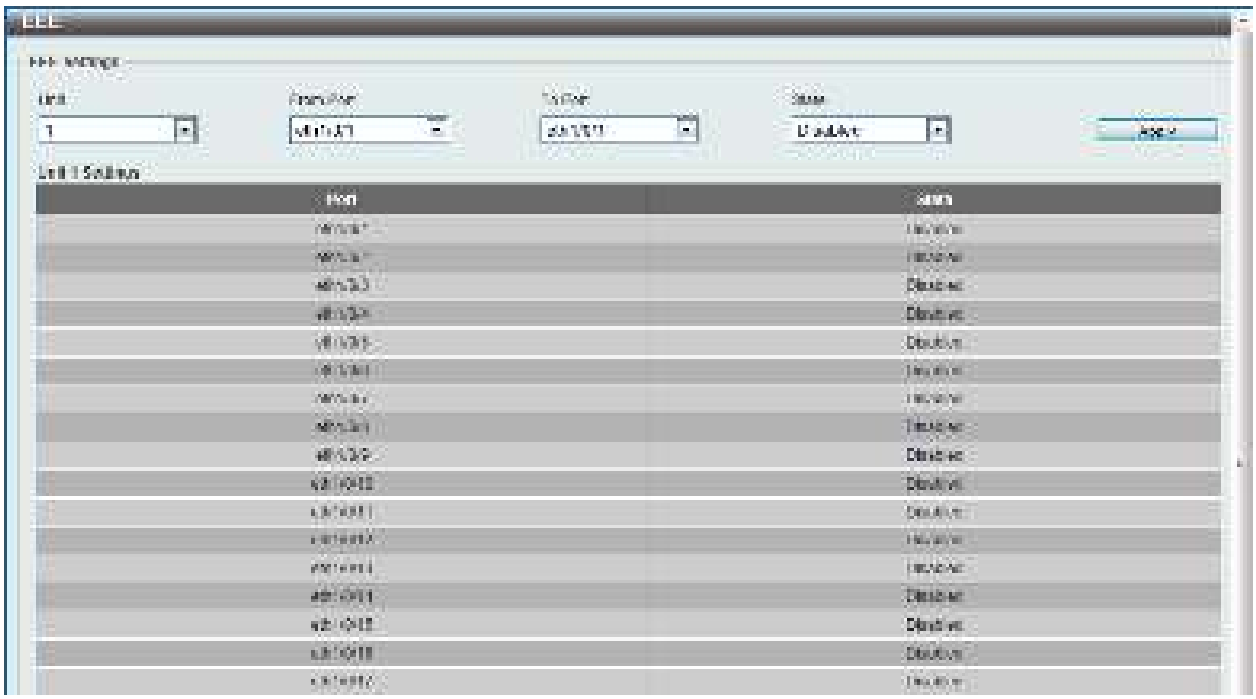


Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of this feature here.

Click the **Apply** button to accept the changes made.

13. Toolbar

Save
Tools
Wizard
Online Help
Surveillance Mode
Logout

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration or the file system of the Switch. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

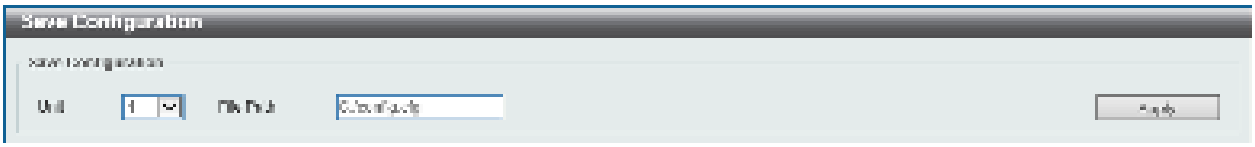


Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

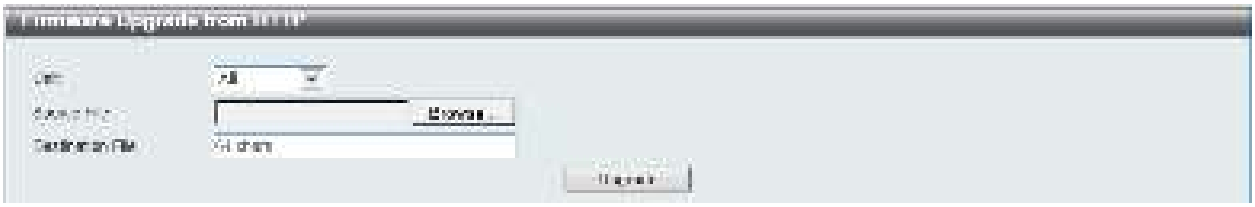


Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the local PC. This field can be up to 64 characters long. Alternatively click the **Browse** button to navigate to the location of the firmware file located on the local PC.
Destination File	Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > firmware Upgrade from TFTP**, as shown below:

Figure 13-3 Firmware Upgrade 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 IP address here. When the **IPv4** option is selected, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

NOTE: The **Source File** (name and path) can be found in the **File System** window on page 89.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

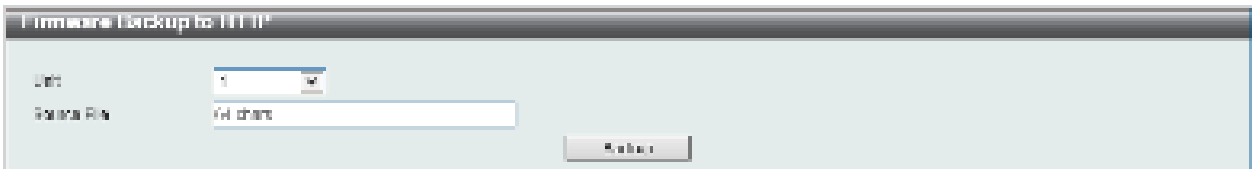


Figure 13-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration 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.

Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

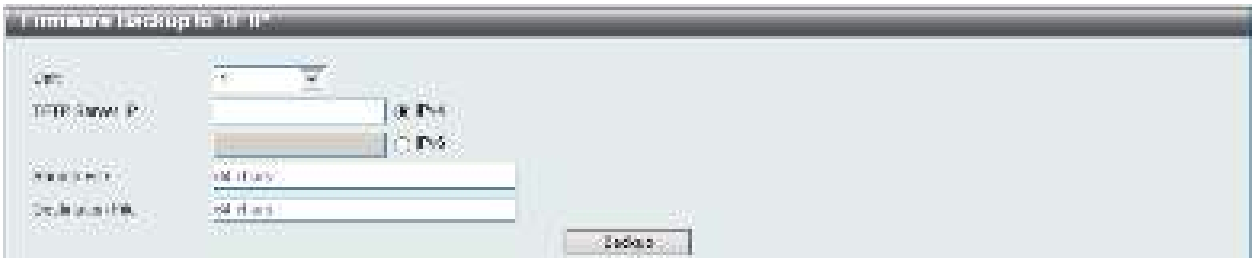


Figure 13-5 Firmware Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here. When the **IPv4** option is selected, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path where the firmware should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 13-6 Configuration Restore from HTTP 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.
Source File	Enter the source filename and path of the configuration file located on the local PC. This field can be up to 64 characters long. Alternatively click the **Browse** button to navigate to the location of the configuration file located on the local PC.
Destination File	Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the current running configuration.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

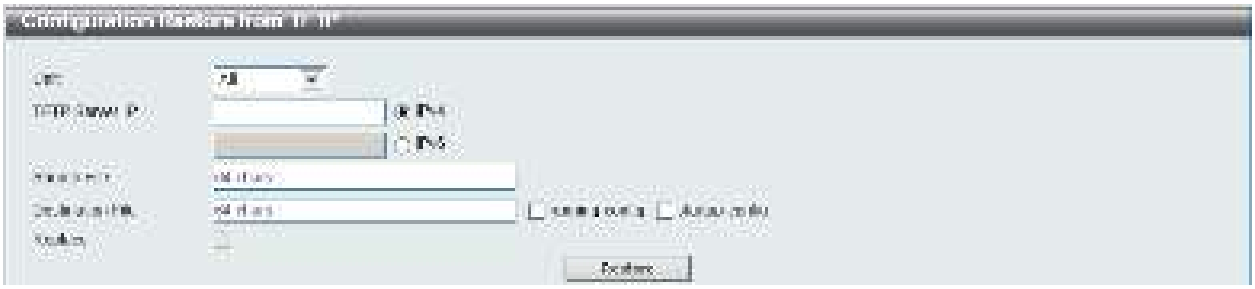


Figure 13-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here. When the **IPv4** option is selected, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the current running configuration.

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.

NOTE: The **Source File** (name and path) can be found in the **File System** window on page 89.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 13-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

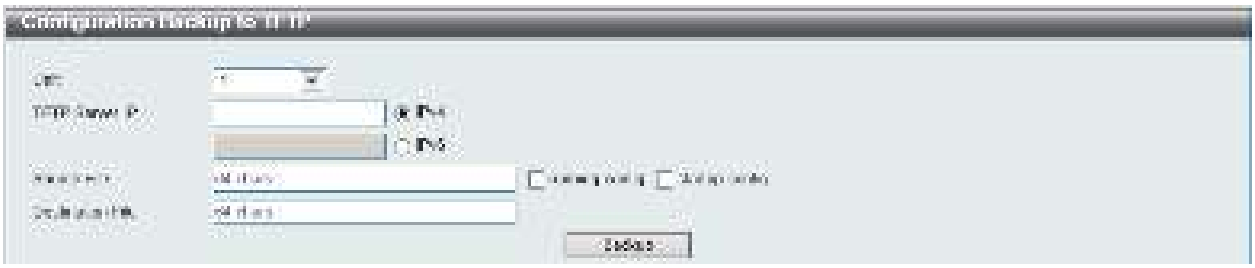


Figure 13-9 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server's IP address here. When the **IPv4** option is selected, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the configuration file located on the switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination 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:

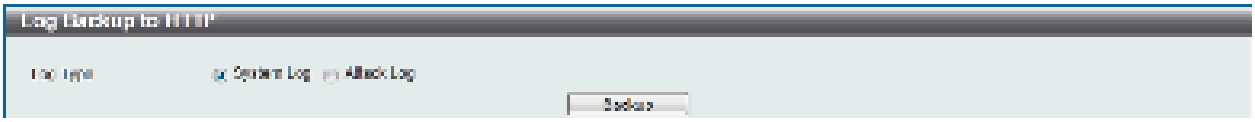


Figure 13-10 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. When **System Log** is selected, the system log will be backed up. When **Attack Log** is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup. Wait for the Web browser to prompt where to save the file on the local PC.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

Figure 13-11 Log Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server's IP address here. When the **IPv4** option is selected, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
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.
Log Type	Select the log type that will be backed up to the TFTP server. When **System Log** is selected, the system log will be backed up. When **Attack Log** is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IPv4/IPv6 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:

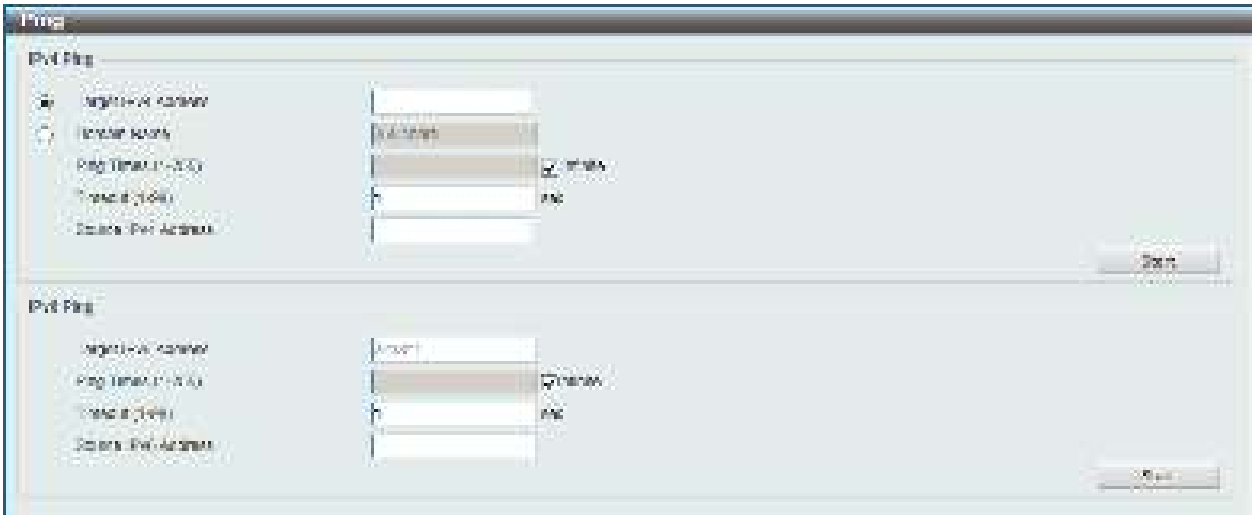


Figure 13-12 Ping Window

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.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Source IPv4 Address	Enter the source IPv4 address. If the current switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address will be used as the packets’ source IP address sent to the remote host, or as primary IP address.

The fields that can be configured for **IPv6 Ping** are described below:

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. Users may enter a number of times between 1 and 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Parameter	Description
Source IPv6 Address	Enter the source IPv6 address. If the current switch has more than one IPv6 address, you can enter one of them to this field. When entered, this IPv6 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the **Start** button to initiate the Ping Test for each individual section.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

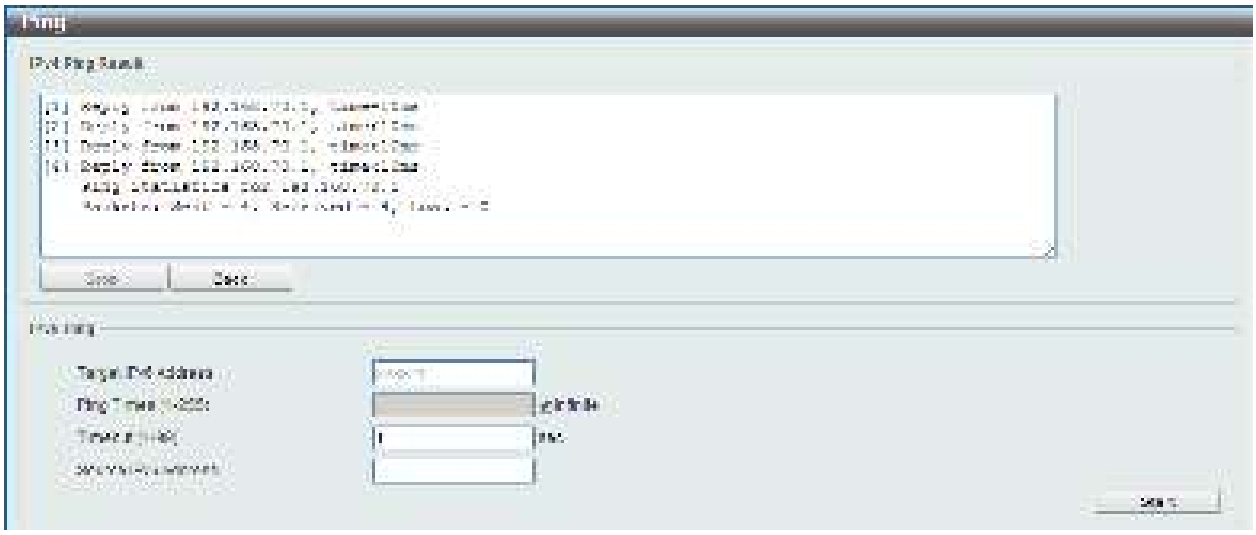


Figure 13-13 Ping - IPv4 Ping Result Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

After clicking the **Start** button in **IPv6 Ping** section, the following **IPv6 Ping Result** section will appear:

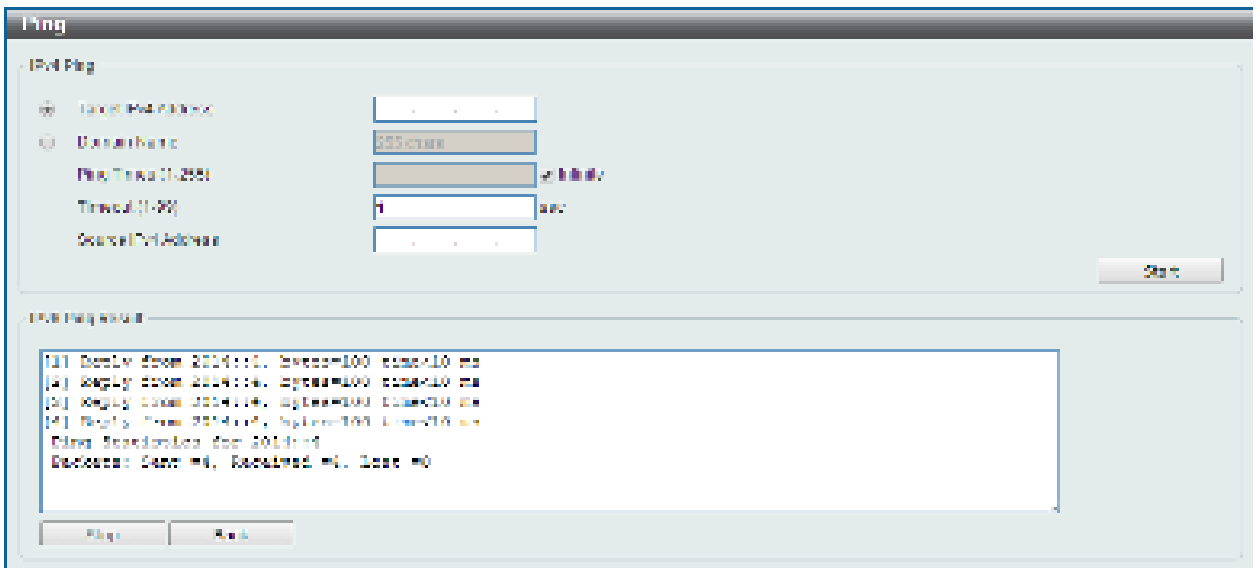


Figure 13-14 Ping - IPv6 Ping Result Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Trace Route

The trace route page allows the user to trace a route between the Switch and a given host on the network.

To view the following window, click **Tools > Trace Route**, as shown below:

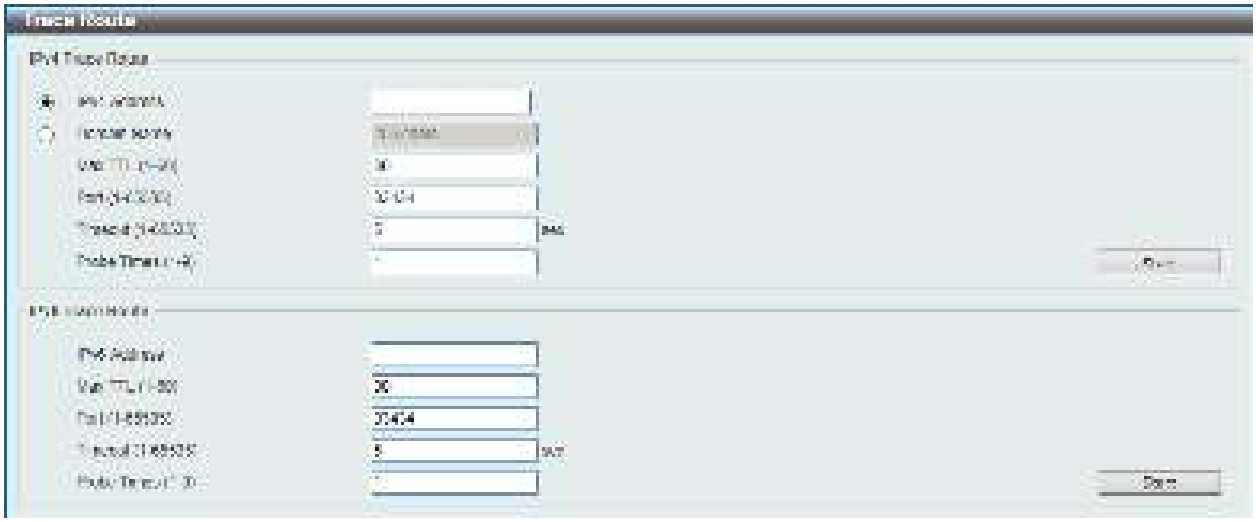


Figure 13-15 Trace Route Window

The fields that can be configured for **IPv4 Trace Route** are described below:

Parameter	Description
IPv4 Address	Select and enter the IPv4 address of the destination here.
Domain Name	Select and enter the domain name of the destination here.
Max TTL	Enter the Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Probe Times	Enter the probe time number here. The range is from 1 to 9. If unspecified, the default value is 1.

The fields that can be configured for **IPv6 Trace Route** are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address of the destination here.
Max TTL	Enter the TTL value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.

Parameter	Description
Probe Times	Enter the probe time number here. The range is from 1 to 9. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

After clicking the **Start** button in **IPv4 Trace Route** section, the following **IPv4 Trace Route Result** section will appear:

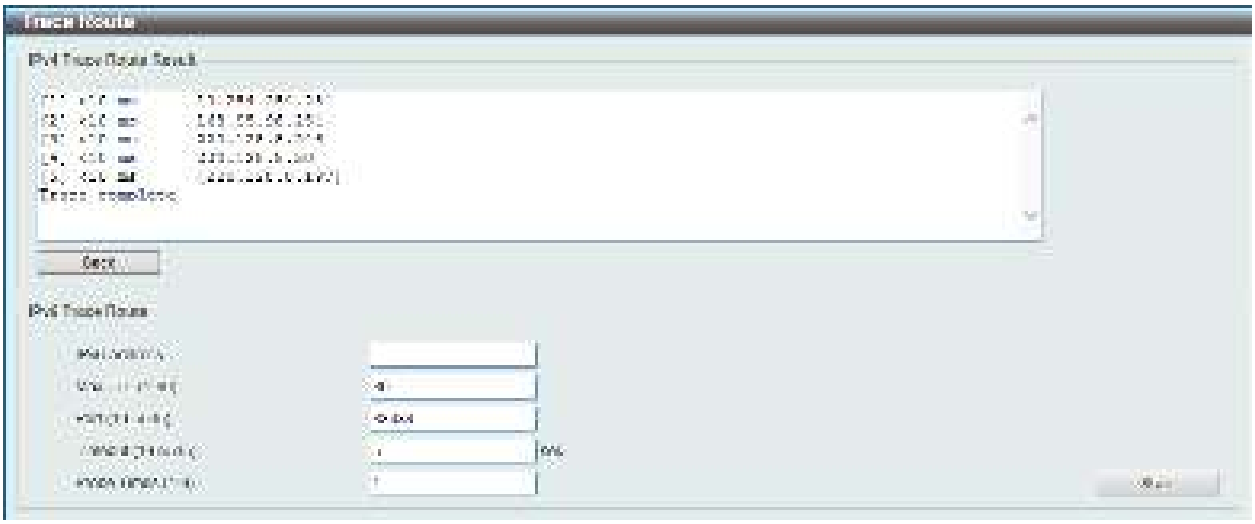


Figure 13-16 Trace Route - IPv4 Trace Route Result Window

Click the **Back** button to stop the trace route and return to the IPv4 Trace Route section.

After clicking the **Start** button in **IPv6 Trace Route** section, the following **IPv6 Trace Route Result** section will appear:

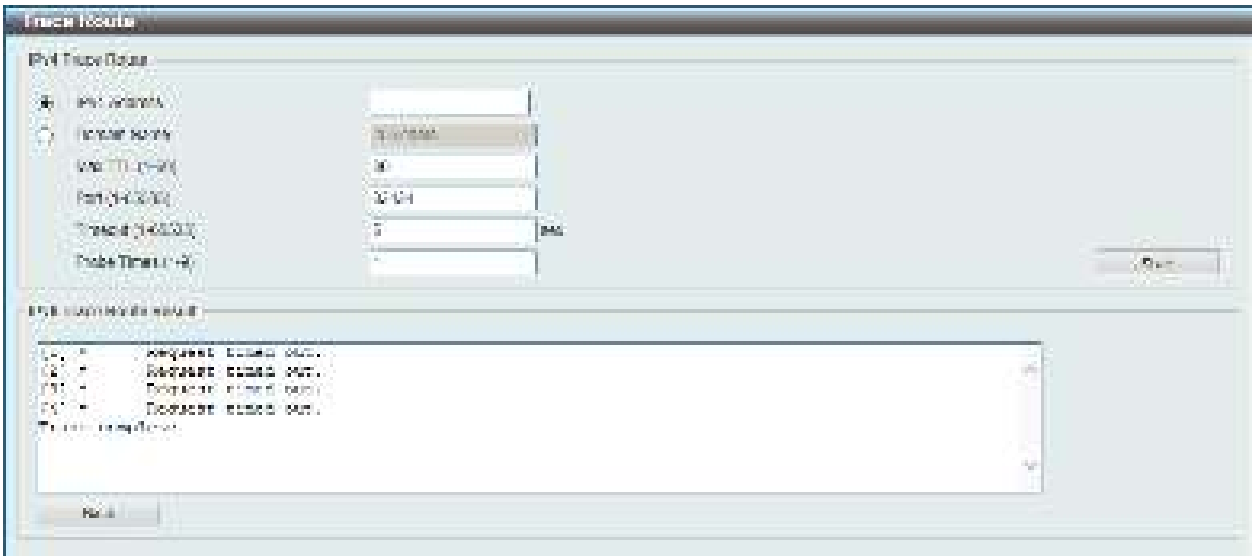


Figure 13-17 Ping - IPv6 Ping Result Window

Click the **Back** button to stop the trace route and return to the IPv6 Trace Route section.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

Figure 13-18 Language Management Window

The fields that can be configured are described below:

Parameter	Description
Language File	Click the **Browse** button to navigate to the location of the firmware file located on the local PC.

Click the **Apply** button to initiate the language pack installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

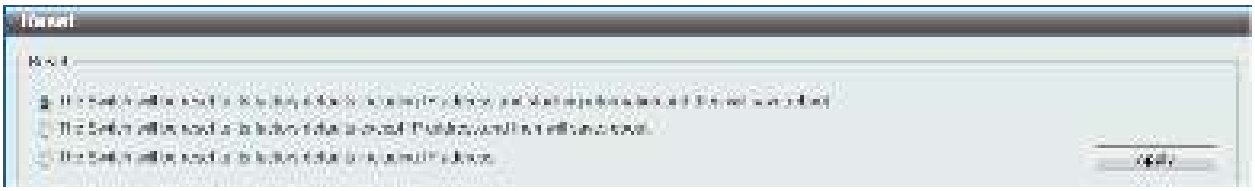


Figure 13-19 Reset Window

Select one of the following options:

- **The Switch will be reset to its factory defaults including IP address and stacking information**, **and the will save**, **reboot.** - To reset the Switch's configuration to its factory default settings.
- **The Switch will be reset to its factory default except IP address**, **and then will save**, **reboot** - To reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.
- **The Switch will be reset to its factory defaults including IP address** - To reset the Switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:

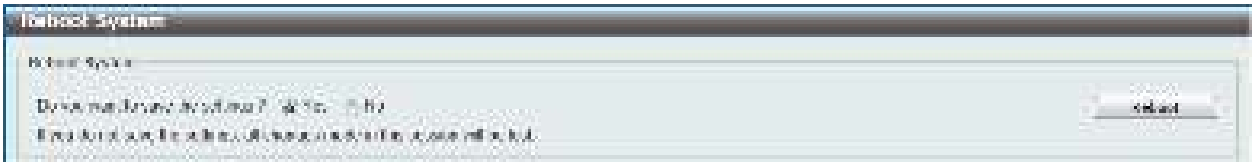


Figure 13-20 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Figure 13-21 Reboot System - Rebooting Window

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 4.

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Surveillance Mode

Click the **Surveillance Mode** button in the toolbar to change the Web UI mode and style from Standard Mode to Surveillance Mode. An unsuccessful change will display a warning message.

NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

After clicking the **Surveillance Mode** option in the **Toolbar**, the following window will appear.

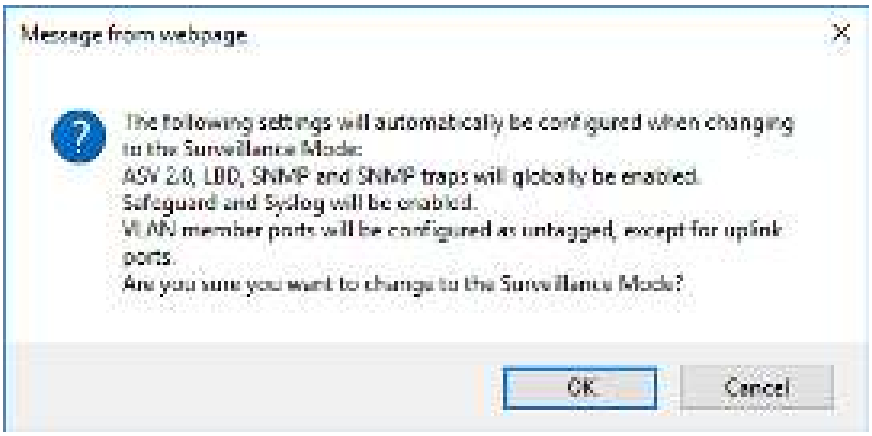


Figure 13-22 Surveillance Mode Confirmation Message

The window above displays a message that the abovementioned configurations need to be changed when access to the Surveillance Mode is given.

Click the **OK** button to continue.

Click the **Cancel** button to return to the **Standard Mode**.

After successfully switching to the Surveillance Mode on the Web UI of the Switch, the following window will appear.

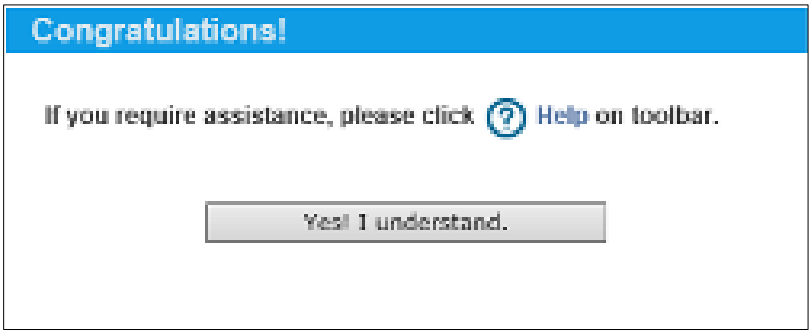


Figure 13-23 Surveillance Mode 'Congratulations' Message

Click the **Yes! I understand** button to continue.

Logout

Click this option to log out of the Web UI of the Switch

14. Surveillance Mode

Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device (such as the number of devices, device type, IP address, power consumption, link speed, and errors). Click on the '**more'** link to get more information about the devices connected to the port.

To return to the Surveillance Overview window after viewing other windows, click the **DGS-1510-28XMP** link.

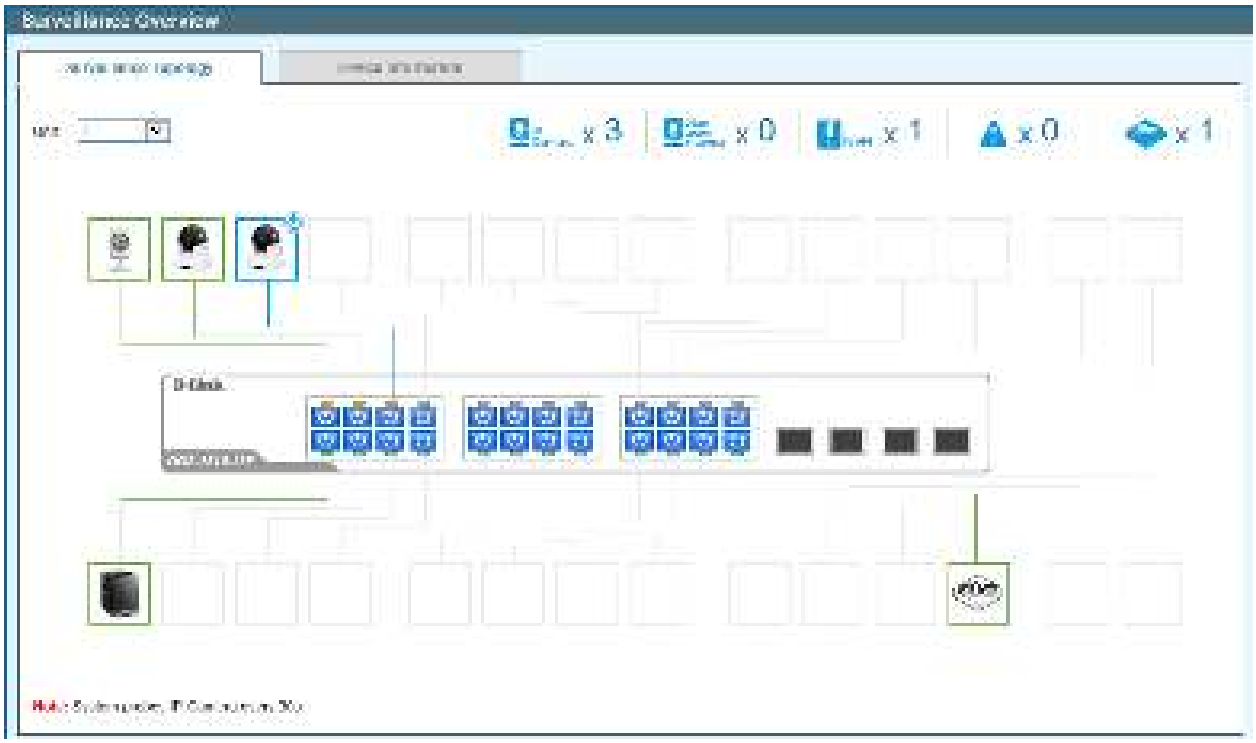


Figure 14-1 Surveillance Overview Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The following icons are available in this window and are described below:

Parameter	Description
	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
	This displays the total amount of D-Link legacy IP cameras (detected by ASV 1.0) connected to the Ethernet ports on the Switch.
	This displays the total amount of Network Video Recorders (NVRs) connected to the Ethernet ports on the Switch.
	This displays the amount of surveillance warnings generated on the Switch.
	This displays the amount of other devices connected to the Ethernet ports on the Switch.
	This displays the device connected to the Ethernet port on the Switch. The green border around the image indicates that the device is a non-PoE device. The PD Alive function cannot be used on this device.
	This displays the device connected to the Ethernet port on the Switch. The blue border around the image indicates that the device is a PoE device and is receiving power from the Switch using PoE. The PD Alive function can be used on this device.
	Click this icon to disable PoE on the port.
	Click this icon to enable PoE on the port.

After clicking the  icon, the following window will appear:

After clicking the  icon, the following window will appear:

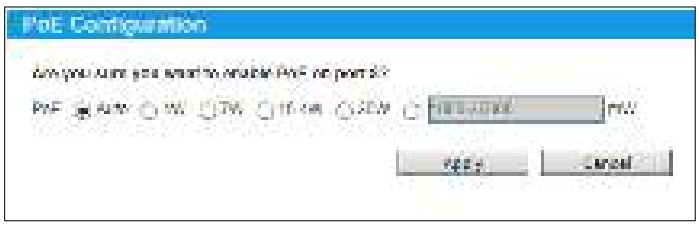


Figure 14-2 PoE Configuration Window

The fields that can be configured are described below:

Parameter	Description
PoE	Select the maximum power that will be supplied on the PoE port. Options to choose from are **Auto**, **4W**, **7W**, **15.4W**, **30W**, and a configurable value from 1000 mW to 30000 mW. The unit is either in watt or milliwatt.

Click the **Apply** button to accept the changes made.

Click the **Cancel** button to discard the changes made.

After hovering (with the mouse pointer) over the **network device** icon, the following additional information will be displayed:

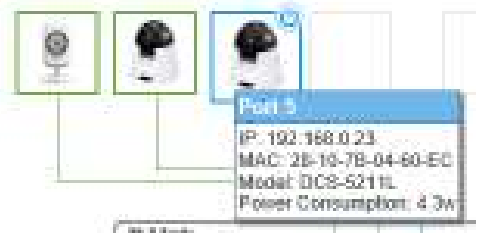


Figure 14-3 Additional Device Information

After clicking (left-click) the **network device** icon, the following window will appear.

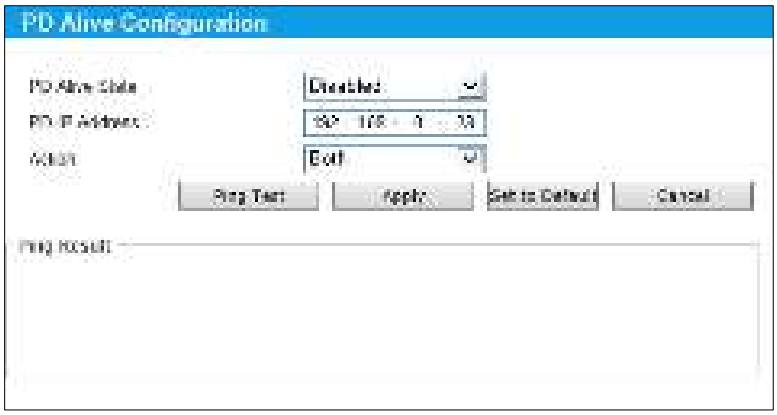


Figure 14-4 PD Alive Configuration Window

The fields that can be configured are described below:

Parameter	Description
PD Alive State	Select to enable or disable the PD Alive function here.
PD IP Address	Enter the IP address of the PD here.
Action	Select the action that will be taken here. Options to choose from are: • **Reset** - Specifies to reset the PoE port state (turn PoE off and on). • **Notify** - Specifies to send logs and traps to notify the administrator. • **Both** - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

Click the **Ping Test** button to initiate the ping test to check if the PD is active or not.

Click the **Apply** button to accept the changes made.

Click the **Set to Default** button to return the settings to the default settings for this PD.

Click the **Cancel** button to discard the changes made.

After clicking **Ping Test** button, the following window will appear.

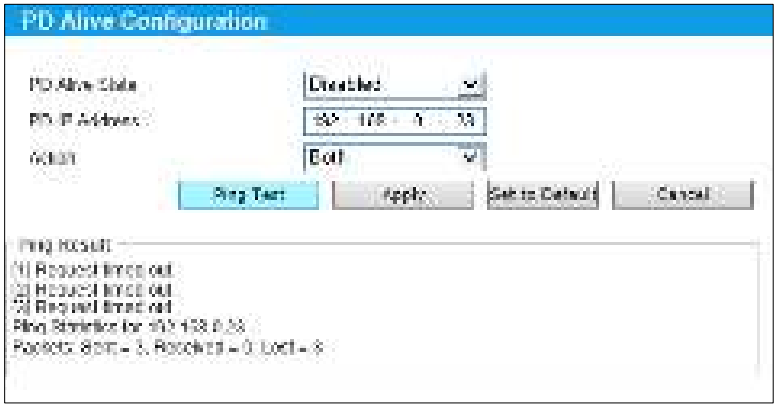


Figure 14-5 PD Alive Configuration Window (Ping Result)

The **Ping Result** will be displayed.

NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.

NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.

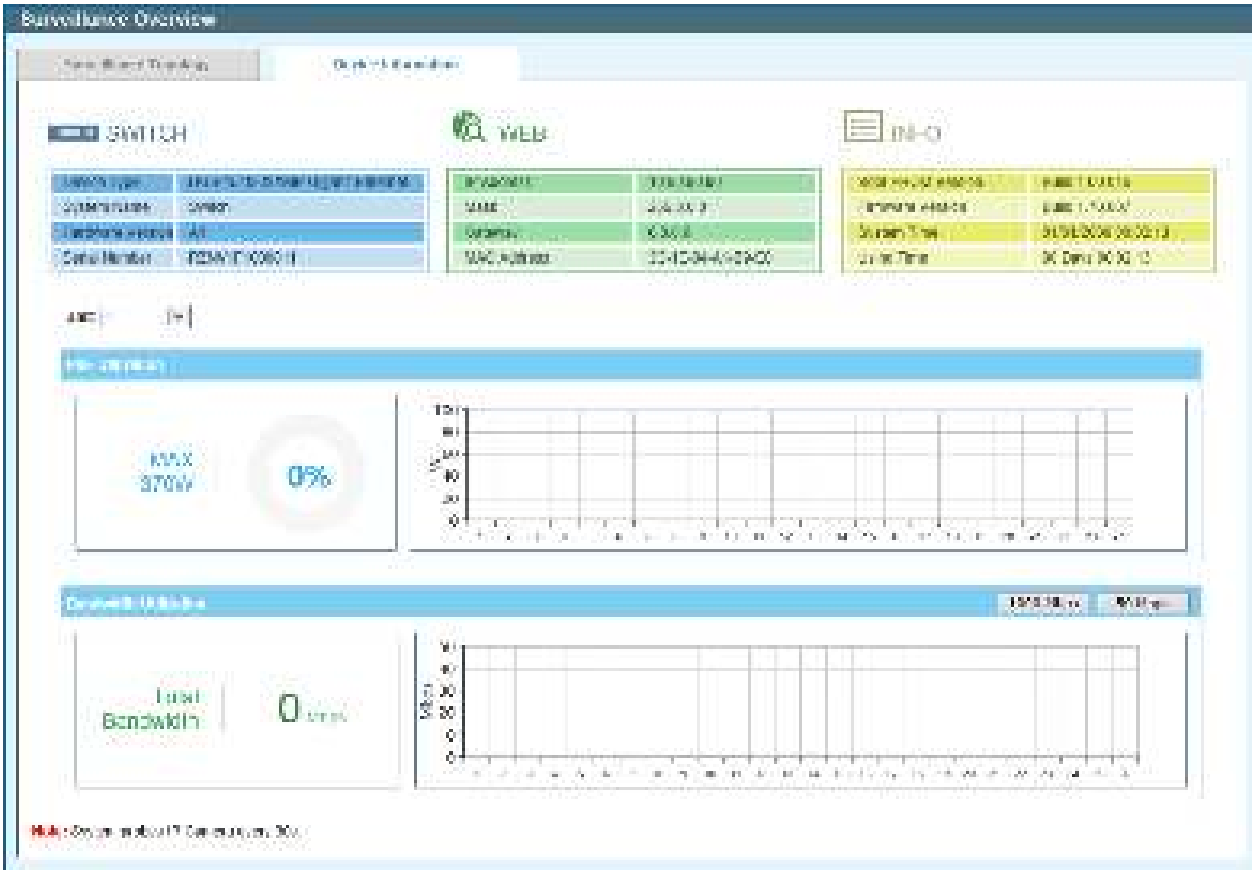


Figure 14-6 Device Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

Click the **1000 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 1 Gbps.

Click the **50 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 50 Mbps.

Port Information

This window is used to display port information like throughput, distance of the network cable, PoE provisioning status, power consumption, Loopback Detection status, group, and how many IP cameras, NVRs, and other devices are connected to the ports.

To view the following window, click **Port Information**, as shown below:

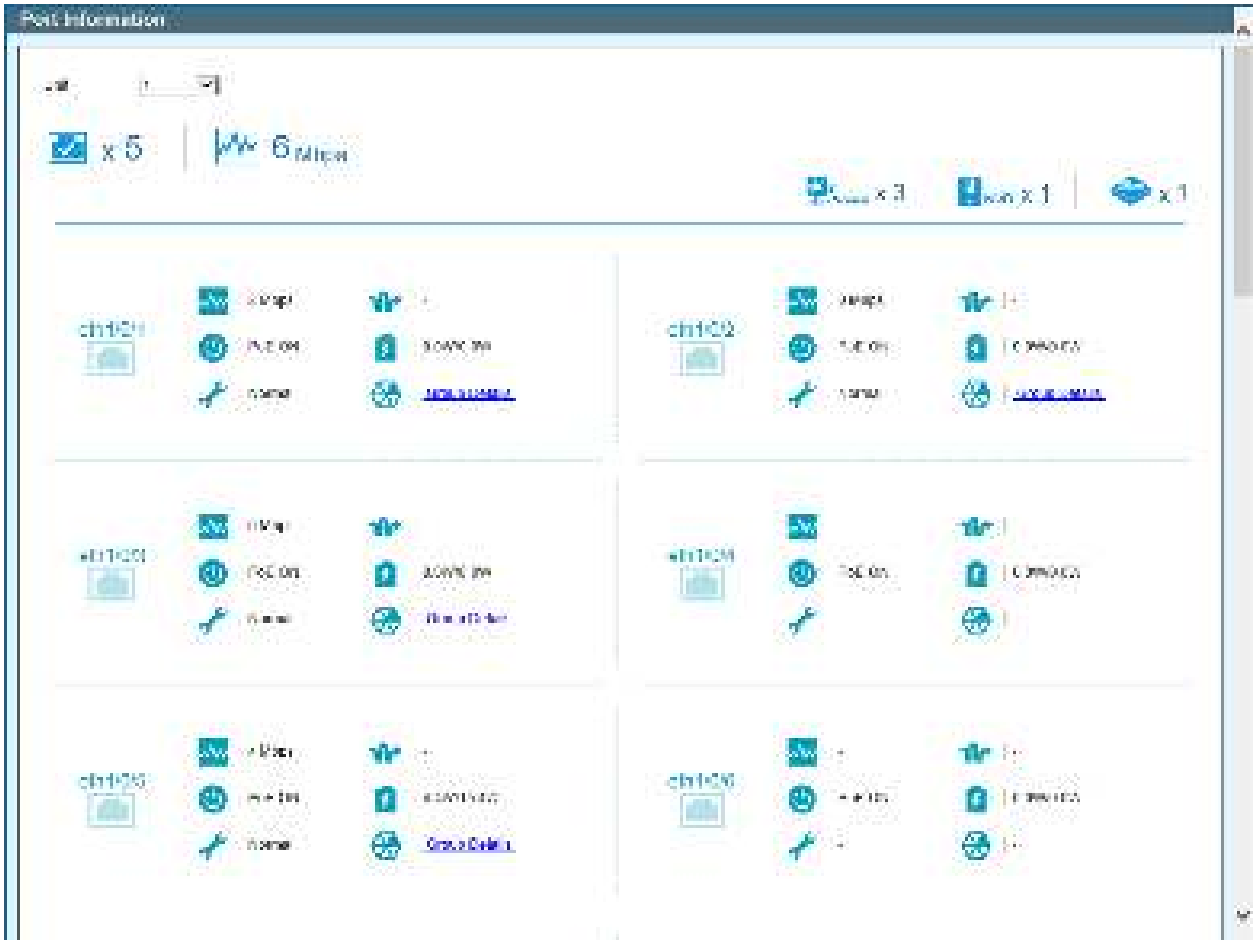


Figure 14-7 Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The following icons are available in this window and are described below:

Parameter	Description
x 5	This displays the total amount of Ethernet devices connected to the Ethernet ports on the Switch.
6 Mbps	The displays the total amount of inbound bandwidth that is being used by the Ethernet devices connected to the Ethernet ports on the Switch.
x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
NVR x 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.

Parameter	Description
x 1	This displays the total amount of other Ethernet devices connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the Ethernet device connected to the respective Ethernet port.
-	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.
PoE ON	This displays the PoE status on the port.
3.8W/15.4W	This displays the power consumption and power class of the PD connected to the Ethernet port. | Normal Loop	This displays the Loopback Detection status on the Ethernet port. **Normal** - Specifies that there are no loops in the network. **Loop** - Specifies that there is a loop in the network. Click the **Loop** link to navigate to the **Health Diagnostic** window.
Group Details	If an ONVIF IP camera or NVR is connected to the port, the **Group Details** link will be available. Select the **Group Details** link to access the Group Details window.
Video Management Server	If a network device is connected to the port that is neither an ONVIF IP camera nor NVR, the device type can be selected. Options to choose from are **Video Management Server**, **VMS Client/Remote Viewer**, **Video Encoder**, **Network Storage**, and **Other IP Surveillance Device**.

Group Details

After clicking **Group Details** link, the following window will appear.

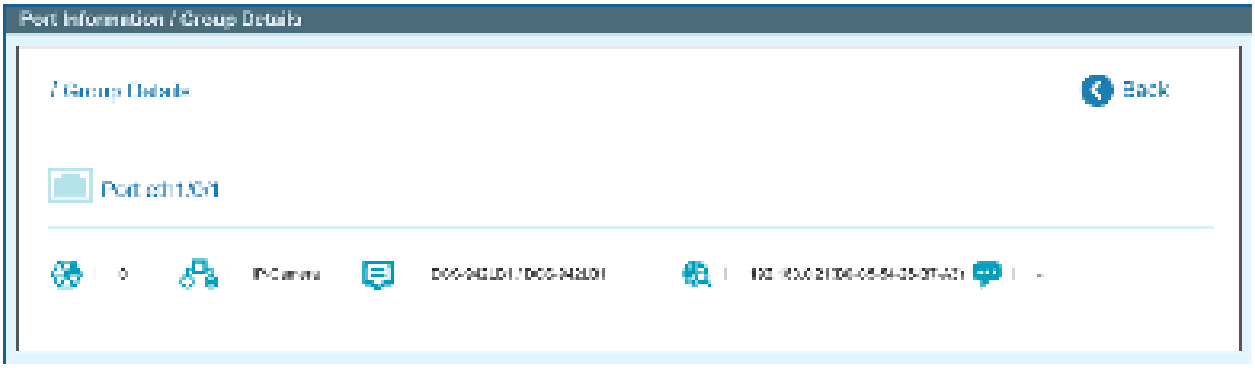


Figure 14-8 Port Information / Group Details Window

The following icons are available in this window and are described below:

Parameter	Description
Port eth1/0/5	This displays the Ethernet port number on the Switch.
0	This displays the group ID of the IP camera or NVR on the port.
IP-Camera	This displays the type of device connected to the port. The can be either **IP-Camera** or **NVR**.

Parameter	Description
DCS-5211L / DCS-5211L	This displays the model name of the IP camera.
192.168.0.23(28-10-7B-04-60-EC)	This displays the IP Address and MAC Address of the IP camera or NVR.
DCS-942LB1	This displays the description of the device connected to the port.

Click the **< Back** option to return to the previous window.

IP-Camera Information

This window is used to display IP camera information.

To view the following window, click **IP-Camera Information**, as shown below:

Figure 14-9 IP-Camera Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The following icons are available in this window and are described below:

Parameter	Description
x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.

Parameter	Description
0Mbps	The displays the total amount of inbound bandwidth that is being used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
4.4w / 15.4w	The displays the total power consumption and power class (of PDs) used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
DCS-942LB1 DCS-942LB1	This displays a photo, the manufacturer, and the model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the IP camera.
4.4W /15.4W	This displays the power consumption and power class of the IP camera.
192.168.0.21 (B0-C5-54-26-B7-A3)	This displays the IP address and MAC address of the IP camera.
DCS-942LB1	This displays the description for the IP camera. Click the icon to modify the description.
	Enter the description for the IP camera here. Click the icon to apply the modified description.

NVR Information

This window is used to display NVR information.

To view the following window, click **NVR Information**, as shown below:

Figure 14-10 NVR Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The following icons are available in this window and are described below:

Parameter	Description
	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
	The displays the total amount of inbound bandwidth that is being used by the NVRs connected to the Ethernet ports on the Switch.
	This displays the Ethernet port number on the Switch.
	This displays a generic photo of the NVR connected to the port.
	This displays the amount of inbound bandwidth that is being used by the NVR.
	This displays the IP address and MAC address of the NVR.
	This displays the description for the NVR. Click the  icon to modify the description.
	Enter the description for the NVR here. Click the  icon to apply the modified description.
	This displays the group ID of the NVR.
	This displays the number of ONVIF IP cameras managed by this NVR.
	This displays information about the ONVIF IP camera that is managed by this NVR.

PoE Information

This window is used to display Power-over-Ethernet (PoE) information.

To view the following window, click **PoE Information**, as shown below:

Figure 14-11 PoE Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The following icons are available in this window and are described below:

Parameter	Description
193w	This displays the maximum PoE budget that can be provided by the Switch.
3.5 W / 15.4 W	This displays the total PoE consumption and power class of PDs connected to the Switch.
22 %	This displays the current PoE utilization (in percentage).
PoE 15W x 1	This displays the number of PoE devices connected to the Switch that is using 15 Watts of power per port.
PoE+ 30W x 0	This displays the number of PoE devices connected to the Switch that is using 30 Watts of power per port.
eth1/0/5 POE	This displays the Ethernet port number on the Switch.
PoE ON	This displays the PoE state on the port. This can be either **PoE ON** or **PoE OFF**.

Parameter	Description
 15.4W	This displays the maximum PoE budget available on this port.
 Delivering  Power Denied	This displays the current PoE status on the port. This status can be one of the following: **-**, **Searching**, **Delivering**, or **Power Denied**. When the **Power Denied** message is displayed, click on the link to redirect the **Health Diagnostic** window for more information.
 3.5W/ 15.4W	This displays the PoE consumption and power class of the PD connected to the port.

PoE Scheduling

This window is used to display and configure the PoE scheduling settings.

To view the following window, click **PoE Scheduling**, as shown below:

Figure 14-12 PoE Scheduling Window

The fields that can be configured in the **Time Range** section are described below:

Parameter	Description
Range Name	Enter the name of the time range schedule here.
From: Time (Week/HH)	Select the starting day and hour in the time range schedule here. Alternatively, click the  icon to open a calendar for easy day and hour selection.
To: Time (Week/HH)	Select the ending day and hour in the time range schedule here. The schedule will end at the end of the selected hour.

Parameter	Description
	Alternatively, click the icon to open a calendar for easy day and hour selection.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured in the **PoE Configuration** section are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.
From Port / To Port	Select the port range that will be used here.
Time Range	Select the time range schedule that will be applied to the selected port(s) here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the time range schedule from the specified port.

After clicking the icon, the following window will appear:

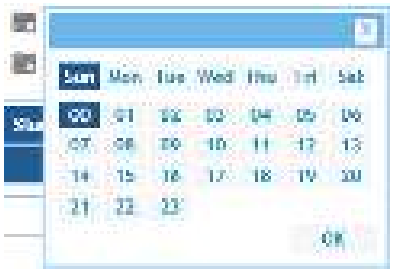


Figure 14-13 Day and Hour Window

Click the **OK** button to use the Day and Hour selected.

Management

File System

This window is used to display and configure the file system settings.

To view the following window, click **Management > File System**, as shown below:

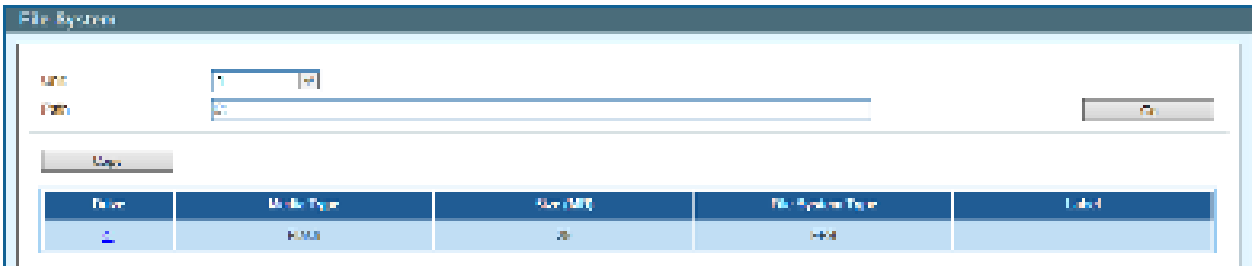


Figure 14-14 File System Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.
Path	Enter the path string here.

Click the **Go** button to navigate to the path entered.

Click the **c:** hyperlink to navigate the C: drive.

After clicking the **c:** hyperlink, the following window will appear.

Figure 14-15 File System (c:) Window

Click the **Previous** button to return to the previous window.

Click the **Create Directory** button to create a new directory within the file system of the Switch.

Click the **Copy** button to copy a specific file to the Switch.

Click the **Boot Up** button to set a specific runtime image as the boot up image.

Click the **Rename** button to rename a specific file's name.

Click the **Delete** button to remove a specific file from the file system.

After clicking the **Copy** button, the following windows will appear.

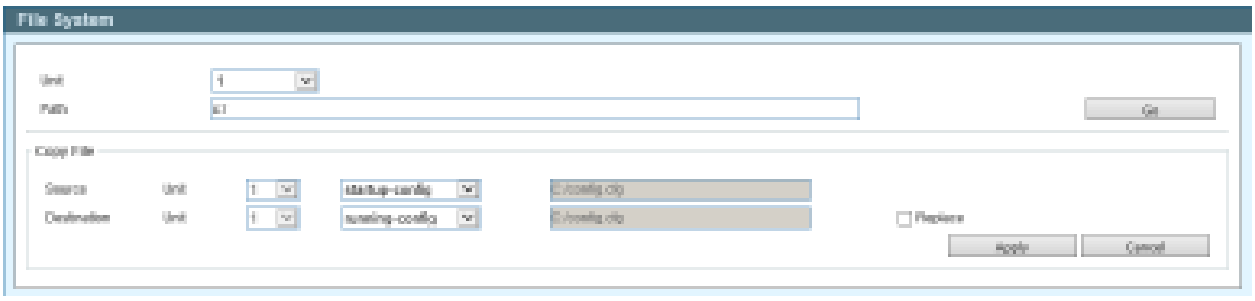


Figure 14-16 File System (Copy) Window

The fields that can be configured are described below:

Parameter	Description
Source	Specifies to configure the source file that will be copied.
Destination	Specifies to configure the destination file that will be copied.
Unit	Select the unit ID of the Switch in the stack that will be used here.

Parameter	Description
startup-config	Select this option to use the startup configuration of the Switch in the copy.
running-config	Select this option to use the running configuration of the Switch in the copy.
Source File	Select this option and then manually enter the path and name of the source file that will be copied in the space provided.
Destination File	Select this option and then manually enter the path and name of the destination file that will be copied in the space provided.
Replace	Select this option to replace the current running configuration with the source file.

Click the **Apply** button to initiate the copy.

Click the **Cancel** button the discard the process.

Time

Clock Settings

This window is used to display and configure the time settings on the Switch.

To view the following window, click **Time > Clock Settings**, as shown below:

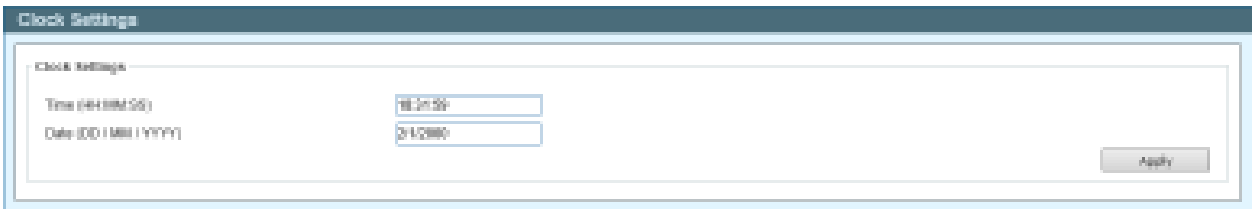


Figure 14-17 Clock Settings Window

The fields that can be configured are described below:

Parameter	Description
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.
Date (DD/MM/YYYY)	Enter the current day, month, and year to update the system clock.

Click the **Apply** button to accept the changes made.

SNTP Settings

This window is used to display and configure the Simple Network Time Protocol (SNTP) settings.

To view the following window, click **Time > SNTP Settings**, as shown below:

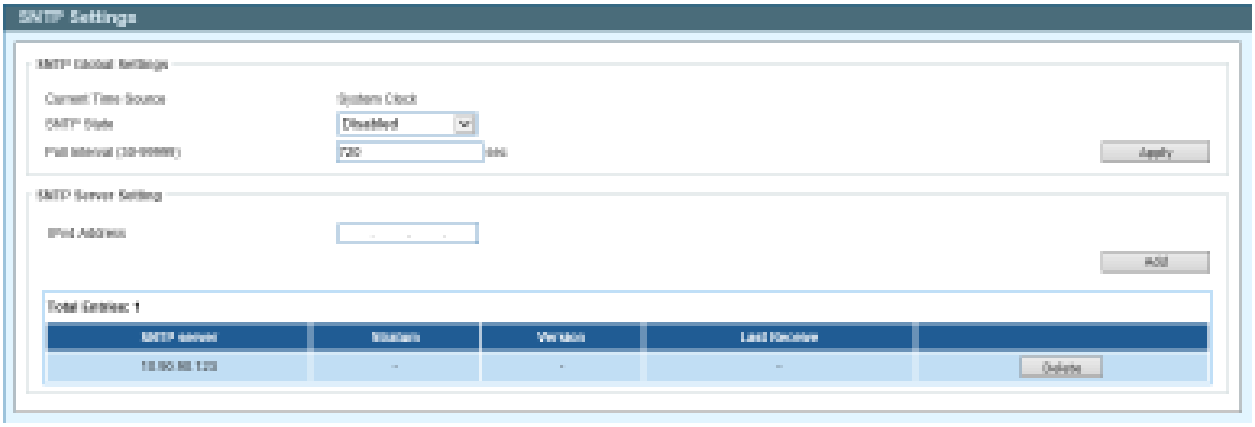


Figure 14-18 SNTP Settings Window

The fields that can be configured in the **SNTP Global Settings** section are described below:

Parameter	Description
SNTP State	Select to enable or disable the SNTP feature here.
Poll Interval	Enter the poll interval value here. The range is from 30 to 99999 seconds. By default, this value is 720 seconds.

Click the **Apply** button to accept the changes made.

The fields that can be configured in the **SNTP Server Setting** section are described below:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server here.

Click the **Add** button to add the SNTP server to the configuration.

Click the **Delete** button to remove the SNTP server from the configuration.

Surveillance Settings

This window is used to display and configure the surveillance settings. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

To view the following window, click **Surveillance Settings**, as shown below:

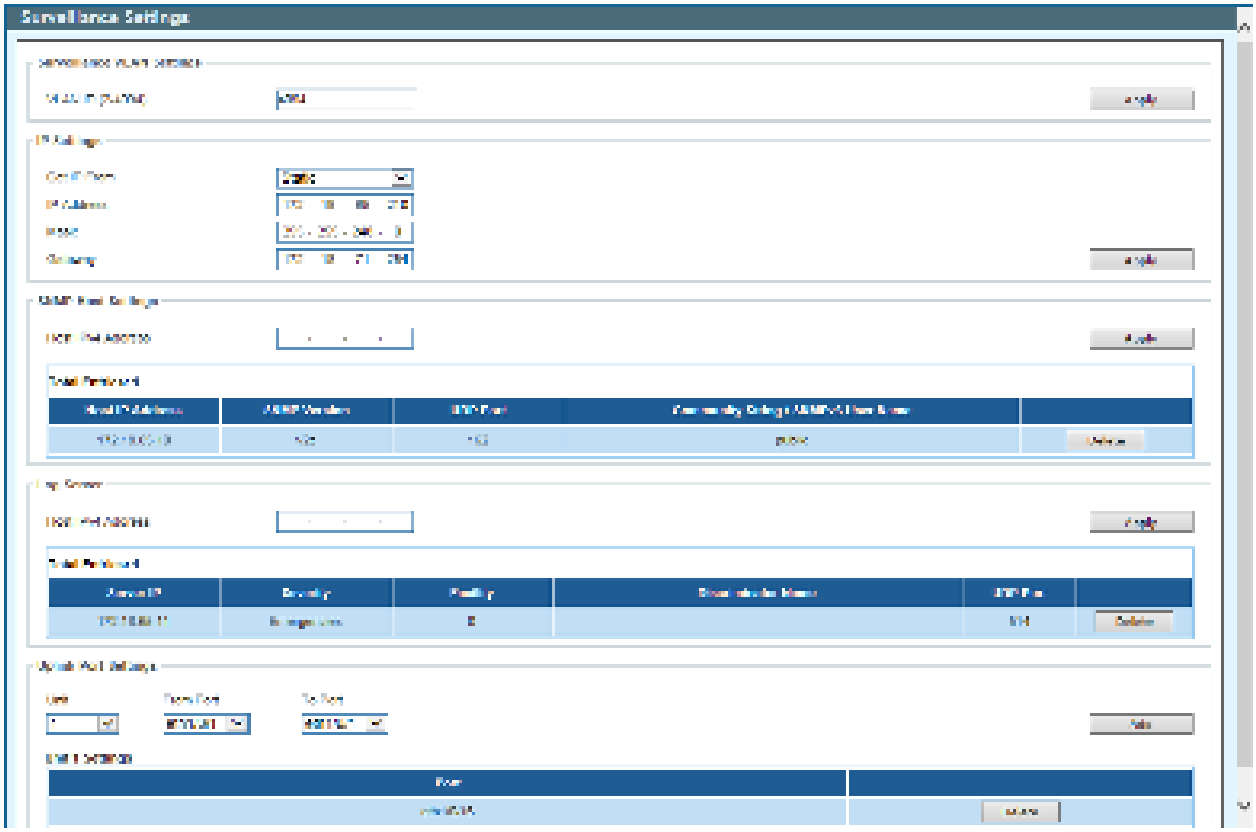


Figure 14-19 Surveillance Settings Window

The fields that can be configured in the **Surveillance VLAN Settings** section are described below:

Parameter	Description
VLAN ID	Enter the ID of the surveillance VLAN here. The range is from 2 to 4094.

Click the **Apply** button to accept the changes made.

The fields that can be configured in the **IP Settings** section are described below:

Parameter	Description
Get IP From	Select the method used to configure the IP address settings on the Switch here. Options to choose from are: • **Static** - Specifies that the IP address settings will be manually configured. • **DHCP** - Specifies that the IP address settings will be automatically obtained from a DHCP server on the network.
IP Address	Enter the IPv4 address of the Switch here.
Mask	Enter the IPv4 subnet mask of the Switch here.
Gateway	Enter the IPv4 address of the default gateway here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in the **SNMP Host Settings** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP host here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

The fields that can be configured in the **Log Server** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the syslog server here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

The uplink ports join all surveillance VLANs since they forward surveillance traffic to other switches. It is recommended to connect uplink ports to the other switches because the discovery process is disabled on these ports.

The fields that can be configured in the **Uplink Port Settings** section are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.
From Port / To Port	Select the uplink port range that will be used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Surveillance Log

This window is used to display the surveillance log.

To view the following window, click **Surveillance Log**, as shown below:

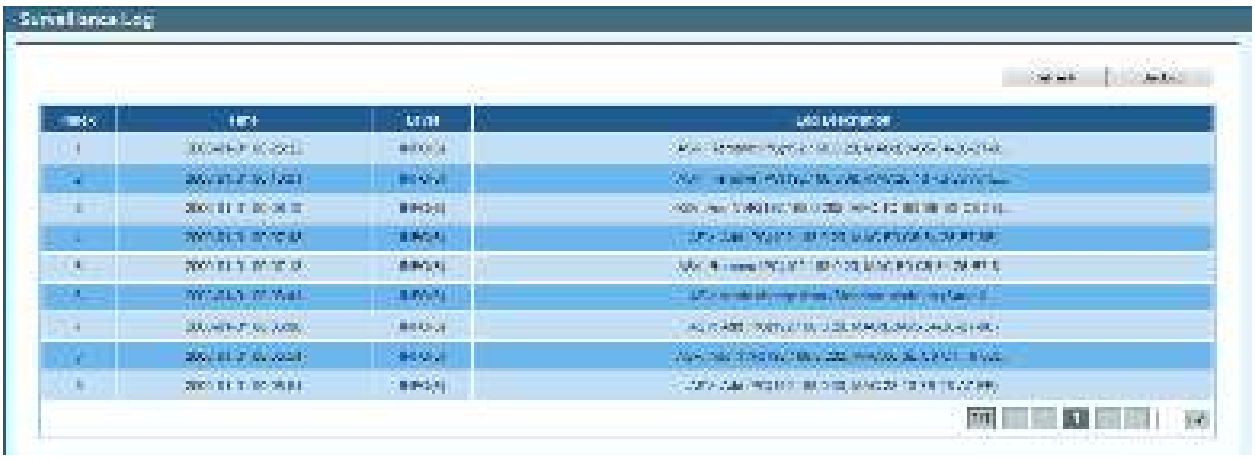


Figure 14-20 Surveillance Log Window

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Backup** button to upload the surveillance log to the PC using HTTP.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Health Diagnostic

This window is used to display Health Diagnostics information, Discovered Surveillance Devices information, and initiate a cable distance test on all or selected ports on the Switch. For each link-up port, the system will check the link status, PoE status and error counters periodically. This page will refresh every 30s.

To view the following window, click **Health Diagnostic**, as shown below:

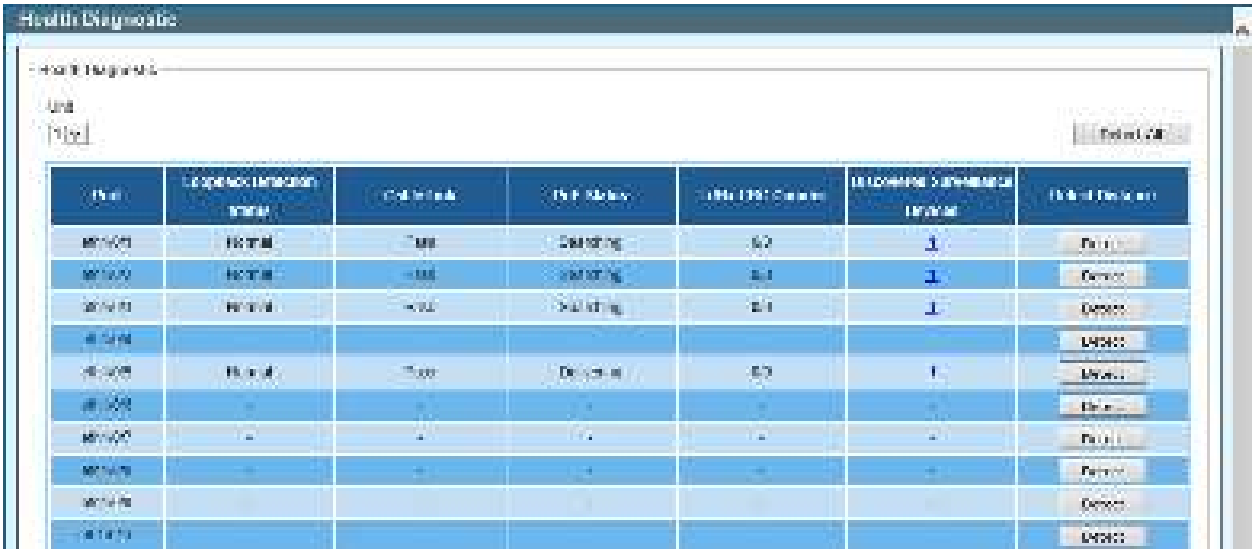


Figure 14-21 Health Diagnostic Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit ID of the Switch in the stack that will be used here.

The fields that are displayed in the table are described below:

Parameter	Description
Port	This field displays the Ethernet port number.
Loopback Detection Status	This field displays the Loopback Detection status on the Ethernet port. It can be one of the following: • **Normal** - No loop is detected on the port. • **Loop** - A loop is detected on the port.
Cable Link	This field displays the cable link status. It can be one of the following: • **PASS** - The port link is up and operating in the full-duplex mode. • **10M Half** - The port link is up and operating at 10 Mbps speed and in the half-duplex mode. • **100M Half** - The port link is up and operating at 100 Mbps speed and in the half-duplex mode.
PoE Status	This field displays the PoE status. It can be one of the following: **PASS**, **MPS (Maintain Power Signature) Absent**, **PD Short**,

Parameter	Description
	Overload, **Power Denied**, **Thermal Shutdown**, **Startup Failure**, or **Classification Failure**.
Tx/Rx CRC Counter	This field displays the TX/RX CRC counter.
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (1) to view the group details associated with IP camera or NVR connected to the port. For more information, refer to **Group Details** on page 397.
Detect Distance	Click the **Detect** button to initiate a cable distance test on the specified port.

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 4.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

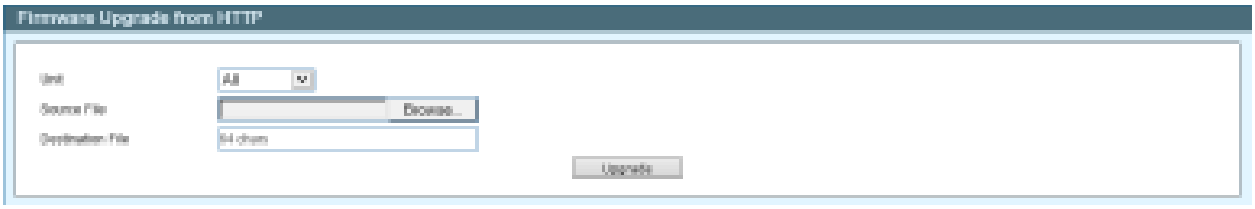


Figure 14-22 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the local PC. This field can be up to 64 characters long. Alternatively click the **Browse** button to navigate to the location of the firmware file located on the local PC.
Destination File	Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

NOTE: The **Source File** (name and path) can be found in the **File System** window on page 403.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

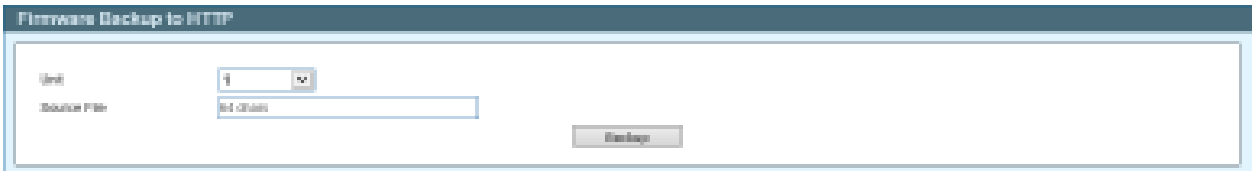


Figure 14-23 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration 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.

Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

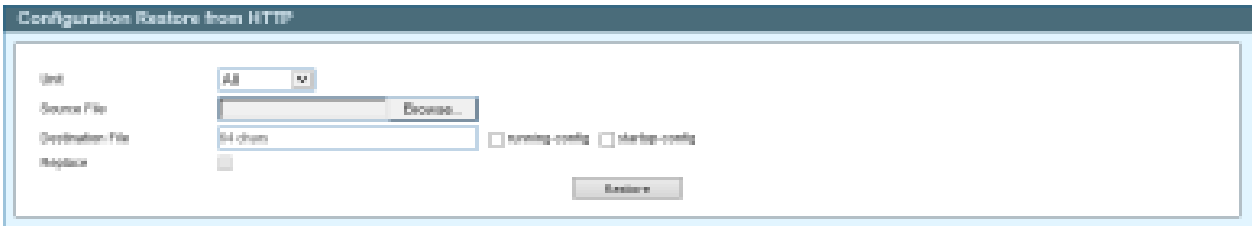


Figure 14-24 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the local PC. This field can be up to 64 characters long. Alternatively click the **Browse** button to navigate to the location of the configuration file located on the local PC.

Parameter	Description
Destination File	Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the current running configuration.

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.

NOTE: The **Source File** (name and path) can be found in the **File System** window on page 403.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

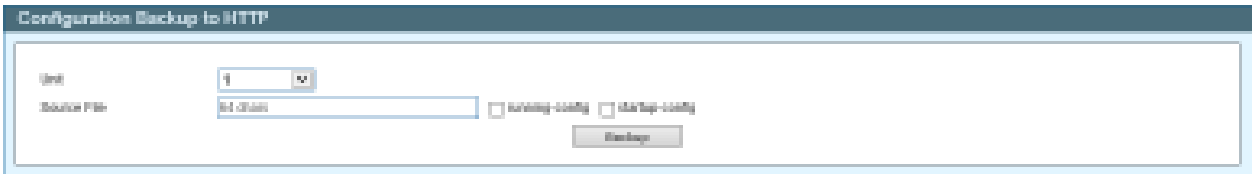


Figure 14-25 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

Figure 14-26 Language Management Window

The fields that can be configured are described below:

Parameter	Description
Language File	Click the **Browse** button to navigate to the location of the firmware file located on the local PC.

Click the **Apply** button to initiate the language pack installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

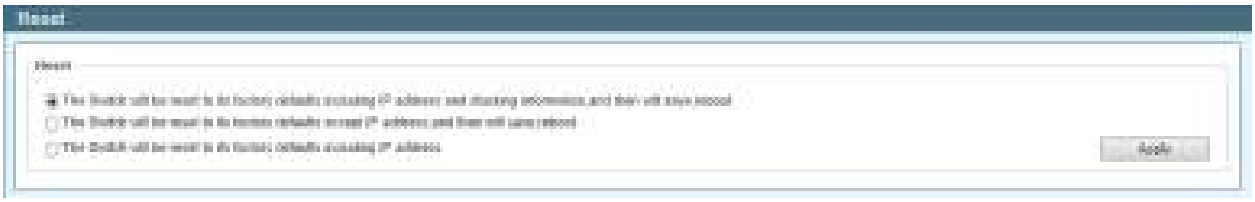


Figure 14-27 Reset Window

Select one of the following options:

- **The Switch will be reset to its factory defaults including IP address and stacking information**, **and the will save**, **reboot.** - To reset the Switch's configuration to its factory default settings.
- **The Switch will be reset to its factory default except IP address**, **and then will save**, **reboot** - To reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.
- **The Switch will be reset to its factory defaults including IP address** - To reset the Switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the Switch.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:

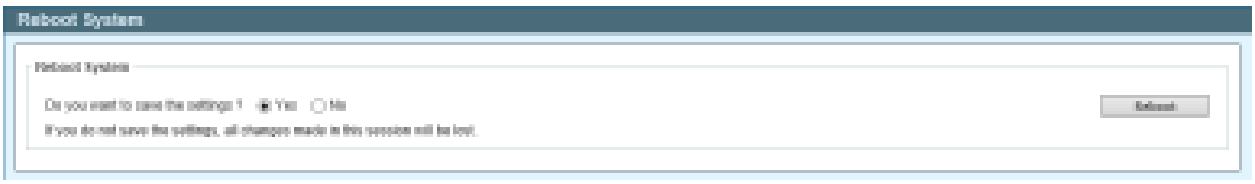


Figure 14-28 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration or the file system of the Switch. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

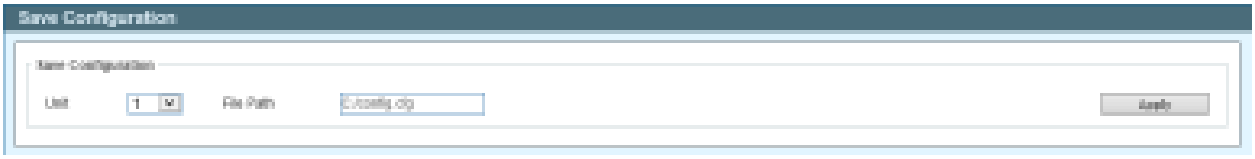


Figure 14-29 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here.
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

Help

Click this option to access the built-in Surveillance Help window.

After clicking the **Help** option, the following window will appear.

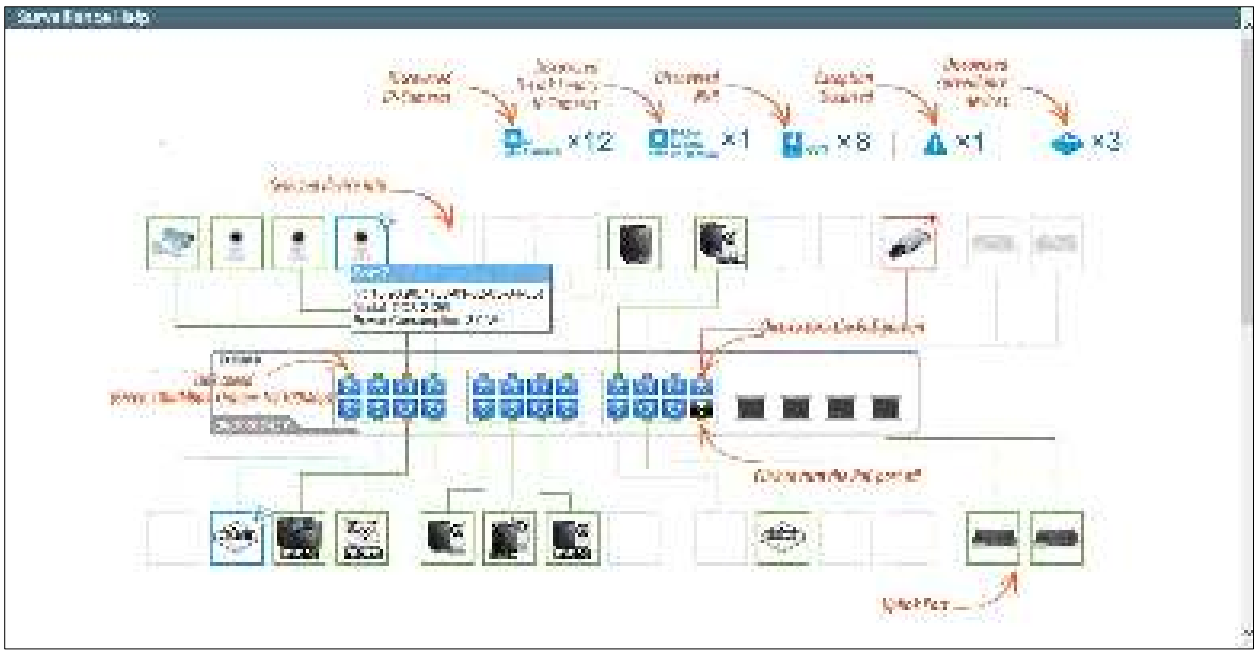


Figure 14-30 Help (Diagram) Window

Figure 14-31 Help (Table) Window

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Standard Mode

Click the **Standard Mode** button in the toolbar to change the Web UI mode and style from Surveillance Mode to Standard Mode.

NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

Logout

Click this option to log out of the Web UI of the Switch

Appendix A - System Log Entries

The following tables list the system log entries and their corresponding meanings that will appear in the System Log of this switch.

802.1X

Log Description	Severity
Event Description: 802.1X Authentication failure. Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: reason: The reason for the failed authentication. The possible reason may be: (1) user authentication failure. (2) no server(s) responding. (3) no servers configured. (4) no resources. (5) user timeout expired. username: The user that is being authenticated. interface-id: The switch interface number. mac-address: The MAC address of the authenticated device.	Critical
Event Description: 802.1X Authentication successful. Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: username: The user that is being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.	Informational

AAA

Log Description	Severity
Event Description: This log will be generated when AAA global state is enabled or disabled. Log Message: AAA is <status> Parameters Description: status: The status indicates the AAA enabled or disabled.	Informational
Event Description: This log will be generated when login successfully. Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. Username: It indicates the username for authentication.	Informational
Event Description: This log will be generated when login failure.	Warning

Log Description	Severity
Log Message: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	
Event Description: This log will be generated when the remote server does not respond to the login authentication request. Log Message: Login failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address. username: It indicates the username for authentication.	Warning
Event Description: This log will be generated when enable privilege successfully. Log Message: Successful enable privilege through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. Username: It indicates the username for authentication.	Informational
Event Description: This log will be generated when enable privilege failure. Log Message: Enable privilege failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event Description: This log will be generated when the remote server does not respond to the enable password authentication request. Log Message: Enable privilege failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol.	Warning

Log Description	Severity
server-ip: It indicates the AAA server IP address. username: It indicates the username for authentication.	
Event Description: This log will be generated when RADIUS assigned a valid VLAN ID attributes. Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) Parameters Description: server-ip: It indicates the RADIUS server IP address. vid: The assign VLAN ID that authorized by from RADIUS server. Interface-id: It indicates the port number of the client authenticated. Username: It indicates the username for authentication.	Informational
Event Description: This log will be generated when RADIUS assigned a valid bandwidth attributes. Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface -id> (Username: <username>) Parameters Description: server-ip: It indicates the RADIUS server IP address. Direction: It indicates the direction for bandwidth control, e.g.: ingress or egress. Threshold: The assign threshold of bandwidth that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. Username: It indicates the username for authentication.	Informational
Event Description: This log will be generated when RADIUS assigned a valid priority attributes. Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port <interface -id> (Username: <username>) Parameters Description: server-ip: It indicates the RADIUS server IP address. priority: The assign priority that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. Username: It indicates the username for authentication.	Informational
Event Description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource. Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port <interface -id> (<acl-script>) Parameters Description: server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server.	Warning
Event Description: This log is generated when the RADIUS assigned ACL script is applied to the system due to insufficient resources. Log Message: RADIUS server <server-ip> assigns <username> ACL success at port < interface -id> (<acl-script>) Parameters Description: server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server.	Informational

ARP Spoofing Prevention

Log Description	Severity
Event Description: A fake ARP packet detected by ARP Spoofing Prevention. Log Message: Gateway <ipaddr> is under attack by <macaddr> from <interface-id> Parameters Description: ipaddr: The IP address of the gateway. macaddr: The MAC address of a hacker. interface-id: The interface where a hacker is located.	Warning

Auto Save Configuration

Log Description	Severity
Event Description: Record the event when the configure information of DDP is saved automatically. Log Message:CONFIG-6-DDPSAVECONFIG: [Unit <unitID>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) Parameters Description: Unit: Box ID username: Represent current login user. ipaddr: Represent client IP address.	Informational

Auto Surveillance VLAN

Log Description	Severity
Event Description: When a new surveillance device is detected on an interface. Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: Interface name. mac-address: Surveillance device MAC address.	Informational
Event Description: When an interface which is enabled surveillance VLAN joins the surveillance VLAN automatically. Log Message: <interface-id> add into surveillance VLAN <vid> Parameters Description: interface-id: Interface name. vid: VLAN ID.	Informational
Event Description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent. Log Message: <interface-id> remove from surveillance VLAN <vid> Parameters Description: interface-id: Interface name. vid: VLAN ID.	Informational
Event Description: When an IPC is added in the surveillance VLAN, the log message will be sent. Log Message: ASV: Add IPC(<ipaddr>) Parameters Description: ipaddr: Represent the IP address of the IPC.	Informational

Log Description	Severity
Event Description: When an IPC is removed from the surveillance VLAN, the log message will be sent. Log Message: ASV: Remove IPC(<ipaddr>) Parameters Description: ipaddr: Represent the IP address of the IPC.	Informational
Event Description: When an NVR is added in the surveillance VLAN, the log message will be sent. Log Message: ASV: Add NVR(<ipaddr>) Parameters Description: ipaddr: Represent the IP address of the NVR.	Informational
Event Description: When an NVR is removed from the surveillance VLAN, the log message will be sent. Log Message: ASV: Remove NVR(<ipaddr>) Parameters Description: ipaddr: Represent the IP address of the NVR.	Informational
Event Description: When the mode of ASV 2.0 is changed by Web GUI, the log message will be sent. Log Message: ASV: Mode change from <mode> to <mode> Parameters Description: mode: Represent the mode of ASV 2.0 and the mode can be standard or surveillance.	Informational

BPDU Attack Protection

Log Description	Severity
Event Description: Record the event when the BPDU attack happened. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Parameters Description: interface-id: Interface on which detected STP BPDU attack. mode: BPDU Protection mode of the interface. Mode can be drop, block, or shutdown	Informational
Event Description: Record the event when the STP BPDU attack recovered. Log Message: <interface-id> recover from BPDU under protection state Parameters Description: interface-id: Interface on which detected STP BPDU attack.	Informational

Configuration/Firmware

Log Description	Severity
Event description: Firmware upgraded successfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address.	Informational

Log Description	Severity
pathFile: Path and file name on server.	
Event description: Firmware upgraded unsuccessfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event description: Firmware uploaded successfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event description: Firmware uploaded unsuccessfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event description: Configuration downloaded successfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event description: Configuration downloaded unsuccessfully.	Warning

Log Description	Severity
Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	
Event description: Configuration uploaded successfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event description: Configuration saved to flash by console. Log Message: [Unit <unitID>,]Configuration saved to flash by console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Configuration saved to flash by remote. Log Message: [Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters description: unitID: The unit ID. username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Log message uploaded successfully. Log Message: [Unit <unitID>,] Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>])	Informational

Log Description	Severity
Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address.	
Event description: Log message uploaded unsuccessfully. Log Message: [Unit <unitID>,] Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address.	Warning
Event description: Unknown type files downloaded unsuccessfully. Log Message: [Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning

NOTE: 1. The user's session refers to Console, Web, SNMP, Telnet, and SSH sessions.
2. If the Switch is in the standalone state, there will be no unit ID in the log message.
3. If the configuration or firmware was downloaded or uploaded through the console, there will be no IP address and MAC address information in the log message.

DAI

Log Description	Severity
Event Description: This log will be generated when DAI detect invalid ARP packet. Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) Parameters Description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	Warning
Event Description: This log will be generated when DAI detect valid ARP packet. Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>).	Informational

Log Description	Severity
Parameters Description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	

DDM

Log Description	Severity
Event Description: when the any of SFP parameters exceeds from the warning threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded Parameters Description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Warning
Event Description: when the any of SFP parameters exceeds from the alarm threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded Parameters Description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Critical
Event Description: when the any of SFP parameters recovers from the warning threshold. Log Message: Optical transceiver <interface-id> <component> back to normal Parameters Description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power	Warning

DHCPv6 Client

Log Description	Severity
Event Description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled]	Informational

Log Description	Severity
Parameters Description: <ipif-name>: Name of the DHCPv6 client interface.	
Event Description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name> Parameters Description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The ipv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing Parameters Description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The ipv6 address obtained from a DHCPv6 server renews success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success Parameters Description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The ipv6 address obtained from a DHCPv6 server starts rebinding. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding Parameters Description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The ipv6 address obtained from a DHCPv6 server rebinds success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success Parameters Description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The ipv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted Parameters Description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational

DHCPv6 Relay

Log Description	Severity
Event Description: DHCPv6 relay on a specify interface's administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Parameters Description:	Informational

Log Description	Severity
<ipif-name>: Name of the DHCPv6 relay agent interface.	

DNS Resolver

Log Description	Severity
Event Description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted. Log Message: Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domainname: the domain name string. ipaddr: IP address.	Informational

DoS Prevention

Log Description	Severity
Event Description: Detect DOS attack. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>) Parameters Description: dos-type: DOS attack type ip-address: IP address. interface-id: Interface name	Notice

ErrDisable

Log Description	Severity
Event Description: When a port enters the error-disabled state. Log Message: Port <interface-id> enters error disable state due to <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning
Event Description: When a port leaves the error-disabled state. Log Message: Port <interface-id> leaves the error disable state which is previously caused by <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning
Event Description: When a port enters the error-disabled state. Log Message: Port <interface-id> VLAN <vid> enters error disable state due to <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning

Log Description	Severity
vid: The VLAN ID.	
Event Description: When a port leaves the error-disabled state. Log Message: Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid: The VLAN ID.	Warning

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
Event Description: Port is linked on half duplex mode. Log Message: ASV: Port < interface-id> Half duplex detected Parameters Description: interface-id: Interface name	Informational

JWAC

Log Description	Severity
Event Description: when a host has passed the authentication. Log Message: JWAC host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: Username: The host username. IP: The host IP address mac-address: The host MAC addresses. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Informational
Event Description: When a host fail to pass the authentication. Log Message: JWAC host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: Username: The host username. IP: The host IP address mac-address: The host MAC addresses. interface-id: The interface on which the host is authenticated.	Critical

Log Description	Severity
vlan-id: The VLAN ID on which the host exists.	
Event Description: when the authorized user number on the whole device has reached the maximum user limit. Log Message: JWAC enters stop learning state	Warning
Event Description: when the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: JWAC recovers from stop learning state	Warning

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up. Log Message: Link Aggregation Group <group_id> link up Parameters Description: group_id: The group id of the link down aggregation group.	Informational
Event Description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group_id> link down Parameters Description: group_id: The group id of the link down aggregation group.	Informational
Event Description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id> Parameters Description: ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
Event Description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id> Parameters Description: ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

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 detect loop. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Parameters Description: interface-id: Interface on which loop is detected. vlan-id: VLAN 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
Event Description: Record the event when an interface loop recovered.	Critical

Log Description	Severity
Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered Parameters Description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	
Event Description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number. Log Message: Loop VLAN numbers overflow	Critical

LLDP-MED

Log Description	Severity
Event Description: LLDP-MED topology change detected. Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice
Event Description: Conflict LLDP-MED device type detected. Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5)	Notice

Log Description	Severity
6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	
Event Description: Incompatible LLDP-MED TLV set detected. Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice

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. username: Represent current login user.	Informational

Log Description	Severity
Event 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
Event Description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>)	Critical

Log Description	Severity
Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	
Event Description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

MAC-based Access Control

Log Description	Severity
Event Description: A host has passed the authentication. Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists after it is authenticated.	Informational
Event Description: A host has aged out. Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists before it is aged out.	Informational
Event Description: A host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The originated VLAN ID on which the host exists.	Critical
Event Description: The authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state	Warning
Event Description: The authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: MAC-based Access Control recovers from stop learning state	Warning
Event Description: The authorized user number on an interface has reached the maximum user limit. Log Message: <interface-id> enters MAC-based Access Control stop learning state Parameters Description: interface-id: The interface on which the host is authenticated.	Warning

Log Description	Severity
Event Description: The authorized user number on an interface is below the maximum user limit in a time interval. Log Message: <interface-id> recovers from MAC-based Access Control stop learning state Parameters Description: interface-id: The interface on which the host is authenticated.	Warning

MSTP Debug Enhancement

Log Description	Severity
Event Description: Used to record the event that Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
Event Description: Used to record the event that Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
Event Description: Used to record MSTP instance topology change event. Log Message: Topology changed (Instance : <Instance-id>,<interface_id>, MAC:<macaddr>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. interface_id: The port number which detect or receive topology change information. macaddr: The system of bridge mac address.	Notice
Event Description: Used to record MSTP instance new root bridge selected. Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :<priority>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. macaddr: The system of bridge mac address. priority: The bridge priority value must be divisible by 4096.	Informational
Event Description: Used to record MSTP instance new root port selected. Log Message: New root port selected (Instance:<Instance-id>, <interface_id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. interface_id: The port number which detect or receive topology change information.	Notice
Event Description: Used to record MSTP instance port state change event. Log Message: Spanning Tree port status change (Instance :<Instance-id>, <interface_id>) <old_status> -> <new_status> Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. interface_id: The port number which detect or receive topology change information. old status: new status: The port of STP state. The value may be Disable, Discarding, Learning, Forwarding	Notice

Log Description	Severity
Event description: Used to record MSTP instance port role change event. Log Message: Spanning Tree port role change (Instance :<Instance-id>, <interface_id>) <old_role> -> <new_role> Parameters description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. Interface_id: The port number which detect or receive topochange information. old role: new role : The port role of stp. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	Informational
Event Description: Use to record action to create an MST instance. Log Message: Spanning Tree instance created (Instance :<Instance-id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	Informational
Event Description: Use to record action to delete an MST instance. Log Message: Spanning Tree instance deleted (Instance :<Instance-id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	Informational
Event Description: Use to record action to change the STP version. Log Message: Spanning Tree version change (new version :<new_version>) Parameters Description: new_version: Running under which version of STP.	Informational
Event Description: Used to record the configuration name and revision level changed in the MST Configuration Identification. Log Message: Spanning Tree MST configuration ID name and revision level change (name: <name>, revision level <revision_level>) Parameters Description: name: The name given for a specified MST region. revision_level: Switches using the same given name but with a different revision level are considered members of different MST regions.	Informational
Event Description: Use to record action to maps a VLAN(s) to an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. startvlanid: The start vid of add vlan range. endvlanid: The end vid of add vlan range.	Informational
Event Description: Use to record action to delete a VLAN(s) from an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. startvlanid: The start vid of delete vlan range.	Informational

Log Description	Severity
endvlanid: The end vid of delete vlan range.	
Event Description: Used to record the event that port role change to alternate due to guard root. Log Message: Spanning Tree port role change (Instance :<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. Interface_id: The port number which detect the event.	Informational

Peripheral

Log Description	Severity
Event Description: Fan Recovered. Log Message: Unit <id>, <fan-descr> back to normal Parameters Description: Unit <id>: The unit ID. fan-descr: The FAN ID and position.	Critical
Event Description: Fan Fail. Log Message: Unit <id> <fan-descr> failed Parameters Description: Unit <id>: The unit ID. fan-descr: The FAN ID and position.	Critical
Event Description: Temperature sensor enters alarm state. Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> Parameters Description: unitID: The unit ID. thermal-sensor-descr: The sensor ID and position. degree: The current temperature.	Critical
Event Description: Temperature recovers to normal. Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal Parameters Description: unitID: The unit ID. thermal-sensor-descr: The sensor ID and position.	Critical
Event Description: Power failed. Log Message: Unit <unit-id> <power-descr> failed Parameters Description: unitID: The unit ID. power-descr: The power position and ID.	Critical
Event Description: Power is recovered. Log Message: Unit <unit-id> <power-descr> back to normal Parameters Description: unitID: The unit ID. power-descr: The power position and ID.	Critical
Event Description: Press the factory reset button. Log Message: Unit <unit-id> factory reset button pressed Parameters Description: unitID: The unit ID.	Critical

PoE

Log Description	Severity
Event Description: Total power usage threshold is exceeded Log Message: Unit <unit-id> usage threshold <percentage> is exceeded Parameters Description: unit-id: The box ID. percentage: The usage threshold.	Warning
Event Description: Total power usage threshold is recovered. Log Message: Unit <unit-id> usage threshold <percentage> is recovered Parameters Description: unit-id: The box ID. percentage: The usage threshold.	Warning
Event Description: PD doesn't reply the ping request. Log Message: PD alive check failed. (Port: <portNum>, PD: <ipaddr>) Parameters Description: portNum: The port number. ipaddr: The IP (IPv4/IPv6) address of PD.	Warning
Event Description: Power removal due to absence of Maintain Power Signature (MPS). Log Message: ASV: Port <port-type><interface-id> PoE MPS Absent Parameters Description: port-type: The port type. interface-id: The interface name.	Warning
Event Description: Short circuit condition detected. Log Message: ASV: Port <port-type><interface-id> PoE PD short Parameters Description: port-type: The port type. interface-id: The interface name.	Warning
Event Description: Overload condition detected. Log Message: ASV: Port <port-type><interface-id> PoE Overload Parameters Description: port-type: The port type. interface-id: The interface name.	Warning
Event Description: Power has been denied or removed due to fault. Log Message: ASV: Port <port-type><interface-id> PoE Power Denied Parameters Description: port-type: The port type. interface-id: The interface name.	Warning
Event Description: Power has been denied or removed due to overheat. Log Message: ASV: Port <port-type><interface-id> PoE Thermal Shutdown Parameters Description: port-type: The port type. interface-id: The interface name.	Warning
Event Description: PoE startup failure on port. Log Message: ASV: Port <port-type><interface-id> PoE Startup Failure Parameters Description: port-type: The port type. interface-id: The interface name.	Warning
Event Description: Cannot classify PD.	Warning

Log Description	Severity
Log Message: ASV: Port <port-type><interface-id> PoE Classification Failure Parameters Description: port-type: The port type. interface-id: The interface name.	

Port Security

Log Description	Severity
Event Description: Address full on a port. Log Message: MAC address <macaddr> causes port security violation on <interface-id> Parameters Description: macaddr: The violation MAC address. interface-id: The interface name.	Warning
Event Description: Address full on system. Log Message: Limit on system entry number has been exceeded	Warning

Safeguard

Log Description	Severity
Event Description: the host enters the mode of exhausted. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode Parameters Description: unit-id: The Unit ID	Warning
Event Description: the host enters the mode of normal. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode Parameters Description: unit-id: The Unit ID	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event Description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event Description: SSH server is disabled. Log Message: SSH server is disabled	Informational

Stacking

Log Description	Severity
Event Description: Hot insertion.	Informational

Log Description	Severity
Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion Parameters Description: unitID: Box ID. Macaddr: MAC address.	
Event Description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal Parameters Description: unitID: Box ID. Macaddr: MAC address.	Informational
Event Description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>) Parameters Description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain. unitID: Box ID. Macaddr: MAC address.	Informational
Event Description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>) Parameters Description: unitID: Box ID.	Informational
Event Description: Slave changed to master. Log Message: Slave changed to master. Master (Unit: <unitID>) Parameters Description: unitID: Box ID.	Informational
Event Description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>) Parameters Description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical
Event Description: Stacking port linkup. A Stacking port will act as a SIO interface or a member of a SIO interface (SIO Trunk). This log entry is only available on projects that stacking port has got a port number indicator on device's panel. Log Message: Stacking port <port> link up Parameters Description: port: Represents the logical port number of a Stacking port.	Critical
Event Description: Stacking port link down. A Stacking port will act as a SIO interface or a member of a SIO interface (SIO Trunk). This log entry is only available on projects that stacking port has got a port number indicator on device's panel. Log Message: Stacking port <port> link down Parameters Description: port: Represents the logical port number of a Stacking port.	Critical
Event Description: SIO interface linkup. For SIO Trunk, the first member port link up will trigger this event. Log Message: SIO interface Unit <unitID> <SIOn> link up Parameters Description: unitID: Box ID.	Critical

Log Description	Severity
SIOn: Represents the SIO interface number. Current Supported SIO interface number should be SIO1 and SIO2.	
Event Description: SIO interface link down. For SIO Trunk, the last member port link down will trigger this event. Log Message: SIO interface Unit <unitID> <SIOn> link down Parameters Description: unitID: Box ID. SIOn: Represents the SIO interface number. Current Supported SIO interface number should be SIO1 and SIO2.	Critical

Storm Control

Log Description	Severity
Event Description: Storm occurrence. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Parameters Description: Broadcast: Storm is resulted by broadcast packets(DA = FF:FF:FF:FF:FF:FF). Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast. Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets interface-id: The interface ID on which a storm is occurring.	Warning
Event Description: Storm cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Parameters Description: Broadcast: Broadcast storm is cleared. Multicast: Multicast storm is cleared. Unicast: Unicast storm (including both known and unknown unicast packets) is cleared. interface-id: The interface ID on which a storm is cleared.	Informational
Event Description: Port shut down due to a packet storm. Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm Parameters Description: interface-id: The interface ID on which is error-disabled by storm. Broadcast: The interface is disabled by broadcast storm. Multicast: The interface is disabled by multicast storm. Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).	Warning

System Log Summary

Log Description	Severity
Event Description: This log will be generated when system warm start. Log Message: [Unit <unitID>,]System warm start Parameters Description: unitID: The unit ID.	Critical
Event Description: This log will be generated when system cold start.	Critical

Log Description	Severity
Log Message: [Unit <unitID>,]System cold start Parameters Description: unitID: The unit ID.	
Event Description: This log will be generated when system start up. Log Message: [Unit <unitID>,]System started up. Parameters Description: unitID: The unit ID.	Critical

Telnet

Log Description	Severity
Event Description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
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

Log Description	Severity
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: interface-id: Interface name. vid: VLAN ID	Informational

Web

Log Description	Severity
Event Description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event Description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event Description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
Event Description: Web (SSL) session timed out. Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login SSL server.	Informational

Log Description	Severity
ipaddr: The IP address of SSL client.	
Event Description: Logout through Web(SSL). Log Message: Logout through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Web-Authentication

Log Description	Severity
Event Description: When a host has passed the authentication. Log Message: Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: Username: The host username. IP: The host IP address mac-address: The host MAC addresses. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Informational
Event Description: When a host fail to pass the authentication. Log Message: Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: Username: The host username. IP: The host IP address mac-address: The host MAC addresses. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Critical
Event Description: when the authorized user number on the whole device has reached the maximum user limit. Log Message: Web-Authentication enters stop learning state	Warning
Event Description: when the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: Web-Authentication recovers from stop learning state	Warning

Appendix B - Trap Entries

The following tables list the trap log entries and their corresponding meanings that will appear in the switch.

802.1X

Trap Name	Description	OID
dDot1xExtLoggedSuccess	The trap is sent when a host has successfully logged in (passed 802.1X authentication). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171 .14.30.0.1
dDot1xExtLoggedFail	The trap is sent when a host failed to pass 802.1X authentication (login failed). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171 .14.30.0.2

Authentication Fail

Trap Name	Description	OID
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

BPDU Attack Protection

Trap Name	Description	OID
dBpduProtectionAttackOccur	This trap is sent when the BPDU attack happened on an interface. Binding objects: (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.171 .14.47.0.1
dBpduProtectionAttackRecover	This trap is sent when the BPDU attack recovered on an interface. Binding objects: (1) ifIndex	1.3.6.1.4.1.171 .14.47.0.2

DDM

Trap Name	Description	OID
dDdmAlarmTrap	A notification is generated when an abnormal alarm situation occurs or recovers from an abnormal alarm	1.3.6.1.4.1.171 .14.72.0.1

Trap Name	Description	OID
	situation to normal status. Only when the current value> low warning or current value <high warning will send recover trap. Binding objects: (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	
dDdmWarningTrap	A notification is generated when an abnormal warning situation occurs, or recovers from an abnormal warning situation to normal status. Binding objects: (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.2

DHCP Server Screen Prevention

Trap Name	Description	OID
dDhcpFilterAttackDetected	When DHCP Server Screen is enabled, if the switch received the forge DHCP Server packet, the switch will trap the event if any attacking packet is received. Binding objects: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1

DoS Prevention

Trap Name	Description	OID
dDosPreveAttackDetectedPacket	The trap is sent when detect DoS attack. Binding objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.59.0.2

ErrDisable

Trap Name	Description	OID
dErrDisNotifyPortDisabledAssert	The trap is sent when a port enters into error disabled state. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
dErrDisNotifyPortDisabledClear	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2

General Management

Trap Name	Description	OID
dGenMgmtLoginFail	This trap is sent when the user login failed to the switch. Binding objects: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171 .14.165.0.1

Gratuitous ARP Function

Trap Name	Description	OID
agentGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171 .14.75.0.1

IMPB

Trap Name	Description	OID
dImpbViolationTrap	The address violation notification is generated when IP-MAC-Port Binding address violation is detected. Binding objects: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress	1.3.6.1.4.1.171 .14.22.0.1

LACP

Trap Name	Description	OID
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1. 5.4
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1. 5.3

LBD

Trap Name	Description	OID
dLbdLoopOccurred	This trap is sent when an interface loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171 .14.46.0.1
dLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171 .14.46.0.2
dLbdVlanLoopOccurred	This trap is sent when an interface with a VID loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .14.46.0.3
dLbdVlanLoopRestart	This trap is sent when an interface loop with a VID restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171 .14.46.0.4

LLDP

Trap Name	Description	OID
lldpRemTablesChange	An lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2. 0.0.1
lldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8802.1.1.2. 1.5.4795.0.1

MAC-based Access Control

Trap Name	Description	OID
dMacAuthLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171 .14.153.0.1

Trap Name	Description	OID
dMacAuthLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171 .14.153.0.2
dMacAuthLoggedAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171 .14.153.0.3

MAC-notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicates the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfo	1.3.6.1.4.1.171 .14.3.0.1

MSTP

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

Peripheral

Trap Name	Description	OID
dEntityExtPowerStatusChg	Power Status change notification. Binding objects: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.171 .14.5.0.3
dEntityExtFanStatusChg	Fan status change notification. Binding objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171 .14.5.0.1
dEntityExtThermalStatusChg	Temperature status change notification. Binding objects:	1.3.6.1.4.1.171 .14.5.0.2

Trap Name	Description	OID
	(1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	
dEntityExtFactoryResetButton	Press factory reset button notification. Binding objects: (1) dEntityExtUnitIndex	1.3.6.1.4.1.171 .14.5.0.5

PoE

Trap Name	Description	OID
pethMainPowerUsageOnNotification	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 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
dPoeIfPowerDeniedNotification	This Notification indicates if PSE state diagram enters the state POWER_DENIED. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171 .14.24.0.1
dPoeIfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171 .14.24.0.2
dPoeIfPowerShortCircuitNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortShortCounter	1.3.6.1.4.1.171 .14.24.0.3
dPoeIfPdAliveFailOccurNotification	This trap indicates if the PD device has the stop working or no response problem. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseGroupIndex (2) pethPsePortIndex (3) dPoeIfPdAliveCfgPdIpType (4) dPoeIfPdAliveCfgPdIpAddr	1.3.6.1.4.1.171 .14.24.0.4

Port

Trap Name	Description	OID
linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

Port Security

Trap Name	Description	OID
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171.14.8.0.1

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Trap Name	Description	OID
dSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhaust. Binding objects:	1.3.6.1.4.1.171.14.19.1.1.0.1

Trap Name	Description	OID
	(1) dSafeguardEngineCurrentMode	
dSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171 .14.19.1.1.0.2

Stack

Trap Name	Description	OID
dStackInsertNotification	Unit Hot Insert notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171 .14.9.0.1
dStackRemoveNotification	Unit Hot Remove notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171 .14.9.0.2
dStackFailureNotification	Unit Failure notification. Binding objects: (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.171 .14.9.0.3
dStackTPChangeNotification	The stacking topology change notification. Binding objects: (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.171 .14.9.0.4
dStackRoleChangeNotification	The stacking unit role change notification. Binding objects: (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.171 .14.9.0.5

SIM

Trap Name	Description	OID
swSingleIPMSColdStart	The commander switch will send this notification when its member generates a cold start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.11
swSingleIPMSWarmStart	The commander switch will send this notification when its member generates a warm start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.12
swSingleIPMSLinkDown	The commander switch will send this notification when its member generates a link down notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171 .12.8.6.0.13

Trap Name	Description	OID
swSingleIPMSLinkUp	The commander switch will send this notification when its member generates a link up notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171 .12.8.6.0.14
swSingleIPMSAuthFail	The commander switch will send this notification when its member generates an authentication failure notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.15
swSingleIPMSnewRoot	The commander switch will send this notification when its member generates a new root notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.16
swSingleIPMSTopologyChange	The commander switch will send this notification when its member generates a topology change notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171 .12.8.6.0.17

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

Storm Control

Trap Name	Description	OID
dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .14.25.0.1
dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171 .14.25.0.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.171 .14.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.171 .14.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.171 .14.14.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.171 .14.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.171 .14.14.0.5

Web-Authentication

Trap Name	Description	OID
dWebAuthLoggedSuccess	The trap is sent when a host has successfully logged in (passed Web-Authentication). Binding objects: (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.171 .14.154.0.1
dWebAuthLoggedFail	The trap is sent when a host has failed to pass Web-Authentication (login failed). Binding objects: (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.171 .14.154.0.2

Appendix C - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DGS-1510 is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, JWAC, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps), and 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0”, the effective bandwidth will be set “no_limited”, and if the bandwidth is configured less than “0” or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0 to 7	Required

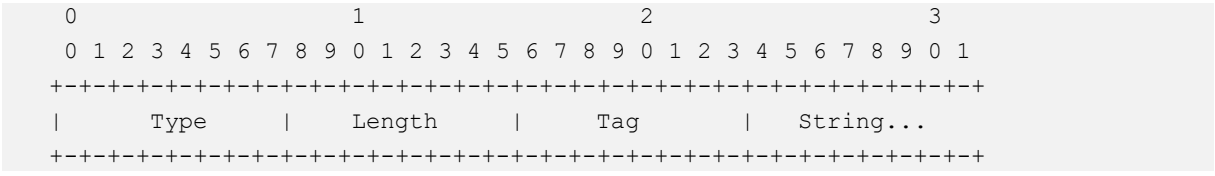
If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.



The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others	When the switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the switch will check all existing

Tag field value	String field format
(0x00, 0x03 ~ 0x1F, >0x1F)	VLAN IDs and check if there is one matched. If the switch can find one matched, it will move to that VLAN. If the switch cannot find the matched VLAN ID, it will think the VLAN setting string as a “VLAN Name”. Then it will check that it can find out a matched VLAN Name.

NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3), and the 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

To assign the **ACL** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for an ACL.

VSA14 ACL Script

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	Used to assign the ACL script. The format is based on **Access Control List (ACL) Commands**.	ACL Script For example: **ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;**	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), and the 802.1X, MAC-based Access Control, JWAC or WAC authentication is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject. For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

NAS-Filter-Rule (92)

The table below shows the parameters for NAS-Filter-Rule:

RADIUS Tunnel Attribute	Description	Value	Usage
NAS-Filter-Rule	This attribute indicates the filter rules to be applied for the user.	A string (concatenating the individual filter rules, separated by a NULL (0x00) octet)	Required

Filter Rule Format

Use the permit command to add a permit entry. Use the deny command to add a deny entry.

{permit | deny} in tcp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***TCP-PORT-RANGE***]**

{permit | deny} in udp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***UDP-PORT-RANGE***]**

{permit | deny} in icmp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***ICMP-TYPE***]**

{permit | deny} in ip from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

{permit | deny} in *IP-PROT-VALUE* **from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

Parameters

Parameter	Description
in	Specifies the ingress traffic.
any	Specifies any source IP address or any destination IP address to be configured.
DST-IP-ADDR	Specifies a specific destination host IP address.
DST-IP-NET-ADDR	Specifies a group of destination IP addresses with a mask width of the form 1.2.3.4/24.
DST-IPV6-ADDR	Specifies a specific destination host IPv6 address.
DST-IPV6-NET-ADDR	Specifies a group of destination IPv6 network of the form 2000::1/64.
tcp, udp, icmp	Specifies Layer 4 protocols.
ip	Specifies that any protocol will match.
IP-PROT-VALUE	Specifies the IP protocol value. The valid value is from 0 to 255.
TCP-PORT-RANGE	(Optional) Specifies to match TCP port or port range. The form is like: 22-23, 80.
UDP-PORT-RANGE	(Optional) Specifies to match UDP port or port range. The form is like: 56, 67-68.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.

Example

This example shows how to deny host's telnet service on the RADIUS server.

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

This example shows how to limit host to access a group of IP address on the RADIUS server.

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	IPv6 filter rule, Used to accept IPv6 address related inputs.	This attribute indicates either of the following IP modes for NAS-Filter-Rule 1=Forward IPv4 and IPv6 traffic 2=Forward IPv4-only traffic (drop any IPv6 traffic) If this attribute is not assigned by RADIUS server, forward IPv4-only traffic, any IPv6 packet will be dropped.	Required

NOTE: If both proprietary ACL script (VSA14) and standard NAS-Filter-Rule (92) are assigned at the same time, NAS-Filter-Rule (92) will take effect, and VSA14 will be ignored.

Appendix D - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link switch.

RADIUS Authentication Attributes:

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID

Number	IETF Attribute
95	NAS-IPv6-Address

RADIUS Accounting Attributes:

Number	IETF Attribute
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

Appendix E - ERPS Information

Only hardware-based ERPS (external PHY) supports the fast link drop interrupt feature with a recovery time of 50ms.

Model Name	ERPS	Port 1 to 20
DGS-1510-20	Hardware-based	
	Software-based	V

Model Name	ERPS	Port 1 to 8	Port 9 to 28
DGS-1510-28 DGS-1510-28P DGS-1510-28X DGS-1510-28XMP	Hardware-based	V	
	Software-based		V

Model Name	ERPS	Port 1 to 8	Port 9 to 24	Port 25 to 32	Port 33 to 52
DGS-1510-52	Hardware-based	V		V	
	Software-based		V		V

Model Name	ERPS	Port 1 to 8	Port 9 to 24	Port 25 to 32	Port 33 to 48	Port 49 to 50	Port 51 to 52
DGS-1510-52X (HW: A1)	Hardware-based	V		V		V	
	Software-based		V		V		V

Model Name	ERPS	Port 1 to 16	Port 17 to 24	Port 25 to 40	Port 41 to 48	Port 49 to 52
DGS-1510-52X (HW: A2) DGS-1510-52XMP	Hardware-based		V		V	
	Software-based	V		V		V