D-Link
Building Networks for People

xStack®

Web UI Reference Guide

Product Model: xStack® DES-3810 Series
Layer 3 Managed Ethernet Switch
Release 2.20

IPv6 READY

March 2012 P/N 651ES3810045G

Table of Contents

Intended Readers

The ***DES-3810 Series Web UI Reference Guide*** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: **You have mail**. **Bold** font is also used to represent filenames, program names and commands. For example: **use the copy command**.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type *filename* means that the actual filename should be typed instead of the word shown in italic.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Table 1. Typographical Conventions

Notes, Notices, and Cautions

A **NOTE** indicates important information that helps make better use of the device.

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

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

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon () is used to indicate cautions and precautions that need to be reviewed and followed.

Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment observe the following precautions:

- Observe and follow service markings.
  - Do not service any product except as explained in the system documentation.
  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose the user to electrical shock.
  - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - Damage to the power cable, extension cable, or plug.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when the operating instructions are correctly followed.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in the troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of the system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If unsure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging the system, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at the Switch's location:
  - 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
  - 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If using an extension cable is necessary, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect the system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also, refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

- Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.

CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

NOTE: A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.

CAUTION: Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if uncertain that suitable grounding is available.

CAUTION: The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside the system. To prevent static damage, discharge static electricity from your body before touching any of the electronic components, such as the microprocessor. This can be done by periodically touching an unpainted metal surface on the chassis.

The following steps can also be taken prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until ready to install the component in the system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

Chapter 1 Web-based Switch Configuration

Introduction

All software functions of the DES-3810 Series Switch can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Logging in to the Web Manager

To begin managing the Switch, simply run the browser installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

NOTE: The factory default IP address is 10.90.90.90.

This opens the management module's user authentication window, as seen below.

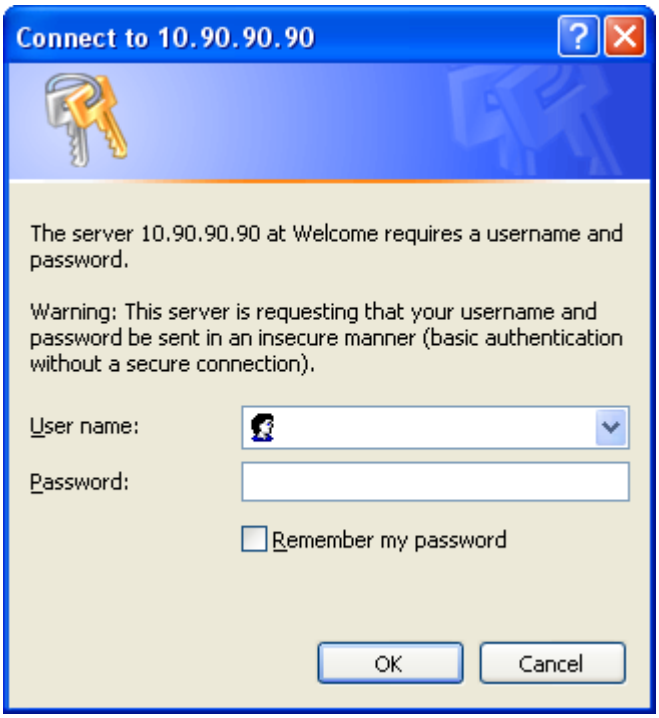


Figure 1-1 Enter Network Password window

Leave both the **User Name** field and the **Password** field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management screens, allows the user to view performance statistics, and permits graphical monitoring of the system status.

Areas of the User Interface

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

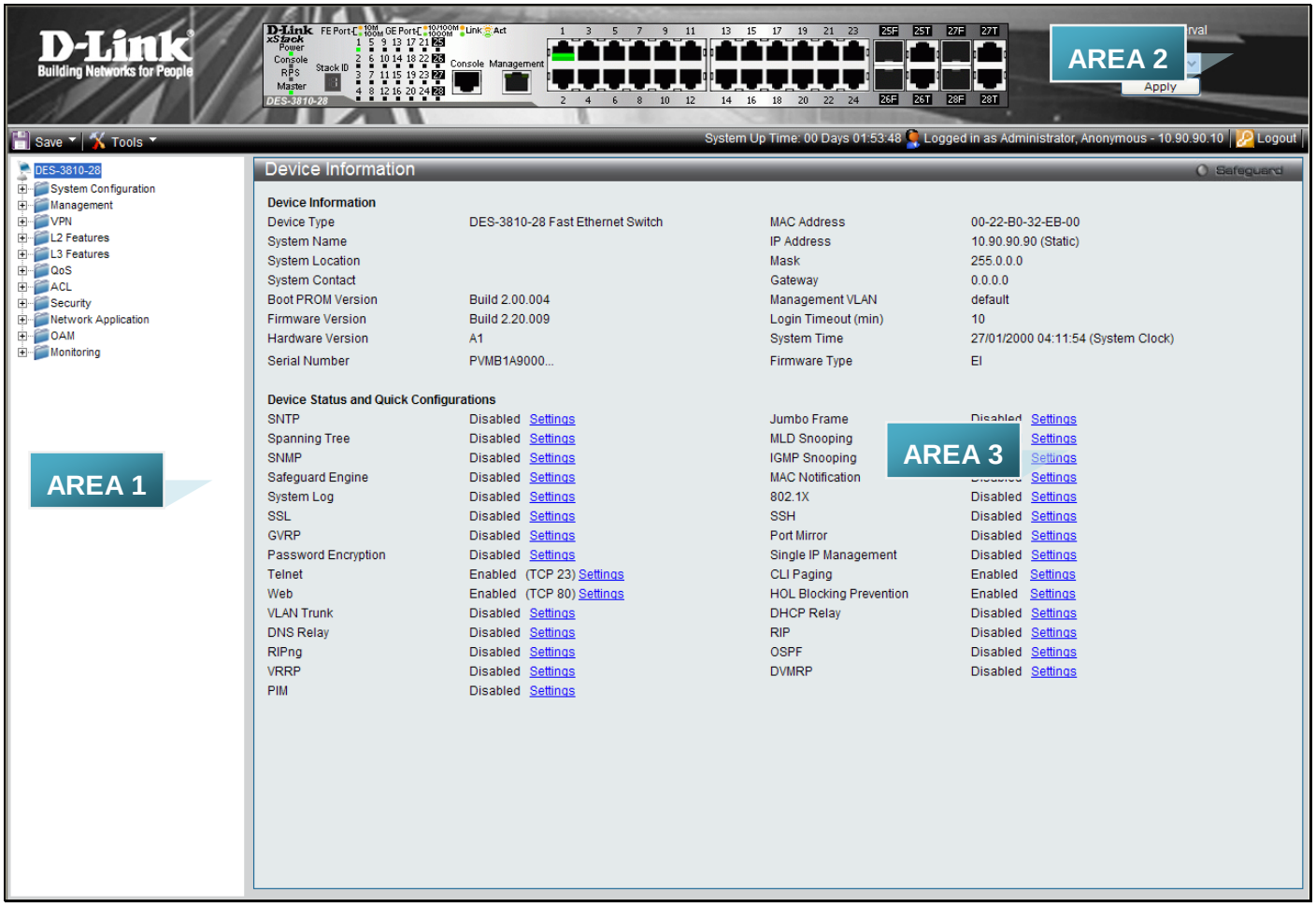


Figure 1-2. Main Web-Manager Screen

Area Number	Function
Area 1	Select the menu or window to display. Open folders and click the hyperlinked menu buttons and subfolders contained within them to display menus. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports, console and management port, showing port activity. Some management functions, including save, reboot, download and upload are accessible here.
Area 3	Presents switch information based on user selection and the entry of configuration data.

Table 2. Areas of the User Interface

Web Pages

When connecting to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list of the main folders available in the Web interface:

System Configuration - In this section the user will be able to configure features regarding the Switch's configuration.

Management - In this section the user will be able to configure features regarding the Switch's management.

L2 Features - In this section the user will be able to configure features regarding the Layer 2 functionality of the Switch.

L3 Features - In this section the user will be able to configure features regarding the Layer 3 functionality of the Switch.

QoS - In this section the user will be able to configure features regarding the Quality of Service functionality of the Switch.

ACL - In this section the user will be able to configure features regarding the Access Control List functionality of the Switch.

Security - In this section the user will be able to configure features regarding the Switch's security.

Network Application - In this section the user will be able to configure features regarding network applications handled by the Switch.

OAM - In this section the user will be able to configure features regarding the Switch's operations, administration and maintenance (OAM).

Monitoring - In this section the user will be able to monitor the Switch's configuration and statistics.

NOTE: Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Chapter 2 System Configuration

Device Information

This window contains the main settings for all the major functions for the Switch. It appears automatically when you log on to the Switch. To return to the **Device Information** window after viewing other windows, click the **DES-3810-28** link.

The **Device Information** window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version, Hardware Version, and many other important types of information. This is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status.

Many functions are hyper-linked for easy access to enable quick configuration from this window.

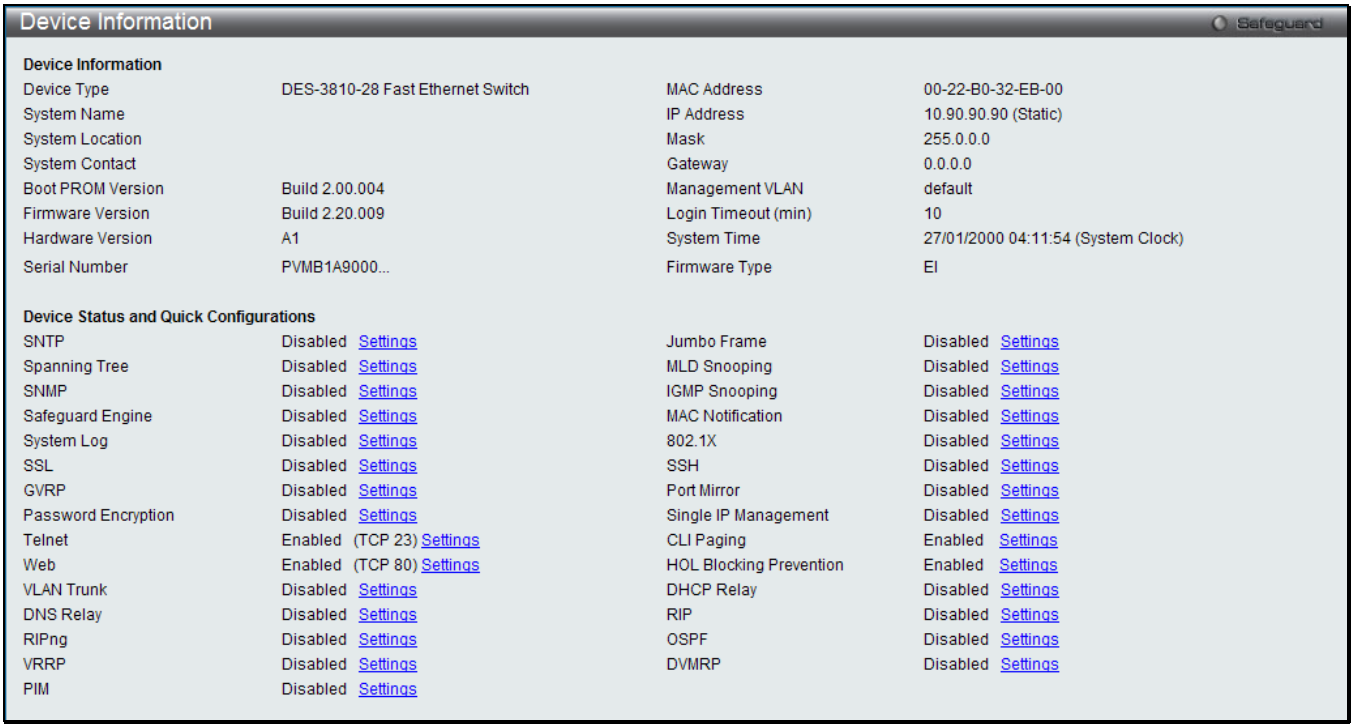


Figure 2-1 Device Information window (EI Mode Only)

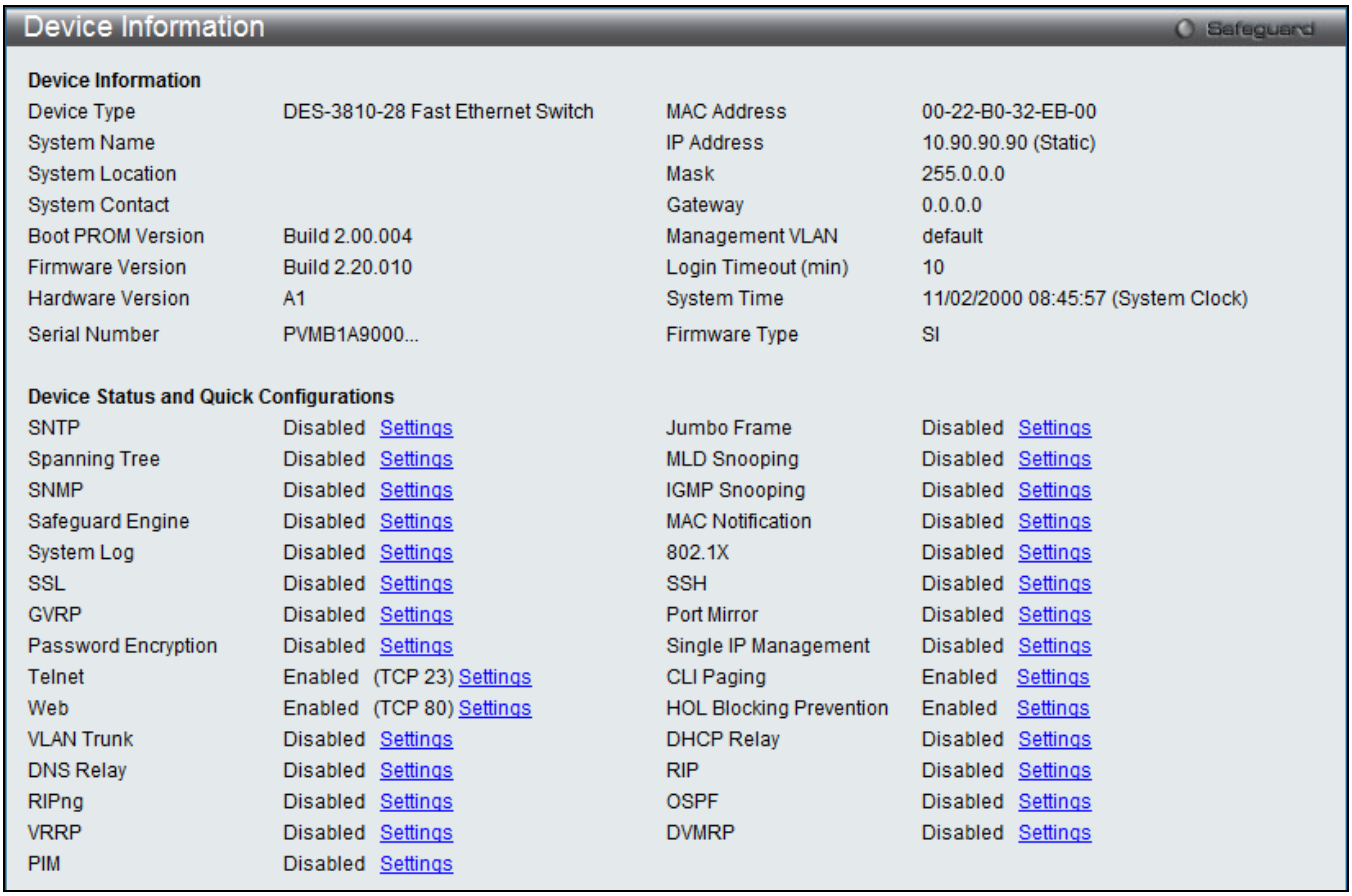


Figure 2-2 Device Information window (SI Mode Only)

Click on the Settings link to navigate to the appropriate feature page for configuration.

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 Configuration > System Information Settings**, as shown below:

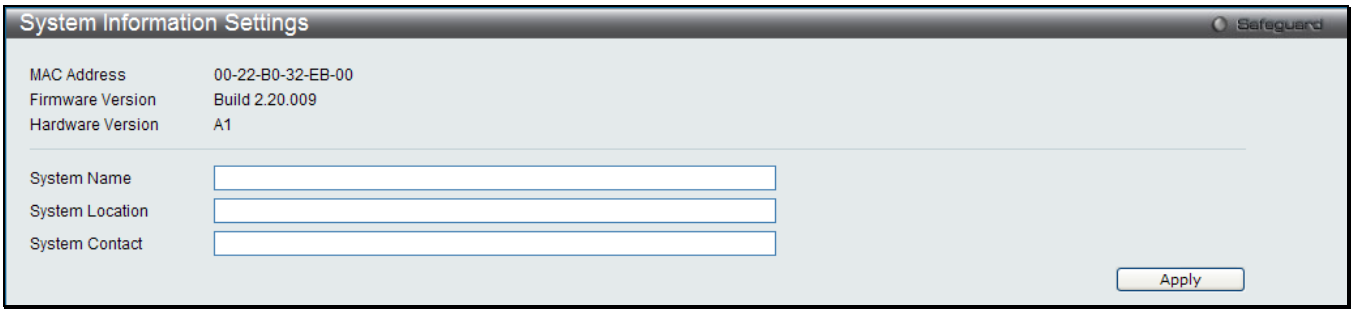


Figure 2-3 System Information Settings window

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.
System Contact	Enter a contact name for the Switch, if so desired.

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

Port Configuration

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 **System Configuration > Port Configuration > DDM > DDM Settings**, as show below:

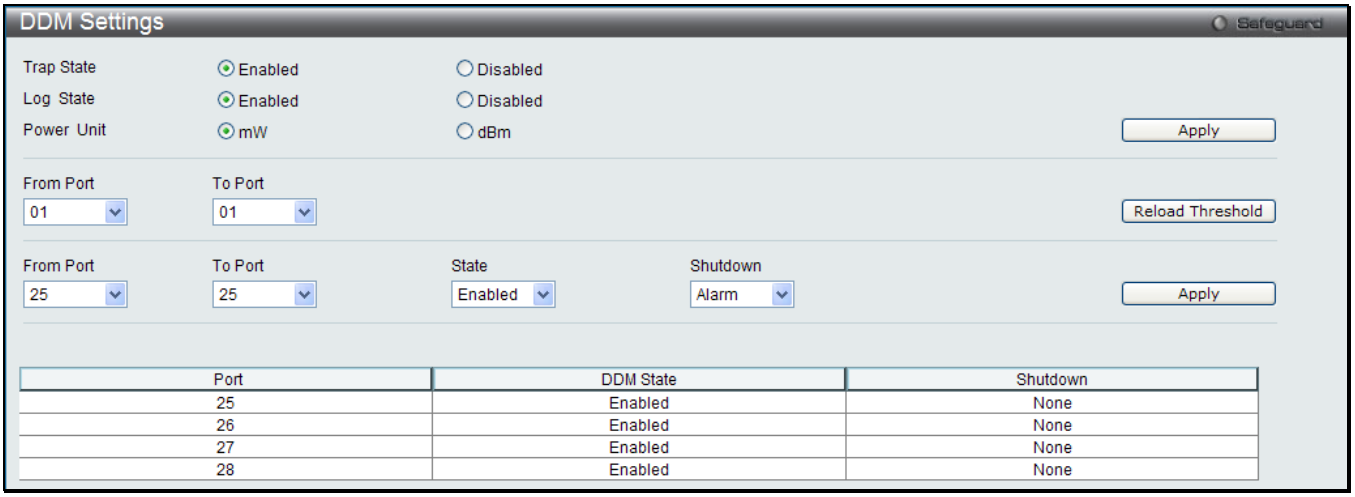


Figure 2-4 DDM Settings window

The fields that can be configured are described below:

Parameter	Description
Trap State	Specify whether to send the trap, when the operating parameter exceeds the alarm or warning threshold.
Log State	Specify whether to send the log, when the operating parameter exceeds the alarm or warning threshold.
Power Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shutdown 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.

Click the **Reload Threshold** button to reload the DDM threshold configuration.

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 **System Configuration > Port Configuration > DDM > DDM Temperature Threshold Settings**, as show below:

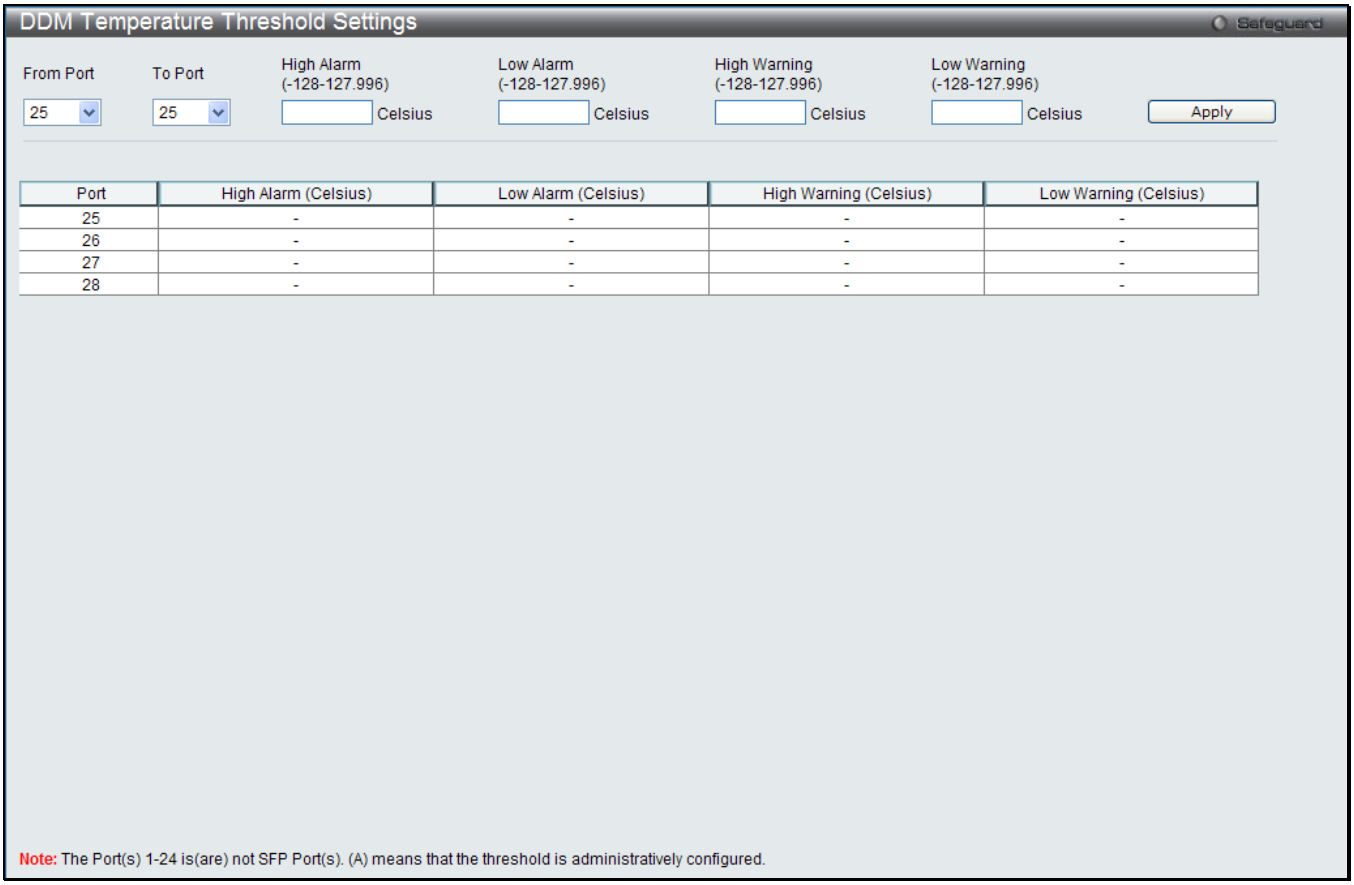


Figure 2-5 DDM Temperature Threshold Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
High Alarm (-128-127.996)	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm (-128-127.996)	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning (-128-127.996)	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning (-128-127.996)	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

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 **System Configuration > Port Configuration > DDM > DDM Voltage Threshold Settings**, as show below:

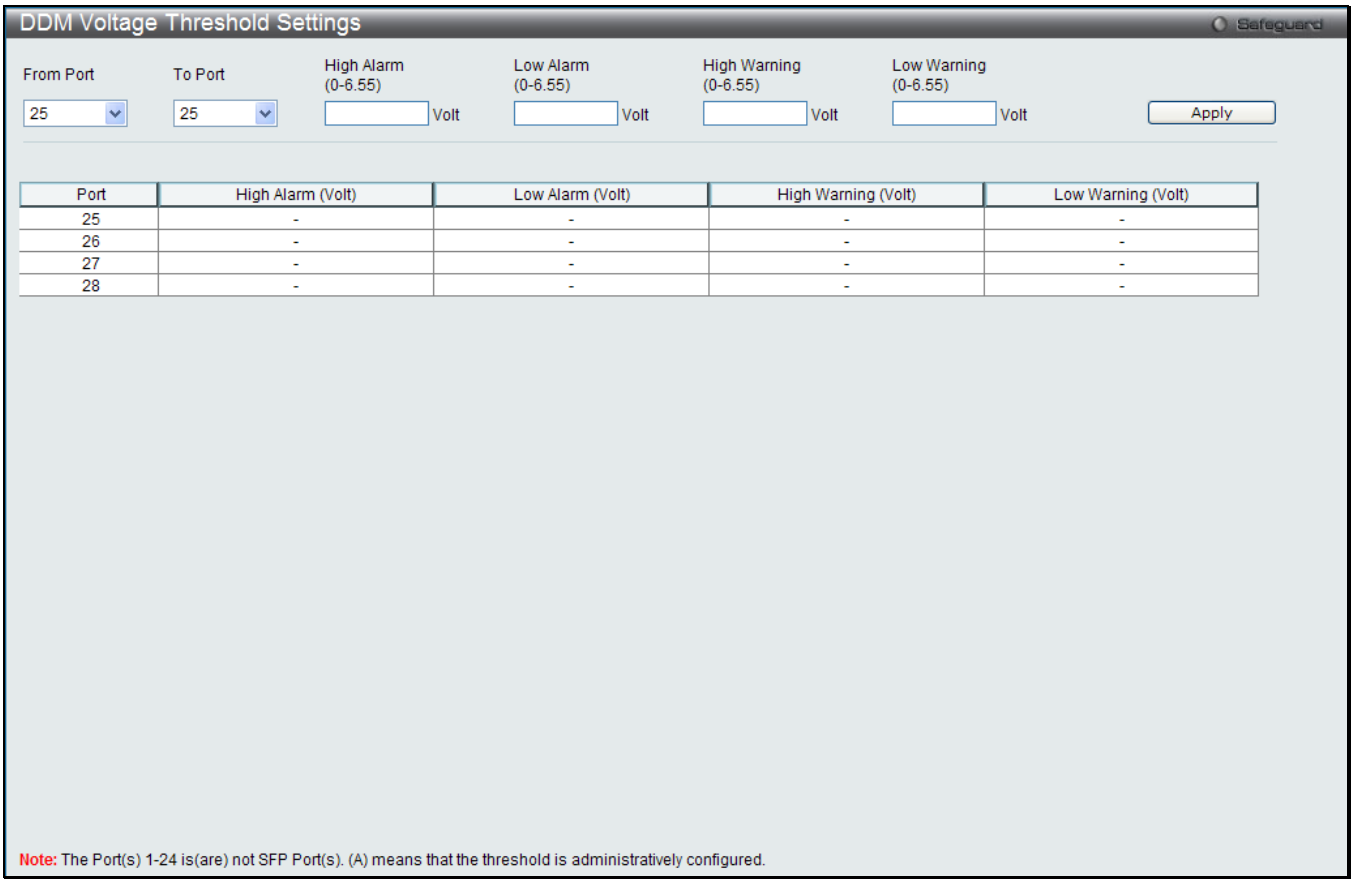


Figure 2-6 DDM Voltage Threshold Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
High Alarm (0-6.55)	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm (0-6.55)	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning (0-6.55)	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning (0-6.55)	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

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 **System Configuration > Port Configuration > DDM > DDM Bias Current Threshold Settings**, as show below:

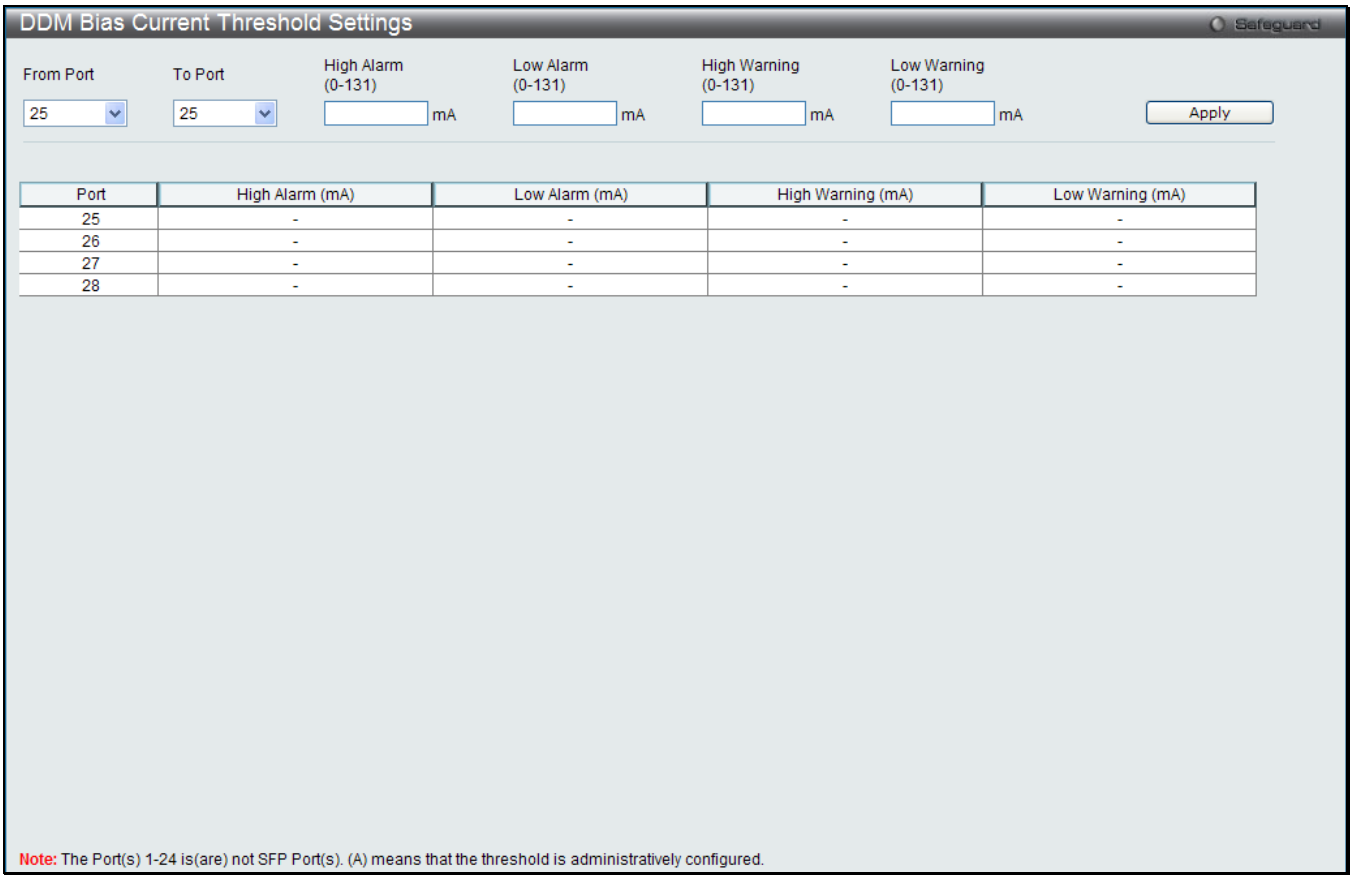


Figure 2-7 DDM Bias Current Threshold Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
High Alarm (0-131)	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm (0-131)	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning (0-131)	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning (0-131)	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

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 **System Configuration > Port Configuration > DDM > DDM TX Power Threshold Settings**, as show below:

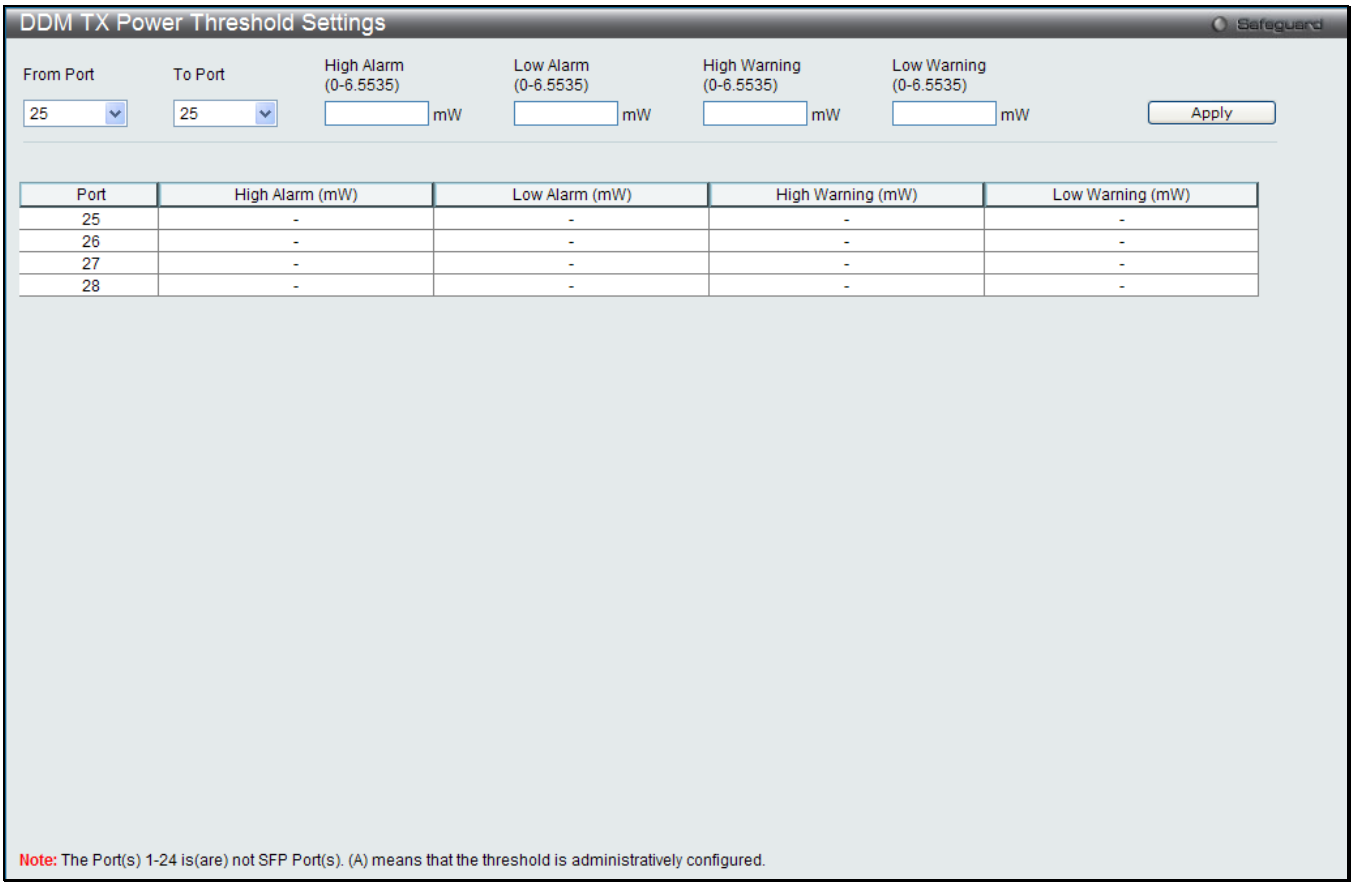


Figure 2-8 DDM TX Power Threshold Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
High Alarm (0-6.5535)	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm (0-6.5535)	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning (0-6.5535)	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning (0-6.5535)	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

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 **System Configuration > Port Configuration > DDM > DDM RX Power Threshold Settings**, as show below:

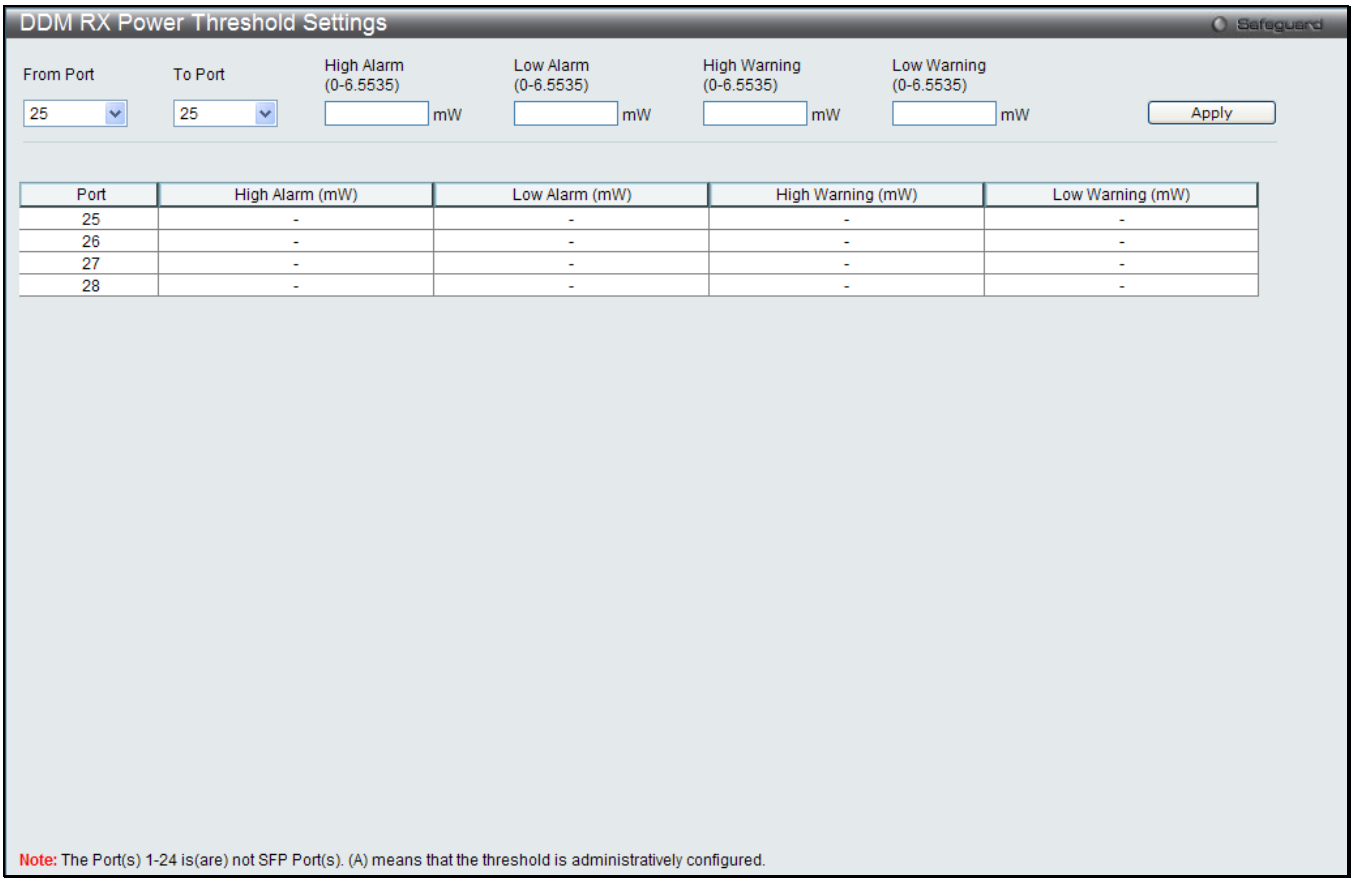


Figure 2-9 DDM RX Power Threshold Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
High Alarm (0-6.5535)	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm (0-6.5535)	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning (0-6.5535)	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning (0-6.5535)	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

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 **System Configuration > Port Configuration > DDM > DDM Status Table**, as show below:

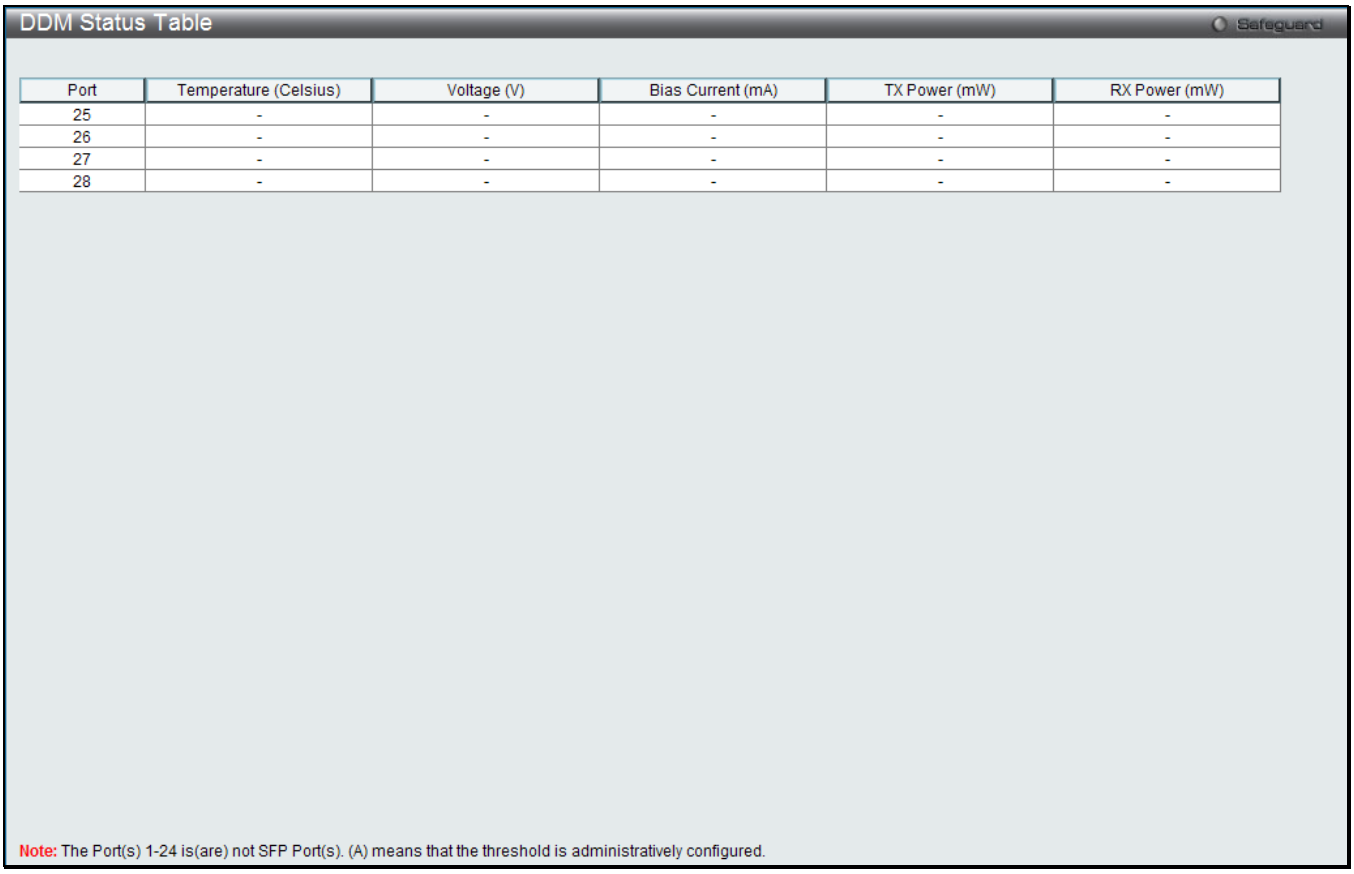


Figure 2-10 DDM Status Table window

Port Settings

This page used to configure the details of the switch ports.

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

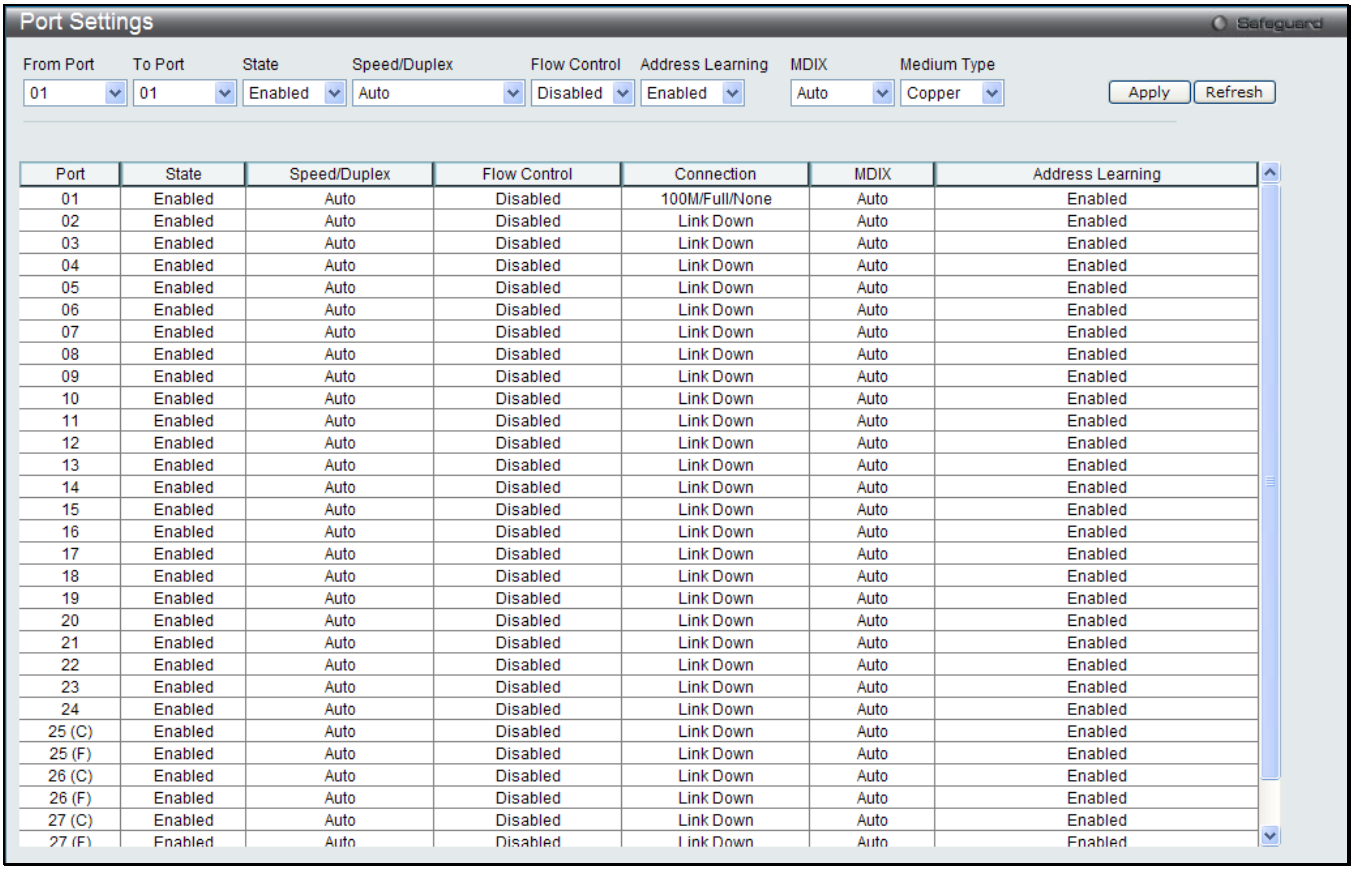


Figure 2-11 Port Settings window

To configure switch ports:

1. Choose the port or sequential range of ports using the From Port and To Port pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Toggle the State field to either enable or disable a given port or group of ports.
Speed/Duplex	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. *Auto* denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The *Auto* setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *10M Half*, *10M Full, 100M Half*, *100M Full*, *1000M Full_Master*, *1000M Full_Slave, and 1000M Full*. There is no automatic adjustment of port settings with any option other than *Auto*. The Switch allows the user to configure three types of gigabit connections; *1000M Full_Master*, *1000M Full_Slave*, and *1000M Full*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M Full_Master* and *1000M Full_Slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (*1000M Full_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 Full_Slave)* uses loop timing, where the timing comes from a data stream received from the master. If one connection is

	set for *1000M Full_Master*, the other side of the connection must be set for *1000M Full_Slave*. Any other configuration will result in a link down status for both ports.
Flow Control	Displays the flow control scheme used for the various port configurations. 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. The default is *Disabled*.
MDIX	*auto* - Select auto for auto sensing of the optimal type of cabling. *normal* - Select normal for normal cabling. If set to normal state, the port is in MDI mode and can be connected to a PC NIC using a straight-through cable or a port (in MDI mode) on another switch through a cross-over cable. *cross* - Select cross for cross cabling. If set to cross state, the port is in MDIX mode, and can be connected to a port (in MDI mode) on another switch through a straight cable.
Address Learning	Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When address learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is *Enabled*.
Medium Type	If configuring the Combo ports, this defines the type of transport medium to be used, whether *Copper* or *Fiber*.

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

Click the **Refresh** button to refresh the display section of this page.

Port Description Settings

The Switch supports a port description feature where the user may name various ports.

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

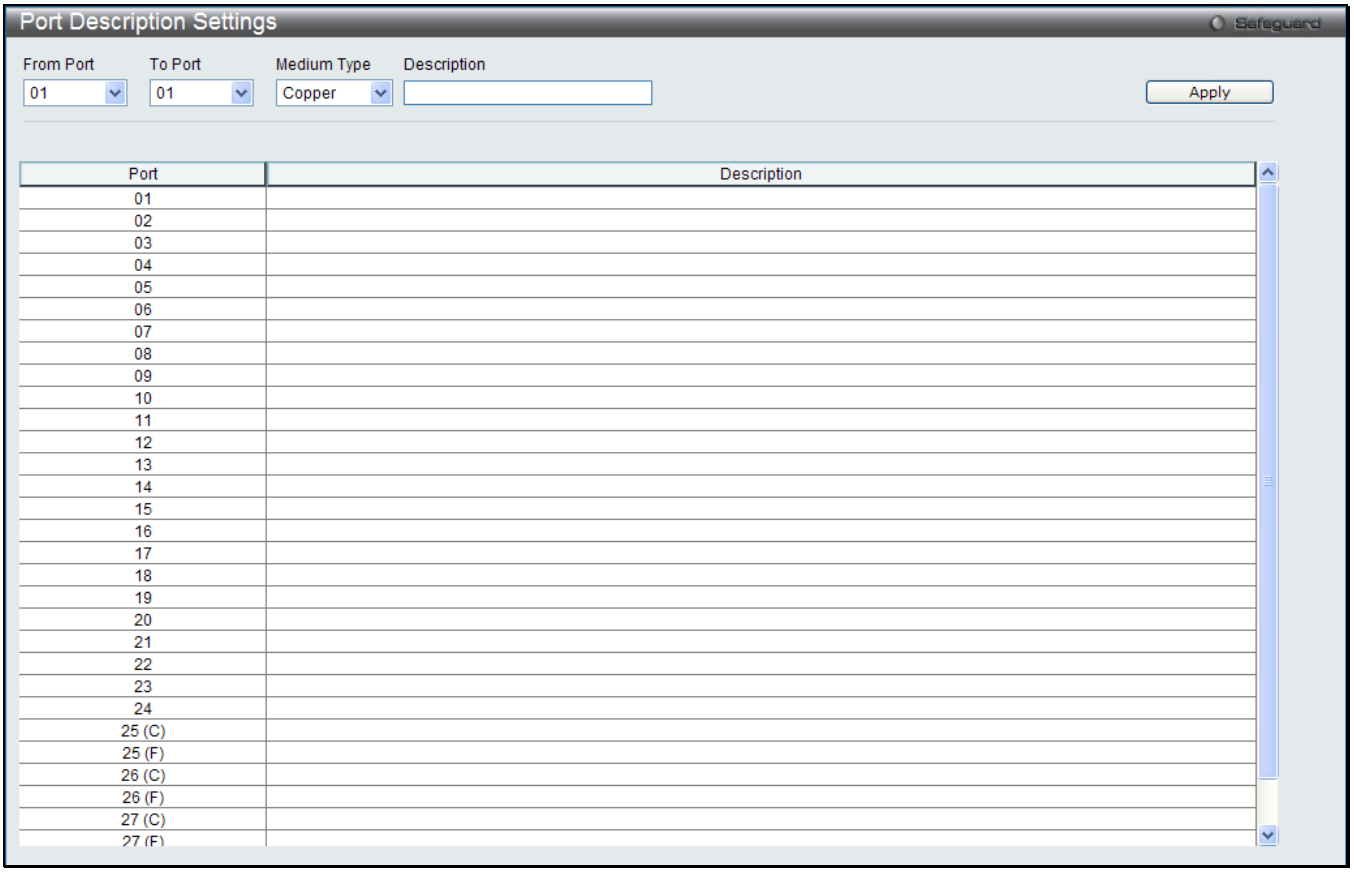


Figure 2-12 Port Description Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Medium Type	Specify the medium type for the selected ports. If configuring the Combo ports, the Medium Type defines the type of transport medium to be used, whether *Copper* or *Fiber.*
Description	Users may then enter a description for the chosen port(s).

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

Port Error Disabled

The following window will display the information about ports that have had their connection status disabled automatically by switch, for reasons such as when a packet storm occurs or when a loop was detected.

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

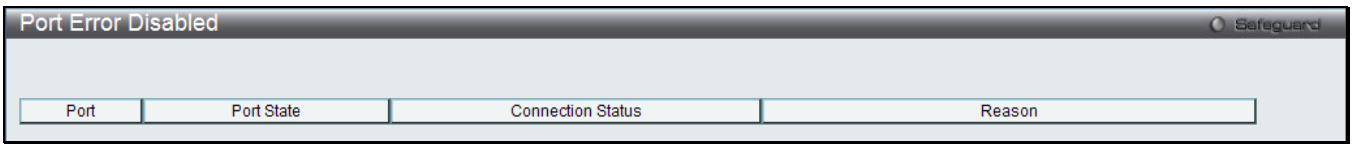


Figure 2-13 Port Error Disabled window

The fields that can be displayed are described below:

Parameter	Description
Port	Displays the port that has been error disabled.
Port State	Describes the current running state of the port, whether enabled or disabled.
Connection Status	This field will read the uplink status of the individual ports, whether enabled or disabled.
Reason	Describes the reason why the port has been error-disabled, such as it has become a shutdown port for storm control.

Jumbo Frame Settings

The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,500 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 10240 bytes.

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

Figure 2-14 Jumbo Frame Settings window

The fields that can be configured are described below:

Parameter	Description
Jumbo Frame	This field will enable or disable the Jumbo Frame function on the Switch. The default is Disabled. The maximum frame size is 1536 bytes.

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

Serial Port Settings

Here the user can adjust the Baud Rate and the Auto Logout values.

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

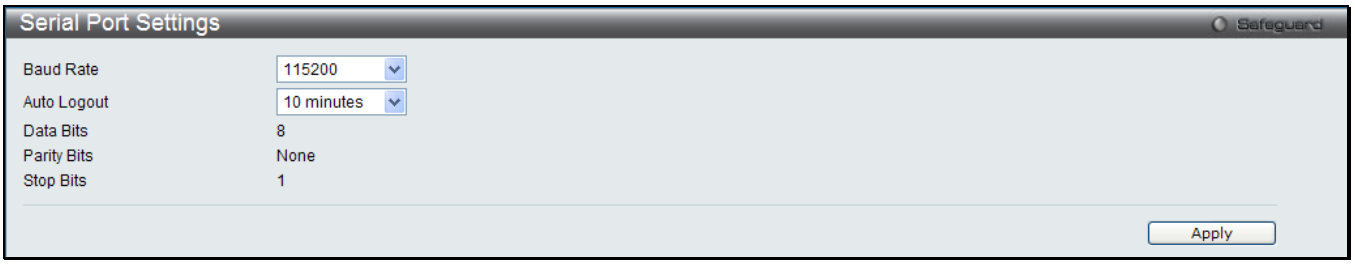


Figure 2-15 Serial Port Settings window

The fields that can be configured or displayed are described below:

Parameter	Description
Baud Rate	This field specifies the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, *9600*, *19200*, *38400* and *115200.* For a connection to the Switch using the console port, the baud rate must be set to *115200*, which is the default setting.
Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: *2, 5, 10, 15 minutes* or *Never*. The default setting is *10 minutes*.
Data Bits	Displays the data bits used for the serial port connection.
Parity Bits	Displays the parity bits used for the serial port connection.
Stop Bits	Displays the stop bits used for the serial port connection.

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

Warning Temperature Settings

On this page the user can configure the system warning temperature parameters.

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

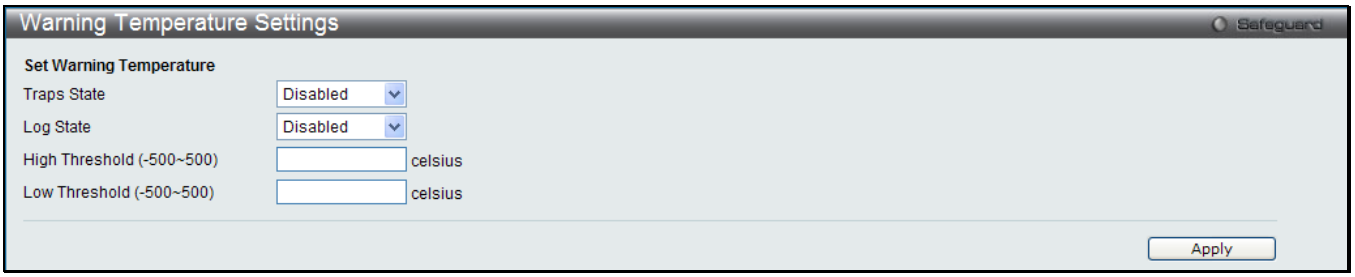


Figure 2-16 Warning Temperature Settings window

The fields that can be configured are described below:

Parameter	Description
Traps State	Here the user can enable or disable the traps state option of the warning temperature setting.
Log State	Here the user can enable or disable the log state option of the warning temperature

	setting.
High Threshold	Here the user can enter the high threshold value of the warning temperature setting.
Low Threshold	Here the user can enter the low threshold value of the warning temperature setting.

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

System Log Configuration

System Log Settings

The Switch allows users to choose a method for which to save the switch log to the flash memory of the Switch.

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

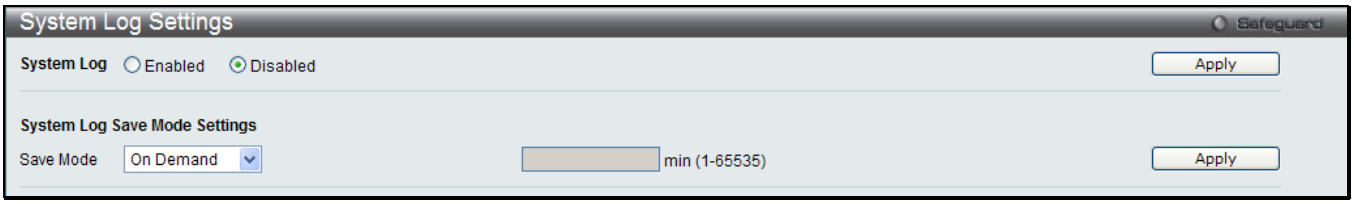


Figure 2-17 System Log Settings window

The fields that can be configured are described below:

Parameter	Description
System Log	Here the user can enable or disable the system log settings. Select Enable or Disable and click to **Apply** button to accept the changes made.
Save Mode	Use the pull-down menu to choose the method for saving the switch log to the flash memory. The user has three options: **Time Interval** – Users who choose this method can configure a time interval by which the Switch will save the log files, in the box adjacent to this configuration field. The user may set a time between 1 and 65535 minutes. **On Demand** – Users who choose this method will only save log files when they manually tell the Switch to do so, either using the Save Log link in the Save folder or clicking the Save Log Now button on this window. **Log Trigger** – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.

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

System Log Server Settings

The Switch can send Syslog messages to up to four designated servers using the System Log Server.

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

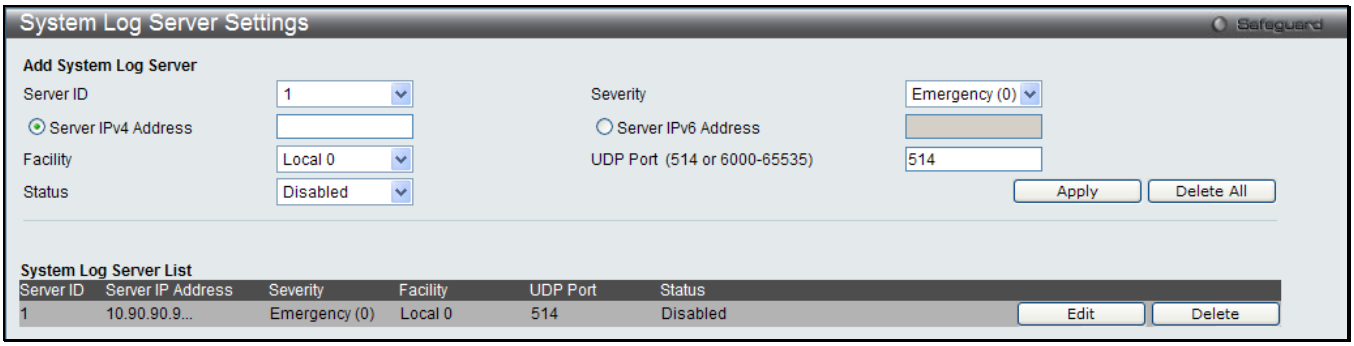


Figure 2-18 System Log Server Settings window

The fields that can be configured are described below:

Parameter	Description
Server ID	Syslog server settings index (1 to 4).
Severity	This drop-down menu allows you to select the higher level of messages that will be sent. All messages which level is higher than selecting level will be sent. The options are Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debug.
Server IPv4 Address	The IPv4 address of the Syslog server.
Server IPv6 Address	The IPv6 address of the Syslog server.
Facility	Use the drop-down menu to select Local 0, Local 1, Local 2, Local 3, Local 4, Local 5, Local 6, or Local 7.
UDP Port	Type the UDP port number used for sending Syslog messages. The default is 514.
Status	Choose Enabled or Disabled to activate or deactivate.

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

Click the **Delete All** button to remove all servers configured.

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

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

System Log

Users can view and delete the local history log as compiled by the Switch's management agent.

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

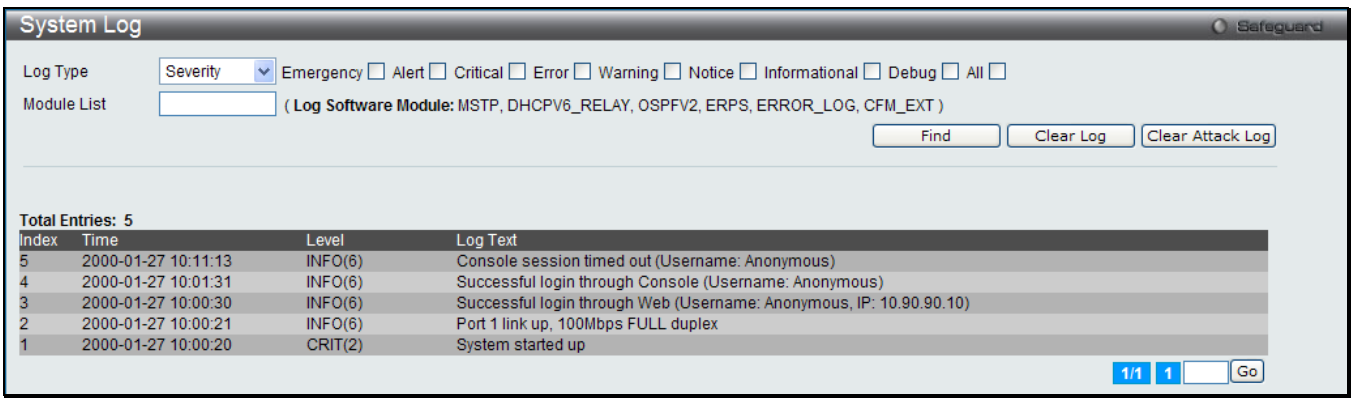


Figure 2-19 System Log window

The fields that can be configured or displayed are described below:

Parameter	Description

Log Type	In the drop-down menu the user can select the log type that will be displayed. **Severity** - When the user selects **Severity** then a secondary tick must be made. Secondary ticks are **Emergency, Alert, Critical, Error, Warning, Notice, Informational** and **Debug**. To view all information in the log simply select the **All** option. **Module List** – When the user selects **Module List**, the module name must be manually entered like MSTP or ERPS. **Attack Log** – When the user selects **Attack Log** all attacks will be listed.
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
Level	Here the level of the log entry is displayed.
Log Text	Displays text describing the event that triggered the history log entry.

Click the **Find** button to display the log in the display section according to the selection made.

Click the **Clear Log** button to clear the entries from the log in the display section.

Click the **Clear Attack Log** button to clear the entries from the attack log in the display section.

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

System Log & Trap Settings

The Switch allows users to configure the system log source IP interface addresses here.

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

Figure 2-20 System Log & Trap Settings window

The fields that can be configured are described below:

Parameter	Description
IP Interface	Here the user can enter the IP interface name used.
IPv4 Address	Here the user can enter the IPv4 address used
IPv6 Address	Here the user can enter the IPv6 address used

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

Click the **Clear** button to clear all the information entered in the fields.

System Severity Settings

The Switch can be configured to allow alerts be logged or sent as a trap to an SNMP agent or both. The level at which the alert triggers either a log entry or a trap message can be set as well. Use the **System Severity Settings** window to set the criteria for alerts. The current settings are displayed below the System Severity Table.

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

Figure 2-21 System Severity Settings window

The fields that can be configured are described below:

Parameter	Description
System Severity	Choose how the alerts are used from the drop-down menu. Select *Log* to send the alert of the Severity Type configured to the Switch's log for analysis. Choose *Trap* to send it to an SNMP agent for analysis, or select *All* to send the chosen alert type to an SNMP agent and the Switch's log for analysis.
Severity Level	This drop-down menu allows you to select the level of messages that will be sent. The options are *Emergency, Alert, Critical, Error, Warning, Notice, Informational* and *Debug.*

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

Time Range Settings

Time range is a time period that the respective function will take an effect on, such as ACL. For example, the administrator can configure the time based ACL to allow users to surf the Internet on every Saturday and every Sunday, meanwhile to deny users to surf the Internet on weekdays.

The user may enter up to 64 time range entries on the Switch.

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

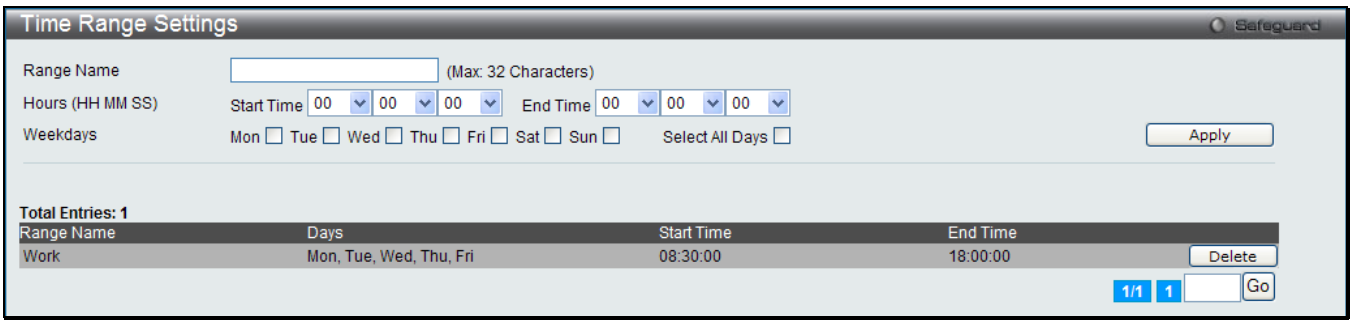


Figure 2-22 Time Range Settings window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the Access Profile table to identify the access profile and associated rule to be enabled during this time range.

Hours (HH MM SS)	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: *Start Time* - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. *End Time* - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.
Weekdays	Use the check boxes to select the corresponding days of the week that this time range is to be enabled. Tick the Select All Days check box to configure this time range for every day of the week.

Click the **Apply** button to accept the changes made. Current configured entries will be displayed in the table at the bottom half of the window.

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.

Time Settings

Users can configure the time settings for the Switch.

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

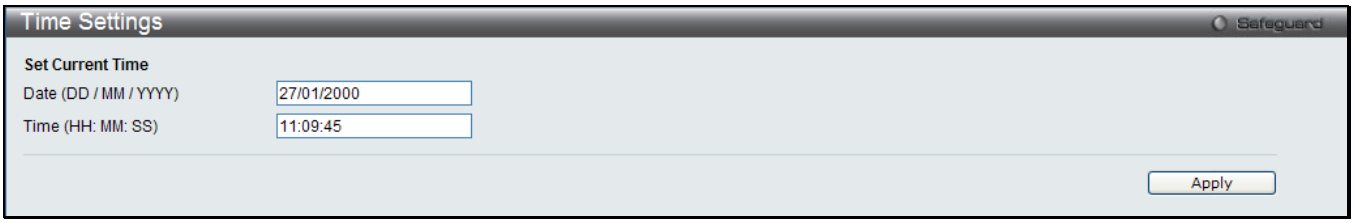


Figure 2-23 Time Settings window

The fields that can be configured are described below:

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

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

User Account Settings

The Switch allows the control of user privileges.

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

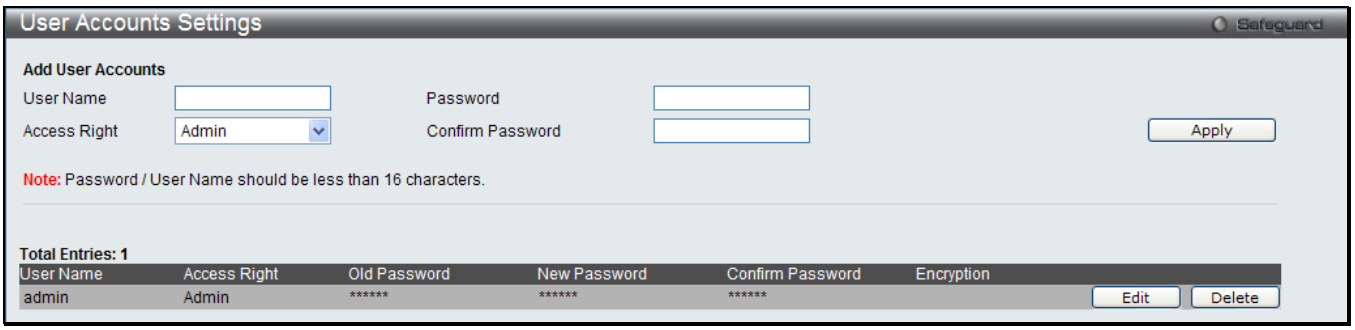


Figure 2-24 User Account Settings window

To add a new user, type in a User Name and New Password and retype the same password in the Confirm New Password field. Choose the level of privilege (Admin, Operator or User) from the Access Right drop-down menu.

Management	Admin	Operator	User
Configuration	Read/Write	Read/Write–partly	No
Network Monitoring	Read/Write	Read/Write	Read-only
Community Strings and Trap Stations	Read/Write	Read-only	Read-only
Update Firmware and Configuration Files	Read/Write	No	No
System Utilities	Read/Write	No	No
Factory Reset	Read/Write	No	No
User Account Management			
Add/Update/Delete User Accounts	Read/Write	No	No
View User Accounts	Read/Write	No	No

The fields that can be configured are described below:

Parameter	Description
User Name	Here the user can type in a new user name for the switch.
Password	Here the user can type in a new password for the switch.
Confirm Password	Here the user can re-type in a new password for the switch.
Access Right	Here the user can specify the access right for this user.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the specified entry.
Click the **Delete** button to remove the specified entry.

NOTICE: In case of lost passwords or password corruption, please refer to the appendix chapter entitled, “Password Recovery Procedure,” which will guide you through the steps necessary to resolve this issue.

NOTE: The username and password should be less than 16 characters.

SRM (EI Mode Only)

SRM Settings

This window is used to configure the Switch Resource Management (SRM) configured mode. Only after the Switch has been rebooted, will this configuration take effect.

To view this window, click **System Configuration > SRM > SRM Settings** as shown below:

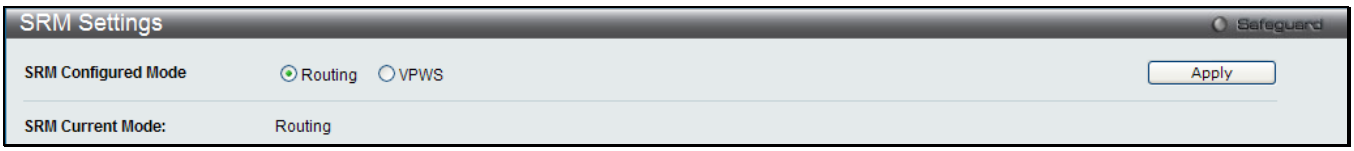


Figure 2-25 SRM Settings window

The fields that can be configured are described below:

Parameter	Description

SRM Configured Mode	Select the *Routing* option to specify that more hardware resources will be assigned to the L3 routing functions. Select the *VPWS* option to specify that more hardware resources will be assigned to MPLS functions.

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

Chapter 3 Management

ARP

Static ARP Settings

The Address Resolution Protocol is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify, and delete ARP information for specific devices. Static entries can be defined in the ARP table. When static entries are defined, a permanent entry is entered and is used to translate IP addresses to MAC addresses.

To view the following window, click **Management > ARP > Static ARP Settings**, as shown below:

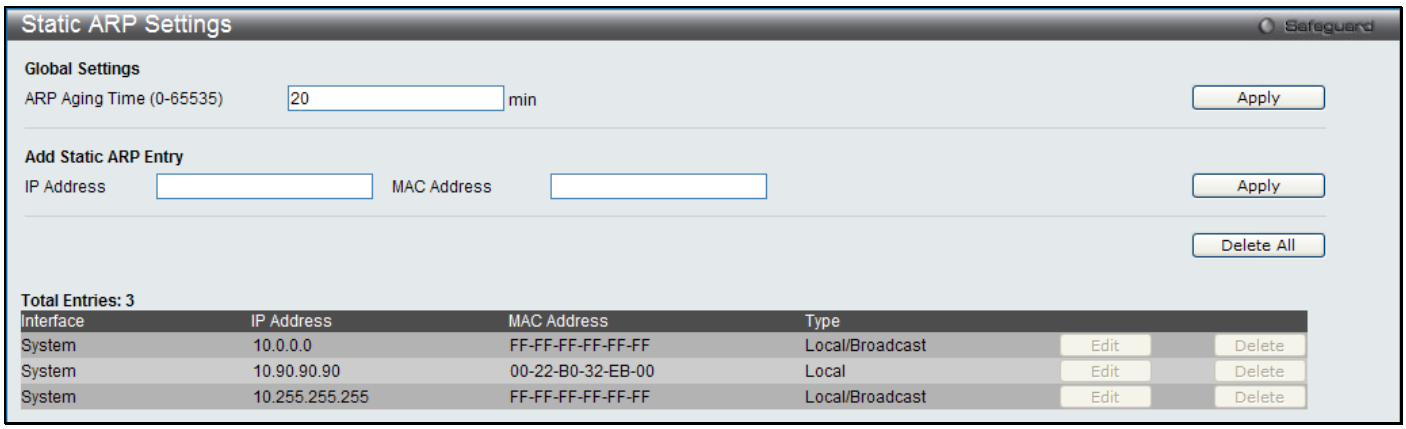


Figure 3-1 Static ARP Settings window

The fields that can be configured are described below:

Parameter	Description
ARP Aging Time (0-65535)	The ARP entry age-out time, in minutes. The default is *20* minutes.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

Click the **Apply** button to accept the changes made for each individual section.
Click the **Delete All** button to remove all the entries listed.
Click the **Edit** button to re-configure the specified entry.
Click the **Delete** button to remove the specified entry.

Proxy ARP Settings

On this page the user can view and edit basic settings concerning the Proxy ARP feature.

The Proxy ARP (Address Resolution Protocol) 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. For example, if hosts A and B are on different physical networks, B will not receive ARP broadcast requests from A and therefore cannot respond. Yet, if the physical network of A is connected by a router or layer 3 switch to B, the router or Layer 3 switch will see the ARP request from A.

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.

To view the following window, click **Management > ARP > Proxy ARP Settings**, as shown below:

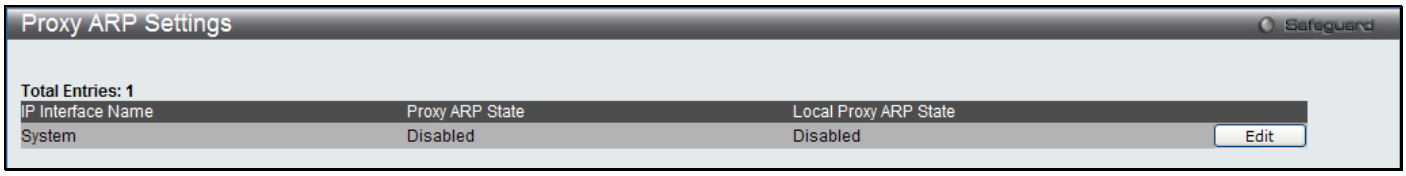


Figure 3-2 Proxy ARP Settings window

Click the **Edit** button to re-configure the specific entry and select the proxy ARP state of the IP interface. By default, both the **Proxy ARP State** and **Local Proxy ARP State** are disabled.

ARP Table

Users can display current ARP entries on the Switch.

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

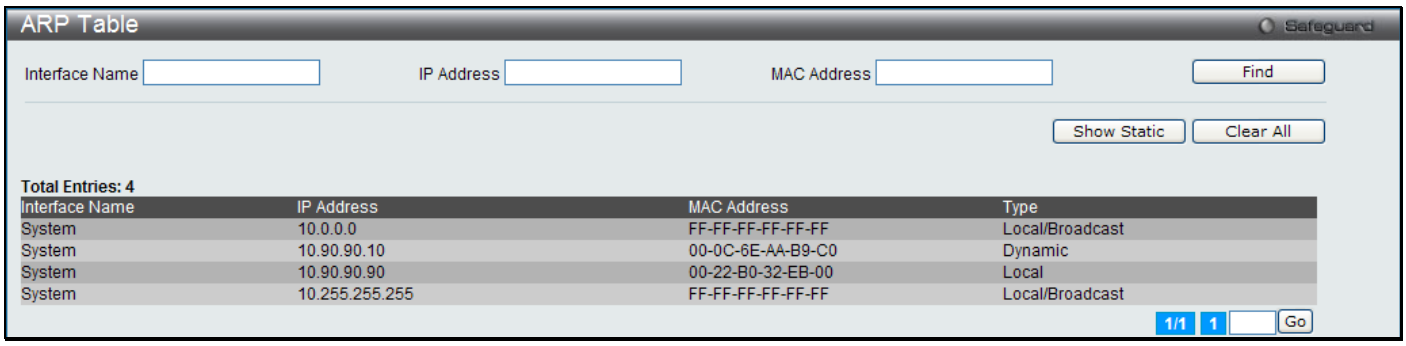


Figure 3-3 ARP Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Here the user can enter or view the Interface name used.
IP Address	Here the user can enter or view the IP Address used.
MAC Address	Here the user can enter or view the MAC Address used.

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

Click the **Show Static** button to display only the static entries in the display table.

Click the **Clear All** button to remove all the dynamic entries listed in the table.

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

Gratuitous ARP

Gratuitous ARP Global Settings

The user can enable or disable the gratuitous ARP global settings here.

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

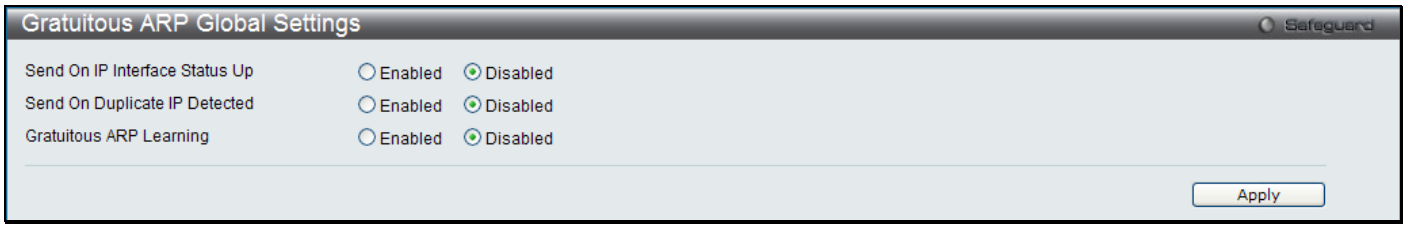


Figure 3-4 Gratuitous ARP Global Settings window

The fields that can be configured are described below:

Parameter	Description
Send On IP Interface Status Up	The command is used to enable/disable sending of gratuitous ARP request packets while the IP interface is becoming up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled, and only one gratuitous ARP packet will be broadcast.
Send On Duplicate IP Detected	The command is used to enable/disable the sending of gratuitous ARP request packet while a duplicate IP is detected. By default, the state is disabled. For this command, the duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that match the system's own IP address. In this case, the system knows that somebody out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packets for this duplicate IP address.
Gratuitous ARP Learning	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. The command is used to enable/disable learning of ARP entry in 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. By default, the state is disabled.

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

NOTE: With the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet.

Gratuitous ARP Settings

The user can configure the IP interface's gratuitous ARP parameter.

To view the following window, click **Management > Gratuitous ARP > Gratuitous ARP Settings**, as shown below:

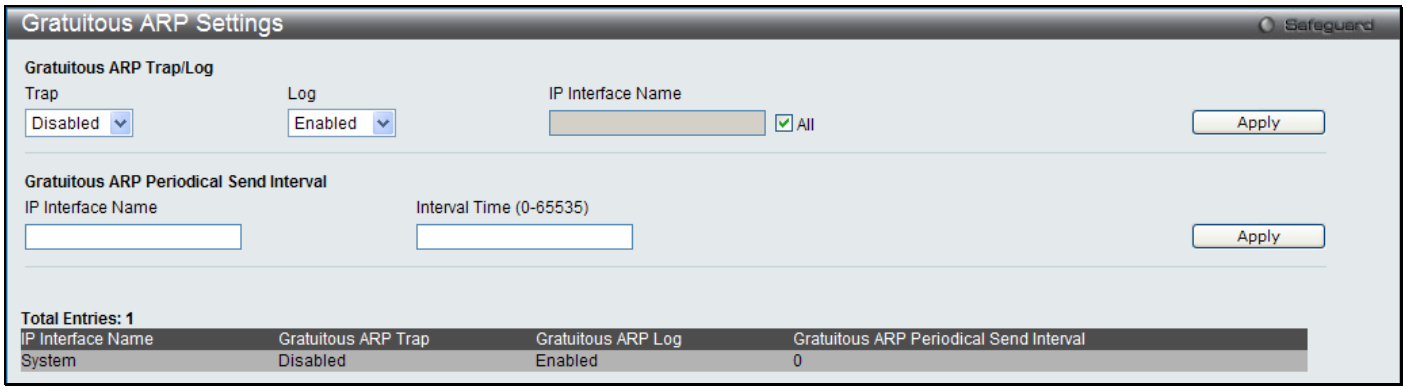


Figure 3-5 Gratuitous ARP Settings window

The fields that can be configured are described below:

Parameter	Description
Trap	Here the user can enable or disable the trap option. By default the trap is disabled.
Log	Here the user can enable or disable the logging option. By default the event log is enabled.
IP Interface Name	Here the user can enter the interface name of the Layer 3 interface. Select **All** to enable or disable gratuitous ARP trap or log on all interfaces.
Interval Time (0-65535)	Here the user can enter the periodically send gratuitous ARP interval time in seconds. 0 means that gratuitous ARP request will not be sent periodically. By default the interval time is 0.

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

IPv6 Neighbor Settings

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

To view the following window, click **Management > IPv6 Neighbor Settings**, as shown below:

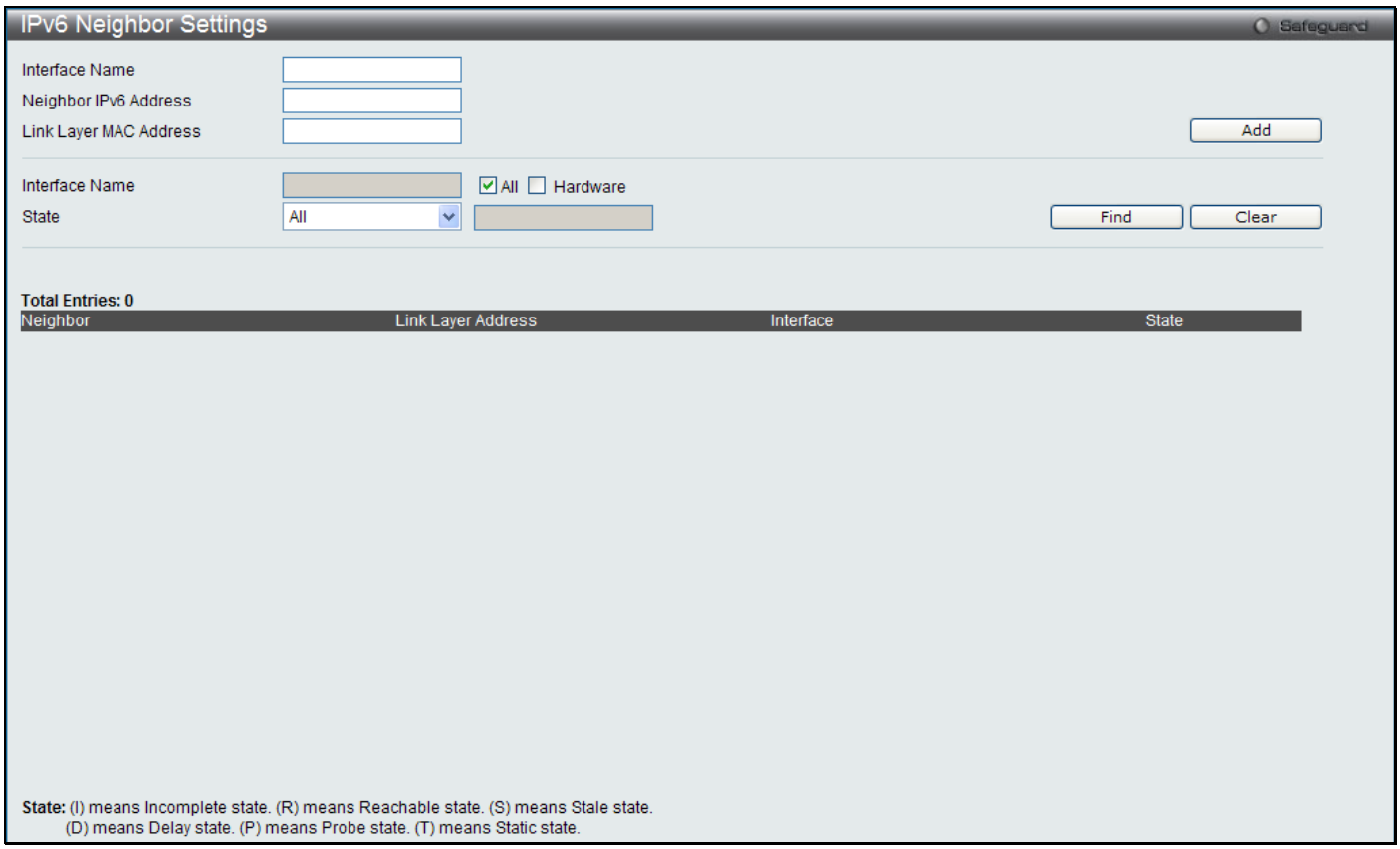


Figure 3-6 IPv6 Neighbor Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the interface name, where the IPv6 neighbor will be created.
Neighbor IPv6 Address	Enter the neighbor IPv6 address.
Link Layer MAC Address	Enter the link layer MAC address.
Interface Name	Enter the interface name, where the IPv6 neighbor will be shown. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part

	of the window, tick the **All** check box. Select the **Hardware** option to display all the neighbor cache entries which were written into the hardware table.
State	Use the drop-down menu to select All, Address, Static, or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

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

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

Click the **Clear** button to clear all the information entered in the fields.

IP Interface

System IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. The Web manager will display the Switch's current IP settings.

NOTE: The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

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

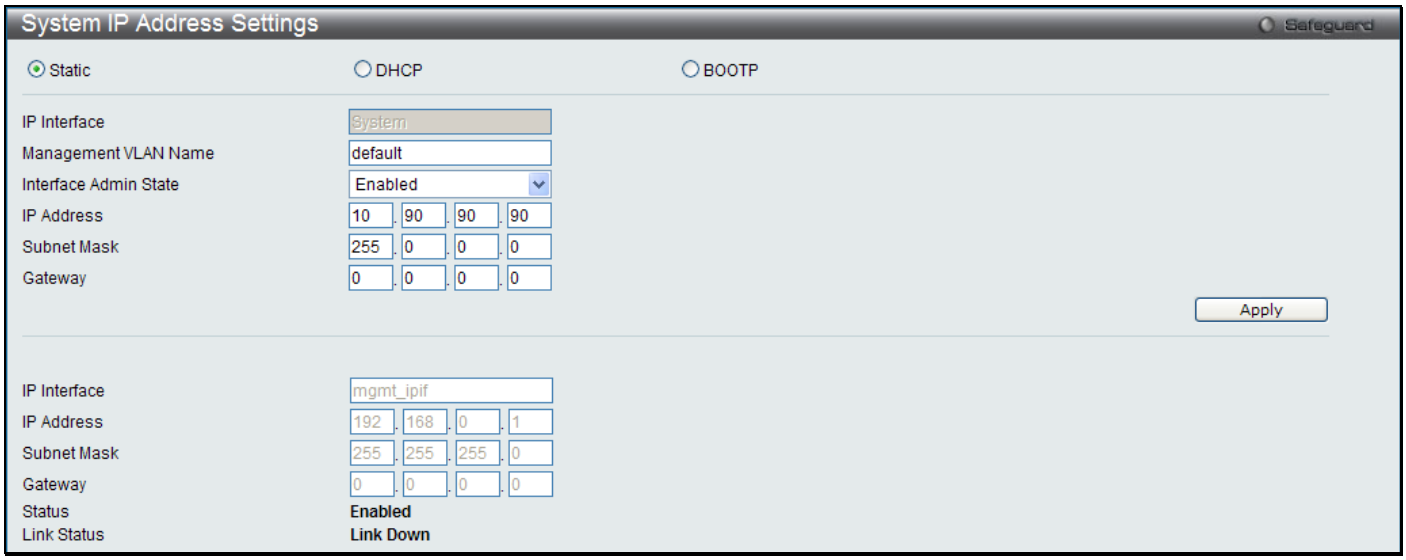


Figure 3-7 System IP Address Settings window

The fields that can be configured are described below:

Parameter	Description
Static	Allows the entry of an IP address, subnet mask, and a default gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between *0* and *255*. This address should be a unique address on the network assigned for use by the network administrator.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

The following table will describe the fields that are about the **System** Interface.

Parameter	Description
IP Interface	Here the System interface name will be displayed.
Management VLAN Name	This allows the entry of a VLAN name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via Web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the **Trusted Host** window (**Security > Trusted Host)**. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Trusted Host table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP addresses are assigned.
Interface Admin State	Use the drop-down menu to enable or disable the configuration on this interface.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between *0* and *255*. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

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

The following table will describe the fields that are about the **Management** Interface. The management interface can be accessed by connecting to the **Management port**.

Parameter	Description
IP Interface	Here the management interface name will be displayed.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between *0* and *255*. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
Status	Specifies whether the management port is enabled or disabled.
Link Status	Specifies whether a physical connection is made to the Management Port.

Interface Settings

Users can display the Switch's current IP interface settings.

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

Figure 3-8 Interface Settings window

The fields that can be configured are described below:

Parameter	Description
IP Interface Name	Here the user can enter the name of the IP interface to search for.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Add** button to add a new entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.
Click the **IPv4 Edit** button to edit the IPv4 settings for the specific entry.
Click the **IPv6 Edit** button to edit the IPv6 settings for the specific entry.
Click the **Delete** button to remove the specific entry.

NOTE: To create IPv6 interfaces, the user has to create an IPv4 interface then edit it to IPv6.

After clicking the **Add** button, the following page will appear:

Figure 3-9 IPv4 Interface Settings window

The fields that can be configured are described below:

Parameter	Description
IP Interface Name	Here the user can enter the name of the IP interface being created.
IPv4 Address	Here the user can enter the IPv4 address used.
Subnet Mask	Here the user can enter the IPv4 subnet mask used.
VLAN Name	Here the user can enter the VLAN Name used.
Interface Admin State	Here the user can select to enable or disable the Interface Admin State.
Secondary Interface	The user can select this option to use this Interface as a Secondary Interface. When the primary IP is not available, the VLAN will switch to the secondary interface. It will switch back when the primary IP was recovered.

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

After clicking the **IPv4 Edit** button, the following page will appear:

Figure 3-10 IPv4 Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Get IP From	Here the user can specify the method this Interface will use to acquire an IP Address.
IP Interface Name	Here the user can enter the name of the IP interface being configured.
IPv4 Address	Here the user can enter the IPv4 address used.
Subnet Mask	Here the user can enter the IPv4 subnet mask used.
VLAN Name	Here the user can enter the VLAN Name used.
IPv4 State	Here the user can select to enable or disable IPv4 State.
Interface Admin State	Here the user can select to enable or disable the Interface Admin State.

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

After clicking the **IPv6 Edit** button, the following page will appear:

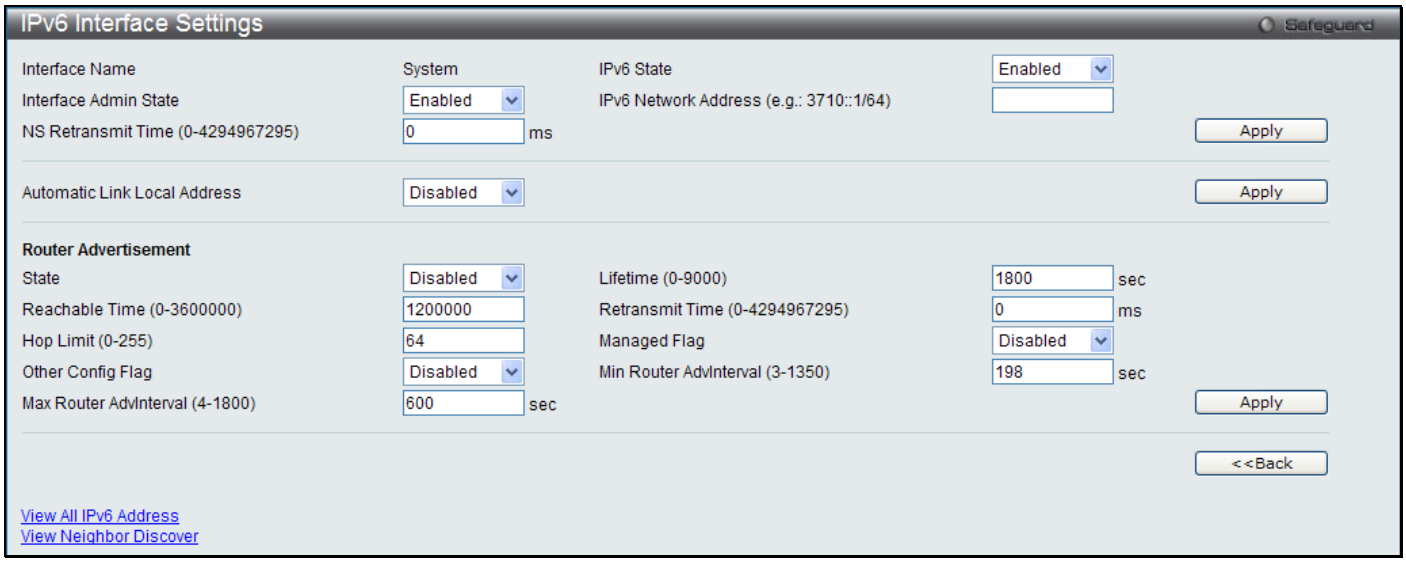


Figure 3-11 IPv6 Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Here the IPv6 interface name is displayed
IPv6 State	Here the user can select to enable or disable IPv6 State.
Interface Admin State	Here the user can select to enable or disable the Interface Admin State.
IPv6 Network Address	Here the user can enter the IPv6 network address used.

NS Retransmit Time (0-1294967295)	Enter the Neighbor solicitation's retransmit timer in millisecond here. It has the same value as the RA retransmit time in the configuration of the IPv6 ND RA command. If this field is configure, it will duplicate the enter into the RA field.
Automatic Link Local Address	Here the user can select to enable or disable the Automatic Link Local Address.
State	Here the user can enable or disable the router advertisement state.
Lifetime (0-9000)	Here the user can enter the lifetime value of the router as the default router in second.
Reachable Time (0-3600000)	Here the user can enter the amount of time that a node can consider a neighboring node reachable after receiving a reachable confirmation in millisecond.
Retransmit Time (0-4294967295)	Here the user can enter the amount of time between retransmissions of the router advertisement message in millisecond, and the router advertisement packet will take it to the host.
Hop Limit (0-255)	Here the user can enter the default value of the hop limit field in the IPv6 header for packets sent by hosts that will receive this RA message.
Managed Flag	When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain an address in the addition to the addresses derived from the stateless address configuration.
Other Config Flag	When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain the address configuration information.
Min Router Advinterval	The minimum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds. This value must be no less than 3 seconds and no greater than .75 times the maximum router advertisement interval. The default value for this field is 198 seconds.
Max Router Advinterval	The maximum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds. This value must be no less than 4 seconds and no greater than 1800 seconds. The default value for this field is 600 seconds.

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

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

Click the View All IPv6 Address link to view all the current IPv6 address

Click the View Neighbor Discover link to view all the neighbor discovery information entries.

After clicking the View All IPv6 Address link, the following page will appear:

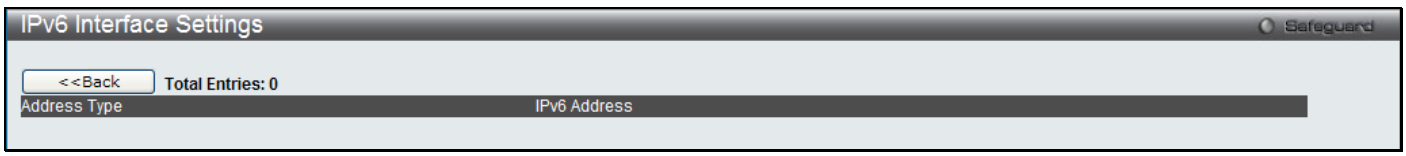


Figure 3-12 IPv6 Interface Settings - View All IPv6 Address window

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

After clicking the View Neighbor Discover link, the following page will appear:

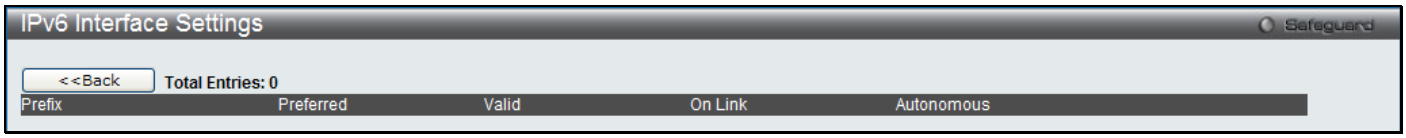


Figure 3-13 IPv6 Interface Settings - View Neighbor Discover window

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

Loopback Interface Settings

This window is used to configure loopback interfaces. A loopback interface is a logical IP interface which is always active, until a user disables or deletes it. It is independent of the state of any physical interfaces.

To view this window, click **Management > IP Interface > Loopback Interface Settings**, as show below:

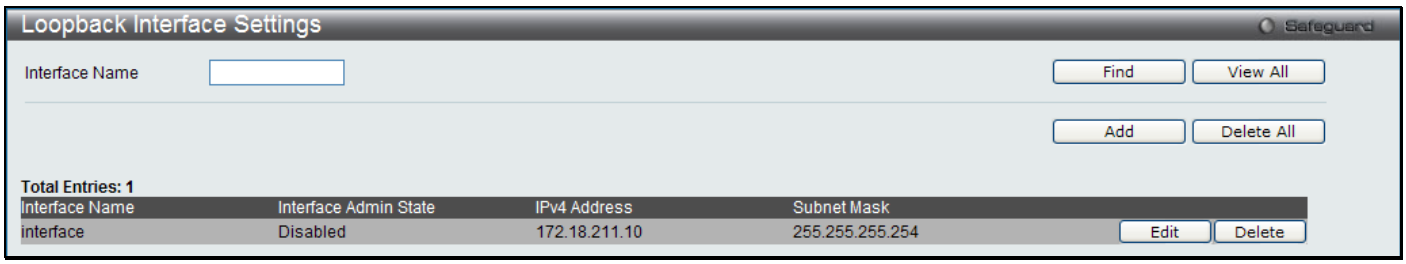


Figure 3-14 Loopback Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter an interface name.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Add** button to create a new entry.
Click the **Delete All** button to remove all the entries listed in the table.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

Click the **Add** or **Edit** button to see the following window.

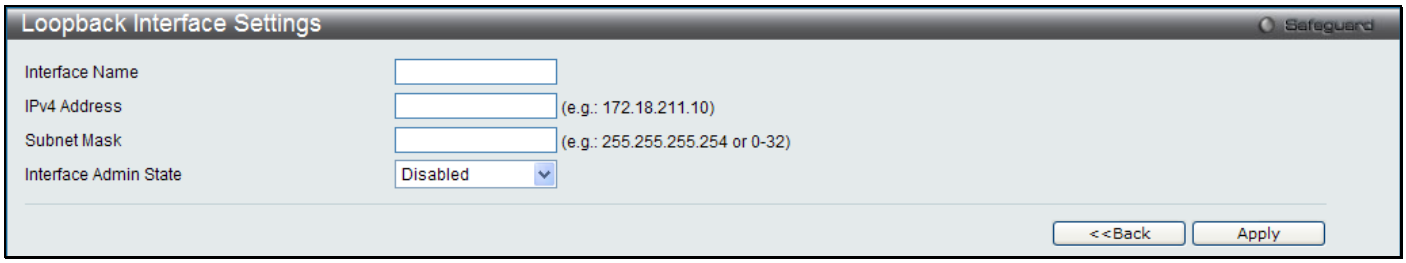


Figure 3-15 Loopback Interface Settings - Add/Edit window

The fields that can be configured are described below:

Parameter	Description
Interface Name	The name of the loopback interface. The loopback interface has the same name domain space as the regular interface. So the name can't be a duplicate of any of the regular interfaces.
IPv4 Address	Enter a 32-bit IPv4 address for the loopback interface.
Subnet Mask	Enter a subnet mask to be applied to the loopback interface.
Interface Admin State	Use the drop-down menu to enable or disable the loopback interface.

Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Apply** button to accept the changes made for each individual section.

Management Settings

Users can stop the scrolling of multiple pages beyond the limits of the console when using the Command Line Interface.

This window is also used to enable the DHCP auto configuration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the **Upload Log File** window description located in the **Tools** section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.

This window also allows the user to implement the Switch's built-in power saving feature. When power saving is 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.

Users can also configure Password Encryption on the Switch.

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

Figure 3-16 Management Settings window

The fields that can be configured are described below:

Parameter	Description
CLI Paging State	Command Line Interface paging stops each page at the end of the console. This allows you to stop the scrolling of multiple pages of text beyond the limits of the console. CLI Paging is Enabled by default. To disable it, click the Disabled radio button.
DHCP Auto Configuration State	Enable or disable the Switch's DHCP auto configuration feature. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch.
Password Encryption State	Password encryption will encrypt the password configuration in configuration files. Password encryption is Disabled by default. To enable password encryption, click the Enabled radio button.

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

Out of Band Management Settings

On this page the user can configure the details of the RJ-45 out of band management port.

To view the following window, click **Management > Out of Band Management Settings**, as shown below:

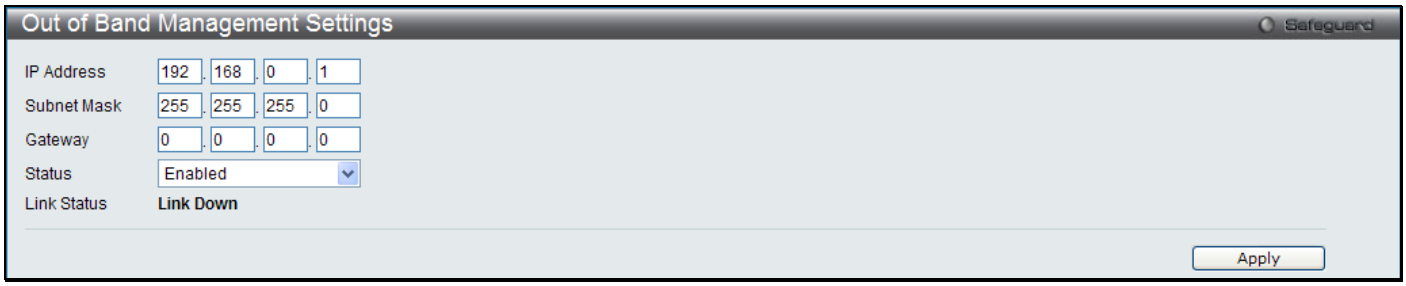


Figure 3-17 Out of Band Management Settings window

The fields that can be configured or displayed are described below:

Parameter	Description
IP Address	The user can enter the IP address used here.
Subnet Mask	The user can enter the subnet mask used here.
Gatewa	The user can enter the Gateway IP address used here.
Status	The user can enable or disable the out of band management status here.
Link Status	The user can view the link status here.

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

Session Table

Users can display the management sessions since the Switch was last rebooted.

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

Figure 3-18 Session Table window

Click the **Refresh** button to refresh the display table so that new entries will appear.

Single IP Management

Simply put, D-Link Single IP Management 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:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. 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).
- All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.
- A SIM group accepts up to 32 switches (numbered 1-32), not including the Commander Switch (numbered 0).
- 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 default 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:

1. **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:
    a. It has an IP Address.
    b. It is not a command switch or member switch of another Single IP group.
    c. It is connected to the member switches through its management VLAN.
2. **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:
    a. It is not a CS or MS of another IP group.
    b. It is connected to the CS through the CS management VLAN.
3. **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:
    a. It is not a CS or MS of another Single IP group.
    b. 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.
- CSs must change their 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 DES-3810-28 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.

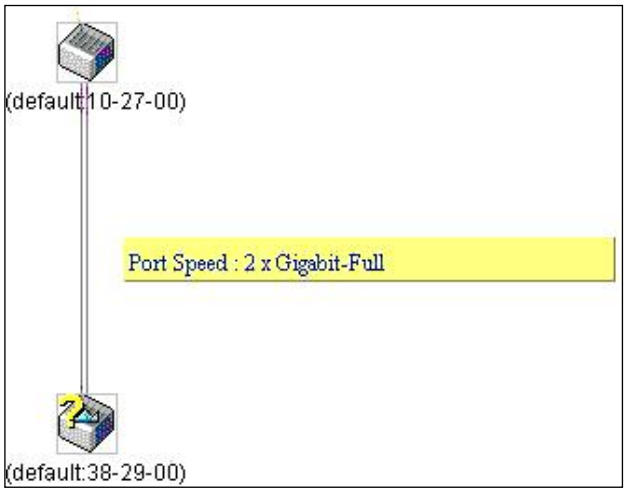
Upgrade to v1.61

To better improve SIM management, the DES-3810-28 Series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including:

1. The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintenance packets that previously set SIM members will emit 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.

2. 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, as shown in the adjacent picture.



3. This version will support switch upload and downloads for firmware, configuration files and log files, as follows:
    a. **Firmware** – The switch now supports MS firmware downloads from a TFTP server.
    b. **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.
    c. **Log** – The Switch now supports uploading MS log files to a TFTP server.
4. 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

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 > Single IP Management > Single IP Settings**, as shown below:

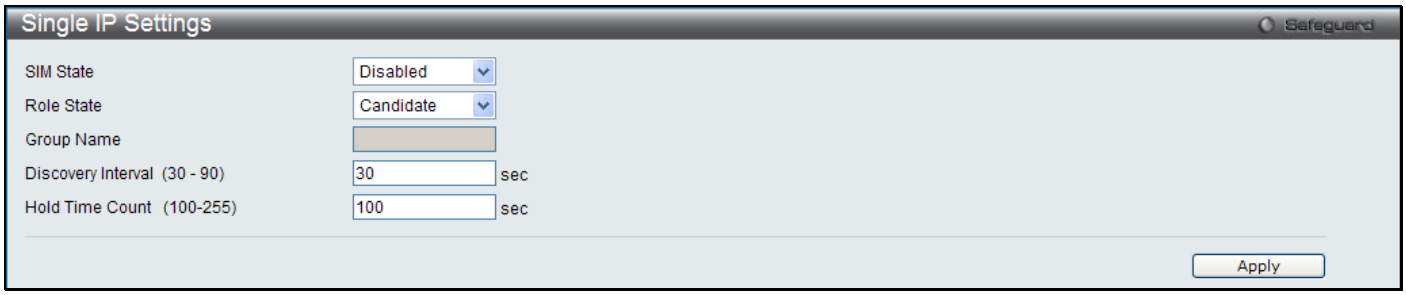


Figure 3-19 Single IP Settings window

The fields that can be configured are described below:

Parameter	Description
SIM State	Use the pull-down menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable.
Role State	Use the pull-down menu to change the SIM role of the Switch. The two choices 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* – Choosing this parameter will 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 in this textbox. This is optional. This name is used to segment switches into different SIM groups.
Discovery Interval (30-90)	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from *30* to *90* seconds. The default value is *30* seconds.
Hold Time Count (100-255)	This parameter may be set for the time, in seconds; the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from *100* to *255* seconds. The default value is *100* seconds.

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**.

Topology

This window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer.

To view the following window, click **Management > Single IP Management > Topology**, as shown below:
The Java Runtime Environment on your server should initiate and lead you to the **Topology** window, as seen below.

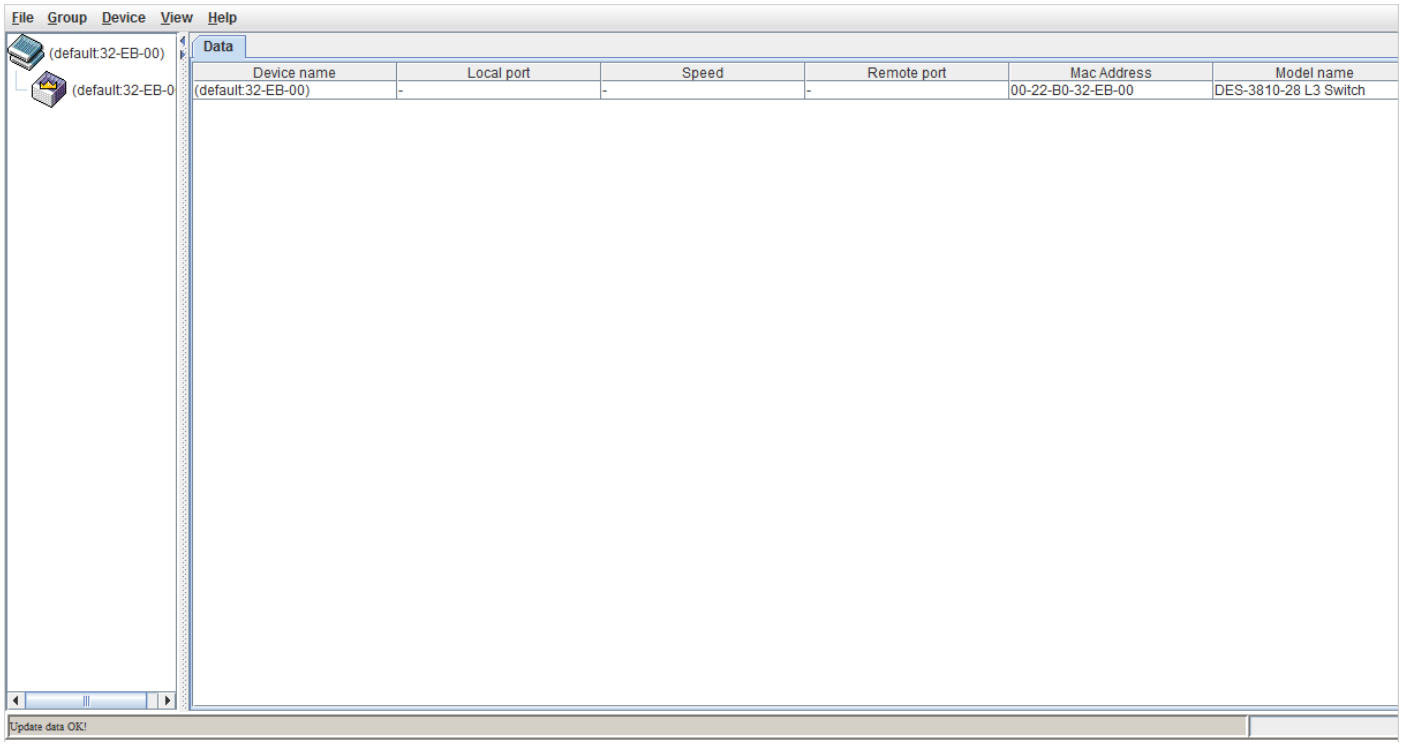


Figure 3-20 Topology window

The **Topology** window holds the following information on the **Data** tab:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no device is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
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.

Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	Displays the number of the physical port on the MS or CaS to which the CS is connected. The CS will have no entry in this field.
MAC Address	Displays the MAC Address of the corresponding Switch.
Model Name	Displays the full Model Name of the corresponding Switch.

To view the **Topology View** window, open the **View** drop-down menu in the toolbar and then click **Topology**, which will open the following Topology Map. This window will refresh itself periodically (20 seconds by default).

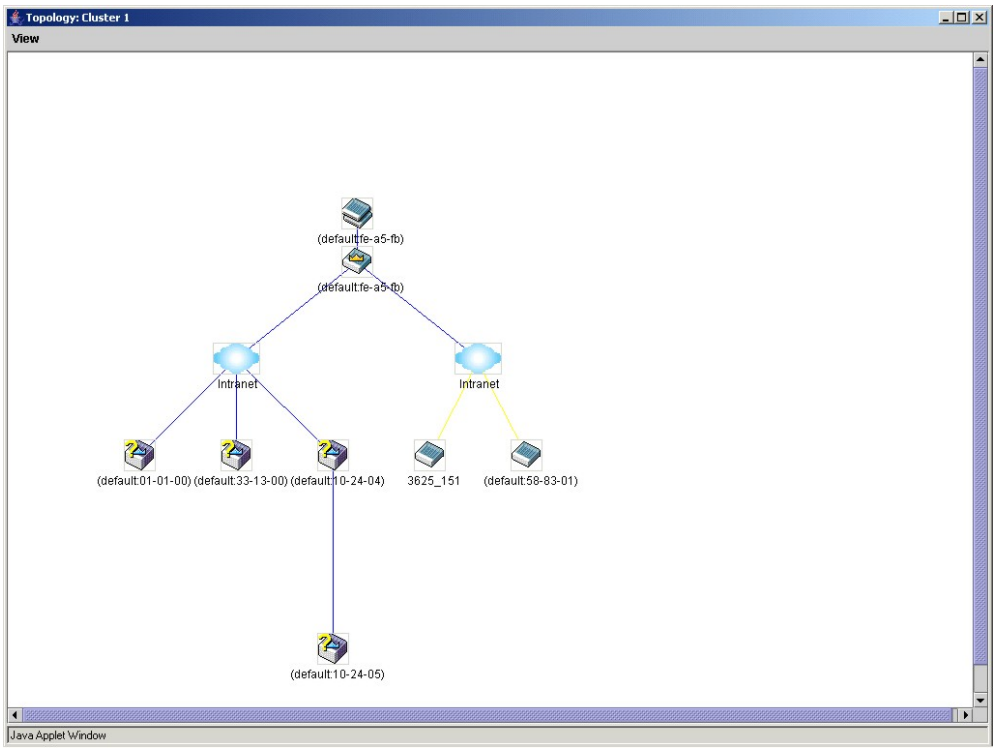


Figure 3-21 Topology View window

This window will display how the devices within the Single IP Management 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. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example.

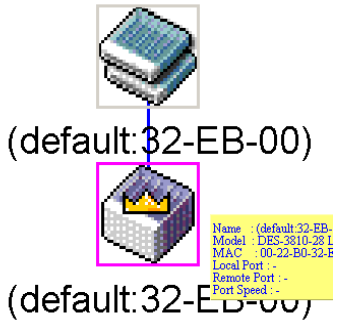


Figure 3-22 Tool Tips window

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

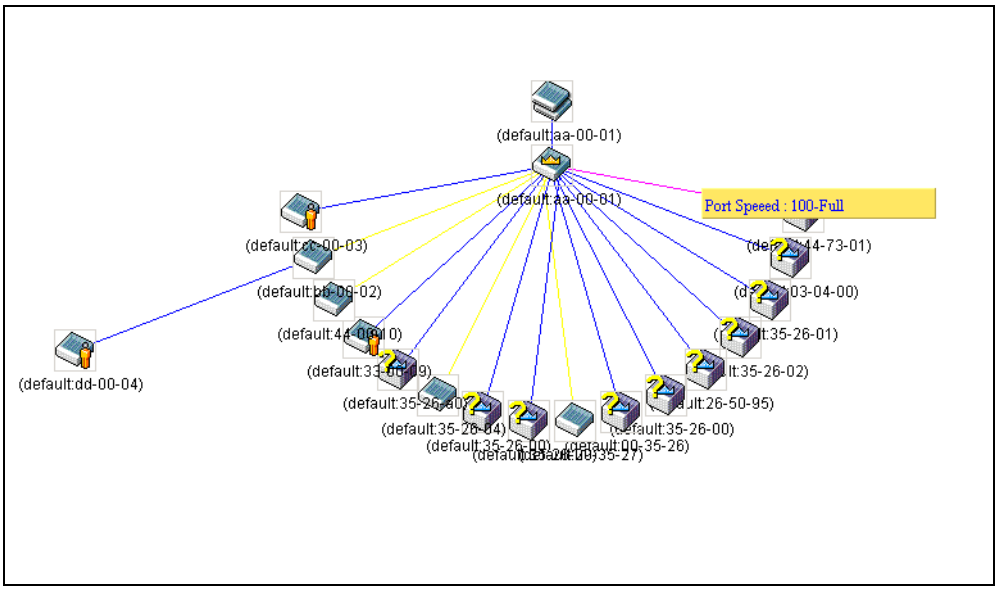


Figure 3-23 Connection Speed window

Right-Click

Right-clicking on a device will 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 Icon

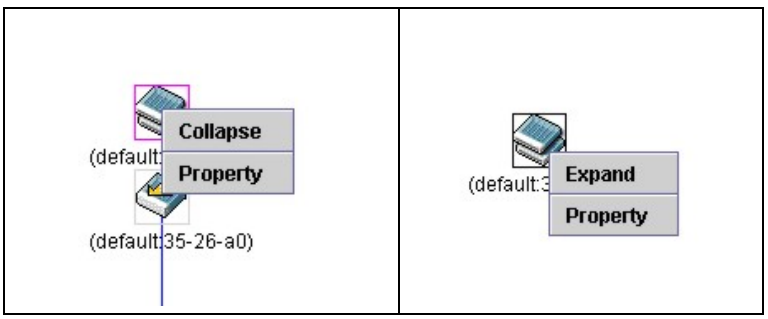


Figure 3-24 Group Icon window

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.

- **Property** – To pop up a window to display the group information.

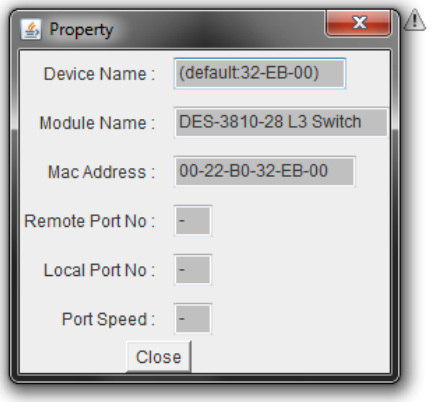


Figure 3-25 Properties window

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.
Remote Port No	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.
Local Port No	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.
Port Speed	Displays the connection speed between the CS and the MS or CaS

Click the **Close** button to close the property window.

Commander Switch Icon

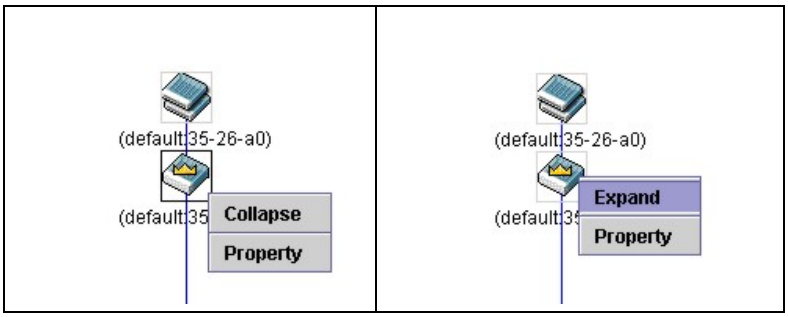


Figure 3-26 Commander Switch Icon window

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Property** – To pop up a window to display the group information.

Member Switch Icon

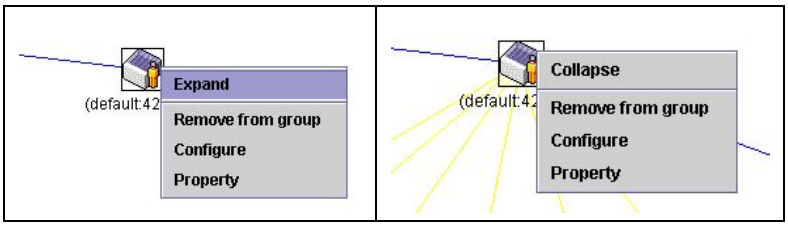


Figure 3-27 Member Switch Icon window

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Remove from group** – Remove a member from a group.
- **Configure** – Launch the web management to configure the Switch.
- **Property** – To pop up a window to display the device information.

Candidate Switch Icon

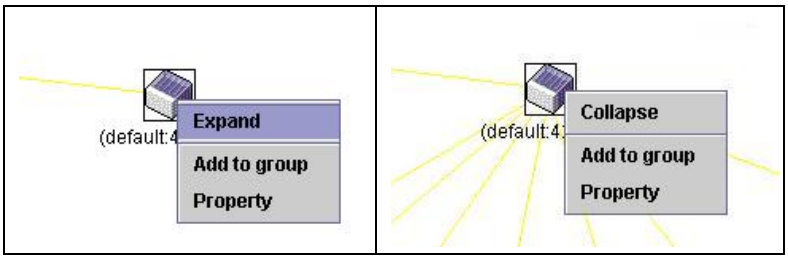


Figure 3-28 Candidate Switch Icon window

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Add to group** – Add a candidate to a group. Clicking this option will reveal the following dialog box for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the dialog box.

Figure 3-29 Input Password window

- **Property** – To pop up a window to display the device information.

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.

Figure 3-30 Menu Bar window

File

- **Print Setup** – Will view the image to be printed.
- **Print Topology** – Will print the topology map.
- **Preference** – Will set display properties, such as polling interval, and the views to open at SIM startup.

Group

- **Add to group** – Add a candidate to a group. Clicking this option will reveal the following dialog box for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the dialog box.

Figure 3-31 Input Password window

- **Remove from Group** – Remove an MS from the group.

Device

- **Configure** – Will open the Web manager for the specific device.

View

- **Refresh** – Update the views with the latest status.
- **Topology** – Display the Topology view.

Help

- **About** – Will display the SIM information, including the current SIM version.

Firmware Upgrade

This screen is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Version**. To specify a certain Switch for firmware download, click its corresponding check box under the **Port** heading. To update the firmware, enter the **Server IP Address** where the firmware resides and enter the **Path/Filename** of the firmware. Click **Download** to initiate the file transfer.

To view the following window, click **Management > Single IP Management > Firmware Upgrade**, as show below:

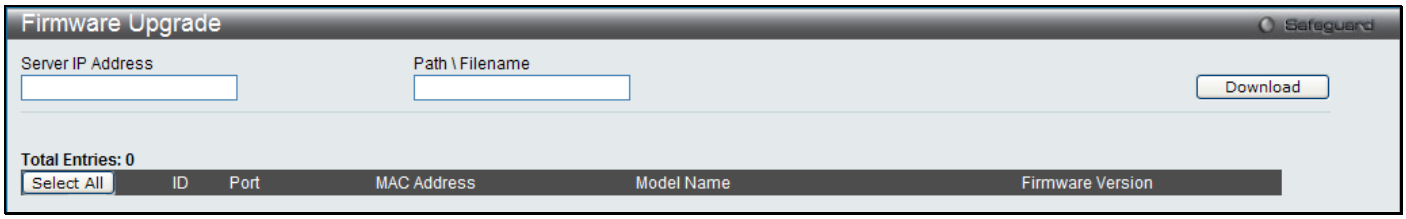


Figure 3-32 Firmware Upgrade window

Configuration File Backup/Restore

This screen 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 and will be specified by **ID**, **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Firmware Version**. To update the configuration file, enter the **Server IP Address** where the file resides and enter the **Path/Filename** of the configuration file. Click **Restore** to initiate the file transfer from a TFTP server to the Switch. Click **Backup** to backup the configuration file to a TFTP server.

To view the following window, click **Management > Single IP Management > Configuration File Backup/Restore**, as show below:

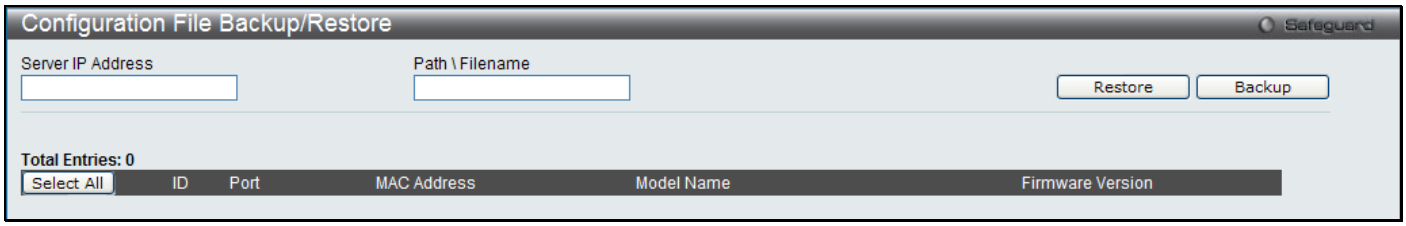


Figure 3-33 Configuration File Backup/Restore window

Upload Log File

The following window is used to upload log files from SIM member switches to a specified PC. To upload a log file, enter the Server IP address of the SIM member switch and then enter a Path\Filename on your PC where you wish to save this file. Click **Upload** to initiate the file transfer.

To view the following window, click **Management > Single IP Management > Upload Log File**, as show below:

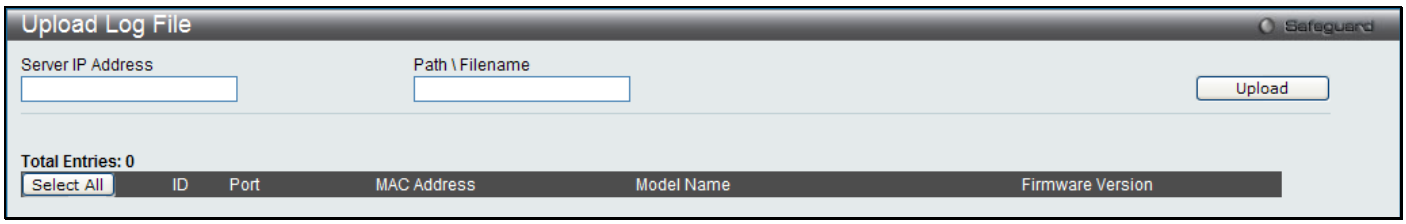


Figure 3-34 Upload Log File window

SNMP Settings

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

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

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

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

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

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

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

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

Traps

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

MIBs

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

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

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

SNMP Global Settings

SNMP global state settings can be enabled or disabled.

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

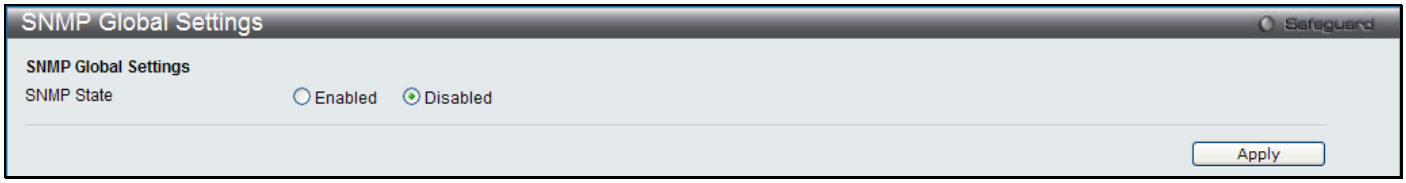


Figure 3-35 SNMP Global Settings window

The fields that can be configured are described below:

Parameter	Description
SNMP State	Enable this option to use the SNMP feature.

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

SNMP Traps Settings

Users can enable and disable the SNMP trap support function of the switch and SNMP authentication failure trap support, respectively.

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

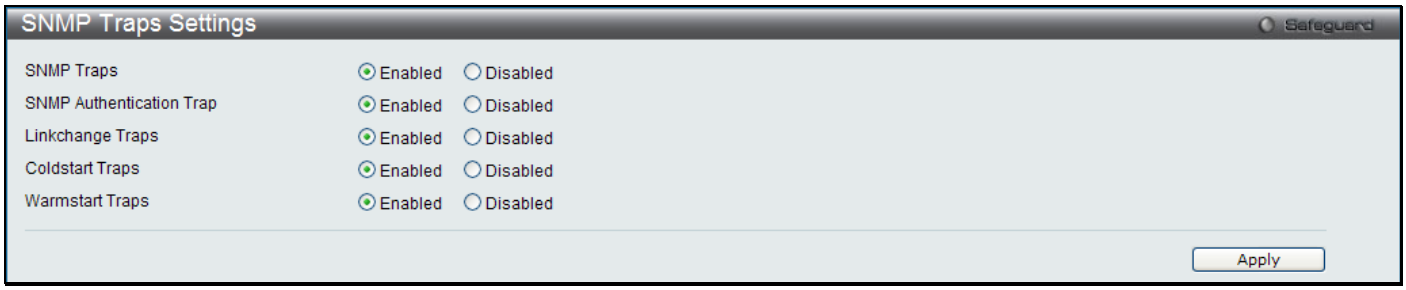


Figure 3-36 SNMP Traps Settings window

The fields that can be configured are described below:

Parameter	Description
SNMP Traps	Enable this option to use the SNMP Traps feature.
SNMP Authentication Trap	Enable this option to use the SNMP Authentication Traps feature.
Linkchange Traps	Enable this option to use the SNMP Link Change Traps feature.
Coldstart Traps	Enable this option to use the SNMP Cold Start Traps feature.
Warmstart Traps	Enable this option to use the SNMP Warm Start Traps feature.

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

SNMP Link Change Traps Settings

On this page the user can configure the SNMP link change trap settings.

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

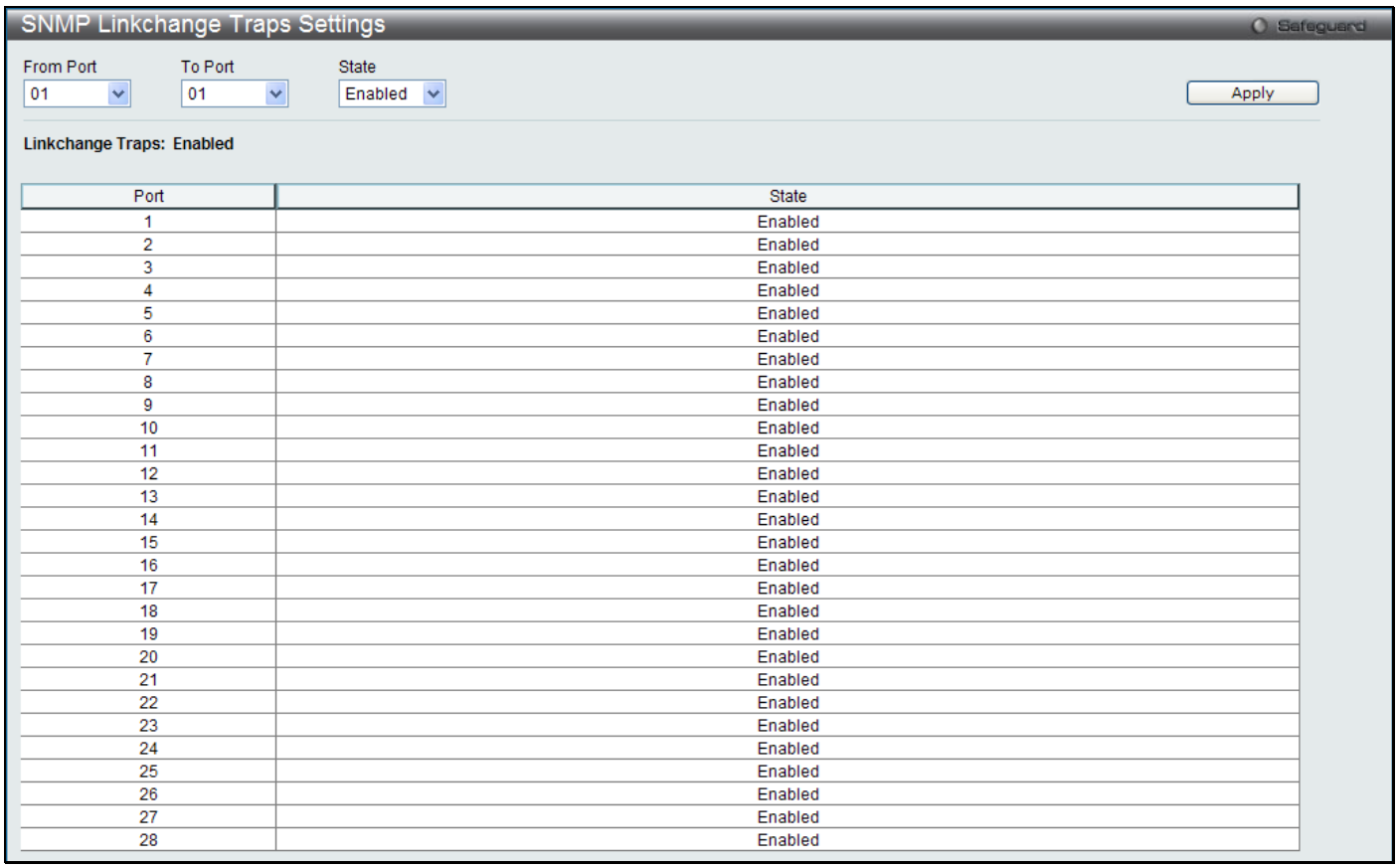


Figure 3-37 SNMP Link Change Traps Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select the starting and ending ports to use.
State	Here the user can enable or disable the SNMP link change Trap.

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

SNMP View Table Settings

Users can 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 Settings > SNMP View Table Settings**, as shown below:

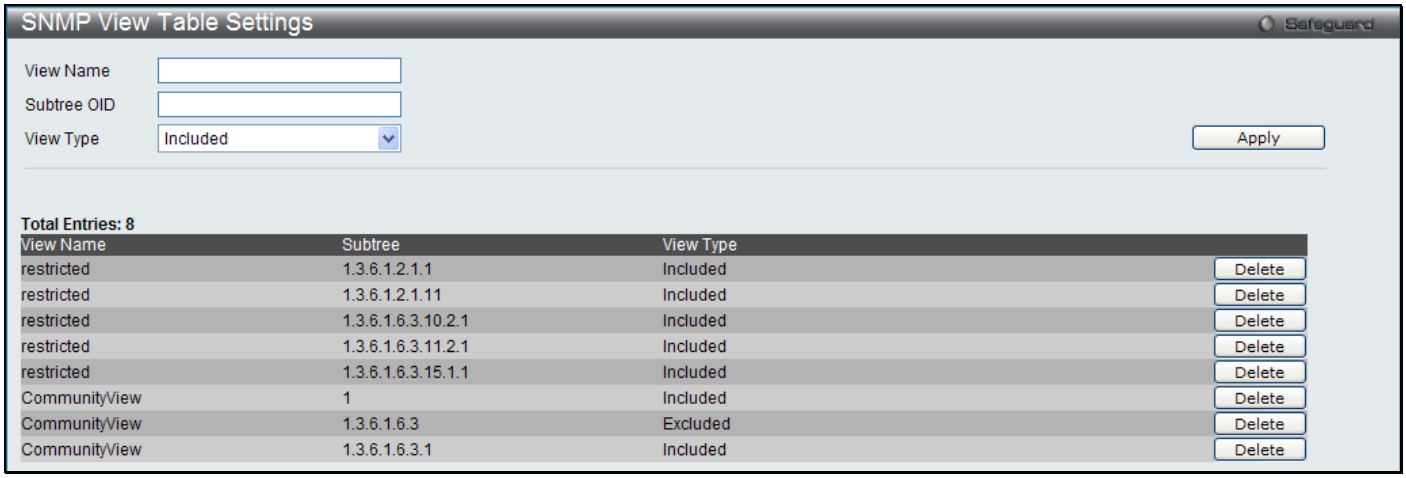


Figure 3-38 SNMP View Table Settings window

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 Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

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

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

SNMP Community Table Settings

Users can 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 Settings > SNMP Community Table Settings**, as shown below:

Figure 3-39 SNMP Community Table Settings window

The fields that can be configured are described below:

Parameter	Description
Community Name	Type 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	Type 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	*Read Only* – Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* – Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

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

Click the **Delete** button to remove the specific 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 Settings > SNMP Group Table Settings**, as shown below:

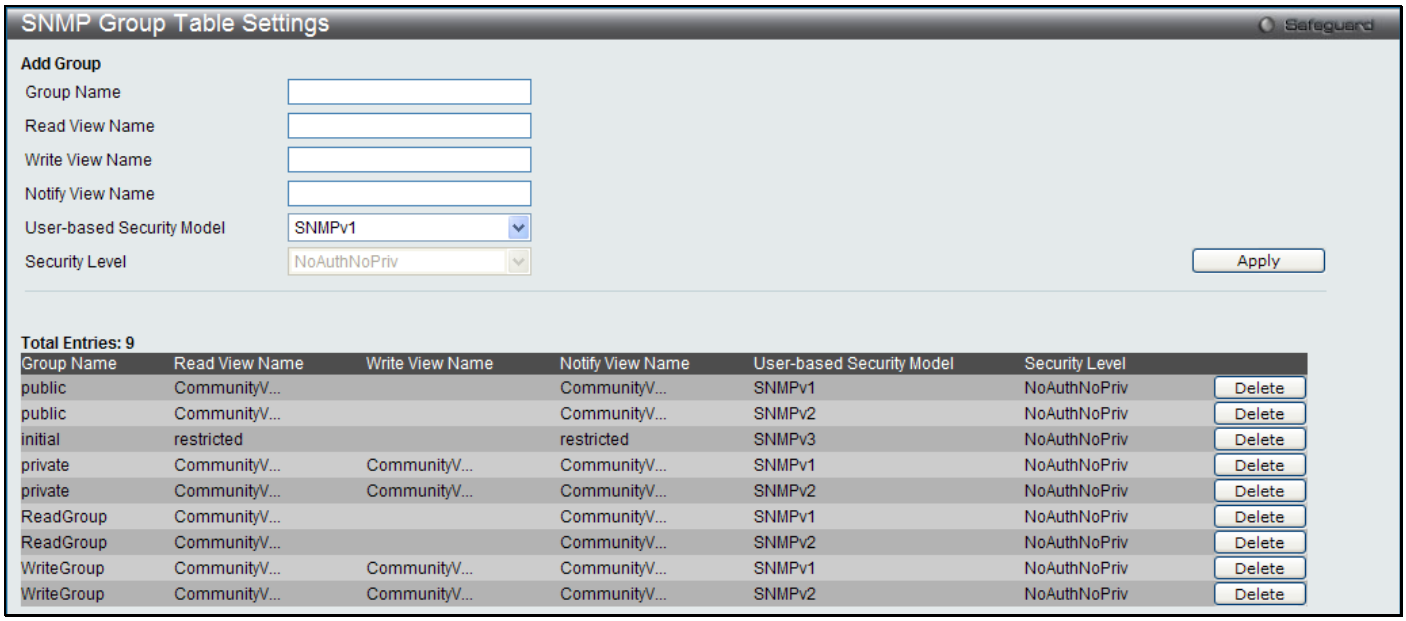


Figure 3-40 SNMP Group Table Settings window

The fields that can be configured are described below:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model	*SNMPv1* – Specifies that SNMP version 1 will be used. *SNMPv2* – Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *SNMPv3* – Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	The Security Level settings only apply to SNMPv3. *NoAuthNoPriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *AuthNoPriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *AuthPriv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

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

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

SNMP Engine ID Settings

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

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

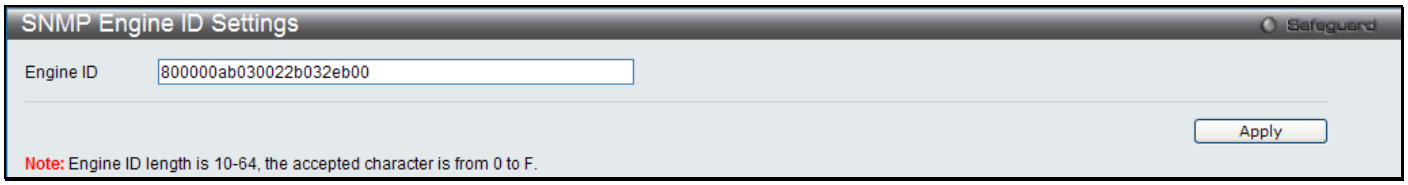


Figure 3-41 SNMP Engine ID Settings window

To change the Engine ID, type the new Engine ID value in the space provided.

The fields that can be configured are described below:

Parameter	Description
Engine ID	The SNMP engine ID displays the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by IANA (D-Link is 171). The fifth octet is 03 to indicate the rest is the MAC address of this device. The sixth to eleventh octets is the MAC address.

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

NOTE: The Engine ID length is 10-64 and accepted characters can range from 0 to F.

SNMP User Table Settings

This window displays all of the SNMP User's currently configured on the Switch.

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

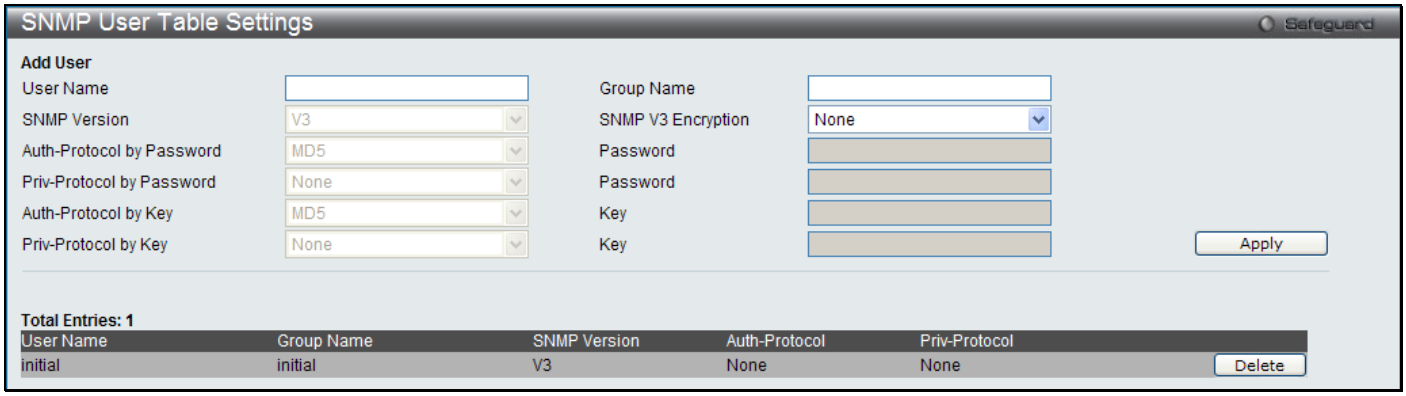


Figure 3-42 SNMP User Table Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V3* – Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	Use the drop-down menu to enable encryption for SNMP V3. This is only operable in SNMP V3 mode. The choices are *None*, *Password*, or *Key*.
Auth-Protocol	*MD5* – Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password. *SHA* – Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.
Priv-Protocol	*None* – Specifies that no authorization protocol is in use. *DES* – Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.

Click the **Apply** button to accept the changes made.
Click the **Delete** button to remove the specific entry.

SNMP Host Table Settings

Users can set up SNMP trap recipients for IPv4.

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

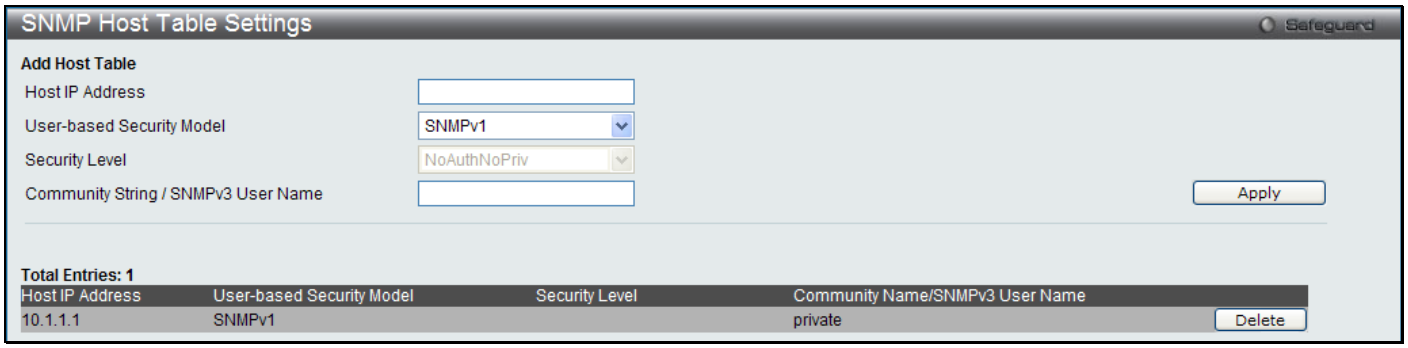


Figure 3-43 SNMP Host Table Settings window

The fields that can be configured are described below:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* – Specifies that SNMP version 1 will be used. *SNMPv2* – Specifies that SNMP version 2 will be used. *SNMPv3* – Specifies that SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level. *AuthNoPriv* – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level. *AuthPriv* – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String / SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

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

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

SNMP v6Host Table Settings

Users can set up SNMP trap recipients for IPv6.

To view the following window, click **Management > SNMP Settings > SNMP v6Host Table Settings**, as shown below:

Figure 3-44 SNMPv6 Host Table Settings window

The fields that can be configured are described below:

Parameter	Description
Host IPv6 Address	Type the IPv6 address of the remote management station that will serve as the SNMP host for the Switch.

User-based Security Model	*SNMPv1* – Specifies that SNMP version 1 will be used. *SNMPv2* – Specifies that SNMP version 2 will be used. *SNMPv3* – Specifies that SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level. *AuthNoPriv* – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level. *AuthPriv* – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String / SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

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

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

RMON Settings

On this page the user can 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 > SNMP Settings > RMON Settings**, as shown below:

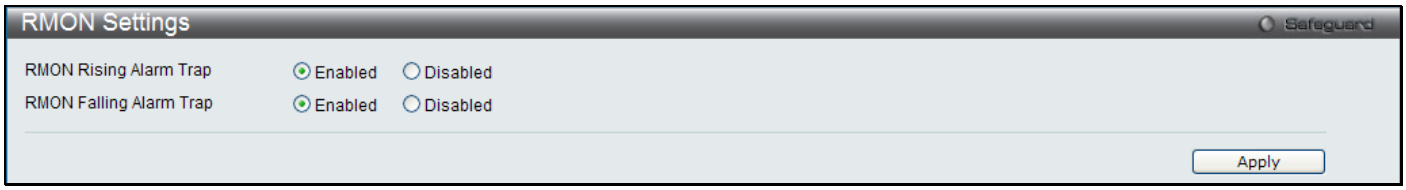


Figure 3-45 RMON Settings window

The fields that can be configured are described below:

Parameter	Description
RMON Rising Alarm Trap	Enable this option to use the RMON Rising Alarm Trap Feature.
RMON Falling Alarm Trap	Enable this option to use the RMON Falling Alarm Trap Feature.

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

Telnet Settings

Users can configure Telnet Settings on the Switch.

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

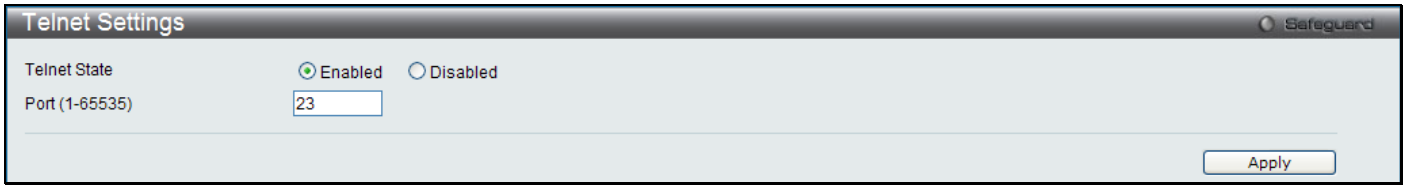


Figure 3-46 Telnet Settings window

The fields that can be configured are described below:

Parameter	Description
Telnet State	Telnet configuration is Enabled by default. If you do not want to allow configuration of the system through Telnet choose Disabled.
Port (1-65535)	The TCP port number used for Telnet management of the Switch. The “well-known” TCP port for the Telnet protocol is *23*.

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

Web Settings

Users can configure the Web settings on the Switch.

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

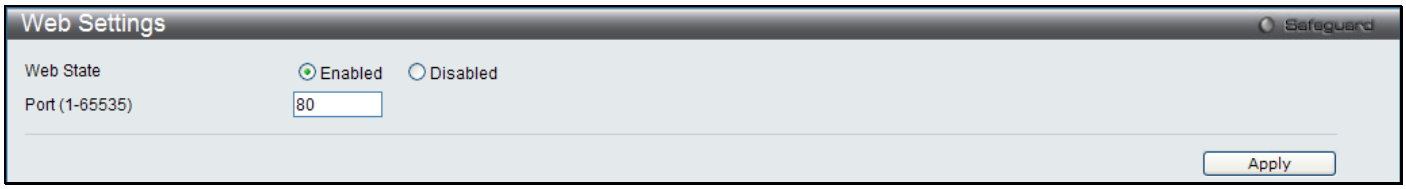


Figure 3-47 Web Settings window

The fields that can be configured are described below:

Parameter	Description
Web Status	Web-based management is Enabled by default. If you choose to disable this by clicking Disabled, you will lose the ability to configure the system through the web interface as soon as these settings are applied.
Port (1-65535)	The TCP port number used for web-based management of the Switch. The “well-known” TCP port for the Web protocol is *80*.

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

Power Saving

Power Saving is one part of D-Link Green Technologies. To learn more about the D-Link Green Technologies, go to http://green.dlink.com/ for more details.

Port LED State Settings

This window allows the user to configure the port LED state.

To view this window, click **Management > Power Saving > LED State Settings** as shown below:

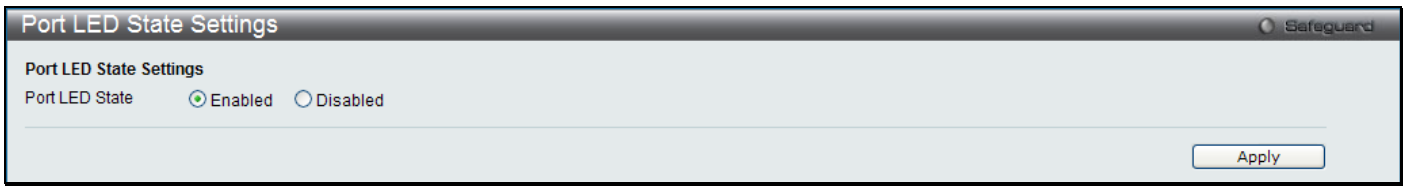


Figure 3-48 Port LED State Settings window

The fields that can be configured are described below:

Parameter	Description
Port LED State	This option can be used to enable or disable the port LED state.

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

Power Saving Settings

This window allows the user to implement the Switch's built-in power saving features and set the schedule to enforce the settings.

To view this window, click **Management > Power Saving > Power Saving Settings** as shown below:

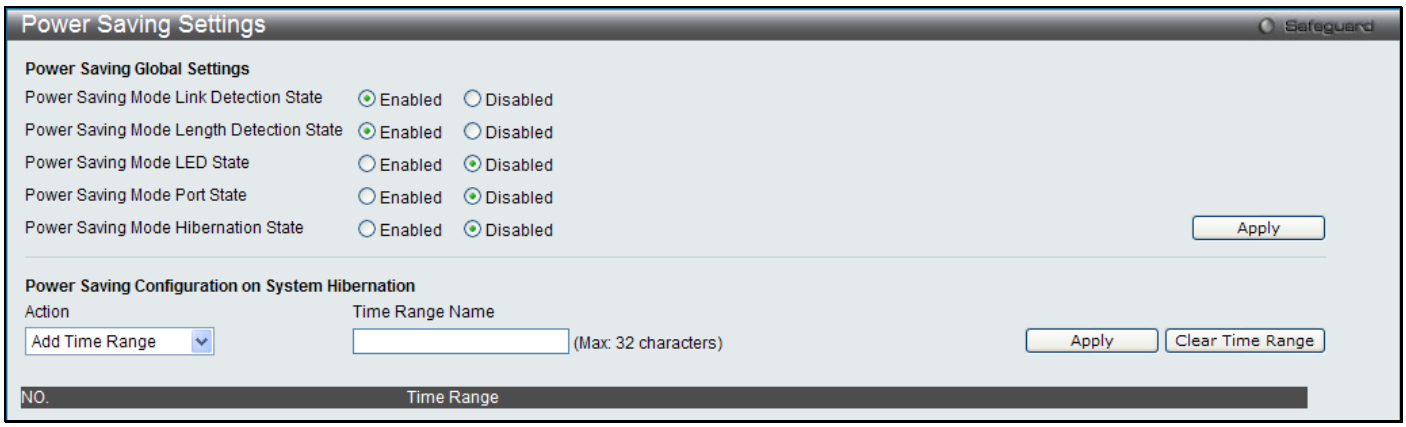


Figure 3-49 Power Saving Settings window

The fields that can be configured are described below:

Parameter	Description
Power Saving Mode Link Detection State	When the Power Saving Mode Link Detection State is 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.
Power Saving Mode Length Detection State	When the Power Saving Mode Length Detection State is enabled, the Switch will automatically determine the length of the cable and adjust the power flow accordingly.
Power Saving Mode LED State	When Power Saving Mode LED State is enabled, the LED's state of ports will be turned off during the configured time range.
Power Saving Mode Port State	When Power Saving Mode Port State is enabled, the ports will be shut down during the configured time range.
Power Saving Mode Hibernation State	When Power Saving Mode Hibernation State is enabled, the Switch will go into a low power state and be idle during the configured time range. It will shut down all the ports, all network function (telnet, ping, etc.) will not work, and only the console connection will work via the RS232 port. If the Switch is an endpoint type PSE (Power Sourcing Equipment), it will not provide power to the port.
Action	Use the drop down menu to add or delete the schedule.
Time Range Name	Specify the name of the schedule.

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

Click the **Clear Time Range** button to remove all the time ranges configured.

Power Saving LED Settings

This window is used to add or delete the power saving schedule on the LED of all ports.

To view this window, click **Management > Power Saving > Power Saving LED Settings** as shown below:

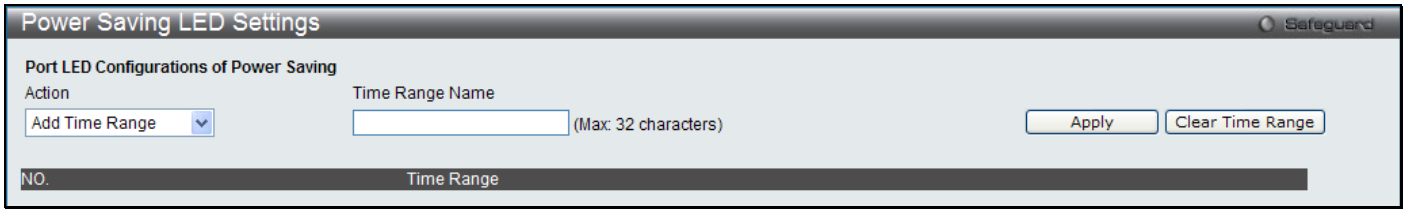


Figure 3-50 Power Saving LED Settings window

The fields that can be configured are described below:

Parameter	Description
Action	Use the drop down menu to add or delete the schedule.
Time Range Name	Enter the name of the schedule used here.

Click the **Apply** button to accept the changes made.
Click the **Clear Time Range** button to remove all the time ranges configured.

Power Saving Port Settings

This window is used to add or delete the power saving schedule on the ports.

To view this window, click **Management > Power Saving > Power Saving Port Settings** as shown below:

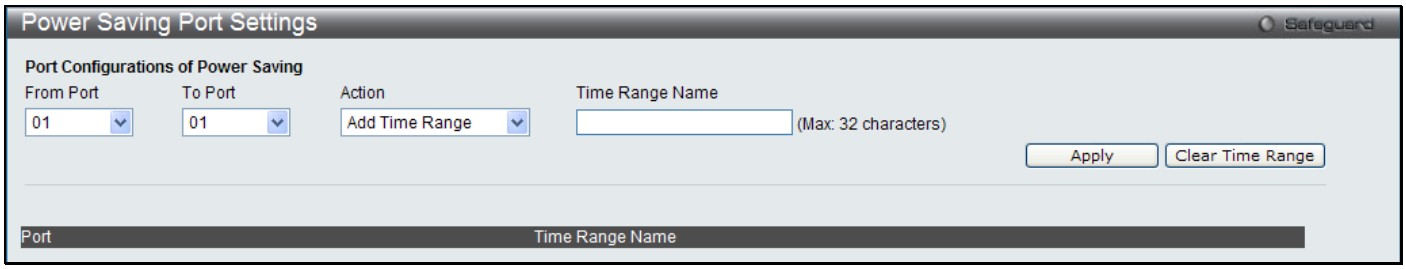


Figure 3-51 Power Saving Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
Action	Use the drop-down menu to add or delete the schedule.
Time Range Name	Enter the name of the schedule used here.

Click the **Apply** button to accept the changes made.
Click the **Clear Time Range** button to remove all the time ranges configured.

Chapter 4 VPN (EI Mode Only)

MPLS
VPWS

MPLS

Multiprotocol Label Switching (MPLS) is a protocol that works between the network layer and the data link layer of the TCP/IP protocol stack and is used to replace conventional IP forwarding with label switching. The most powerful feature of MPLS is that it is not limited by any specific protocol in the data link layer and can use any Layer 2 media to transfer packets.

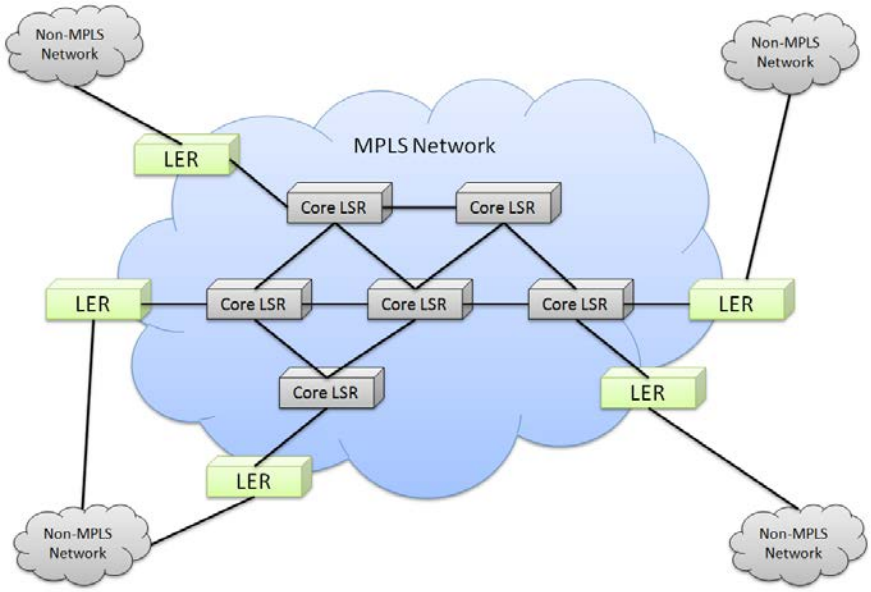


Figure 4-1 MPLS Network Structure

In an MPLS network, the most important node is called a **Label Switching Router (LSR)**. An LSR that is located on the edge of the MPLS domain is known as a **Label Edge Router (LER)**. An LSR that is located within the MPLS domain is known as a **Core LSR**. When a packet is received by a LSR, from another LSR, the sending LSR is known as the **upstream** LSR. The receiving LSR is known as the **downstream** LSR of the sending LSR. Consider the following example. When packets travel from LSR A, through LSR B, to LSR C, LSR A is the upstream LSR of LSR B and LSR C is the downstream LSR of LSR B.

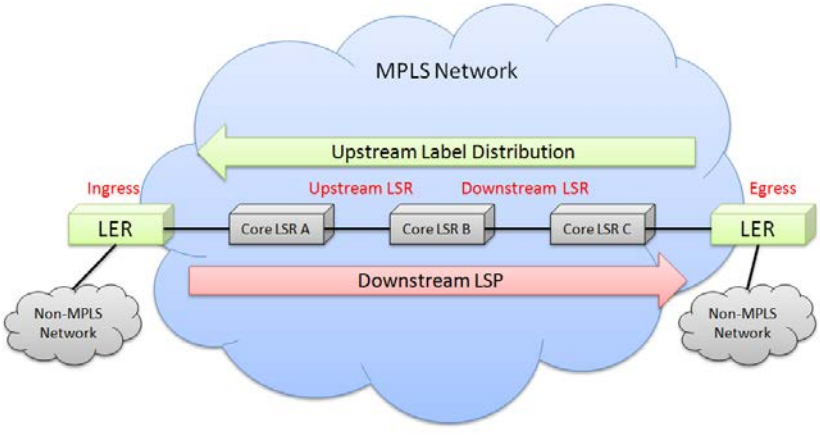


Figure 4-2 MPLS Descriptive Diagram

When a packet enters the MPLS domain, the LER is responsible for adding a label to the packet. Also when a packet leaves the MPLS domain, the LER is responsible for removing the label. Inside the MPLS domain, packets will be transferred based on their label. The path that a packet follows, in and out of an MPLS domain, is known as a **Label Switch Path (LSP)**. The LSP, under normal circumstances, is unidirectional. The first LER, in the LSP, is known as the LSP's **ingress** and the last LER, in the LSP, is known as the LSP's **egress**. There can be only one ingress and egress in an LSP.

When an unlabeled packet enters the ingress router and needs to be passed on to an LSP, the ingress LER first determines the **Forwarding Equivalence Class (FEC)** the packet should be in, and then inserts one or more labels in the packet's MPLS header. The packet is then passed on to the next LSR.

Labels are distributed between LERs and LSRs using the **Label Distribution Protocol (LDP)**. The LDP defines the bi-directional communication between the ingress and the egress LERs of a specific MPLS tunnel, through the MPLS domain. LERs, using LDP, will build and maintain an LSP database that will be used to forward traffic through the MPLS network. Thus, the two peer LERs will constantly exchange this information to effectively control the traffic flow. Labels are always distributed, through the LSP, in the opposite direction of the dataflow. In other words, the label distribution takes place in an upstream direction. The main function of LDP is to **classify FEC**s, **distribute labels**, and **create and maintain LSP**s.

Static LSP – Users can configure the LSP manually by physically defining the outgoing labels of upstream LSRs and incoming labels of downstream LSRs. Static LSPs are configured without the need for LDP or exchange control packets. This configuration has very little data overhead and is suitable for small-scale networks only, where the network layout is simple and static.

Dynamic LSP – Users can configure the LSP to initiate automatically with the use of LDP. Additionally, the **Interior Gateway Protocol (IGP)**, the **Border Gateway Protocol (BGP)**, and the **Resource Reservation Protocol (RSVP)** can also be extended to distribute MPLS labels adding the routing functionality. This configuration is suitable for large-scale networks and is also used for VPN services.

Structure of an MPLS packet header:

Figure 4-3 MPLS Packet Header

The label contains the following fields:

Parameter	Description
Label	This indicates the value field of the label. The length is 20 bits.
EXP	This indicates the bits used for extension. The length is 3 bits. Normally this field is used for the Class of Service (CoS) service.
S	This indicates the bottom of the label stack value. The length is 1 bit. When this value is set, in other words configured as '1', it means that this entry is at the bottom of the label stack.
TTL	This indicates the time-to-live (TTL) value. The length is 8 bits. This field is similar to the TTL in IP packets.

Labels are always encapsulated between the data link layer and the networking layer. This means that encapsulation labels support all protocols available in the data link layer.

LDP

LDP Settings

This window is used to configure the LDP Settings used on this Switch

To view this window, click **VPN > MPLS > LDP > LDP Settings** as shown below:

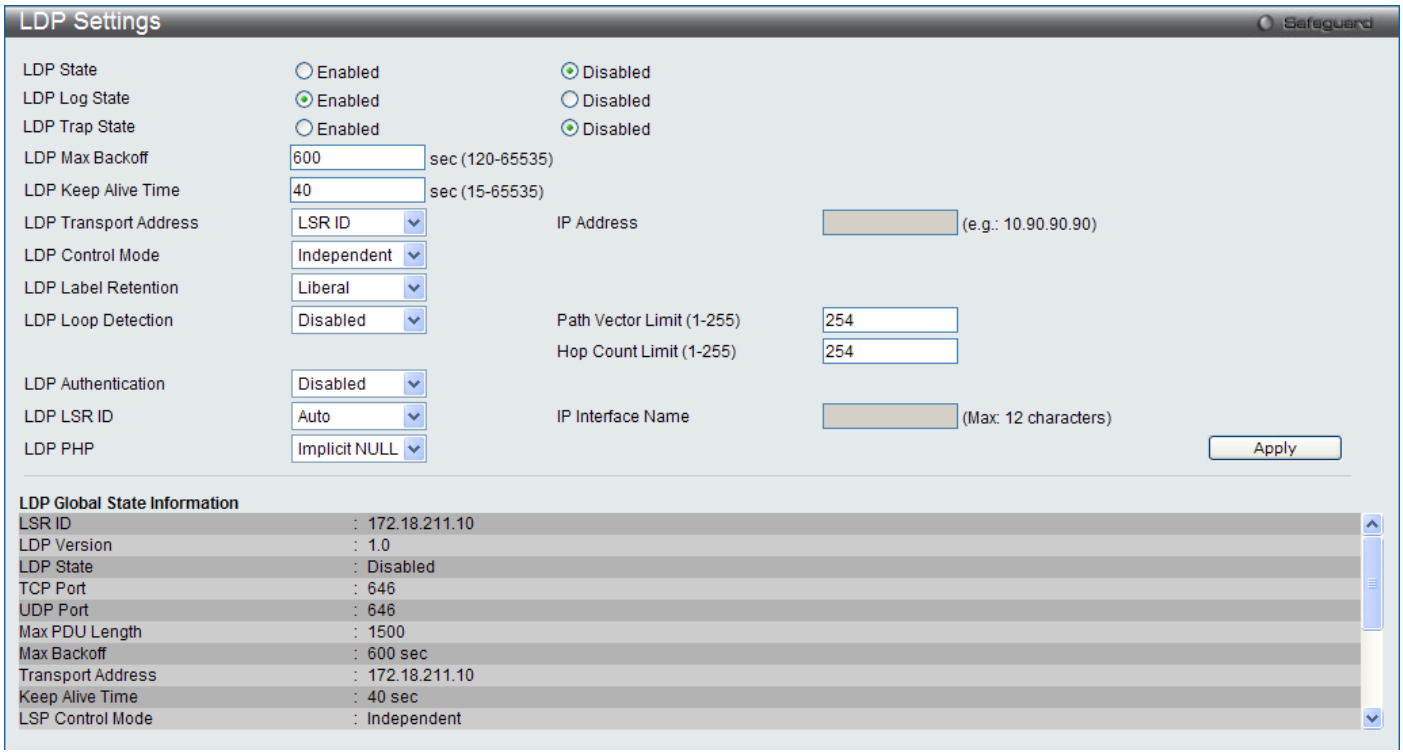


Figure 4-4 LDP Settings window

The fields that can be configured are described below:

Parameter	Description
LDP State	Specifies the state of LDP on the specified interface. Take note that MPLS must be enabled otherwise LDP will be inactive.
LDP Log State	Enable or disable the LDP log state here.
LDP Trap State	Enable or disable the LDP trap state here.
LDP Max Backoff	Enter the maximum back-off time used here. The LDP back-off mechanism prevents two incompatibly configured LSRs from engaging in an endless sequence of session setup failures. If a session setup attempt fails due to an incompatibility, the active LSR delays its next attempt and then retries the session establishment. The delay begins at 15 seconds, and it is increased exponentially with each successive failure until the maximum back-off delay is reached. If a session cannot be established and the trap or log state is enabled, LDP will send a trap or a log to the SNMP server to notify the session establishment failure. This value must be between 120 and 65535 seconds.
LDP Keep Alive Time	Enter the LDP session keep-alive time here. LDP maintains a keep-alive timer for each peer session. If the keep-alive timer expires without the receipt of an LDP PDU from the peer, LDP will conclude that the peer has failed and will terminate the LDP session. Each LSR sends keep-alive messages at regular intervals to its LDP peers to keep the sessions active. This value must be between 15 and 65535 seconds.
LDP Transport Address	Select the LDP transport address mode used here. The transport address is used to establish the LDP TCP connection. By default, the LSR ID is used as the transport address by all of the interfaces. If you select the transport address to a specific *IP address*, this address is used as the transport address by all the interfaces. If you configure the transport address to *Interface*, the IP address of each interface is used as the transport address. Selecting *LSR ID* specifies that the LSR ID will be used as the

	transport address.
LDP Control Mode	Select the LSP control mode used here. In *Independent* LSP Control, each LSR independently binds a label to a FEC and distributes the binding to its label distribution peers. In *Ordered* LSP Control, an LSR only binds a label to a FEC if it is the egress LSR for that FEC, or if it has already received a label binding for that FEC from its next hop for that FEC.
LDP Label Retention	Select the LDP label retention mode here. If the label distribution method is Downstream-Unsolicited and the label retention mode is *Conservative*, it will discard the bindings once the LSR have received label bindings from the LSRs, which are not its next hop for that FEC. If the label retention mode is *Liberal*, it will maintain the bindings. This helps to speed up the setup of LSP in case there is a change in the next hop.
LDP Loop Detection	Enable or disable the LDP loop detection mode here. The LDP loop detection mechanism makes use of the Path Vector and Hop Count TLVs carried by the label request and labeling mapping messages to detect looping LSPs.
Path Vector Limit (1-255)	Enter the path vector limit value used here. This value must be between 1 and 255.
Hop Count Limit (1-255)	Enter the hop count limit used here. This value must be between 1 and 255.
LDP Authentication	Enable or disable the LDP authentication option here. If the authentication is enabled, the LSR applies the MD5 algorithm to compute the MD5 digest for the TCP segment that will be sent to the peer. This computation makes use of the peer password as well as the TCP segment. When the LSR receives a TCP segment with an MD5 digest, it validates the segment by calculating the MD5 digest, using its own record of the password, and comparing the computed digest with the received digest. If the comparison fails, the segment is dropped without any response to the sender. The LSR ignores LDP Hellos from any LSR of which a password has not been configured.
LDP LSR ID	Select the LDP LSR ID mode used here. The LSR ID is used to identify the LSR in the MPLS network and is the IPv4 address of an interface. The recommended interface for the LSR ID is the loopback interface. If the LSR ID is set to *Auto*, this decision will be based on the following rule. If a loopback interface is configured, the LSR ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the loopback with the highest IP address will be used. If no loopback interface is configured, the LSR ID is set to the highest IP address of the physical interfaces. Select and enter **IP Interface** to specify whose IP Interface is used as the LSR ID.
LDP PHP	Select the LDP Penultimate Hop Popping (PHP) behavior used here. If the LSR is set as egress and the PHP is configured to *Implicit NULL*, it will distribute an implicit NULL label to the upstream (Penultimate Hop). The upstream will then do Penultimate Hop Popping. If the label distributed to Penultimate Hop is set as *Explicit NULL*, the Penultimate Hop won't pop it.

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

LDP Statistic Table

This window is used to clear the LDP statistics.

To view this window, click **VPN > MPLS > LDP > LDP Statistic Table** as shown below:

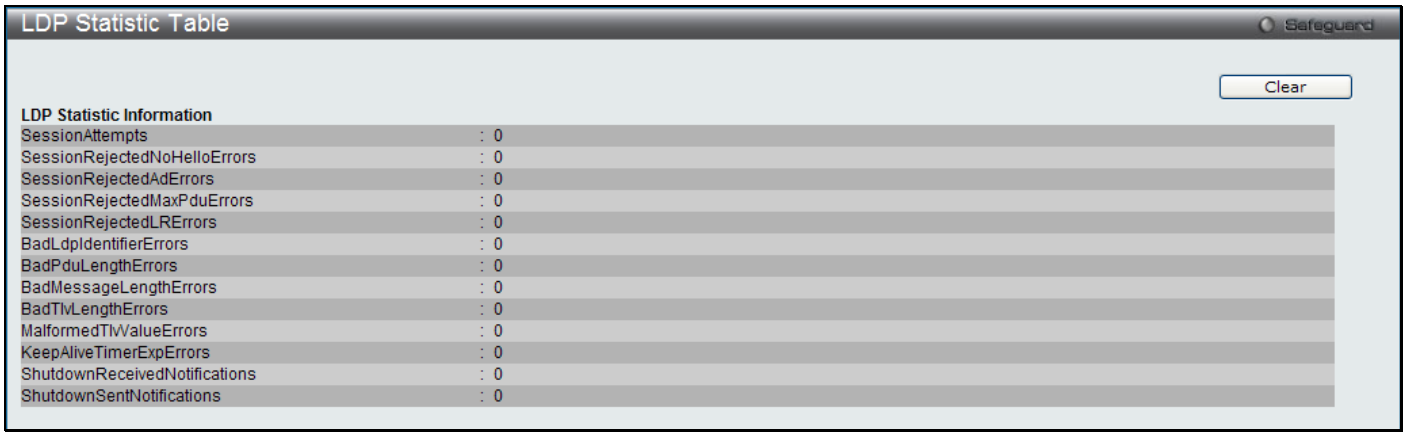


Figure 4-5 LDP Statistic Table window

Click the **Clear** button to clear all the information listed.

LDP IP Interface Settings

This window is used to configure the LDP parameters for a specified interface.

To view this window, click **VPN > MPLS > LDP > LDP IP Interface Settings** as shown below:

Figure 4-6 LDP IP Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface	Enter the IP interface name used here. This name can be up to 12 characters long.
Admin State	Enable or disable the admin state of LDP on the specified interface. Take note that MPLS must be enabled otherwise LDP will be inactive.
Targeted Hello Accept	Specifies to accept or deny targeted hello messages. If a targeted hello message is acceptable, the interface will respond to received targeted hello messages. Otherwise the received targeted hello message will be ignored.
Hold Time (5-65535)	Enter the link hold time value here. LDP sends link hello message periodically to discover directly connected neighbors. LDP will then maintain a hold timer for each discovered neighbor. If the timer expires without the receipt of a hello message from the neighbor, LDP will conclude that the neighbor has failed. This value must be between 5 and 65535 seconds.
Interval (1-65535)	Enter the interval value used here. This value must be between 1 and 65535 seconds.
Distribution Method	Select the LDP label distribution method used here. Selecting *DU* specifies that the distribution mode will be set to Downstream-Unsolicited. Selecting *DoD* specifies that the distribution mode will be set to Downstream-on-Demand.

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

LDP Targeted Peer Settings

This window is used to configure the LDP targeted peer.

To view this window, click **VPN > MPLS > LDP > LDP Targeted Peer Settings** as shown below:

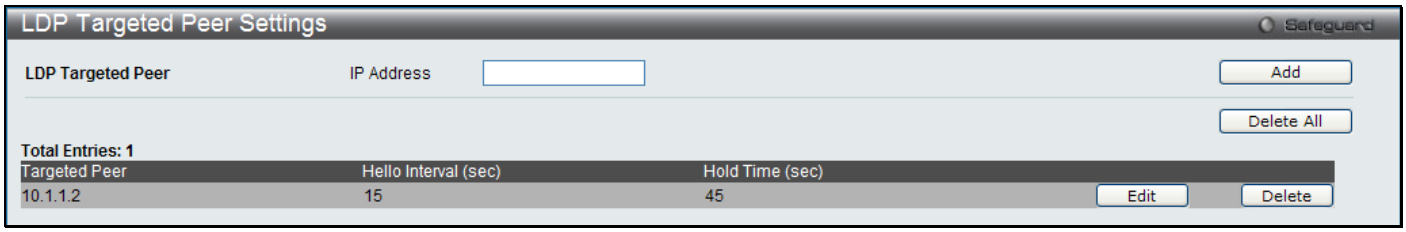


Figure 4-7 LDP Targeted Peer Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the targeted peer's IP address used here. It must be the targeted peer's LSR ID.
Hello Interval	Click the **Edit** button and enter the targeted hello sending interval value used here. This value must be between 5 and 65535 seconds.
Hold Time	Click the **Edit** button and enter the targeted hello hold time used here. This value must be between 15 and 65535 seconds.

Click the **Add** button to add a new entry.
Click the **Delete All** button to remove entries in the list.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specified entry.

LDP Neighbor Table

This window is used to display all adjacencies discovered by LDP.

To view this window, click **VPN > MPLS > LDP > LDP Neighbor Table** as shown below:

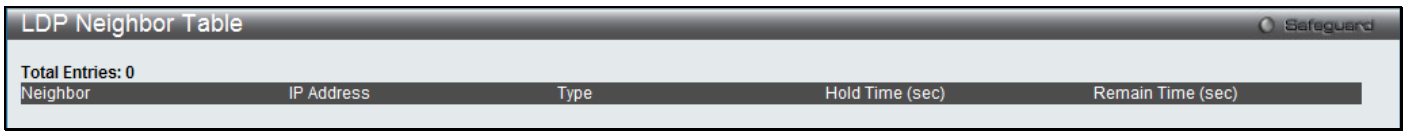


Figure 4-8 LDP Neighbor Table window

LDP Peer Table

This window is used to display LDP peer information.

To view this window, click **VPN > MPLS > LDP > LDP Peer Table** as shown below:

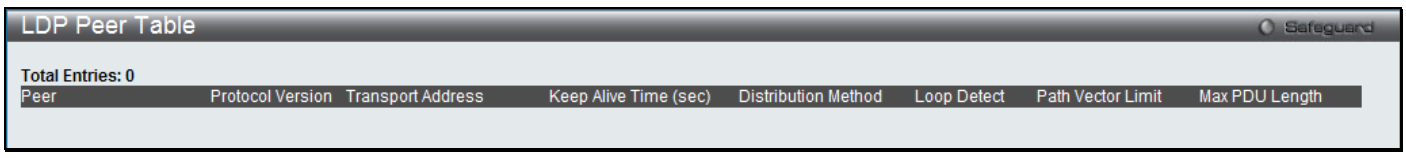


Figure 4-9 LDP Peer Table window

LDP Peer Password Settings

This window is used to configure a LDP peer password.

To view this window, click **VPN > MPLS > LDP > LDP Peer Password Settings** as shown below:

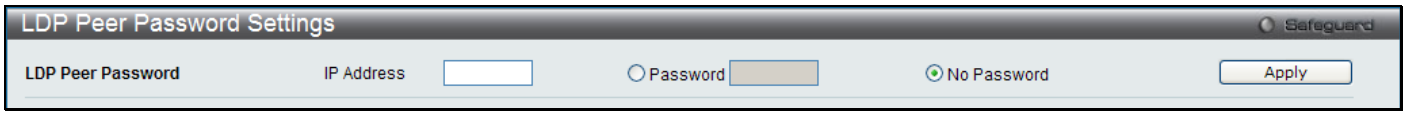


Figure 4-10 LDP Peer Password Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the peer IP address used here. The IP address shall be the peer's LSR ID.
Password	Select and enter the peer password used here. This password can be up to 32 characters long.
No Password	Specifies that the peer password will be set to no password.

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

LDP Session Table

This window is used to display all LDP sessions.

To view this window, click **VPN > MPLS > LDP > LDP Session Table** as shown below:

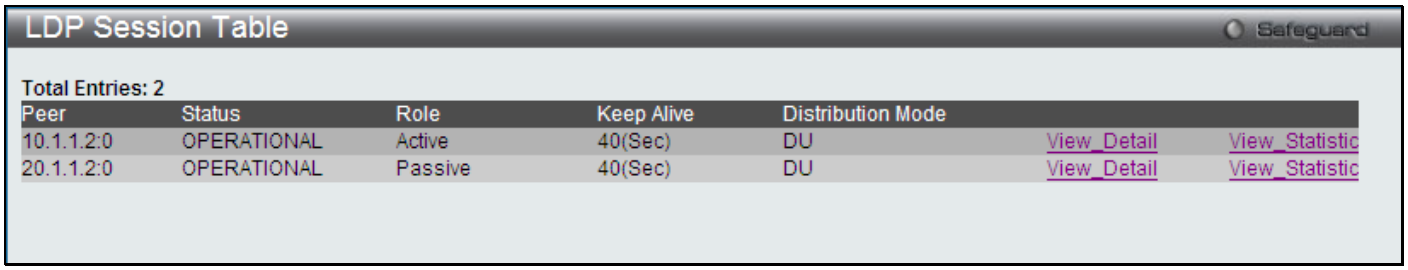


Figure 4-11 LDP Session Table window

Click the View Detail link to navigate to a new window containing more detailed information about the entry.
Click the View Statistic link to navigate to a new window containing more detailed statistic information about the entry.

After click the View Detail link, the following page will be displayed.

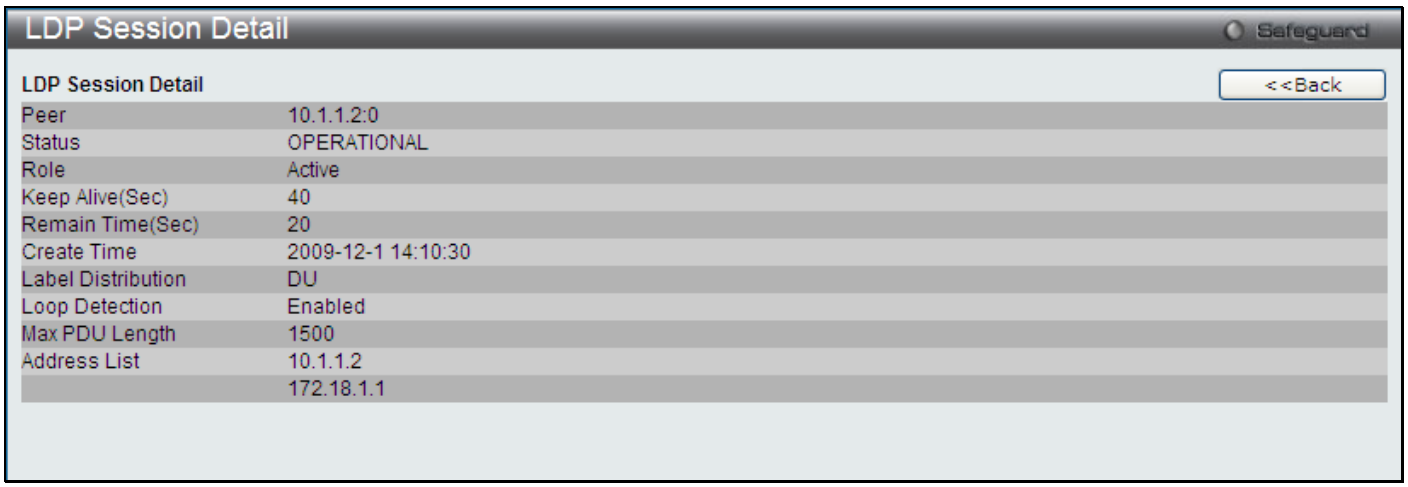


Figure 4-12 LDP Session Detail window

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

After click the View Statistic link, the following page will be displayed.

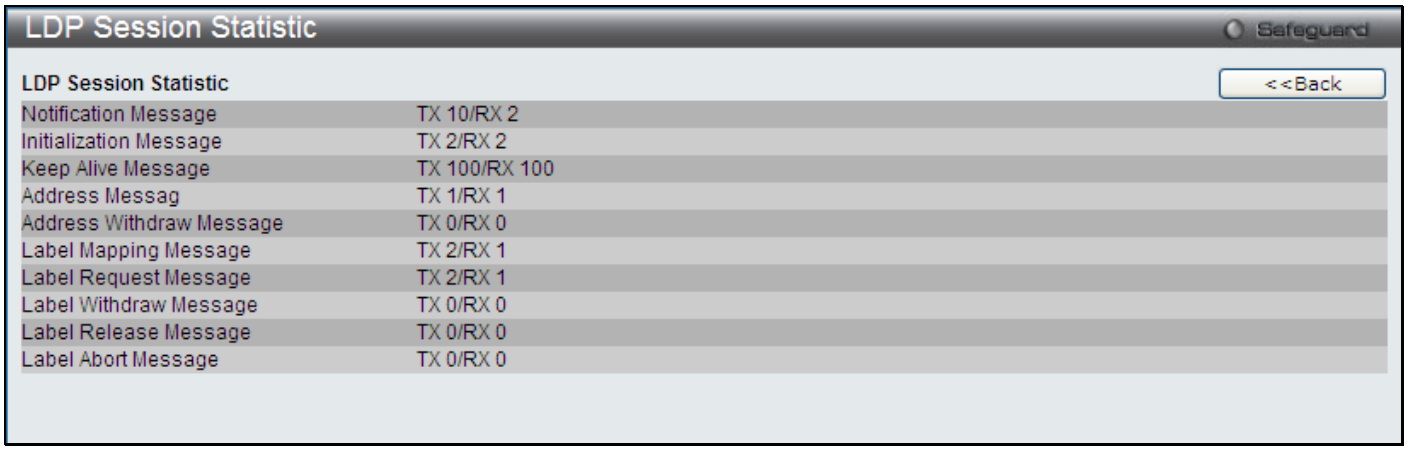


Figure 4-13 LDP Session Statistic window

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

LDP Binding Table

This window is used to display all LDP label binding information.

To view this window, click **VPN > MPLS > LDP > LDP Binding Table** as shown below:

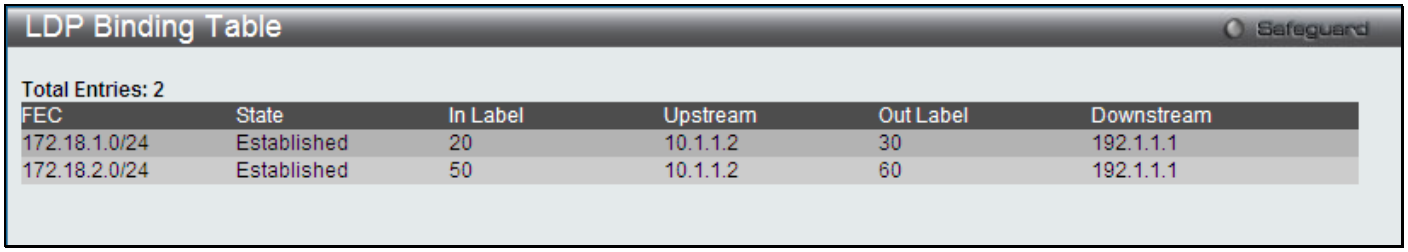


Figure 4-14 LDP Binding Table window

MPLS Settings

This window is used to enable or disable the MPLS function globally. Also on this page the user can configure the Trust EXP, MPLS Log, and MPLS Trap's state.

To view this window, click **VPN > MPLS > MPLS Settings** as shown below:

Figure 4-15 MPLS Settings window

The fields that can be configured are described below:

Parameter	Description
MPLS State	Enable or disable the MPLS function globally here.
Trust EXP	Enable or disable the MPLS trust EXP option here. If the EXP is trusted, the EXP value of the incoming label will be used as the QoS of the incoming packet. Otherwise, the EXP value will not be used for QoS.
Log	Enable or disable the MPLS log state here.

Trap	Enable or disable the MPLS trap state here.

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

MPLS Static LSP Settings

This window is used to configure the MPLS static LSP settings.

To view this window, click **VPN > MPLS > MPLS Static LSP Settings** as shown below:

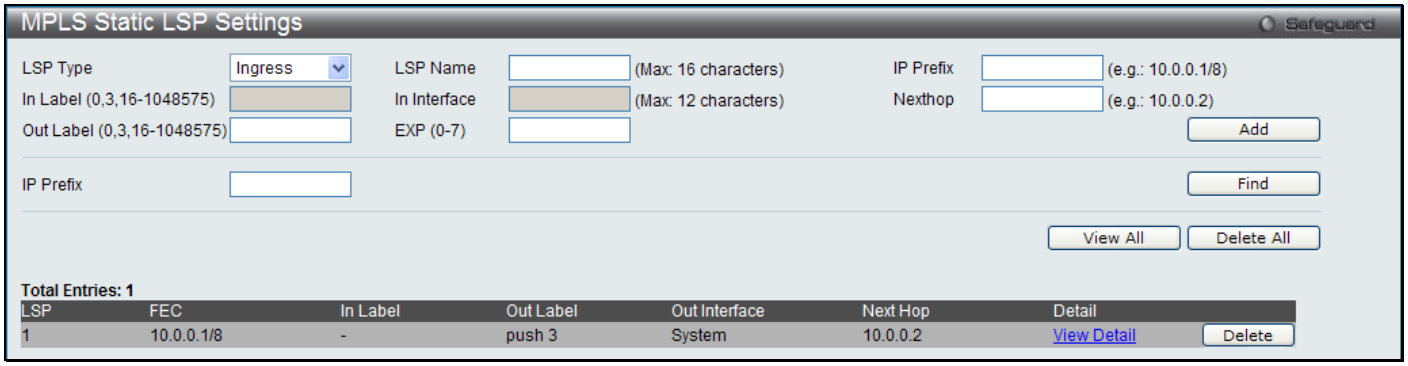


Figure 4-16 MPLS Static LSP Settings window

The fields that can be configured are described below:

Parameter	Description
LSP Type	Select to establish a static *Egress* LSP or a static *Ingress* LSP here.
LSP Name	Enter the LSP name used here. This name can be up to 16 characters long.
IP Prefix	Enter the IP prefix FEC address of the LSP here. The specified FEC will map to the LSP.
In Label	Enter the incoming label value used here.
In Interface	Enter the incoming interface name used here. This name can be up to 12 characters long.
Nexthop	Enter the next hop IP address used here.
Out Label	Enter the outbound label value used here.
EXP	Enter the EXP value used here. By default the EXP is set according to the QoS of the incoming packet. If the EXP is specified, the EXP of the outbound label will be set according to specified value. This value must be between 0 and 7.

Click the **Add** button to add a new entry.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the configure entries.
Click the **Delete All** button to remove entries in the list.
Click the View Detail link to navigate to a new window containing more detailed information about the entry.

After click the View Detail link, the following page will be displayed.

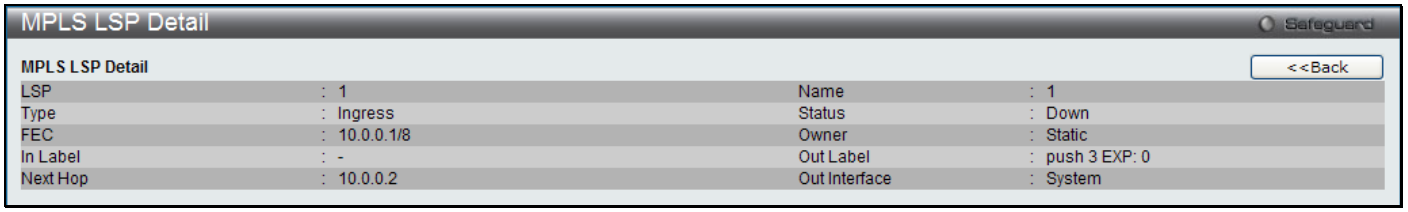


Figure 4-17 MPLS LSP Detail window

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

MPLS Dynamic LSP Table

This window is used to locate and display dynamic MPLS LSP entries.

To view this window, click **VPN > MPLS > MPLS Dynamic LSP Table** as shown below:

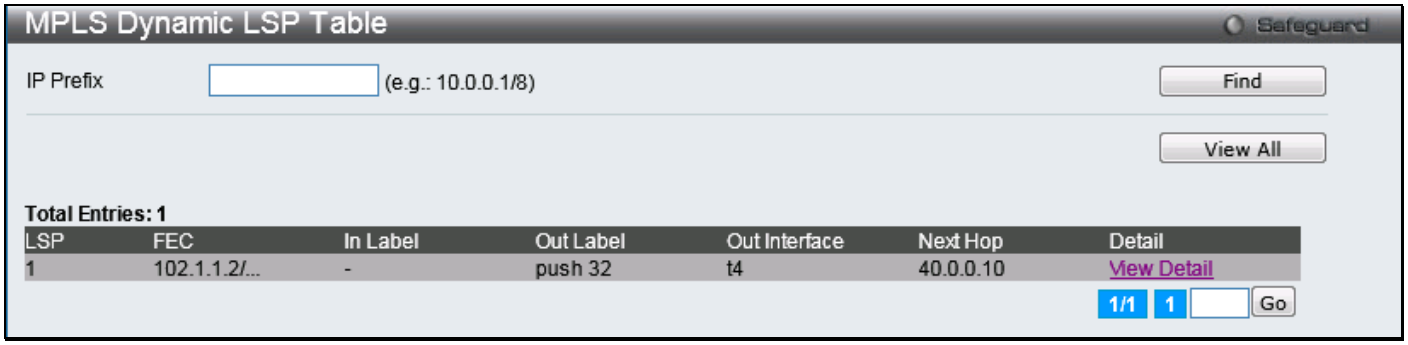


Figure 4-18 MPLS Dynamic LSP Table window

The fields that can be configured are described below:

Parameter	Description
IP Prefix	Enter the IP prefix FEC address of the LSP here.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the configure entries.
Click the View Detail link to navigate to a new window containing more detailed information about the entry.

After click the View Detail link, the following page will be displayed.

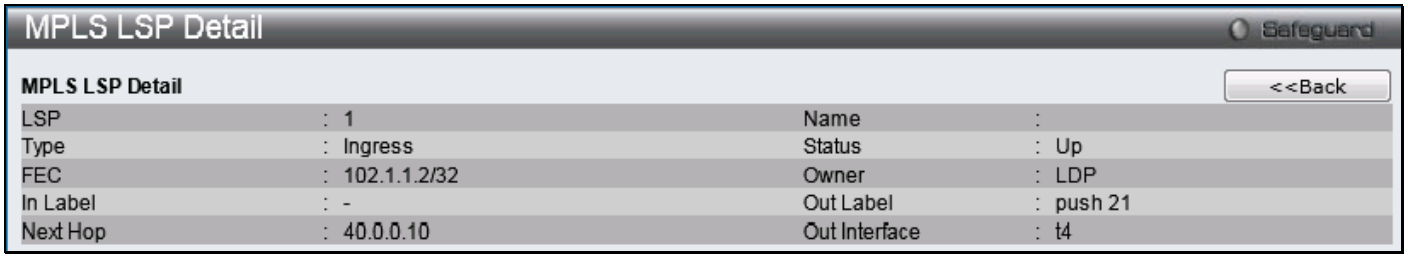


Figure 4-19 MPLS LSP Detail window

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

MPLS FTN Table

The Next-Hop Label Forwarding Entry (NHLFE) is used to guide the MPLS packet forwarding. The NHLFE contains the following information: Tunnel ID, outgoing interface, next hop, outgoing label, and the label operation.

To view this window, click **VPN > MPLS > MPLS FTN Table** as shown below:

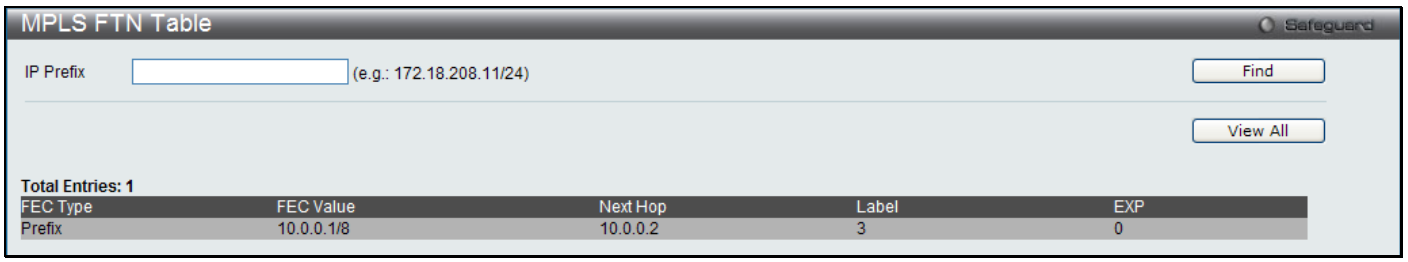


Figure 4-20 MPLS FTN Table window

The fields that can be configured are described below:

Parameter	Description
IP Prefix	Enter the IP prefix FEC address of the LSP here.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the configure entries.

MPLS Interface Settings

This window enables or disables MPLS on the specified interface.

To view this window, click **VPN > MPLS > MPLS Interface Settings** as shown below:

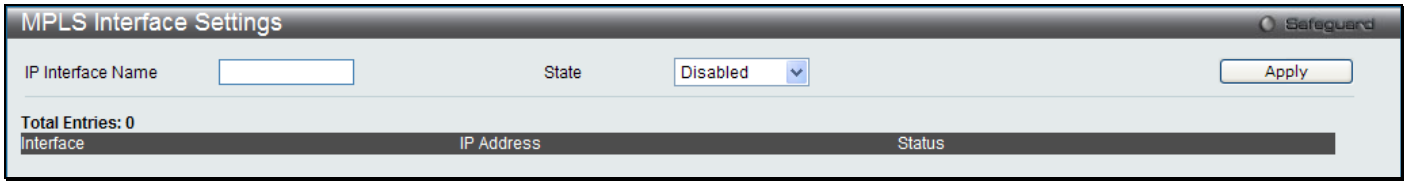


Figure 4-21 MPLS Interface Settings window

The fields that can be configured are described below:

Parameter	Description
IP Interface Name	Enter the IP interface name used here. This name can be up to 12 characters long.
State	Enabled or disabled the MPLS IP interface. By default, the state is disabled on all interfaces.

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

MPLS Class Map Settings

This window is used to configure the mapping between the EXP and CoS. CoS 7 is reserved for the system.
The following table shows the default mapping between EXP and CoS.

EXP	0	1	2	3	4	5	6	7
CoS	2	0	1	3	4	5	6	6

To view this window, click **VPN > MPLS > MPLS Class Map Settings** as shown below:

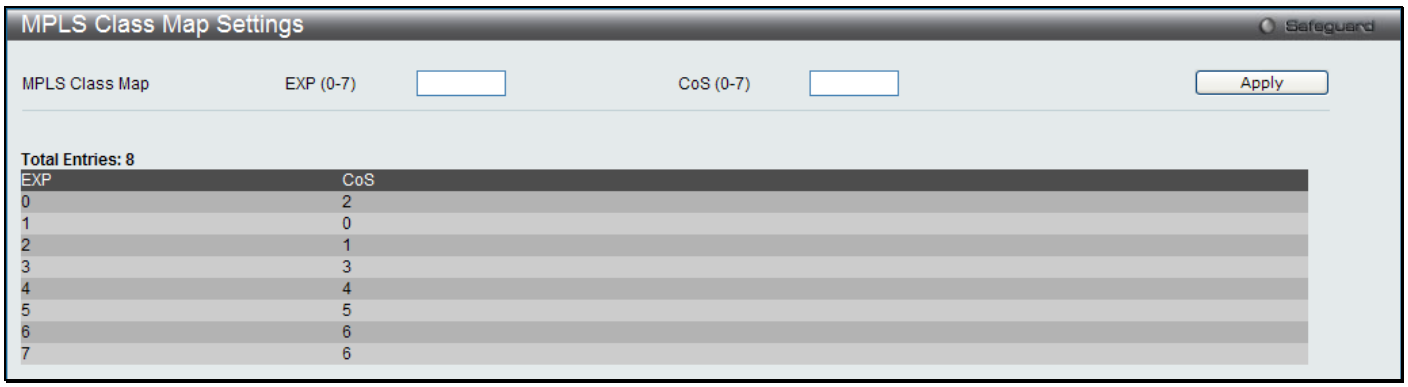


Figure 4-22 MPLS Class Map Settings window

The fields that can be configured are described below:

Parameter	Description
EXP (0-7)	Enter the EXP value, that will be mapped to the CoS, here. This value must be between 0 and 7.

CoS (0-7)	Enter the CoS value used here. This value must be between 0 and 7.

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

MPLS FEC EXP Settings

This window is used to configure the EXP assignment of FEC. If the EXP is not explicitly assigned by creating an LSP, the outbound EXP of the specified FECs will be set according to the configured EXP value. By default, the EXP value in outbound label for all FECs is set according to the incoming packet's QoS.

To view this window, click **VPN > MPLS > MPLS FEC EXP Settings** as shown below:

Figure 4-23 MPLS FEC EXP Settings window

The fields that can be configured are described below:

Parameter	Description
IP Prefix	Enter the IP prefix FEC address used here.
EXP (0-7)	Enter the EXP value in the outbound label for the FEC here. This value must be between 0 and 7. Tick the **Default** check box to set the EXP value according to the incoming packet's QoS.

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

VPWS

The **Virtual Private Wire Service (VPWS)** is a L2VPN solution that provides Layer 2 point-to-point virtual circuit connectivity between customer sites over a provider network. VPWS enables the sharing of a provider's core network infrastructure between IP and L2VPN services, reducing the cost of providing those services. The tunneling mechanism of the VPWS can use any tunneling protocol, like MPLS for the transport layer.

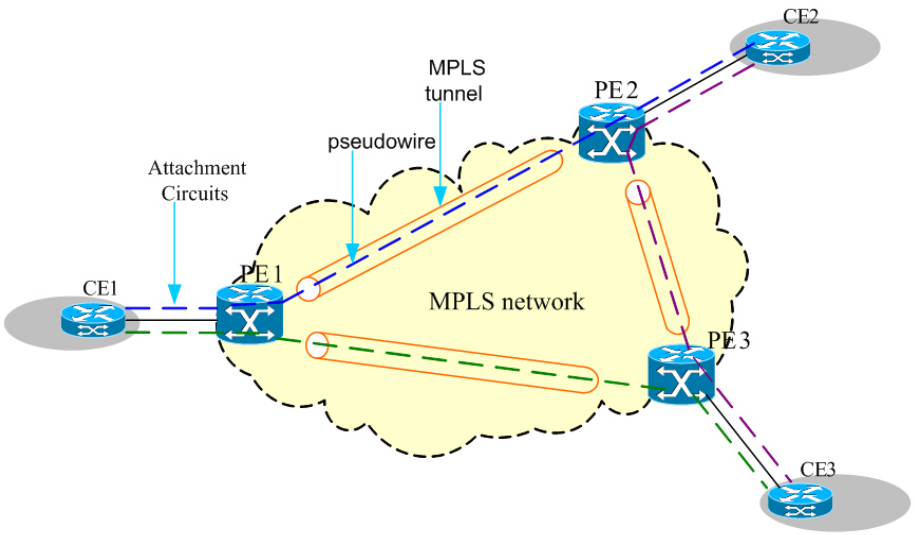


Figure 4-24 MPLS-based VPWS Illustration

In above figure, the MPLS network is a packet switched network (PSN). Each Customer Edge (CE) device is connected to the Provider Edge (PE) via an Attachment Circuit (AC). The PE does a one-to-one mapping between the

Pseudo-Wire (PW) and AC based on local information. A PW is an emulated point-to-point connection over a packet switched network that allows the interconnection of two nodes with any Layer 2 technology.

The required functions of PWs include encapsulating service-specific bit streams, cells, or PDUs arriving at an ingress port and carrying them across an IP path or MPLS tunnel. PWs provide the following functions in order to emulate the behavior and characteristics of the native service.

- Encapsulation of service-specific PDUs or circuit data arriving at the PE-bound port (logical or physical).
- Carriage of the encapsulated data across a PSN tunnel.
- Establishment of the PW, including the exchange and/or distribution of the PW identifiers used by the PSN tunnel endpoints.
- Managing the signaling, timing, order, or other aspects of the service at the boundaries of the PW. Service-specific status and alarm management.

One or more PWs are carried in an MPLS tunnel from one PE to another. Any given frame travels first on its ingress AC, then on a PW, and then on its egress AC. This particular combination forms a virtual circuit between two CE devices.

Virtual Private Network (VPN) - A VPN is the extension of a private network that encompasses links across public networks like the Internet. A VPN enables you to send data between two computers across a public network in a manner that emulates the properties of a point-to-point private link.

Virtual Private Wire Service (VPWS) - A VPWS is a VPN service that provides Layer 2 point-to-point virtual circuit connectivity between customer sites over a provider network.

Packet Switched Network (PSN) - The PSN is the network through which the tunnels supporting the VPN services are set up. On this Switch, the PSN is a MPLS network.

Customer Edge Device (CE) - The CE resides on a customer network and has one or more interfaces directly connected to provider networks.

Provider Edge (PE) - The PE resides on a service provider network and connects one or more CEs to the network.

Provider Router (PR) - The PR resides on a service provider network and provides fast packet switching.

Attachment Circuit (AC) – The AC is the physical or virtual circuit attaching a CE to a PE. The Ethernet port, VLAN or (port, VLAN) pair can be used to identify the AC.

Pseudo-Wire (PW) – The PW is a mechanism that carries the essential elements of an emulated circuit from one PE to another PE over a PSN. The PW-ID and PW-type are used to identify a Pseudo-Wire. The PW-ID is a non-zero, 32-bit, connection ID. The PW-ID and PW-type must be the same at both endpoints.

Tunnel Label - The Tunnel Label is used to allow encapsulated Ethernet packets to cross the MPLS network through the tunnel LSP.

VC Label – The VC Label is used as a de-multiplexer field so that multiple PWs can be carried in a single tunnel. A particular VC Label value must be agreed upon by the ingress and egress PEs, either by using LDP signaling or by using a static configuration. The VC Label must be at the bottom label of an MPLS label stack. The EXP field in the VC Label can be used to carry QoS information. The ingress PE must configure the TTL value of the VC Label to 2.

VPWS Settings

This window is used to configure the VPWS settings.

To view this window, click **VPN > VPWS > VPWS Settings** as shown below:

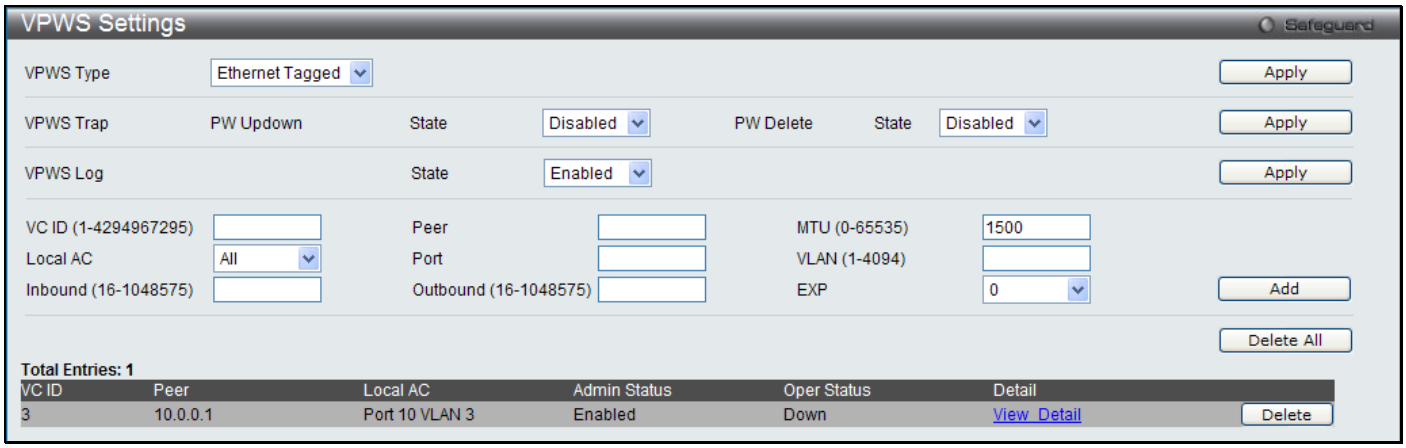


Figure 4-25 VPWS Settings window

The fields that can be configured are described below:

Parameter	Description
VPWS Type	Select the VPWS type used here. VPWS types are used to distinguish between different VPWS services. There are two VPWS types defined for Ethernet service; one is *Ethernet Raw*; and the other is *Ethernet Tagged*. The VPWS type is globally configured. All PWs will operate in Ethernet raw mode, and S-tags are never sent over the PWs for the Ethernet raw type VPWS. The other alternative is all PWs will operate in Ethernet tagged mode, and every frame sent on the PWs must then have an S-tag for the Ethernet tagged type VPWS. The VPWS type must be the same at both sides of the VPWS ends.
VPWS Trap	Enable or disable VPWS trap state here.
PW Updown State	If enabled, a trap will be sent when the PW is in an up or down event. If disabled, then no traps will be sent regarding the PW up or down events.
PW Delete State	If enabled, a trap will be sent when a delete PW event occurs. If disabled, then no traps will be sent regarding a delete PW event.
VPWS Log State	Enable or disable VPWS log state here.
VC ID (1-4294967295)	Enter the VC ID used here. This value must be between 1 and 4294967295.
Peer	Enter the peer IP address of the PW here. The peer IP address must be its LSR ID.
MTU (0-65535)	Enter the local CE-PE link's MTU value that will be advertised to the remote peer here. If the MTU is specified as 0, the LDP will not be advertised to the local MTU. The MTU must be same at both local and remote otherwise the PW will not succeed. If not specified, the default MTU will be used. The default MTU value is 1500. This value must be between 0 and 65535.
Local AC	Select the Local AC method used here. Options to choose from are *All*, *Port*, and *VLAN*.
Port	Enter the AC's ingress port number of the PW here, if the Local AC is identified by Port or by All (Port, VLAN).
VLAN (1-4094)	Enter the AC's ingress VLAN ID of the PW here, if the Local AC is identified by VLAN or by All (Port, VLAN).
Inbound (16-1048575)	Enter the inbound VC label used here. This value must be between 16 and 1048575.
Outbound (16-1048575)	Enter the outbound VC label used here. This value must be between 16 and 1048575.
EXP	Enter the EXP value for the VC used here. If not specified, the EXP value in the outbound label for the VC is set according to the incoming packet's QoS.

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

Click the **Add** button to add a new entry.

Click the **Delete All** button to remove entries in the list.

Click the View Detail link to navigate to a new window containing more detailed information about the entry.

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

After click the View Detail link, the following page will be displayed.

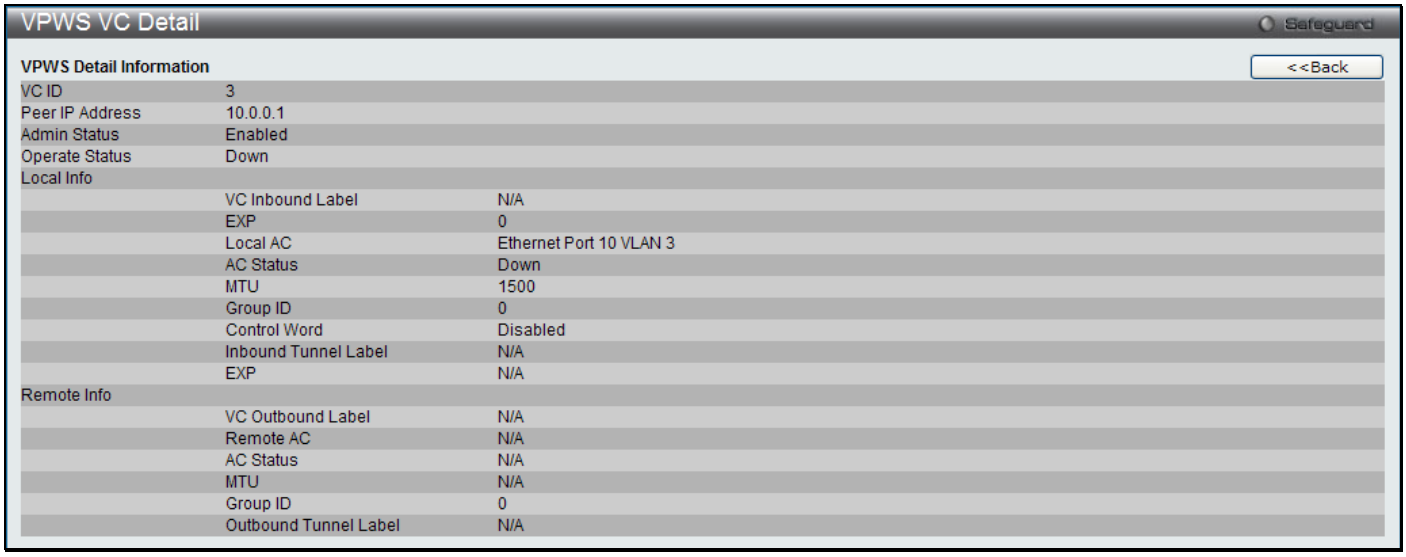


Figure 4-26 VPWS VC Detail window

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

Chapter 5 L2 Features

VLAN
QinQ
Layer 2 Protocol Tunneling Settings
Spanning Tree
Link Aggregation
FDB
L2 Multicast Control
Multicast Filtering
ERPS Settings
Local Loopback Port Settings
LLDP
NLB FDB Settings

VLAN

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes about VLANs on the Switch

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.
- The Switch supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
- The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
- The "default" VLAN has a VID = 1.
- The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** – A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.
- **Egress port** – A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
- Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
- Forwarding rules between ports – decides whether to filter or forward the packet.
- Egress rules – determines if the packet must be sent tagged or untagged.

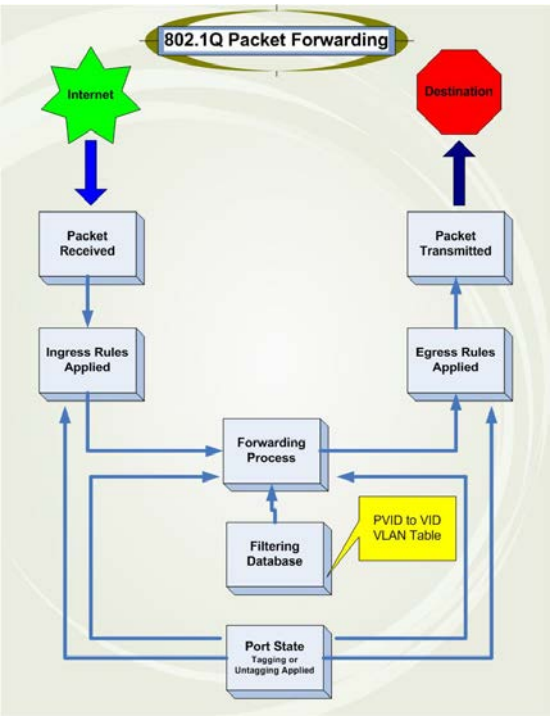


Figure 5-1 Packet Forwarding window

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

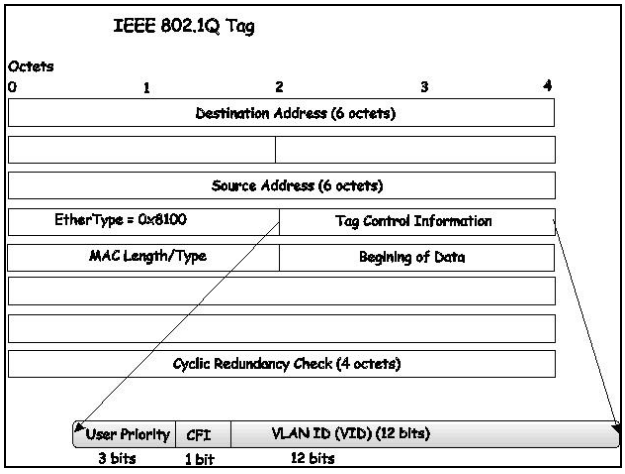


Figure 5-2 802.1Q VLAN Tags window

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

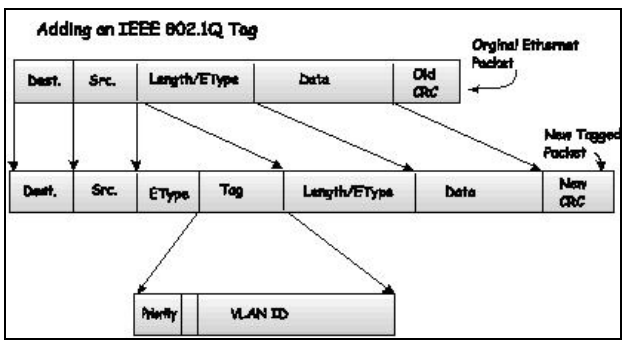


Figure 5-3 802.1Q VLAN Tags window

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it.

If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called “default.” The factory default setting assigns all ports on the Switch to the “default.” As new VLANs are configured in Port-based mode, their respective member ports are removed from the “default.”

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7
Engineering	2	9, 10
Sales	5	1, 2, 3, 4

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet’s destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, first set the port trunk group(s), and then configure the VLAN settings. To change the port trunk grouping with VLANs already in place it is unnecessary to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

802.1Q VLAN Settings

The **VLAN List** tab lists all previously configured VLANs by VLAN ID and VLAN Name.

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

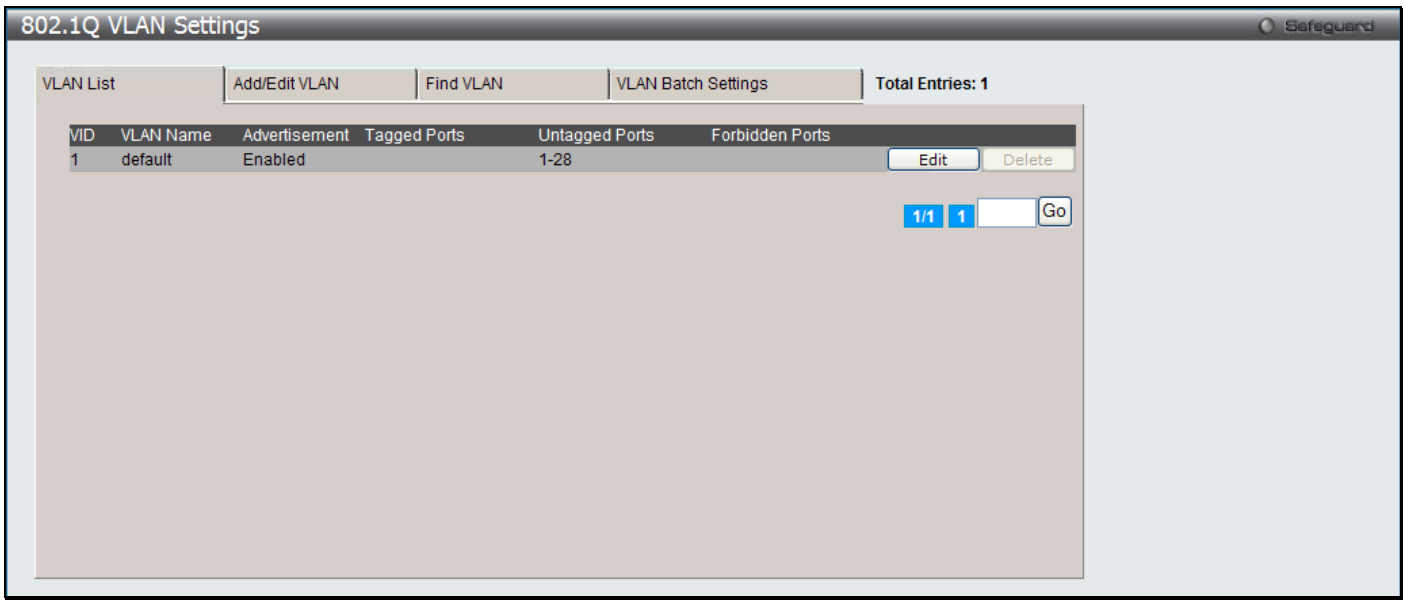


Figure 5-4 802.1Q VLAN Settings window

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.

To create a new 802.1Q VLAN or modify an existing 802.1Q VLAN, click the **Add/Edit VLAN** tab.

A new tab will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN.

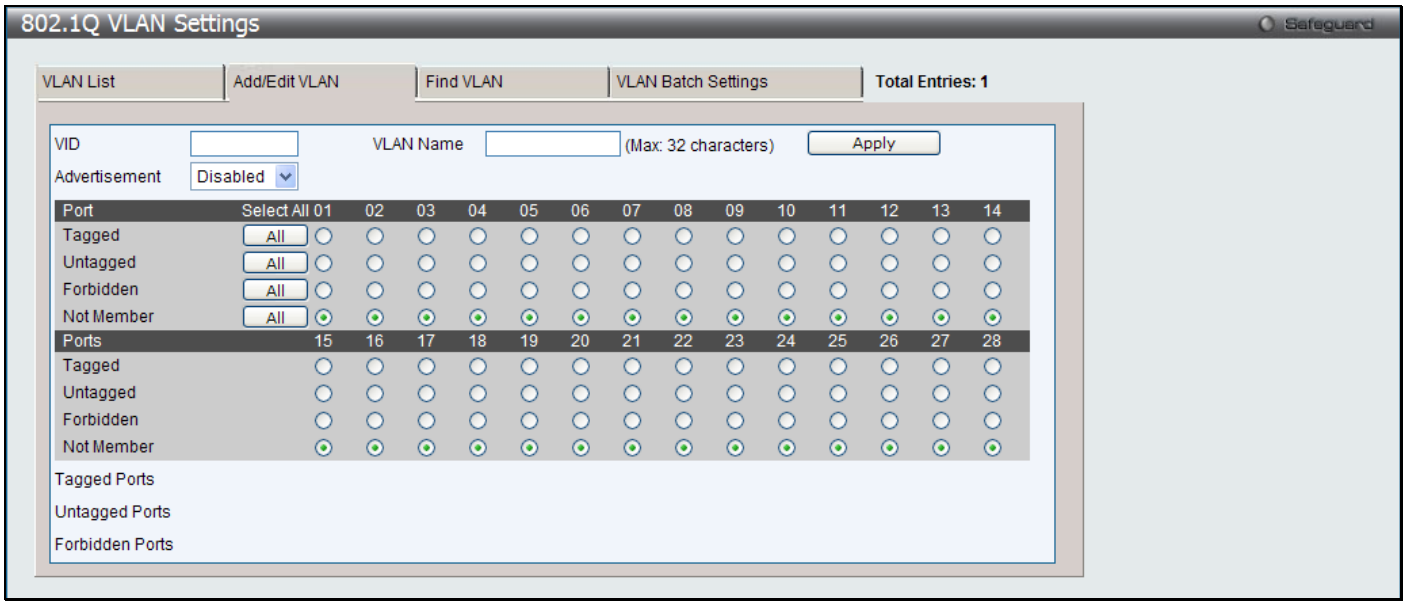


Figure 5-5 802.1Q VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VID	Allows the entry of a VLAN ID or displays the VLAN ID of an existing VLAN in the **Add/Edit VLAN** tab. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN or for editing the VLAN name in the **Add/Edit VLAN** tab.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port	Shows all ports of the Switch for the configuration option.
Tagged	Specifies the port as 802.1Q tagging. Clicking the radio button will designate the port as tagged. Click the **All** button to select all ports.
Untagged	Specifies the port as 802.1Q untagged. Clicking the radio button will designate the port as untagged. Click the **All** button to select all ports.
Forbidden	Click the radio button to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Click the **All** button to select all ports.
Not Member	Click the radio button to allow an individual port to be specified as a non-VLAN member. Click the **All** button to select all ports.

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

To search for a VLAN, click the **Find VLAN** tab. A new tab will appear, as shown below.

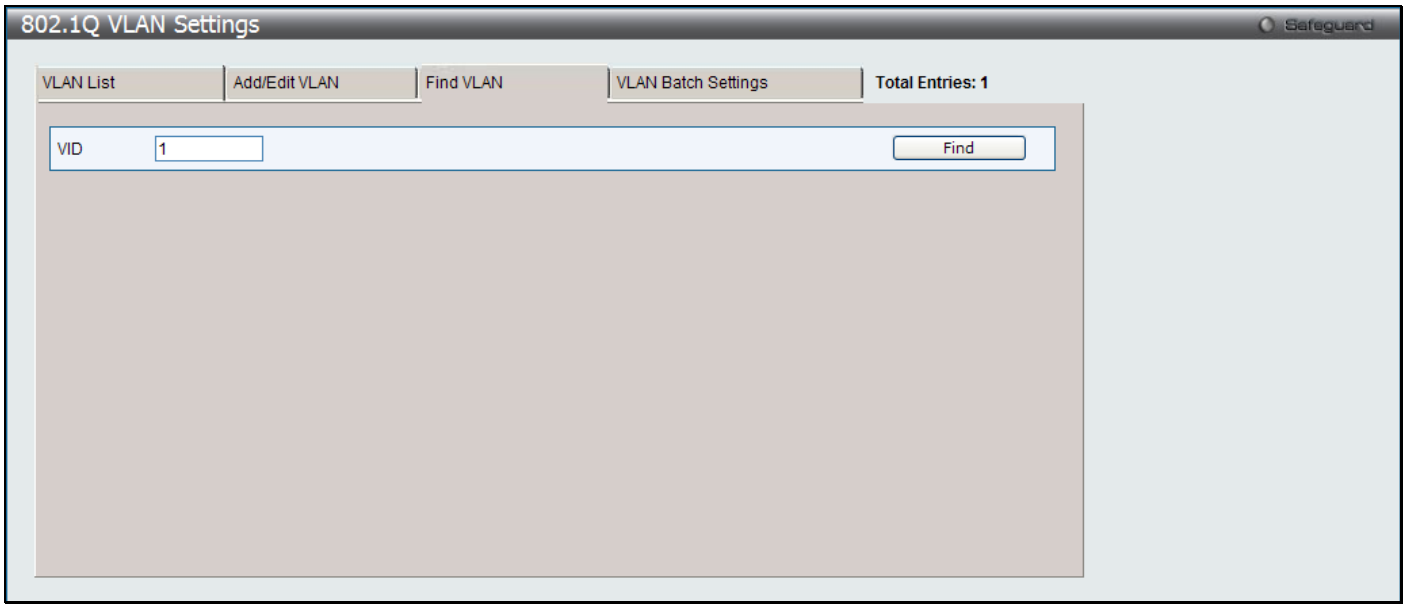


Figure 5-6 802.1Q VLAN Settings window

Enter the VLAN ID number in the **VID** field and then click the **Find** button. You will be redirected to the **VLAN List** tab.

To create, delete and configure a VLAN Batch entry click the **VLAN Batch Settings** tab, as shown below.

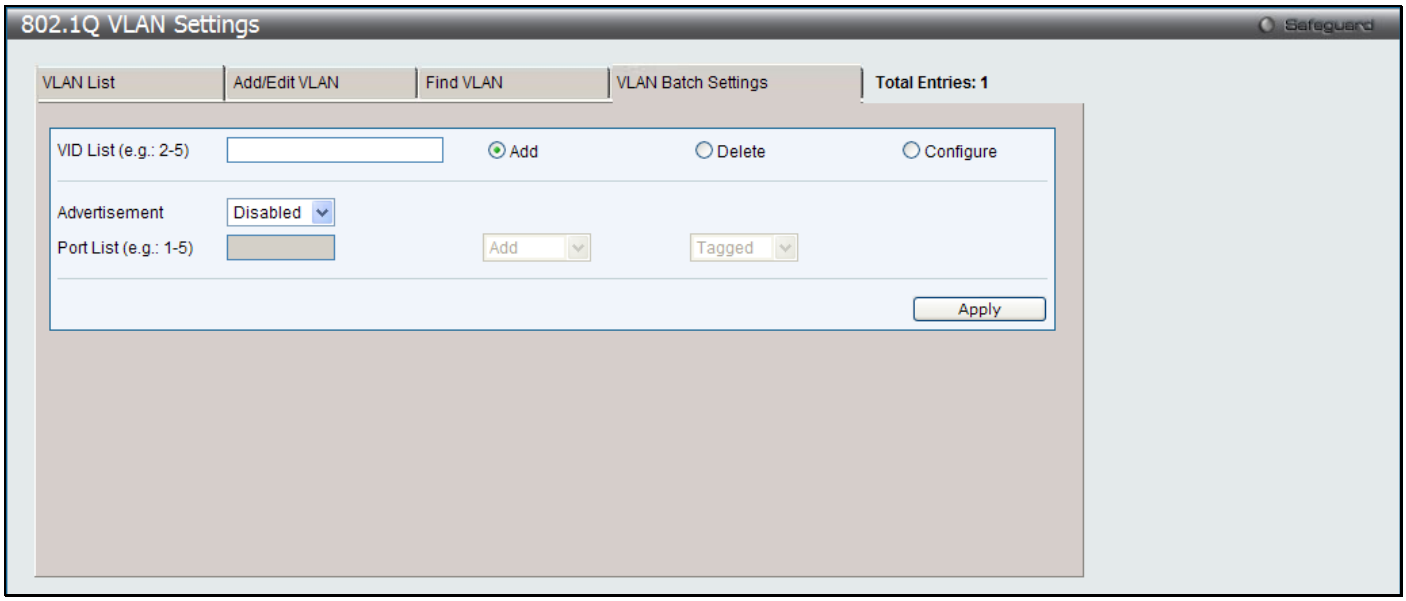


Figure 5-7 802.1Q VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VID List (e.g.: 2-5)	Enter a VLAN ID List that can be added, deleted or configured.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port List (e.g.: 1-5)	Allows an individual port list to be added or deleted as a member of the VLAN.
Tagged	Specifies the port as 802.1Q tagged. Use the drop-down menu to designate the port as tagged.
Untagged	Specifies the port as 802.1Q untagged. Use the drop-down menu to designate the port as untagged.
Forbidden	Specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Use the drop-down menu to designate the port as forbidden.

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

NOTE: The Switch supports up to 4k static VLAN entries.

802.1v Protocol Group Settings

802.1v Protocol Group Settings

The user can create Protocol VLAN groups and add protocols to that group. The 802.1v Protocol VLAN Group Settings support multiple VLANs for each protocol and allows the user to configure the untagged ports of different protocols on the same physical port. For example, it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port. The lower half of the table displays any previously created groups.

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

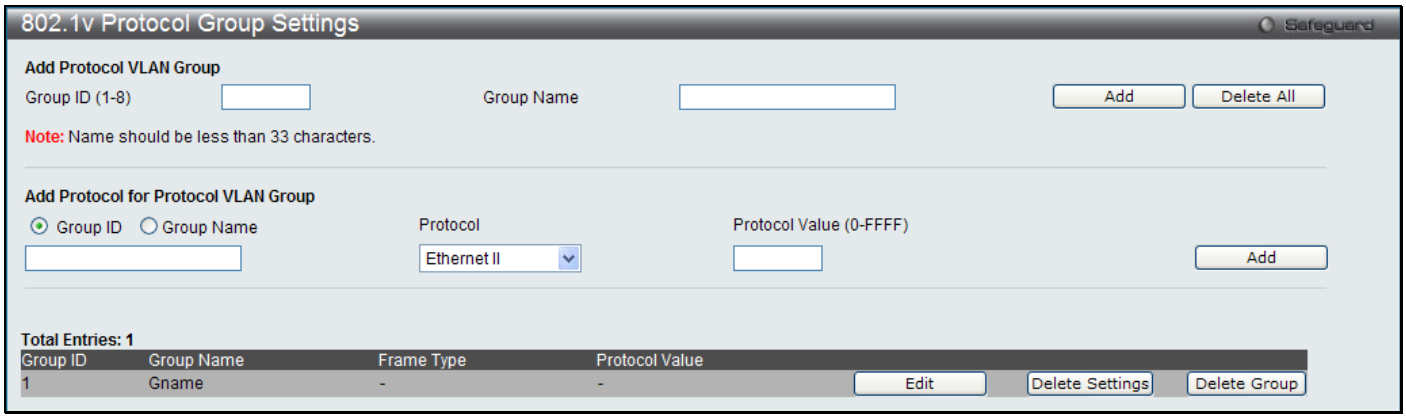


Figure 5-8 802.1v Protocol Group Settings window

The fields that can be configured are described below:

Parameter	Description
Group ID (1-8)	Select an ID number for the group, between *1* and *8*.
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 33 characters.
Protocol	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Use the drop-down menu to toggle between *Ethernet II*, *IEEE802.3 LLC*, and *IEEE802.3 SNAP*.
Protocol Value (0-FFFF)	Enter a value for the Group. The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

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

Click the **Delete All** button to remove all the entries based on the information entered.

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

Click the **Delete Settings** button to remove the Protocol for the Protocol VLAN Group information for the specific entry.

Click the **Delete Group** button to remove the entry completely.

NOTE: The Group name value should be less than 33 characters.

802.1v Protocol VLAN Settings

The user can configure Protocol VLAN settings. The lower half of the table displays any previously created settings.

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

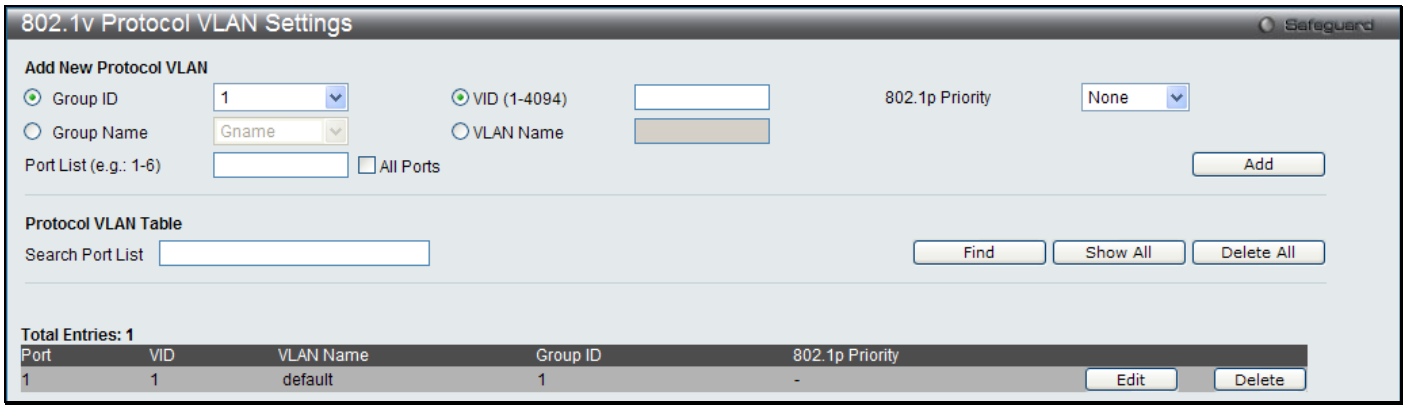


Figure 5-9 802.1v Protocol VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
Group ID	Select a previously configured Group ID from the drop-down menu.
Group Name	Select a previously configured Group Name from the drop-down menu.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to create.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to create.
802.1p Priority	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. Click the corresponding box if you want to set the 802.1p default priority of a packet to the value entered in the Priority (0-7) field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Port List	Select the specified ports you wish to configure by entering the port number in this field, or tick the **All Ports** check box.
Search Port List	This function allows the user to search all previously configured port list settings and display them on the lower half of the table.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Show All** button to display all the Protocol VLANs.
Click the **Delete All** button to clear all previously configured lists.
Click the **Edit** button to re-configure the specified entry.
Click the **Delete** button to remove the specified entry.

GVRP

GVRP Global Settings

Users can determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering

incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings.

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

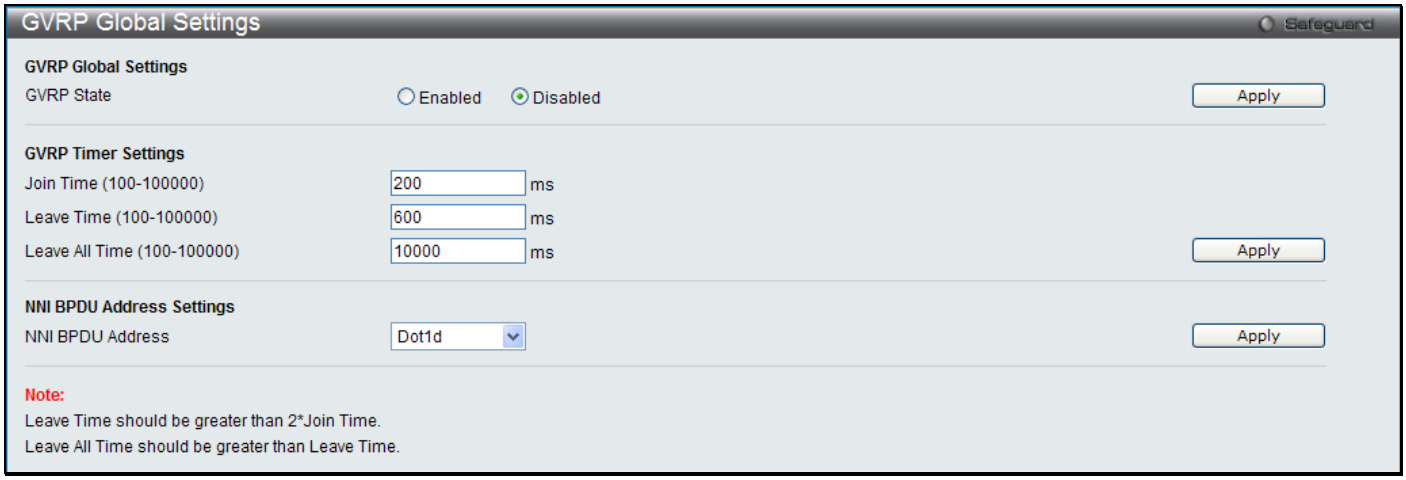


Figure 5-10 GVRP Global Settings window

The fields that can be configured are described below:

Parameter	Description
GVRP State	Here the user can enable or disable the GVRP State.
Join Time (100-100000)	Here the user can enter the Join Time value in milliseconds.
Leave Time (100-100000)	Here the user can enter the Leave Time value in milliseconds.
Leave All Time (100-100000)	Here the user can enter the Leave All Time value in milliseconds.
NNI BPDU Address	Used to determine the BPDU protocol address for GVRP in service provide site. It can use an 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address.

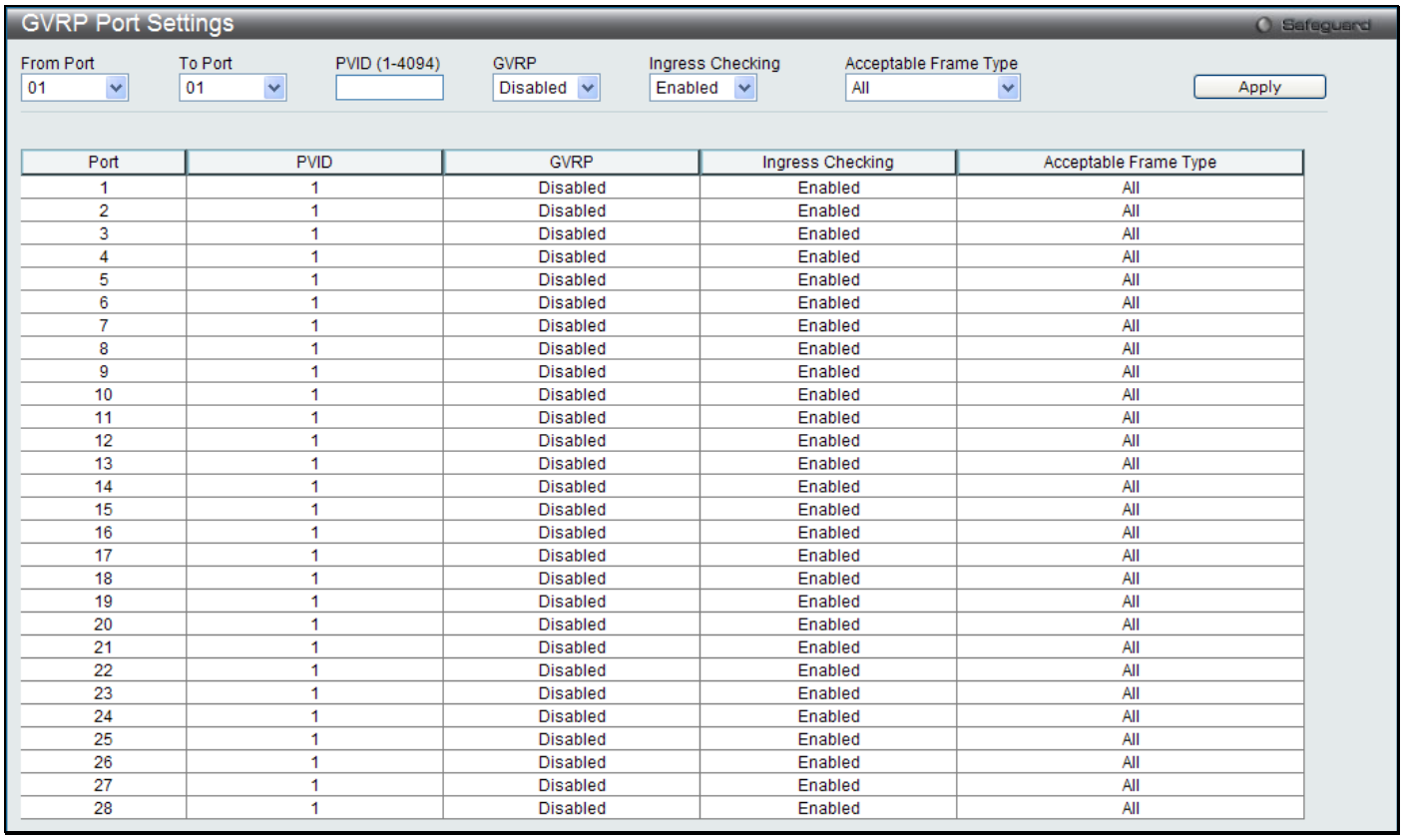
Click the **Apply** button to accept the changes made for each individual section.

NOTE: The **Leave Time** value should be greater than twice the **Join Time** value. The **Leave All Time** value should be greater than the **Leave Time** value.

GVRP Port Settings

On this page the user can configure the GVRP port parameters.

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



Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All
2	1	Disabled	Enabled	All
3	1	Disabled	Enabled	All
4	1	Disabled	Enabled	All
5	1	Disabled	Enabled	All
6	1	Disabled	Enabled	All
7	1	Disabled	Enabled	All
8	1	Disabled	Enabled	All
9	1	Disabled	Enabled	All
10	1	Disabled	Enabled	All
11	1	Disabled	Enabled	All
12	1	Disabled	Enabled	All
13	1	Disabled	Enabled	All
14	1	Disabled	Enabled	All
15	1	Disabled	Enabled	All
16	1	Disabled	Enabled	All
17	1	Disabled	Enabled	All
18	1	Disabled	Enabled	All
19	1	Disabled	Enabled	All
20	1	Disabled	Enabled	All
21	1	Disabled	Enabled	All
22	1	Disabled	Enabled	All
23	1	Disabled	Enabled	All
24	1	Disabled	Enabled	All
25	1	Disabled	Enabled	All
26	1	Disabled	Enabled	All
27	1	Disabled	Enabled	All
28	1	Disabled	Enabled	All

Figure 5-11 GVRP Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
PVID (1-4094)	This field is used to manually assign a PVID to a VLAN. The Switch's default is to assign all ports to the default VLAN with a VID of 1.The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is *Enabled*, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The GARP VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
Ingress Checking	This drop-down menu allows the user to enable the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables ingress filtering. Ingress checking is *Enabled* by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *All*, which mean both tagged and untagged frames will be accepted. *All* is enabled by default.

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

MAC-based VLAN Settings

Users can create new MAC-based VLAN entries, search and delete existing entries. When a static MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentication function operating on this port.

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

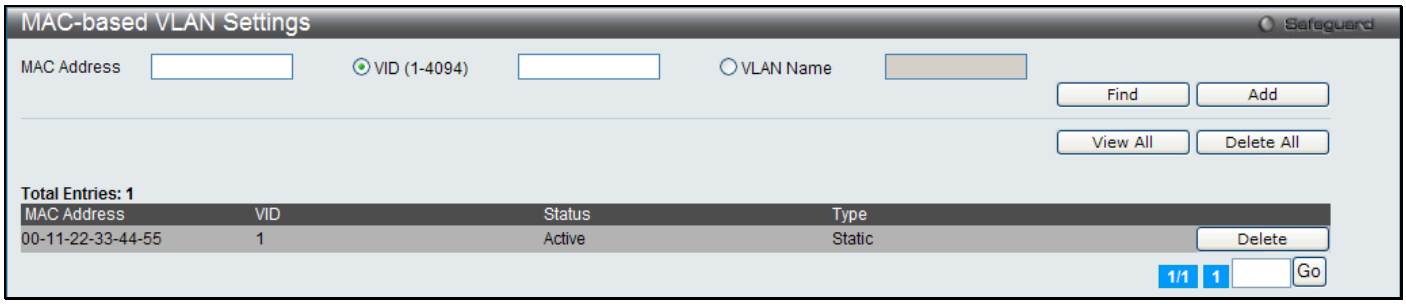


Figure 5-12 MAC-based VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Specify the MAC address to be re-authenticated by entering it into the MAC Address field.
VLAN ID	Select this option and enter the VLAN ID.
VLAN Name	Select this option and enter the VLAN name of a previously configured VLAN.

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

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

Click the **View All** button to display all the existing entries.

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

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.

Private VLAN Settings

A private VLAN is comprised of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. A private VLAN ID is presented by the VLAN ID of the primary VLAN. The command used to associate or de-associate a secondary VLAN with a primary VLAN.

A secondary VLAN cannot be associated with multiple primary VLANs. The untagged member port of the primary VLAN is named as the promiscuous port. The tagged member port of the primary VLAN is named as the trunk port. A promiscuous port of a private VLAN cannot be promiscuous port of other private VLANs. The primary VLAN member port cannot be a secondary VLAN member at the same time, or vice versa. A secondary VLAN can only have the untagged member port. The member port of a secondary VLAN cannot be member port of other secondary VLAN at the same time. When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will behave as the untagged member of the secondary VLAN, and the trunk port of the primary VLAN will behave as the tagged member of the secondary VLAN. A secondary VLAN cannot be specified with advertisement. Only the primary VLAN can be configured as a layer 3 interface. The private VLAN member port cannot be configured with the traffic segmentation function.

On this page the user can configure the private VLAN parameters.

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

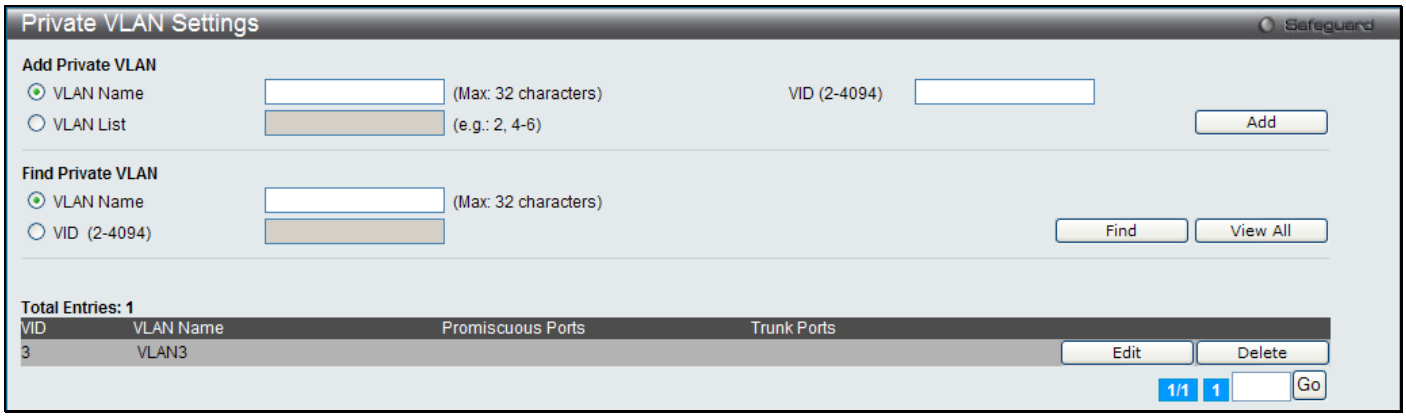


Figure 5-13 Private VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The user can enter a VLAN Name here.
VID (2-4094)	The user can enter a VID value here.
VLAN List	The user can enter a VLAN List here.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Edit** button to re-configure the specified 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.

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

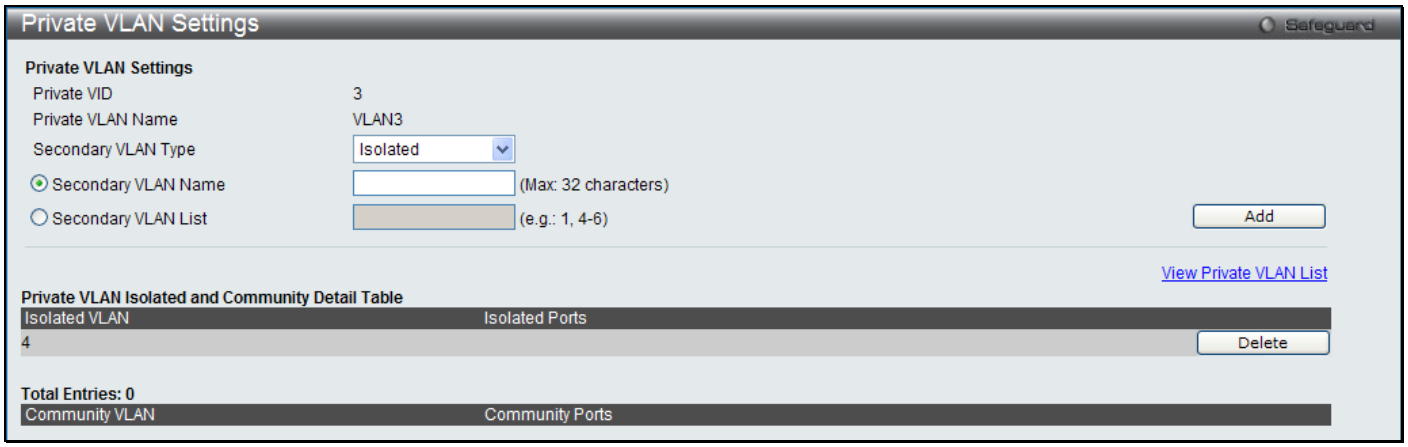


Figure 5-14 Private VLAN Settings - Edit window

The fields that can be configured are described below:

Parameter	Description
Secondary VLAN Type	Use the drop-down menu to select secondary VLAN type between *Isolated* or *Community*.
Secondary VLAN Name	Enter a secondary VLAN name.
Secondary VLAN List	Enter a list of secondary VLAN ID.

Click the **Add** button to add a new entry based on the information entered.
Click the View Private VLAN List link to view all the private VLAN.
Click the **Delete** button to remove the specified entry.

PVID Auto Assign Settings

Users can enable or disable PVID Auto Assign Status. The default setting is enabled.

To view the following window, click **L2 Features > VLAN > PVID Auto Assign Settings**, as shown below:

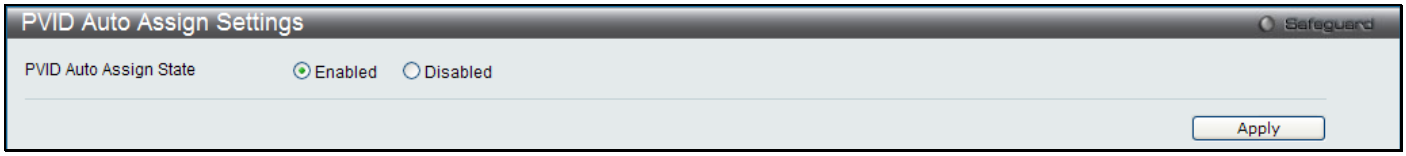


Figure 5-15 PVID Auto Assign Settings window

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

Subnet VLAN

Subnet VLAN Settings

A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.

On this page the user can configure the subnet VLAN parameters.

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

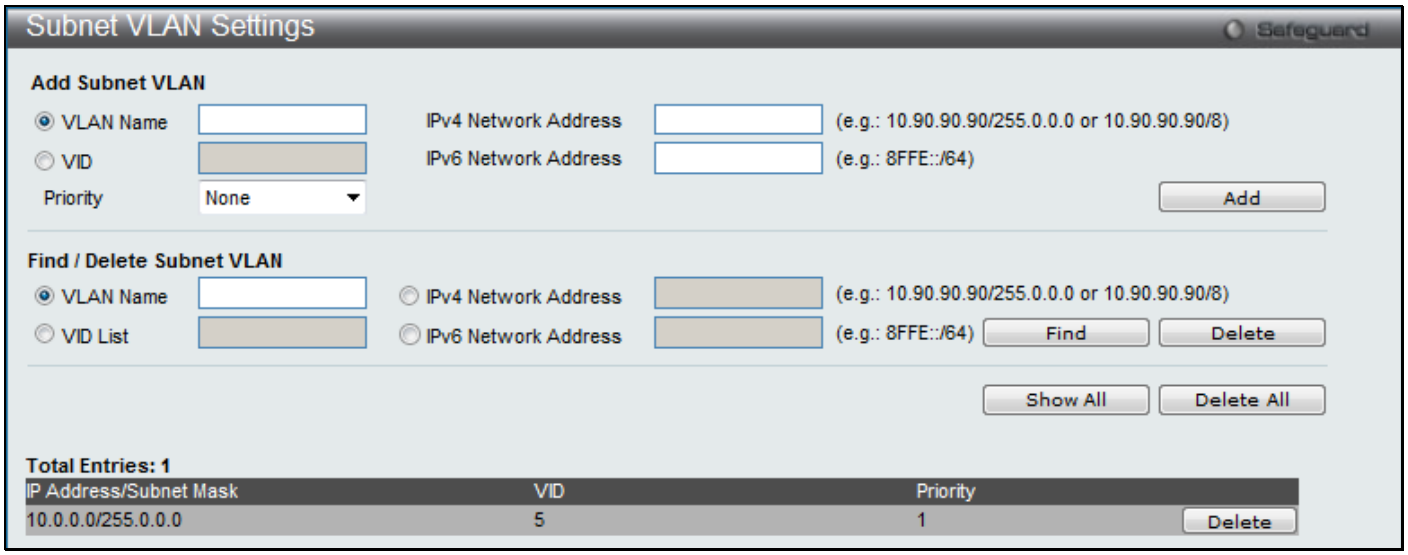


Figure 5-16 Subnet VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The user can enter a VLAN Name here.
VID	The user can enter a VID value here.
IPv4 Network Address	The user can enter the IPv4 address used in here. Remember to include the subnet mask using the **/** notation.
IPv6 Network Address	The user can enter the IPv6 address used in here. Remember to include the subnet mask using the **/** notation.

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

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

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

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

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

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

VLAN Counter Settings

The user can create control entry to count statistics for a specific VLAN, or to count statistics for a specific port on a specific VLAN. The statistics can be either byte count or packet count. The statistics can be counted for different frame types.

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

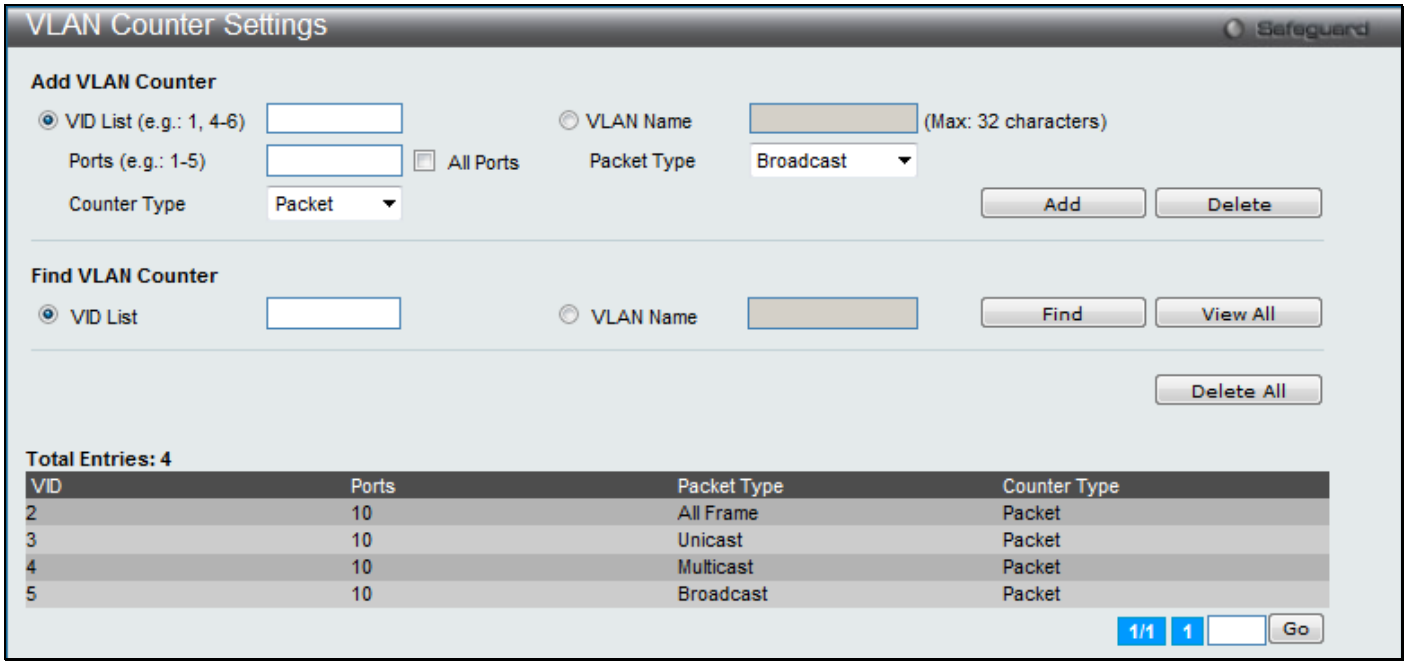


Figure 5-17 VLAN Counter Settings window

The fields that can be configured are described below:

Parameter	Description
VID List	Specifies a list of VLANs by VLAN ID.
VLAN Name	Specifies the VLAN name.
Ports	To enable to count statistics by specific port on specific VLAN.
Packet Type	This option specifies the Packet Type: *Broadcast* - Specifies to count broadcast packets. *Multicast* - Specifies to count multicast packets. *Unicast* – Specifies to count unicast packets. *All* - The statistics will be counted for all packets.
Counter Type	This option specifies the Counter Type: *Packet* - Specifies to count at packet level. *Byte* - Specifies to count at byte level.

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

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

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

Click the **View All** button to display all the existing entries.

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

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

Voice VLAN

Voice VLAN Global Settings

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 Settings**, as shown below:

Figure 5-18 Voice VLAN Global Settings window

The fields that can be configured are described below:

Parameter	Description
Voice VLAN State	The state of the voice VLAN.
Voice VLAN Name	The name of the voice VLAN.
Voice VID (1-4094)	The VLAN ID of the voice VLAN.
Priority	The priority of the voice VLAN, the range is 0 – 7. The default priority is 5.
Aging Time (1-65535)	The aging time to set, the range is 1 – 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.
Log State	Used to enable/disable sending of issue of voice VLAN log.

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

Voice VLAN Port Settings

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

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

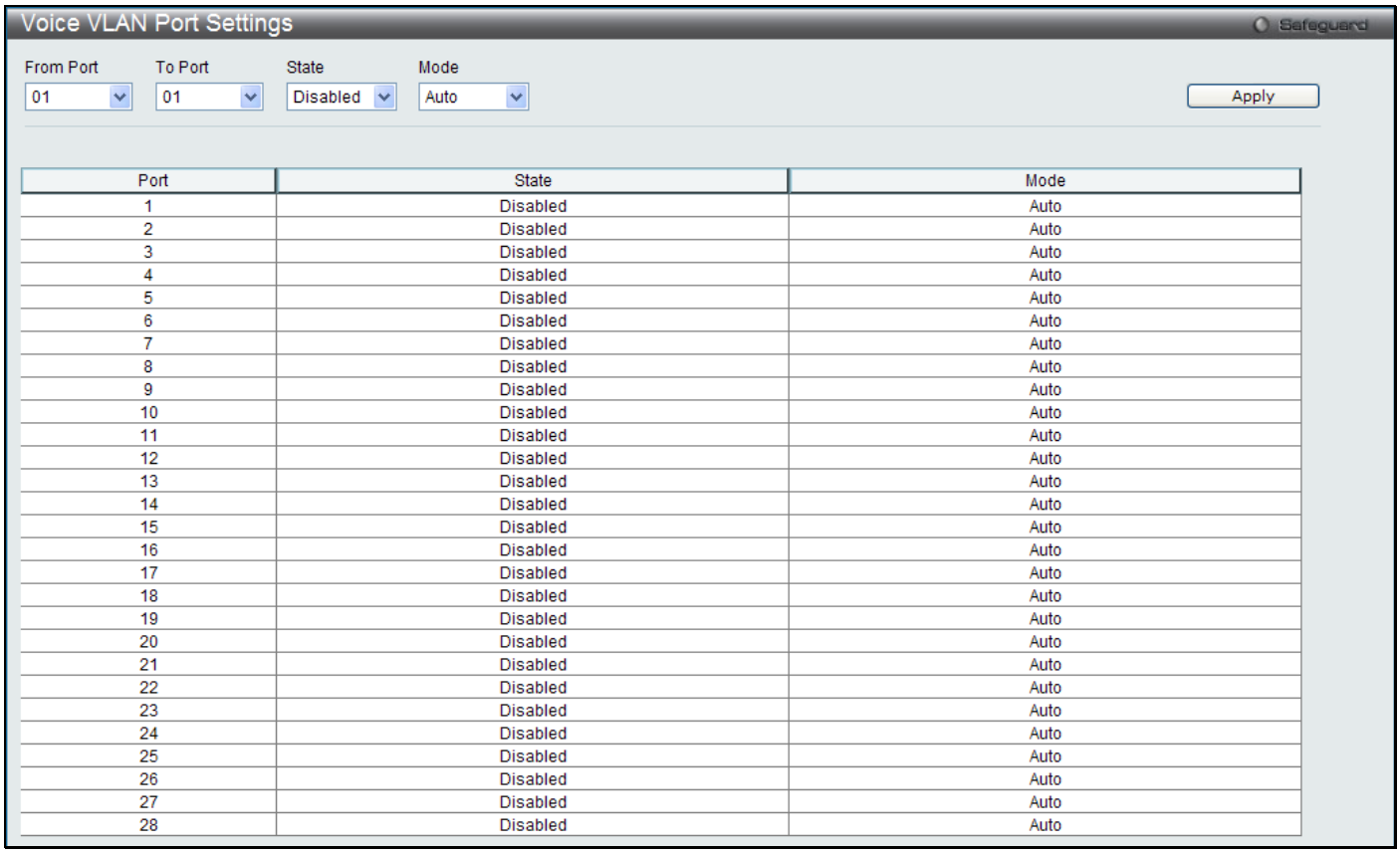


Figure 5-19 Voice VLAN Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of port to display.
State	Here the user can configure the state of the port.
Mode	Here the user can configure the mode of the port.

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

Voice VLAN OUI Settings

This page 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 Settings**, as shown below:

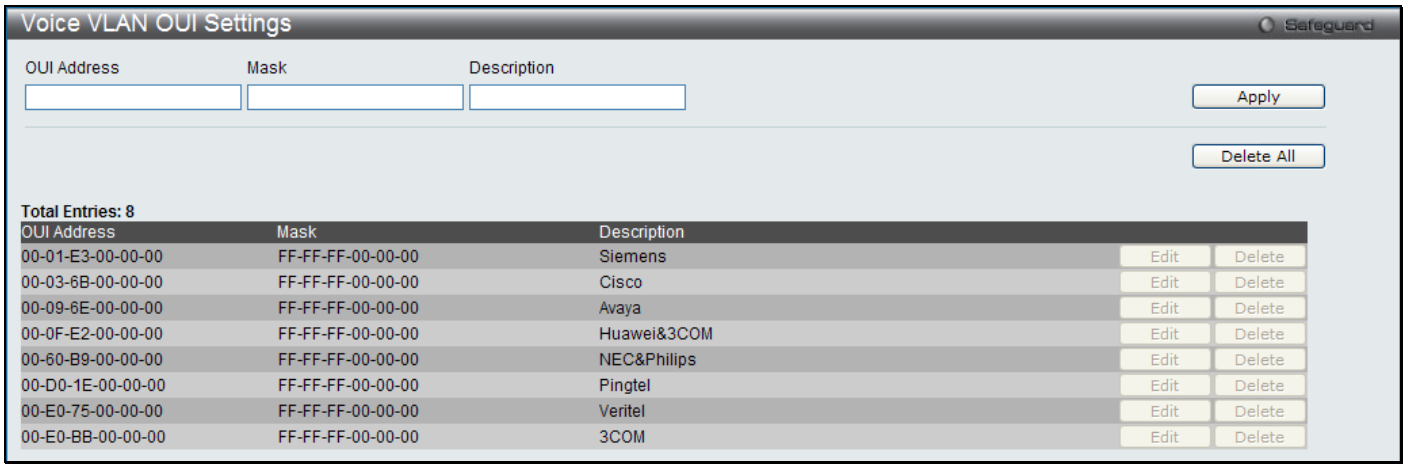


Figure 5-20 Voice VLAN OUI Settings window

The fields that can be configured are described below:

Parameter	Description
OUI Address	User defined OUI MAC address.
Mask	User defined OUI MAC address mask.
Description	The description for the user defined OUI.

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

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

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

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

Voice VLAN Device

This page 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:

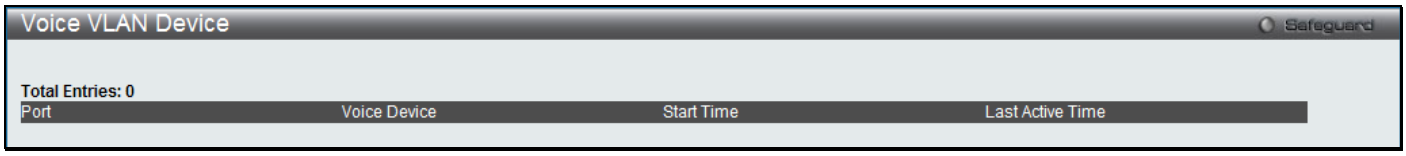
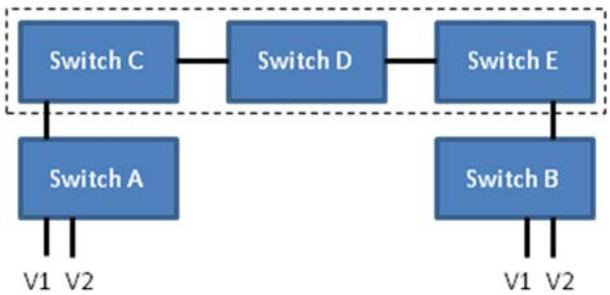


Figure 5-21 Voice VLAN Device window

VLAN Trunk Settings

Enable VLAN on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure for an illustrated example.



Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without a VLAN Trun**k**, you must first configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with VLAN Trunk enabled on a port(s) in each intermediary switch, you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Users can combine a number of VLAN ports together to create VLAN trunks.

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

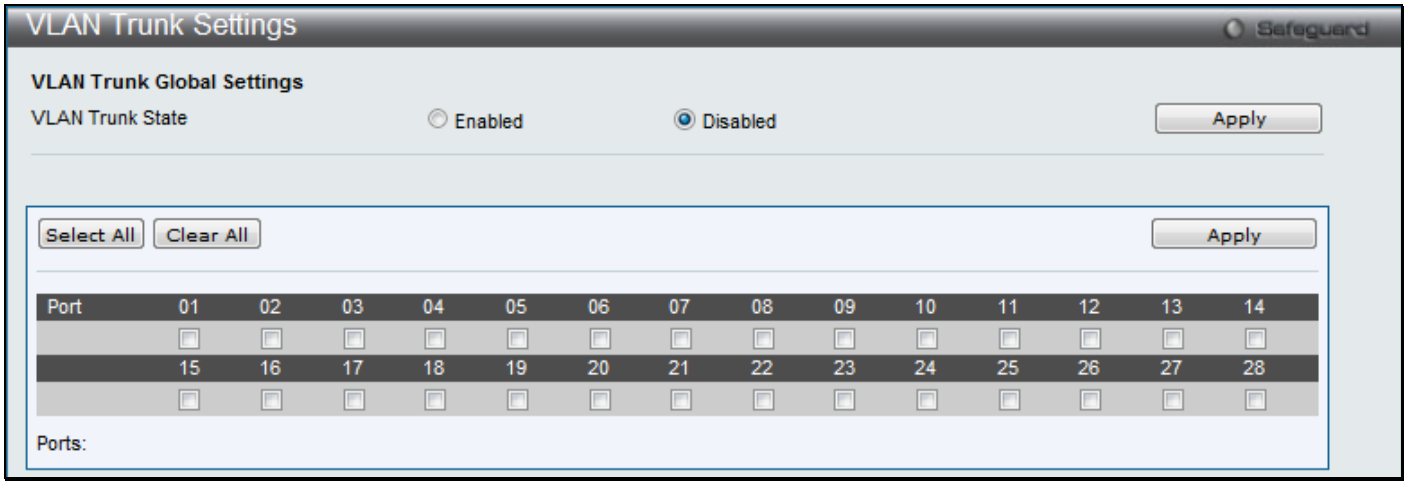


Figure 5-22 VLAN Trunk Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Trunk State	Enable or disable the VLAN trunking global state.
Ports	The ports to be configured.

Click the **Apply** button to accept the changes made for each individual section.
Click the **Clear All** button to clear all the selections made.
Click the **Select All** button to select all the available options in the section.

Browse VLAN

Users can display the VLAN status for each of the Switch's ports viewed by VLAN.

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

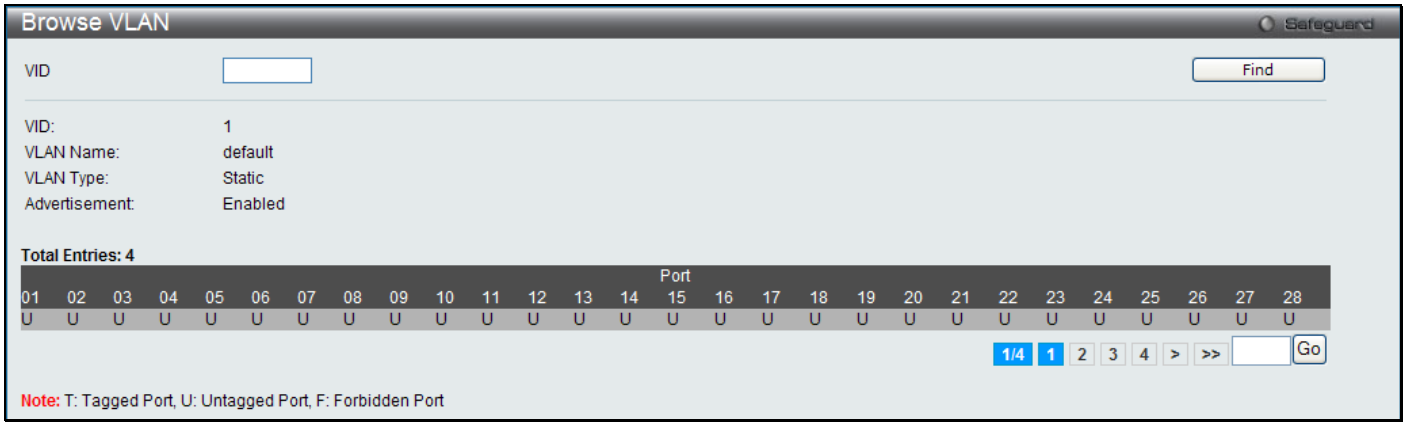


Figure 5-23 Browse VLAN window

The fields that can be configured are described below:

Parameter	Description
VID	Enter a VLAN ID.

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.

NOTE: The abbreviations used in this window are, **Tagged Port (T)**, **Untagged Port (U)** and **Forbidden Port (F)**.

Show VLAN Ports

Users can display the VLAN ports of the Switch's viewed by ports.

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

Figure 5-24 Show VLAN Ports window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter a port or a range of ports to be displayed.

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

Click the **View All** button to display all the existing entries.

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

Q-in-Q

Q-in-Q Settings

Double or Q-in-Q VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

Double VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Double VLAN tagged packet.

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Consider the example below:

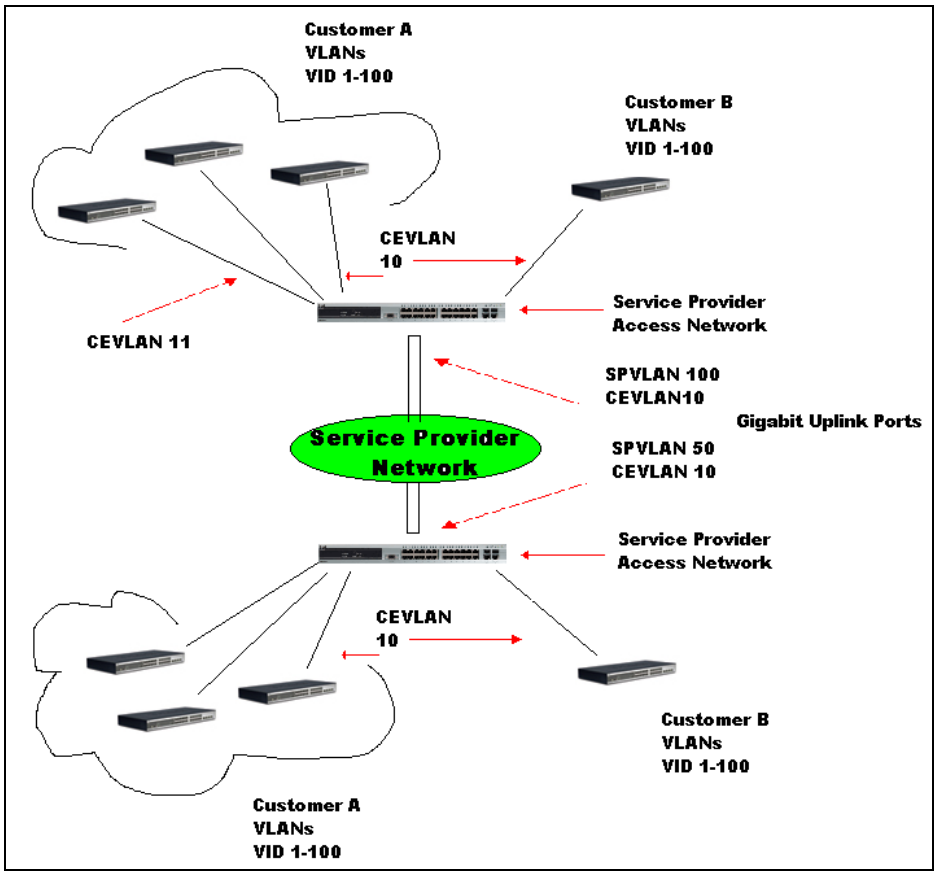


Figure 5-25 Q-in-Q Example window

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs. Both CEVLANs (Customer VLANs), 10 and 11, are tagged with the SPVID 100 on the Service Provider Access Network and therefore belong to one VLAN on the Service Provider's network, thus being a member of two VLANs. In this way, the Customer can retain its normal VLAN and the Service Provider can congregate multiple Customer VLANs within one SPVLAN, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Double VLANs

Some rules and regulations apply with the implementation of the Double VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both double and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Once Double VLANs are enabled, GVRP must be disabled.
7. All packets sent from the CPU to the Access ports must be untagged.
8. The following functions will not operate when the switch is in Double VLAN mode:
    - Guest VLANs.
    - Web-based Access Control.
    - IP Multicast Routing.
    - GVRP.
    - All Regular 802.1Q VLAN functions.

This window is used to configure the Q-in-Q parameters.

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

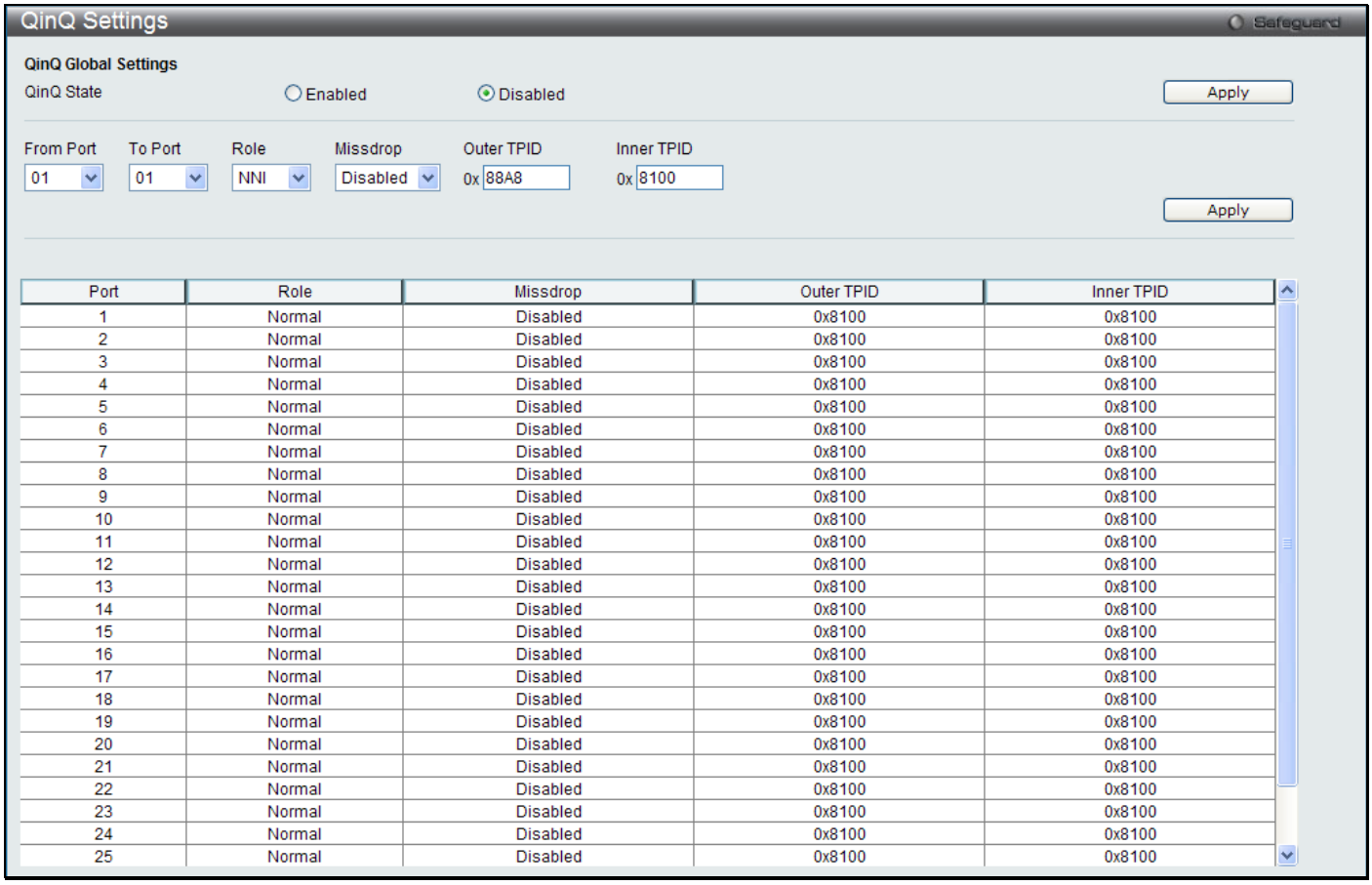


Figure 5-26 QinQ Settings window

The fields that can be configured are described below:

Parameter	Description
QinQ State	Selecting this option enable the QinQ feature.
From Port / To Port	Here the user can select a range of ports to use in the configuration.
Role	Port role in QinQ mode, it can be UNI port or NNI port
Missdrop	This option enables or disables C-VLAN based SP-VLAN assignment miss drop. If Missdrop is enabled, the packet that does not match any assignment rule in the QinQ profile will be dropped. If disabled, then the packet will be forwarded and will be assigned to the PVID of the received port.
Outer TPID	Enter an Outer TPID in SP-VLAN tag here.
Inner TPID	Enter an Inner TPID in SP-VLAN tag here.

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

VLAN Translation Settings

This page can be used to add translation relationship between C-VLAN and SP-VLAN. On ingress at UNI port, the C-VLAN tagged packets will be translated to SP-VLAN tagged packets by adding or replacing according the configured rule. On egress at this port, the SP-VLAN tag will be recovered to C-VLAN tag or be striped. The priority will be the priority in the SP-VLAN tag if the inner priority flag is disabled for the receipt port.

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

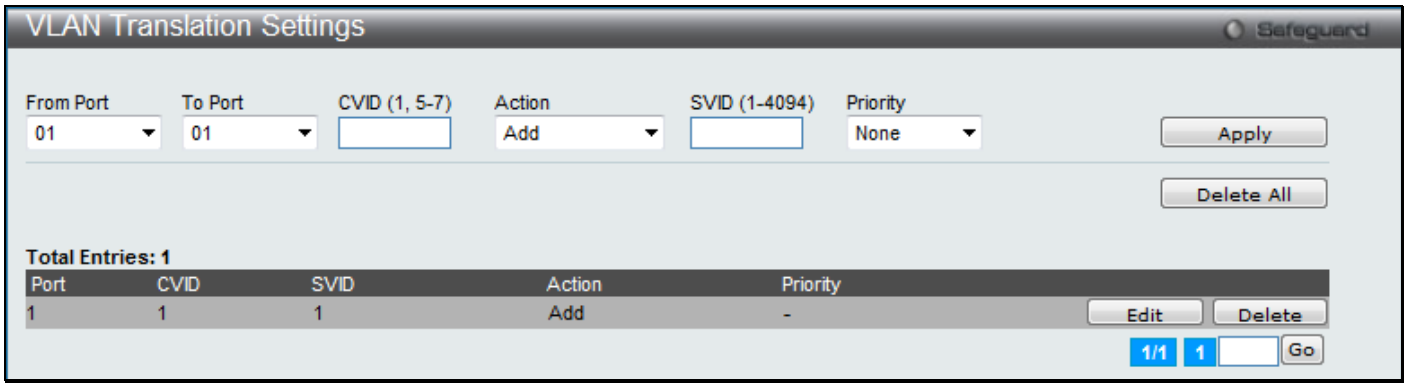


Figure 5-27 VLAN Translation Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of ports to use in the configuration.
CVID (1, 5-7)	Here the user can enter the C-VLAN ID to match.
Action	The action indicates to add an S-tag before a C-tag or to replace the original C-tag by an S-tag.
SVID (1-4094)	Here the user can enter the SP-VLAN ID.
Priority	Here the user can select the priority of the s-tag.

Click the **Apply** button to accept the changes made.
Click the **Delete All** button to remove all the entries listed.
Click the **Edit** button to re-configure the specified 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.

Double Tagged VLAN Translation Settings

On this page the user can configure the double tagged VLAN translation parameters.

To view the following window, click **L2 Features > QinQ > Double Tagged VLAN Translation Settings**, as shown below:

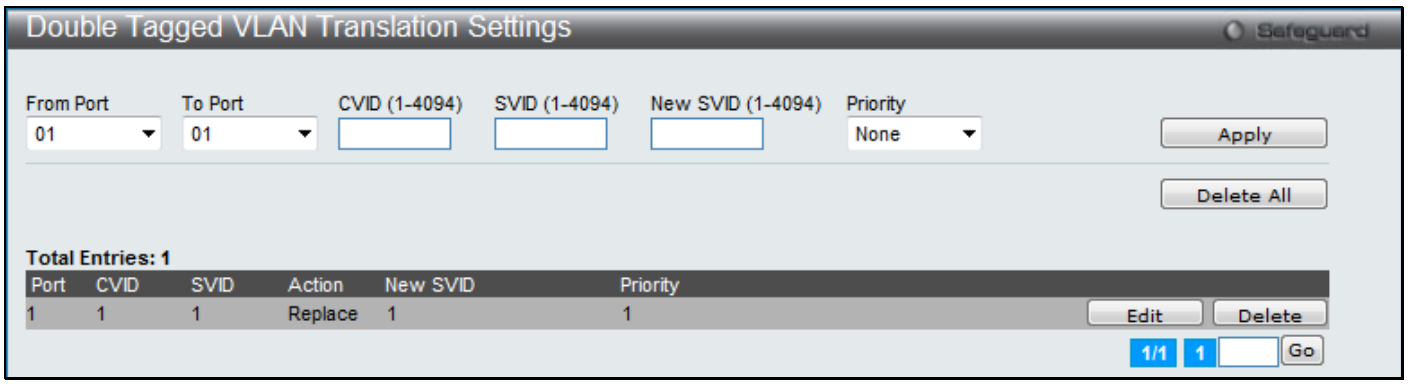


Figure 5-28 Double Tagged VLAN Translation Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of ports to use in the configuration.
CVID(1-4094)	Here the user can enter the C-VLAN ID to match.

SVID (1-4094)	Here the user can enter the S-VLAN ID to match.
New SVID (1-4094)	When both SVID and CVID are matched, replace original SVID with the new SVID
Priority	Here the user can select the priority of the s-tag.

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

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

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

VLAN Translation Port Mapping Settings

This page can be used to configure the port's Q-in-Q S-VLAN assignment rules. These rules are contained in a Q-in-Q profile. Up to one Q-in-Q profile can be added to a port. This setting will not be effective when Q-in-Q mode is disabled.

To view the following window, click **L2 Features > QinQ > VLAN Translation Port Mapping Settings**, as shown below:

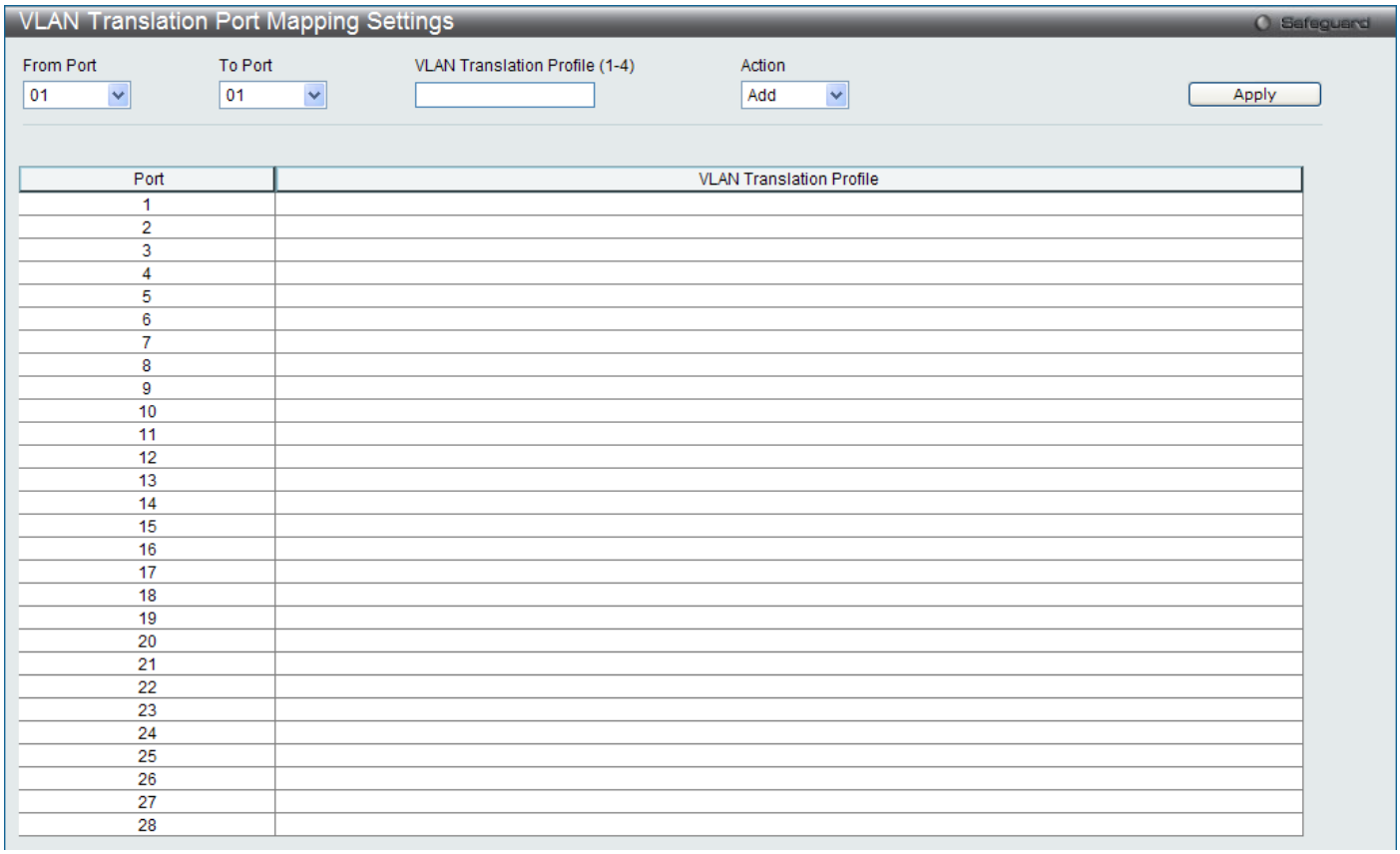


Figure 5-29 VLAN Translation Port Mapping Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of ports to use in the configuration.
VLAN Translation Profile (1-4)	Here the user can enter the VLAN translation profile number.
Action	Here the user can select the action to take. Action that can be selected are **Add**, or **Delete**.

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

VLAN Translation Profile List

This page is used to create a Q-in-Q profile and to assign the SP-VLAN. Multiple rules can be specified for a Q-in-Q profile. Outer tags to frames can be added or replaced to match the translation profiles.

To view the following window, click **L2 Features > QinQ > VLAN Translation Profile Settings**, as shown below:

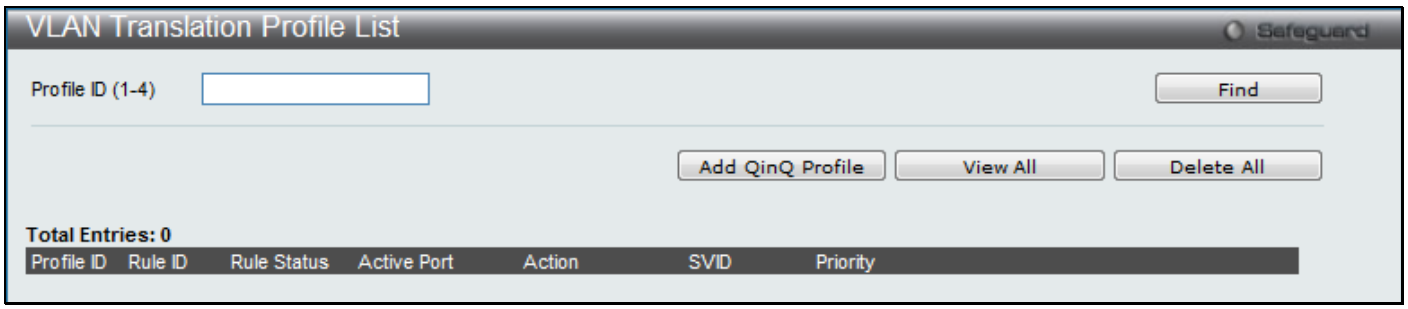


Figure 5-30 VLAN Translation Profile List window

The fields that can be configured are described below:

Parameter	Description
Profile (1-4)	Here the user can enter the number of the profile

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Add QinQ Profile** button to add a new Q-in-Q profile.
Click the **View All** button to display all the existing entries.
Click the **Delete All** button to remove all the entries listed.

After clicking the **Add QinQ Profile** button, the following page will appear:

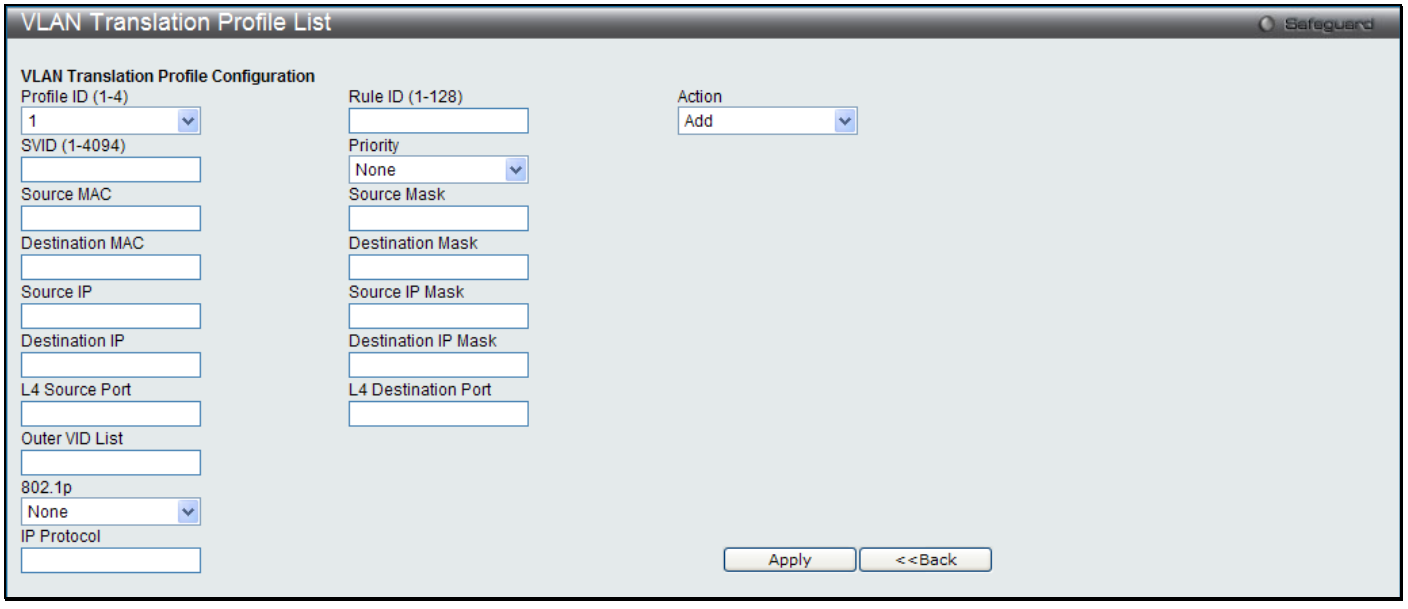


Figure 5-31 VLAN Translation Profile List window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-4)	Here the user can specify the profile ID number to be configured
Rule ID (1-128)	Here the user can specify the rule ID to be added to the profile
Action	Here the user can select the action to add a tag for the assigned SP-VLAN before the C-VLAN tag. If there is an S-TAG in the packet, this rule will not take effect. The user can also select the action that indicates to replace the C-VLAN in the tag by the SP VLAN. If there is no C-TAG in the packet, this rule will not take effect.

SVID (1-4094)	Here the user can specify the SP-VLAN ID to be assigned to the matched packet.
Priority	Here the user can specify the priority of the SP-VLAN. If priority is not specified, the value is default to the port default priority.
Source MAC	Here the user can specify the source MAC address.
Source Mask	Here the user can specify the source MAC address mask.
Destination MAC	Here the user can specify the destination MAC address.
Destination Mask	Here the user can specify the destination MAC address mask.
Source IP	Here the user can specify the source IPv4 address or IPv4 subnet.
Source IP Mask	Here the user can specify the source IPv4 address mask.
Destination IP	Here the user can specify the destination IPv4 address or IPv4 subnet.
Destination IP Mask	Here the user can specify the destination IPv4 address mask.
L4 Source Port	Here the user can specifies the L4 source port ID.
L4 Destination Port	Here the user can specifies the L4 destination port ID.
Outer VID List	Here the user can specify the packet's outer VID range.
802.1p	Here the user can specify the packet's 802.1p priority.
IP Protocol	Here the user can specify the IP Protocol used.

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

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

Layer 2 Protocol Tunneling Settings

With the Q-in-Q double VLAN function, the subscriber's layer 2 traffic is transparent to ISP networks. However, Q-in-Q cannot handle those layer 2 control protocols that makes the network a bit risky and inconvenient. The Layer 2 Protocol Tunneling (L2PT) function resolves the problem by tunneling L2 control protocols to each remote site and makes the central management possible for a company.

To view the following window, click **L2 Features > Layer 2 Protocol Tunneling Settings**, as shown below:

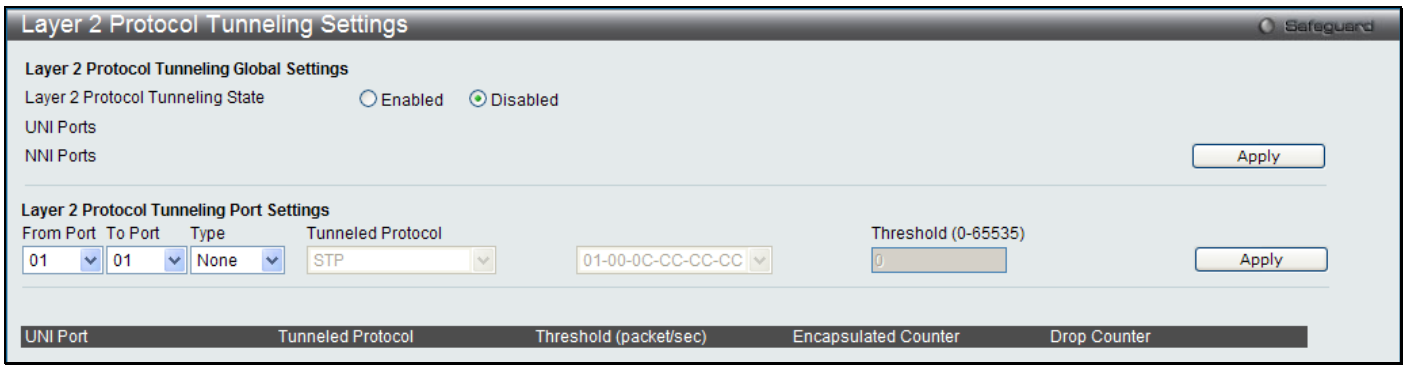


Figure 5-32 Layer 2 Protocol Tunneling Settings window

The fields that can be configured are described below:

Parameter	Description
Layer 2 Protocol Tunneling State	Use the radio buttons to enable or disable the layer 2 protocol tunneling function globally on the Switch.
From Port / To Port	Select a range of ports to use in the configuration.
Type	Use the drop-down menu to select the type of the ports. Available choices are *UNI*, *NNI*

	and *None*. The default type is None.
Tunneled Protocol	When *UNI* is selected in the **Type** drop-down menu, this drop-down menu shows the following options: *STP*- Specify the BPDU received on these UNI will be tunneled. *GVRP* - Specify the GVRP PDU received on these UNI will be tunneled. *Protocol MAC* - Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports. At present, the MAC address can be 01-00-0C-CC-CC-CC or 01-00-0C-CC-CC-CD. *All* - Specify all supported.
Threshold (0-65535)	Enter the drop threshold for packets-per-second accepted on this UNI port. The port drops the PDU if the protocol's threshold is exceeded. The range of the threshold value is 0 to 65535 (packet/second). The value 0 means unlimited. By default, the value is 0.

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

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 802.1Q-2005 MSTP have been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BDPU 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:

1. 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).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. 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:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)
2. 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).
3. 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*	*Listening*	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:

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

STP Bridge Global Settings

On this page the user can configure the STP bridge global parameters.

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

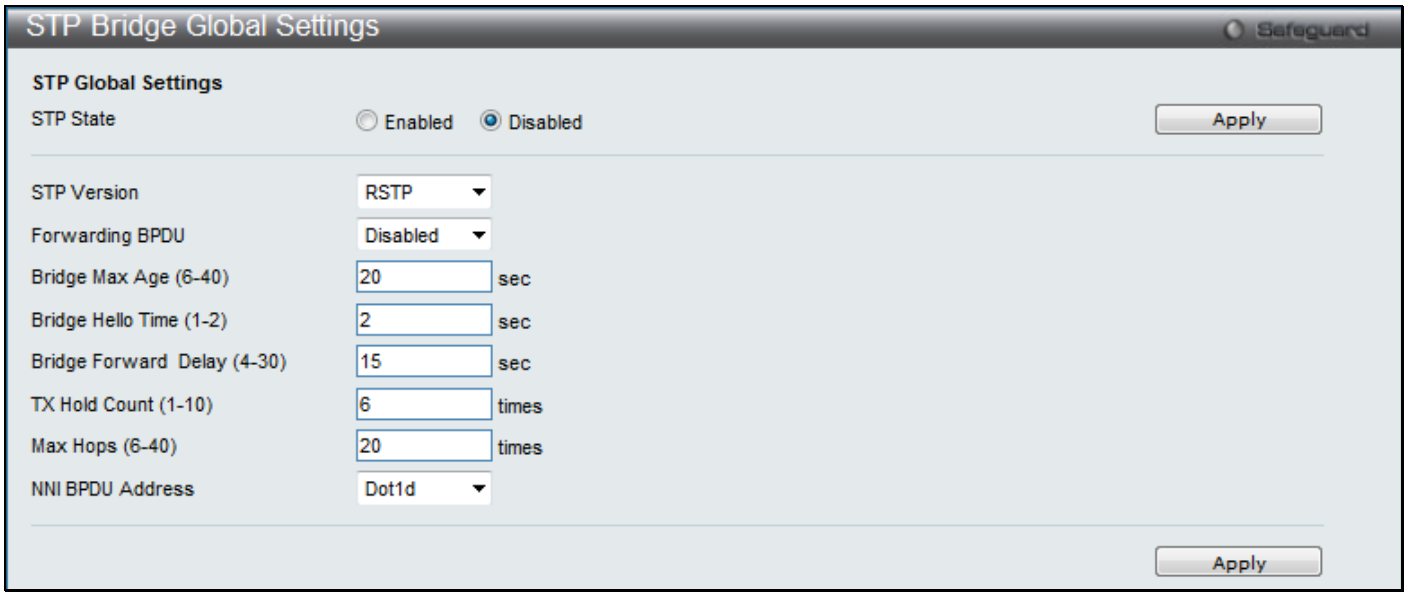


Figure 5-33 STP Bridge Global Settings window

The fields that can be configured are described below:

Parameter	Description
STP State	Use the radio button to globally enable or disable STP.
STP Version	Use the pull-down menu to choose the desired version of STP: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Disabled*.
Bridge Max Age (6-40)	The Max Age 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. The user may choose a time between *6* and *40* seconds. The default value is *20* seconds.
Bridge Hello Time (1-2)	The Hello Time can be set from *1* to *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. The default is *2* seconds.
Bridge Forward Delay (4-30)	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state. The default is *15* seconds

Tx Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6*.
Max Hops (6-40)	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. The user may set a hop count from *6* to *40*. The default is *20*.
NNI BPDU Address	Here the user can enter the NNI BPDU Address used. Among the options, the user can select either *Dot1d* or *Dot1ad*.

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

STP Port Settings

STP can be set up on a port per port basis.

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

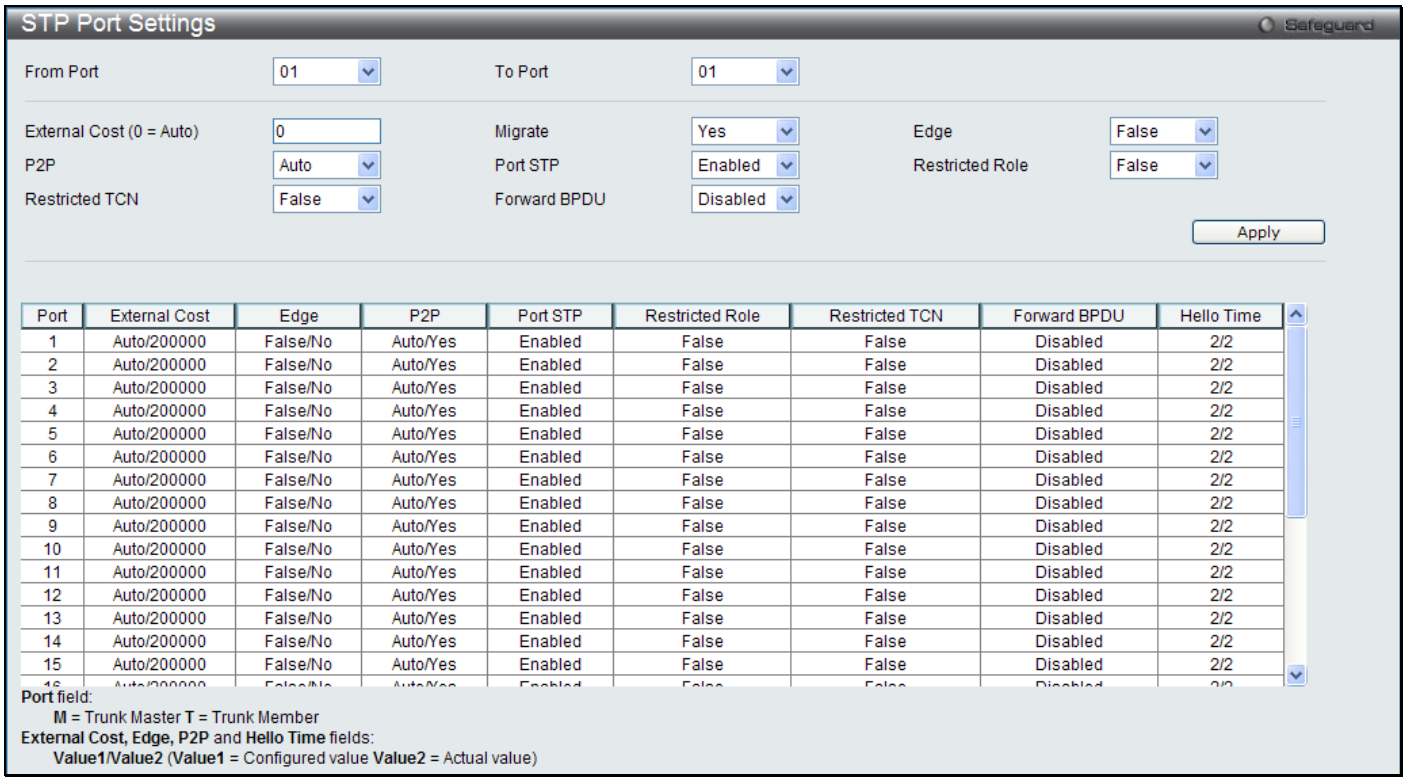


Figure 5-34 STP Port Settings window

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
External Cost (0=Auto)	This 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*. Enter a value between *1* and *200000000* to determine the External Cost. The lower the number, the greater the probability the port will be chosen to forward packets.
P2P	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are

	similar to edge ports; however they are restricted in that a P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A P2P value of *False* indicates that the port cannot have P2P status. *Auto* allows the port to have P2P status whenever possible and operate as if the P2P status were *True*. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were *False*. The default setting for this parameter is *Auto*.
Restricted TCN	Topology Change Notification is a simple BPDU that a bridge sends out to its root port to signal a topology change. Restricted TCN can be toggled between *True* and *False*. If set to *True*, this stops the port from propagating received topology change notifications and topology changes to other ports. The default is *False*.
Migrate	When operating in RSTP mode, selecting *Yes* forces the port that has been selected to transmit RSTP BPDUs.
Port STP	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is *Enabled*.
Forward BPDU	Use the pull-down menu to enable or disable the flooding of BPDU packets when STP is disabled.
Edge	Choosing the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the *False* parameter indicates that the port does not have edge port status. Alternatively, the *Auto* option is available.
Restricted Role	Use the drop-down menu to toggle Restricted Role between *True* and *False*. If set to *True*, the port will never be selected to be the Root port. The default is *False*.

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

MST Configuration Identification

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

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

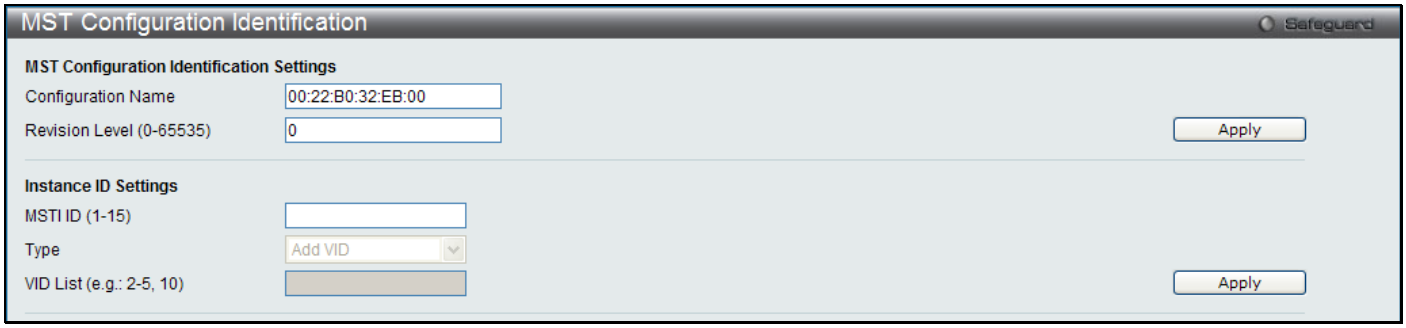


Figure 5-35 MST Configuration Identification window

The fields that can be configured are described below:

Parameter	Description
Configuration Name	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 (0-	This value, along with the Configuration Name, identifies the MSTP region configured on

65535)	the Switch.
MSTI ID (1-15)	Enter a number between *1* and *15* to set a new MSTI on the Switch.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices: *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*.

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

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

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

STP Instance Settings

This window displays MSTIs currently set on the Switch and allows users to change the Priority of the MSTIs.

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

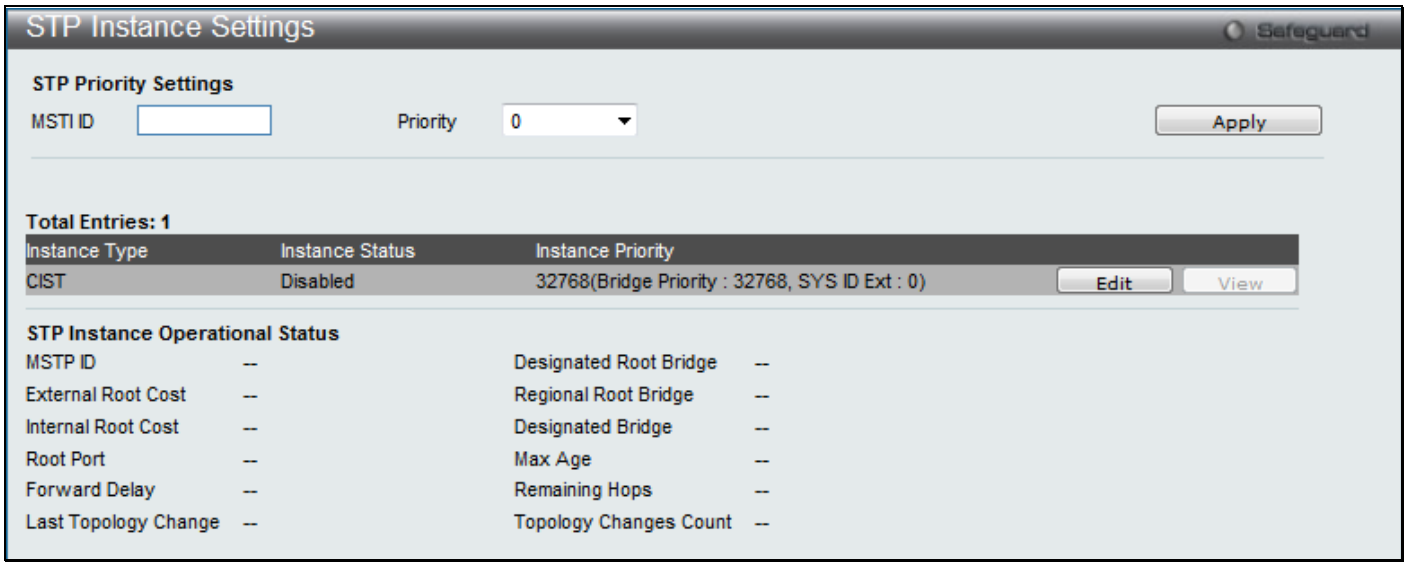


Figure 5-36 STP Instance Settings window

The fields that can be configured are described below:

Parameter	Description
MSTI ID	Enter the MSTI ID in this field. An entry of *0* denotes the CIST (default MSTI).
Priority	Enter the priority in this field. The available range of values is from *0* to *61440*.

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

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

Click the **View** button to display the information of the specific entry.

MSTP Port Information

This window displays the current MSTI configuration information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

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

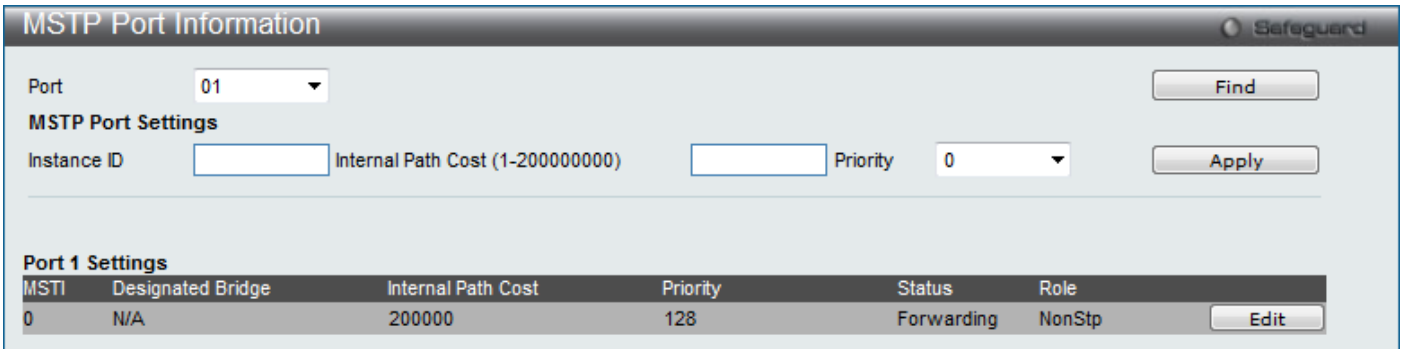


Figure 5-37 MSTP Port Information window

The fields that can be configured are described below:

Parameter	Description
Port	Select a port to view its MSTI settings.
Instance ID	The MSTI ID of the instance to be configured. Enter a value between *0* and *15*. An entry of *0* in this field denotes the CIST (default MSTI).
Internal Path Cost	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of *1* to *200000000* will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission. Selecting *0* (zero) for this parameter will set the quickest route automatically and optimally for an interface.
Priority	Enter a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

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

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

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

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 fourteen port trunk groups with two to eight ports in each group. A potential bit rate of 800 Mbps can be achieved.

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 fourteen link aggregation groups, each group consisting of 2 to 8 links (ports). The (optional) Gigabit ports can only belong to a single link aggregation group.

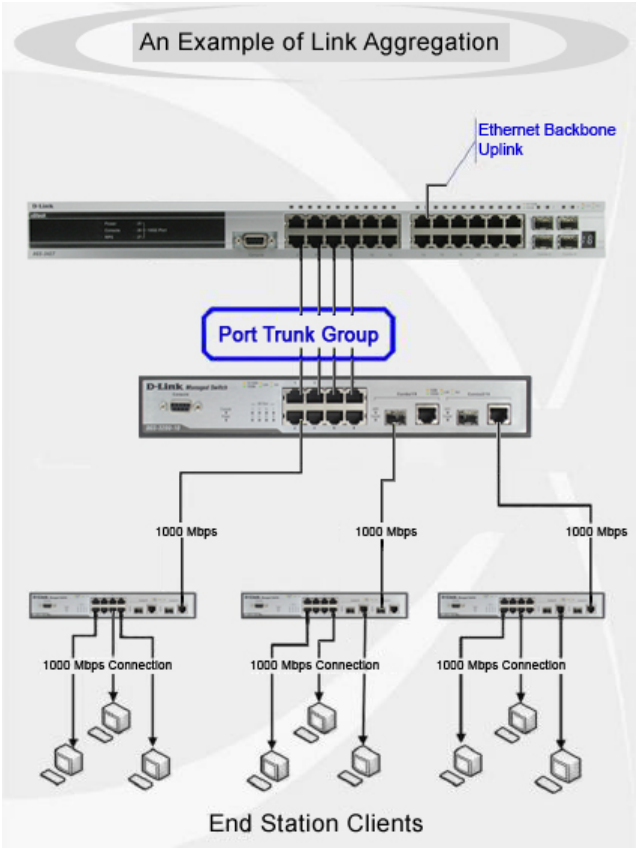


Figure 5-38 Link Aggregation Example window

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, port mirroring 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.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

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

The Spanning Tree Protocol will treat a link aggregation group as a single link, 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.

Port Trunking Settings

On this page the user can configure the port trunk settings for the switch.

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

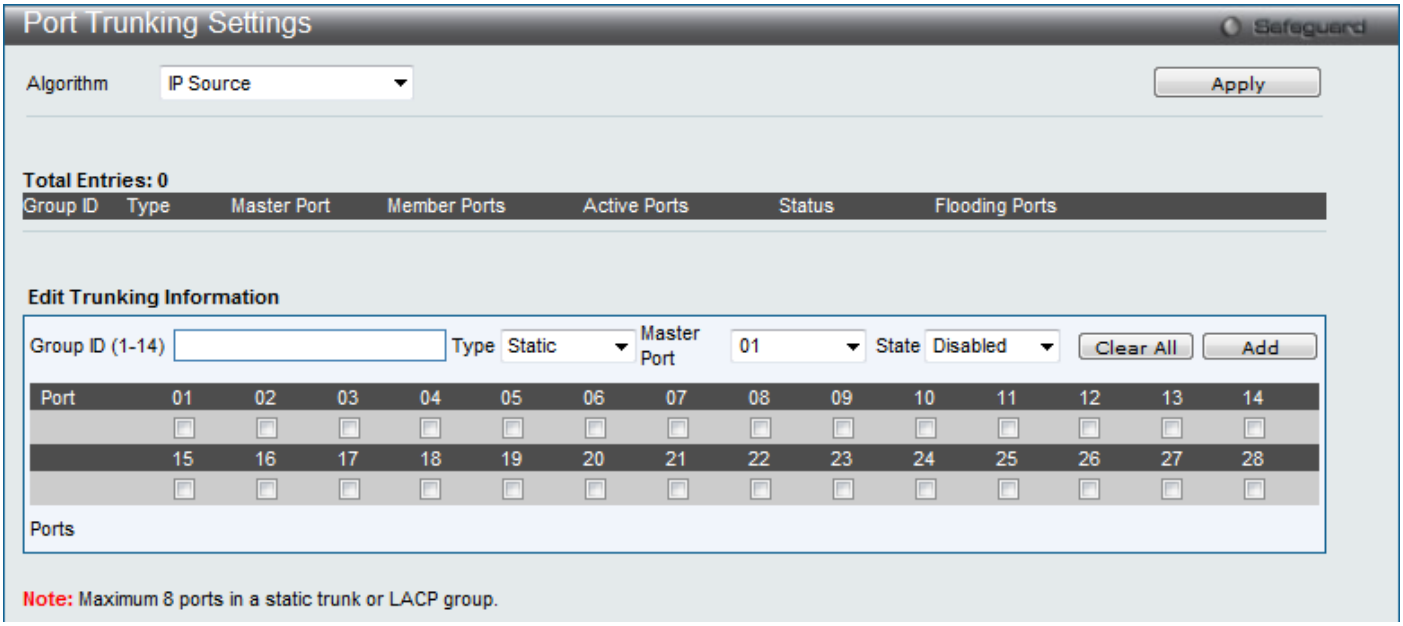


Figure 5-39 Port Trunking Settings window

The fields that can be configured are described below:

Parameter	Description
Algorithm	This is the traffic hash algorithm among the ports of the link aggregation group. Options to choose from are MAC Source Dest, IP Source Dest and Lay4 Source Dest.
Group ID (1-14)	Select an ID number for the group, between *1* and *14.*
Type	This pull-down menu allows users to select between *Static* and *LACP* (Link Aggregation Control Protocol). *LACP* allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Port	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Ports	Display the ports that are currently forwarding packets.

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

Click the **Clear All** button to clear out all the information entered.

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

NOTE: The maximum number of ports that can be configured in one Static Trunk or LACP Group are **8 ports**.

LACP Port Settings

In conjunction with the **Trunking** window, users can create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

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

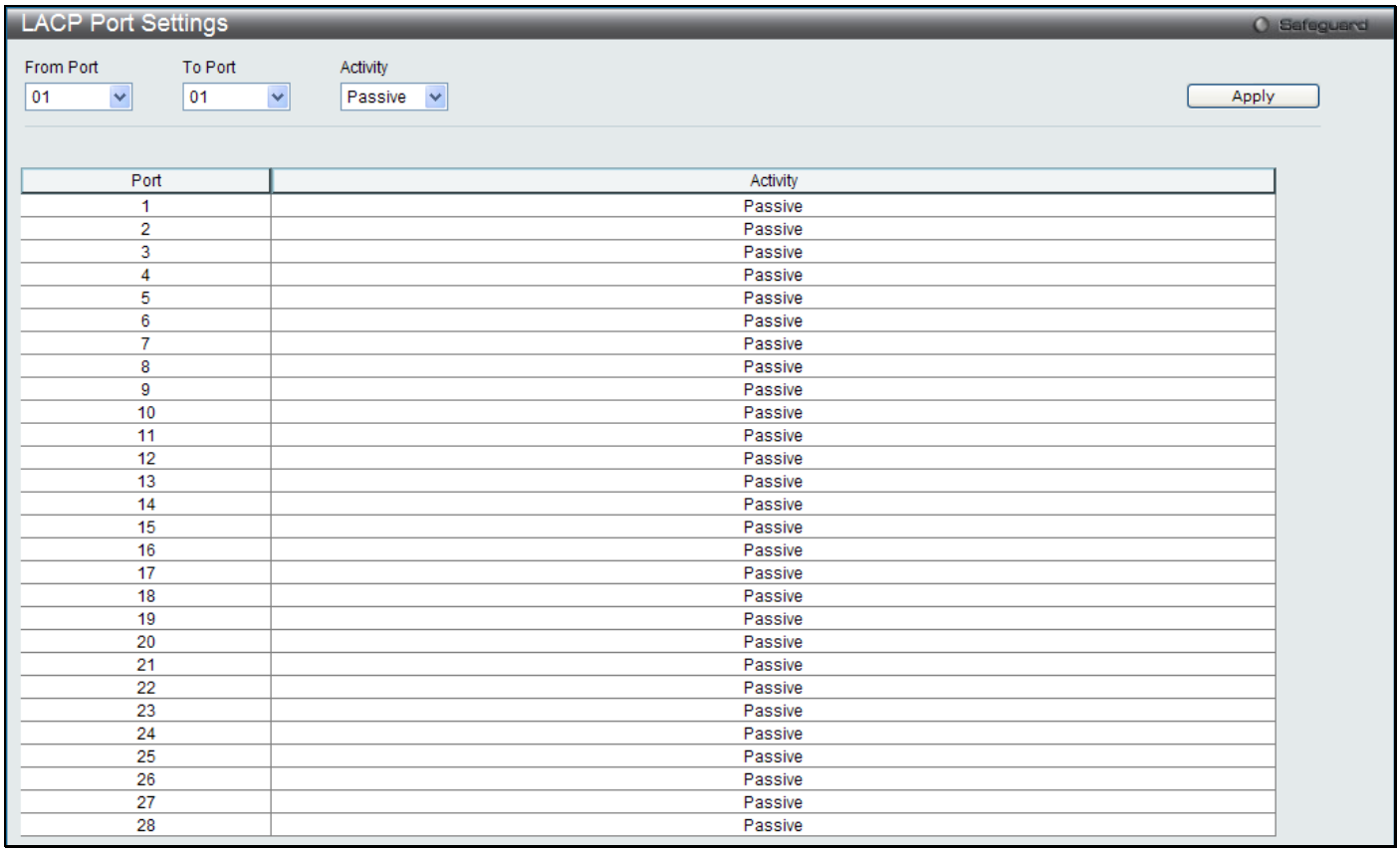


Figure 5-40 LACP Port Settings sindow

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
Activity	*Active* - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. *Passive* - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).

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

FDB

Static FDB Settings

Unicast Static FDB Settings

Users can set up static unicast forwarding on the Switch.

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

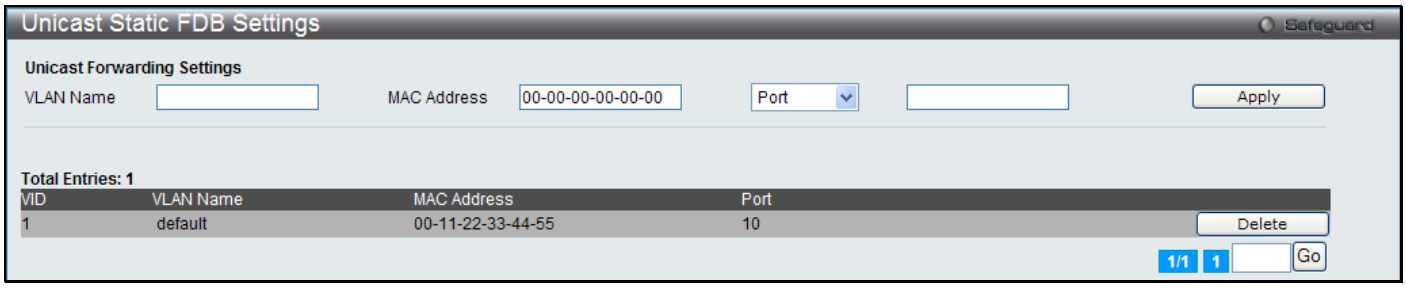


Figure 5-41 Unicast Static FDB Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN name of the VLAN on which the associated unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port / Drop	Allows the selection of the port number on which the MAC address entered above resides This option could also drop the MAC address from the unicast static FDB.

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.

Multicast Static FDB Settings

Users can set up static multicast forwarding on the Switch.

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

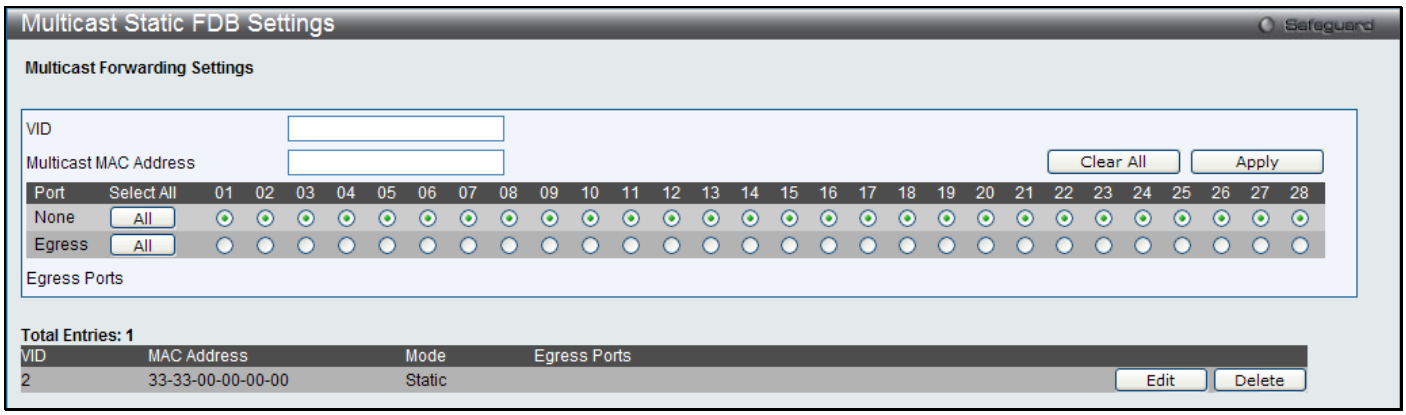


Figure 5-42 Multicast Static FDB Settings window

The fields that can be configured are described below:

Parameter	Description
VID	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address	The static destination MAC address of the multicast packets. This must be a multicast MAC address.
Port	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are:

	None - No restrictions on the port dynamically joining the multicast group. When *None* is chosen, the port will not be a member of the Static Multicast Group. Click the **All** button to select all the ports. *Egress* - The port is a static member of the multicast group. Click the **All** button to select all the ports.

Click the **Clear All** button to clear out all the information entered.

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

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

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

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database. This window allows you to globally set MAC notification on the Switch. Users can set MAC notification for individual ports on the Switch.

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

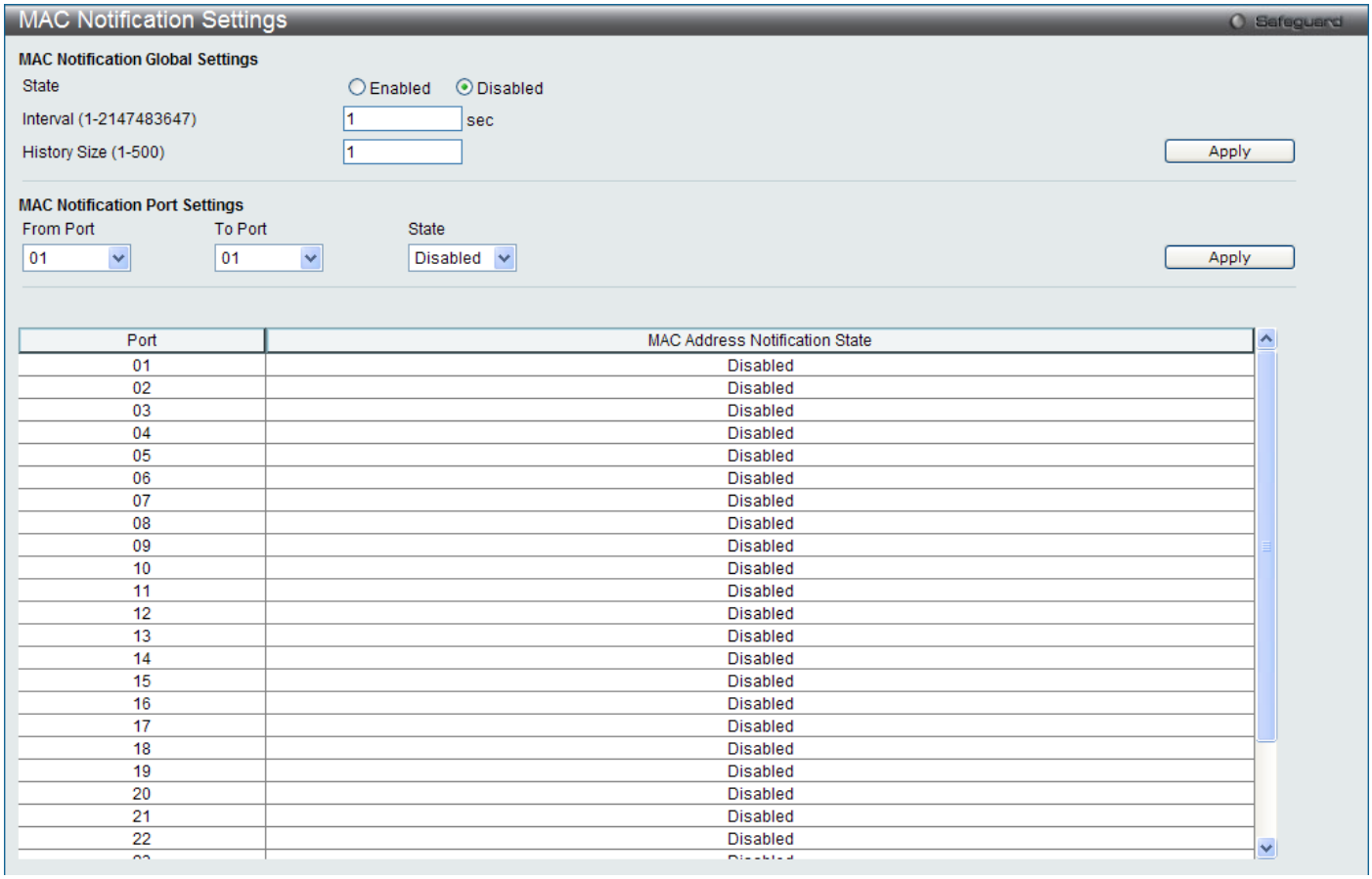


Figure 5-43 MAC Notification Settings window

The fields that can be configured are described below:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval (1-2147483647)	The time in seconds between notifications. Value range to use is *1* to *2147483647*.
History Size (1-500)	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.
From Port / To Port	Select a range of ports to be configured.
State	Enable MAC Notification for the ports selected using the pull-down menu.

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

MAC Address Aging Time Settings

Users can configure the MAC Address aging time on the Switch.

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

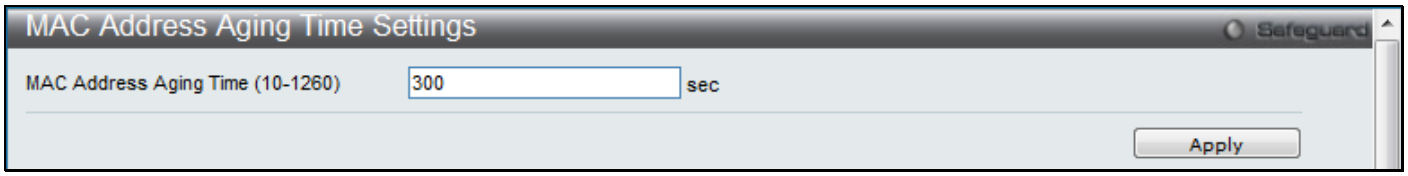


Figure 5-44 MAC Address Aging Time Settings window

The fields that can be configured are described below:

Parameter	Description
MAC Address Aging Time (10-1260)	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this option, type in a different value representing the MAC address' age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1260* seconds. The default setting is *300* seconds.

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

MAC Address Table

This allows the Switch's MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address, VLAN and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

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

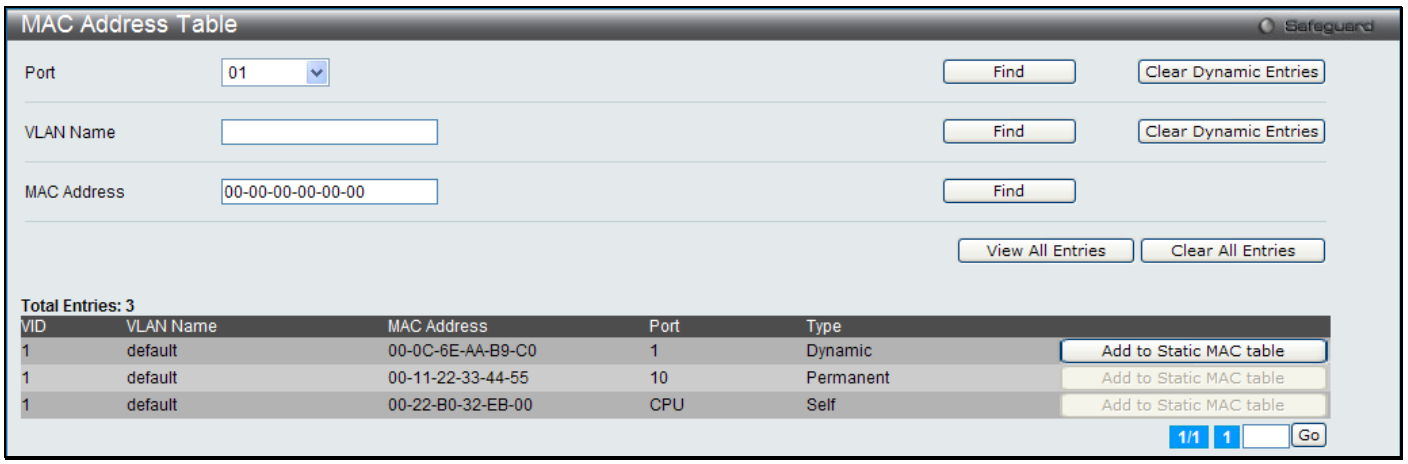


Figure 5-45 MAC Address Table window

The fields that can be configured are described below:

Parameter	Description
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.

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

Click the **Clear Dynamic Entries** button to delete all dynamic entries of the address table.

Click the **View All Entries** button to display all the existing entries.
Click the **Clear All Entries** button to remove all the entries listed in the table.
Click the **Add to Static MAC table** button to add the specific entry to the Static MAC table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP & FDB Table

On this page the user can find the ARP and FDB table parameters.

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

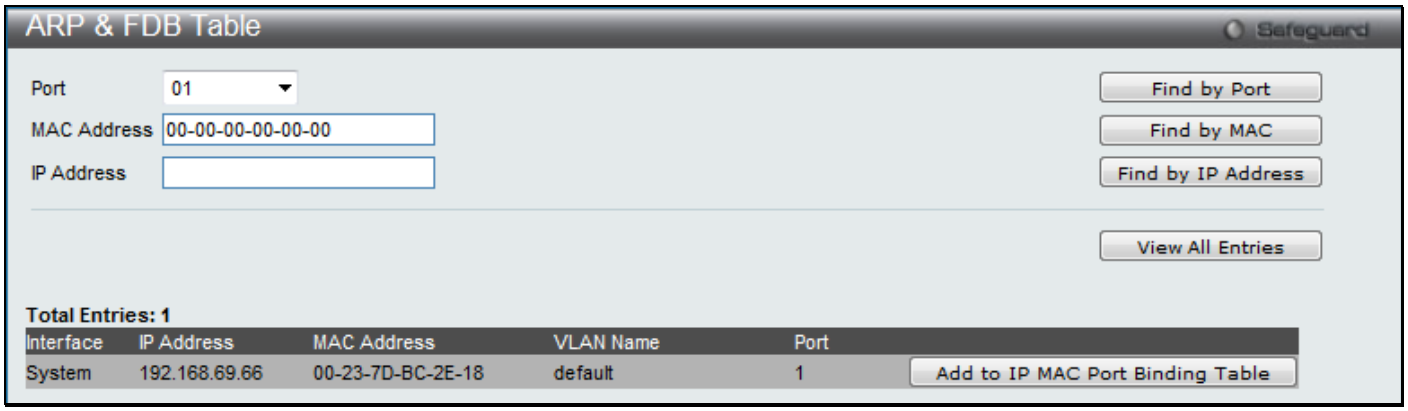


Figure 5-46 ARP & FDB Table window

The fields that can be configured are described below:

Parameter	Description
Port	Here the user can select the port number to use for this configuration.
MAC Address	Here the user can enter the MAC address to use for this configuration.
IP Address	Here the user can enter the IP address the use for this configuration.

Click the **Find by Port** button to locate a specific entry based on the port number selected.
Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.
Click the **Find by IP Address** button to locate a specific entry based on the IP address entered.
Click the **View All Entries** button to display all the existing entries.
Click the **Add to IP MAC Port Binding Table** to add the specific entry to the IP MAC Port Binding Table.

L2 Multicast Control

IGMP Proxy

Based on IGMP forwarding, the IGMP proxy runs the host part of IGMP on the upstream and router part of IGMP on the downstream, and replicates multicast traffic across VLANs on devices such as the edge boxes. It reduces the number of the IGMP control packets transmitted to the core network.

IGMP Proxy Settings

Users can configure the IGMP proxy state and IGMP proxy upstream interface in this page.

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

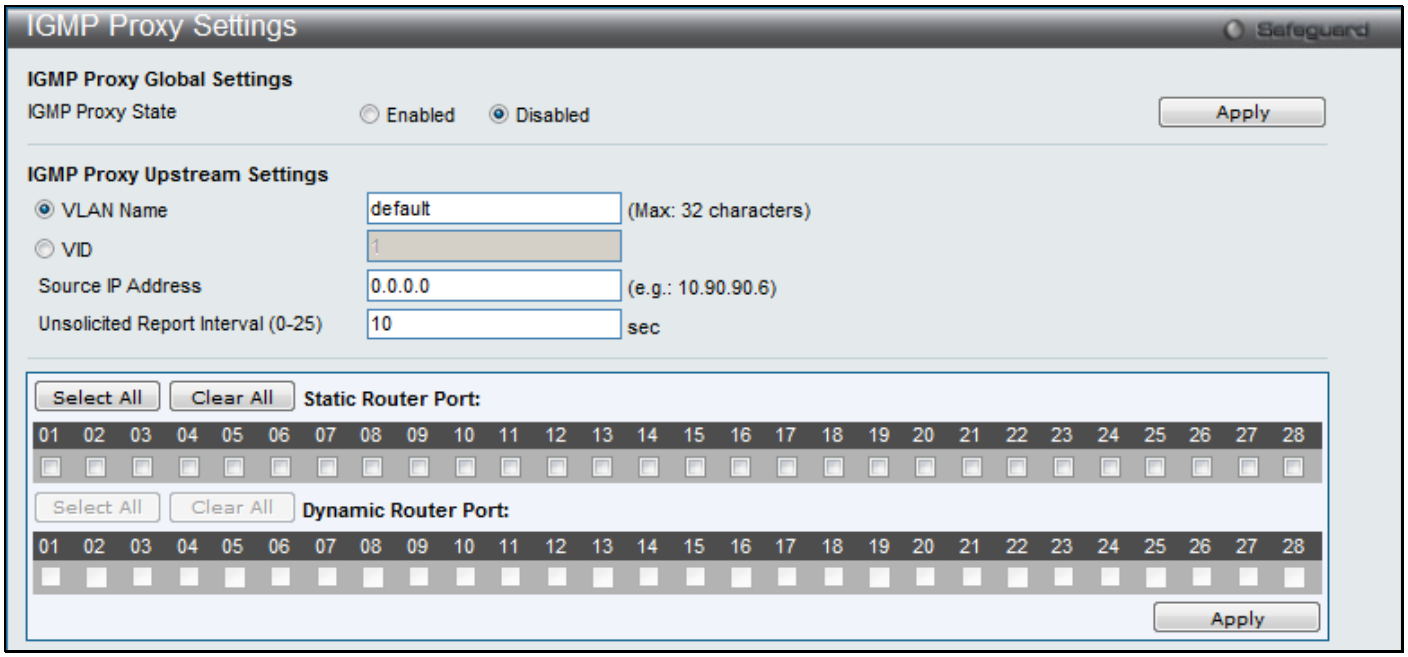


Figure 5-47 IGMP Proxy Settings window

The fields that can be configured are described below:

Parameter	Description
IGMP Proxy State	Here the user can enable or disable the IGMP Proxy Global State.
VLAN Name	The VLAN name for the interface.
VID	The VID for the interface.
Source IP Address	Enter the source IP address of the upstream protocol packet here. If it is not specified, the zero IP address will be used as the protocol source IP address.
Unsolicited Report Interval (0-25)	The Unsolicited report interval. It is the time between repetitions of the host's initial report of membership in a group. Default is 10 seconds. If set to 0, it means to send only one report packet.
Port(s)	Here the user can select the port that will be included in this configuration.

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

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

IGMP Proxy Downstream Settings

Users can configure the IGMP proxy downstream interface in this page. The IGMP proxy downstream interface must be an IGMP snooping enabled VLAN.

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

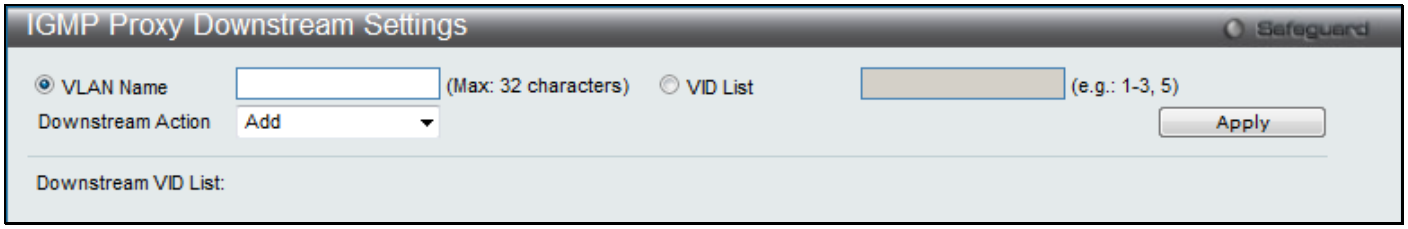


Figure 5-48 IGMP Proxy Downstream Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Specify the VLAN Name which belongs to the IGMP proxy downstream interface.
VID List	Specify a list of VLANs which belong to the IGMP proxy downstream interface.
Downstream Action	Here the user can **Add** or **Delete** a downstream interface.

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

IGMP Proxy Group

On this page the user can view the IGMP Proxy Group settings.

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

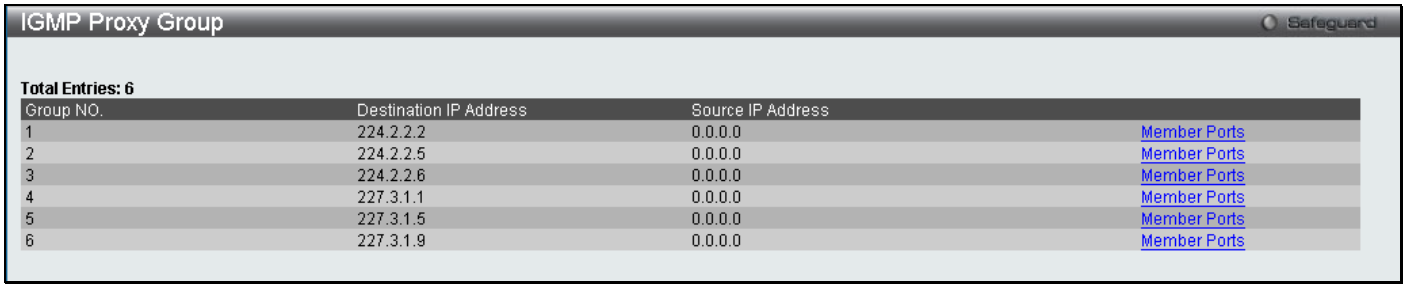


Figure 5-49 IGMP Proxy Group window

Click the Member Ports link to view the IGMP proxy member port information.

After clicking the Member Ports option, the following window will appear.

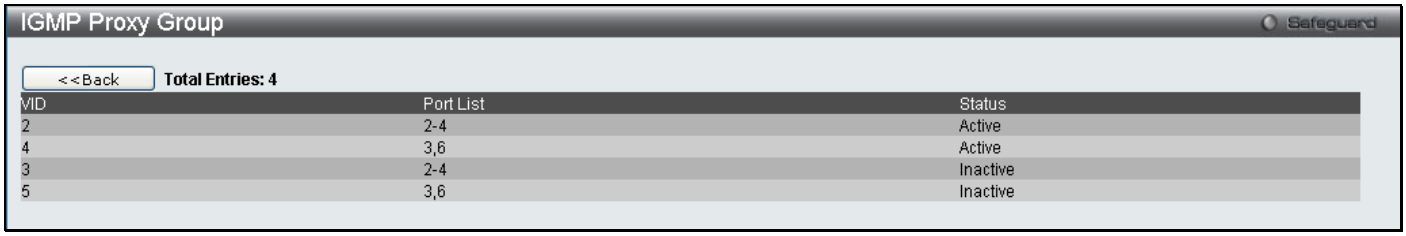


Figure 5-50 IGMP Proxy Group window

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

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. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

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:

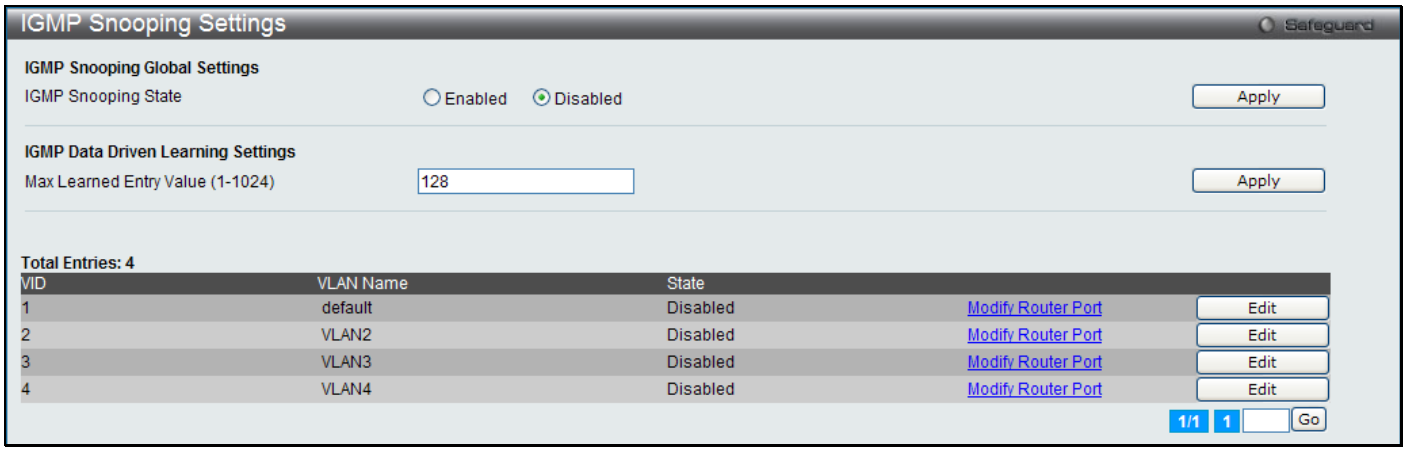


Figure 5-51 IGMP Snooping Settings window

The fields that can be configured are described below:

Parameter	Description
IGMP Snooping State	Here the user can enable or disable the IGMP Snooping state.
Max Learning Entry Value (1-1024)	Here the user can enter the maximum learning entry value.

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

Click the Modify Router Port link to configure the IGMP Snooping Router Port Settings.

Click the **Edit** button to configure the IGMP Snooping Parameters Settings.

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

After clicking the **Edit** button, the following page will appear:

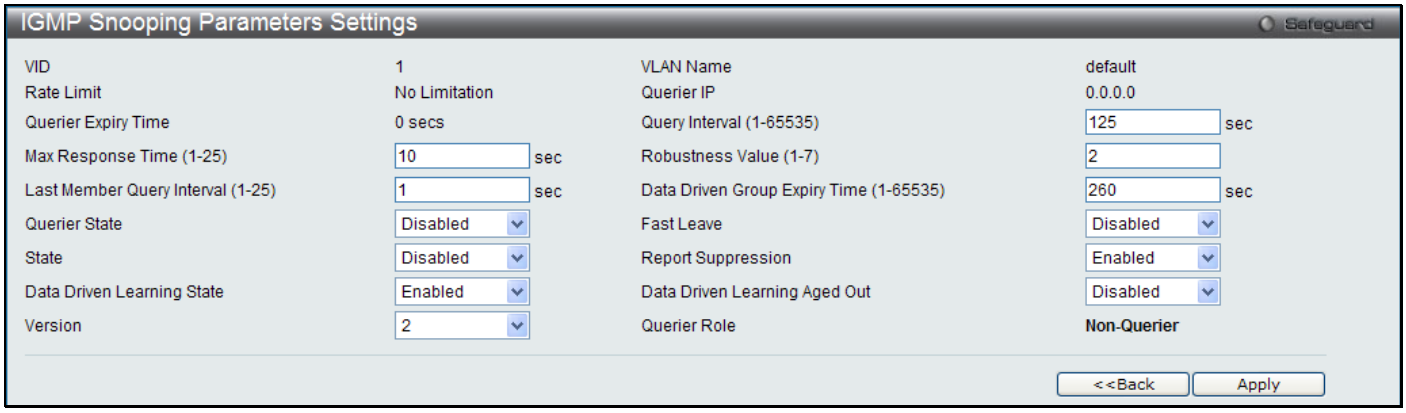


Figure 5-52 IGMP Snooping Parameters Settings window

The fields that can be configured are described below:

Parameter	Description
Query Interval (1-65535)	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds..
Max Response Time (1-25)	Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.
Robustness Value (1-7)	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness value is used in calculating the following IGMP message intervals: By default, the robustness variable is set to 2.
Last Member Query Interval (1-25)	Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.

Data Drive Group Expiry Time (1-65535)	Specify the data driven group lifetime in seconds.
Querier State	Specify to enable or disable the querier state.
Fast Leave	Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.
State	If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). It the state is disabled, then the switch can not play the role as a querier. **NOTE:** that if the Layer 3 router connected to the switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.
Report Suppression	When enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port.
Data Driven Learning State	Specify to enable or disable the data driven learning state.
Data Drive Learning Aged Out	Specify to enable or disable the data drive learning aged out option.
Version	Specify the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be forwarded from the router ports or VLAN flooding.

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

After clicking the Modify Router Port link, the following page will appear:

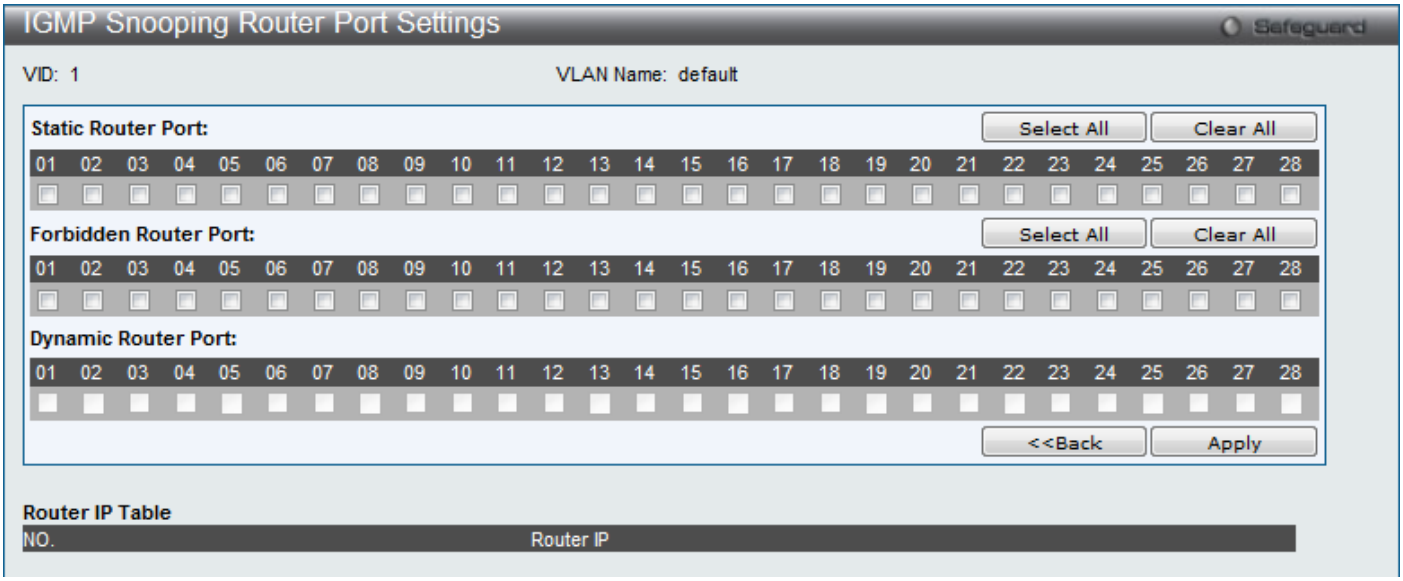


Figure 5-53 IGMP Snooping Router Port Settings window

The fields that can be configured are described below:

Parameter	Description
Static Router Port	This section is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.
Forbidden Router Port	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Dynamic Router Port	Displays router ports that have been dynamically configured.
Ports	Select the appropriate ports individually to include them in the Router Port configuration.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

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

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

IGMP Snooping Rate Limit Settings

On this page the user can configure the IGMP snooping rate limit parameters.

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

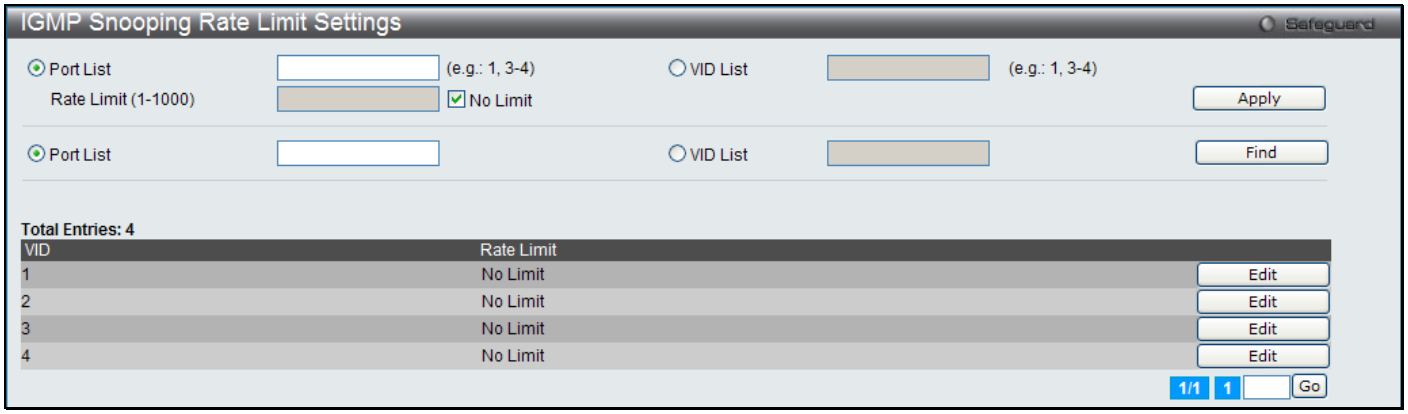


Figure 5-54 IGMP Snooping Rate Limit Settings window

The fields that can be configured are described below:

Parameter	Description
Port List	Here the user can enter the port list used for this configuration.
VID List	Here the user can enter the VID list used for this configuration.
Rate Limit (1-1000)	Here the user can enter the IGMP snooping rate limit used. By selecting the **No Limit** option, the rate limit for the entered port(s) 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.

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

IGMP Snooping Static Group Settings

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

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

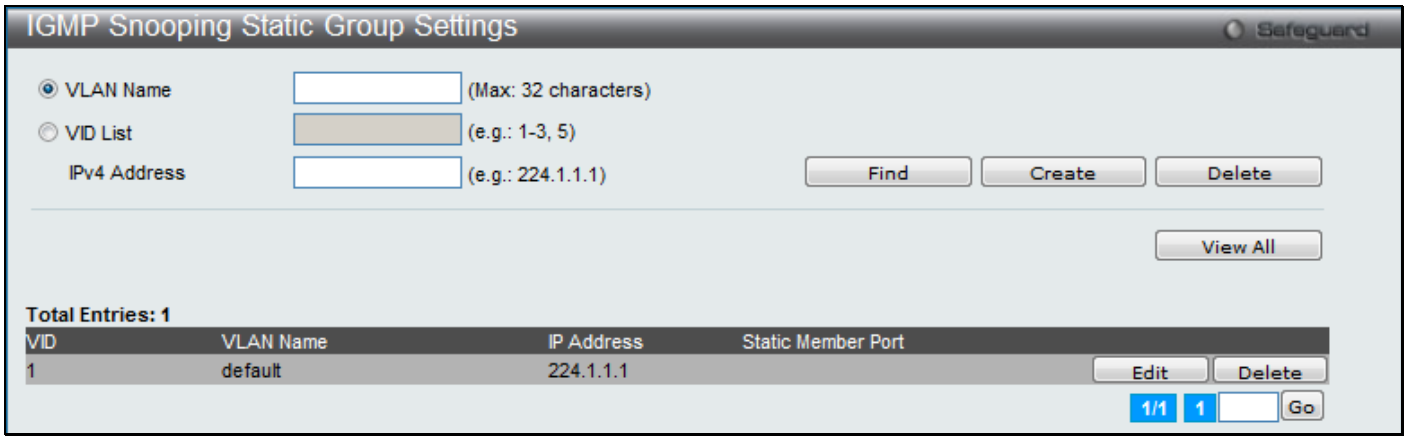


Figure 5-55 IGMP Snooping Static Group Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The *VLAN Name* of the multicast group.
VID List	The *VID List* or of the multicast group.
IPv4 Address	Enter the IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Create** button to add a new entry based on the information entered.
Click the **Delete** button to remove the specific entry based on the information entered.
Click the **View All** button to display all the existing 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.

After clicking the **Edit** button, the following page will appear:

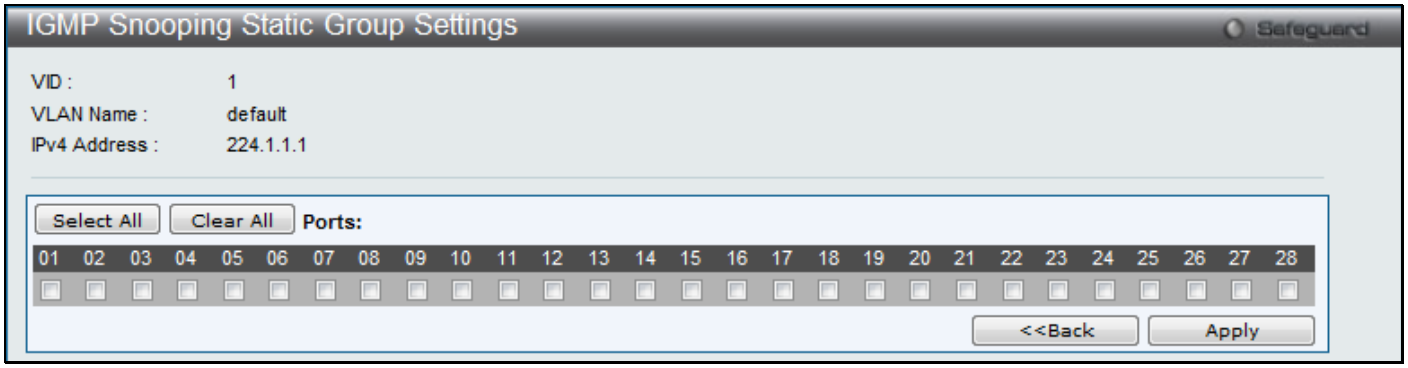


Figure 5-56 IGMP Snooping Static Group Settings window

The fields that can be configured are described below:

Parameter	Description
Ports	Select ports to be configured.

Click the **Select All** button to select all the ports for configuration.
Click the **Clear All** button to unselect all the ports for configuration.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Apply** button to accept the changes made.

IGMP Router Port

Users can display which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.

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

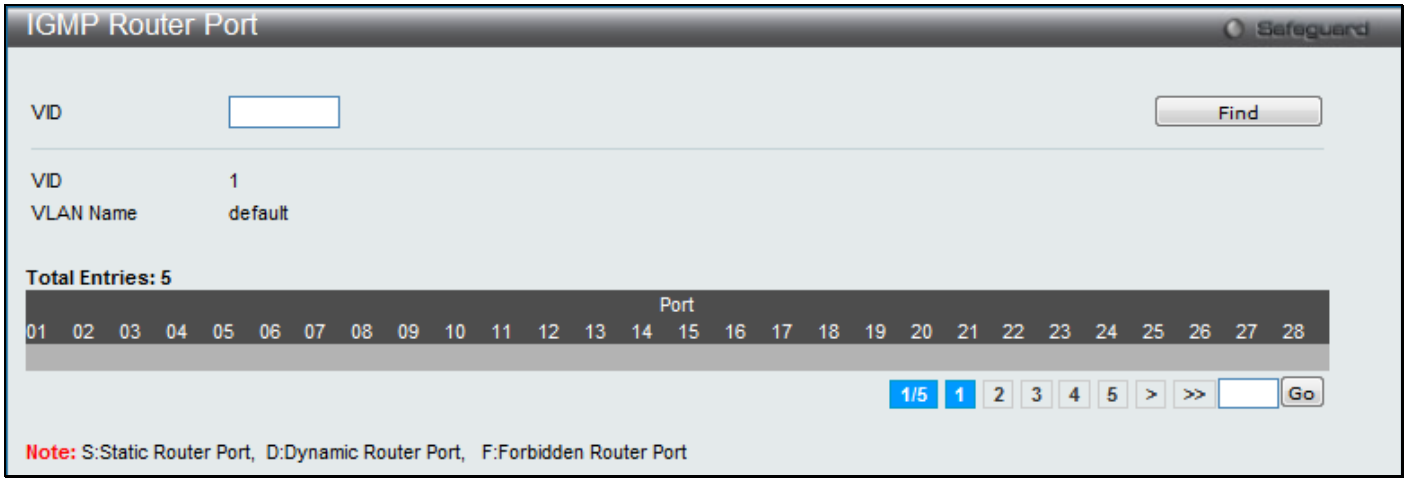


Figure 5-57 IGMP Router Port window

The fields that can be configured are described below:

Parameter	Description
VID	Enter a VLAN ID to be displayed.

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.

NOTE: The abbreviations used in this window are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

IGMP Snooping Group

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

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

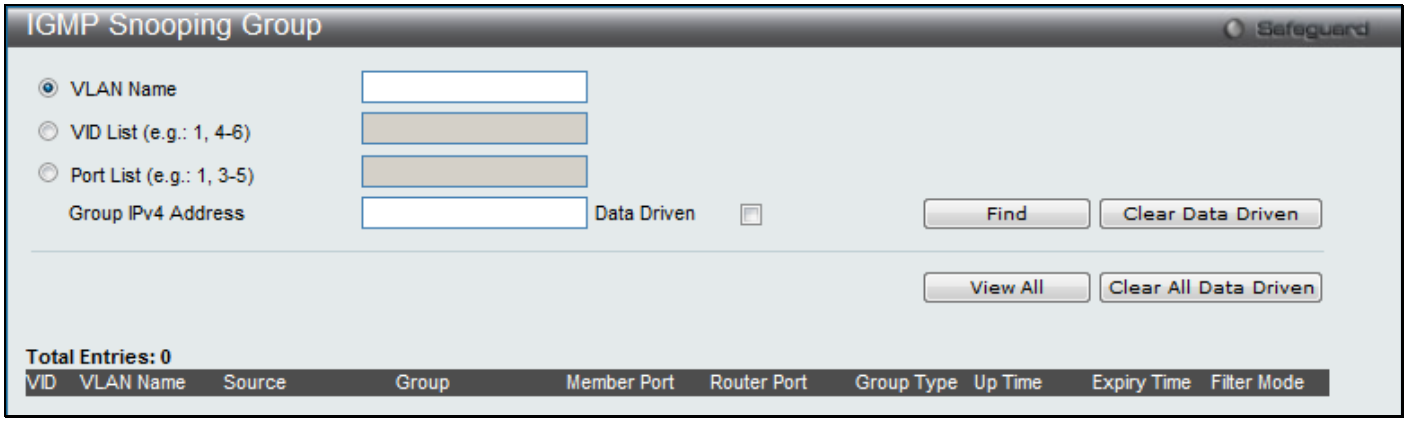


Figure 5-58 IGMP Snooping Group window

The user may search the IGMP Snooping Group Table by either *VLAN Name* or *VID List* by entering it in the top left hand corner and clicking **Find**.

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	Specifies the port number(s) used to find a multicast group.
Group IPv4 Address	Enter the IPv4 address.
Data Driven	If Data Drive is selected, only data driven groups will be displayed.

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

Click the **Clear Data Driven** button to delete the specific IGMP snooping group which is learned by the Data Driven feature of the specified VLAN.

Click the **View All** button to display all the existing entries.

Click the **Clear All Data Driven** button to delete all IGMP snooping groups which are learned by the Data Driven feature.

IGMP Snooping Forwarding Table

This page displays the switch's current IGMP snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

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

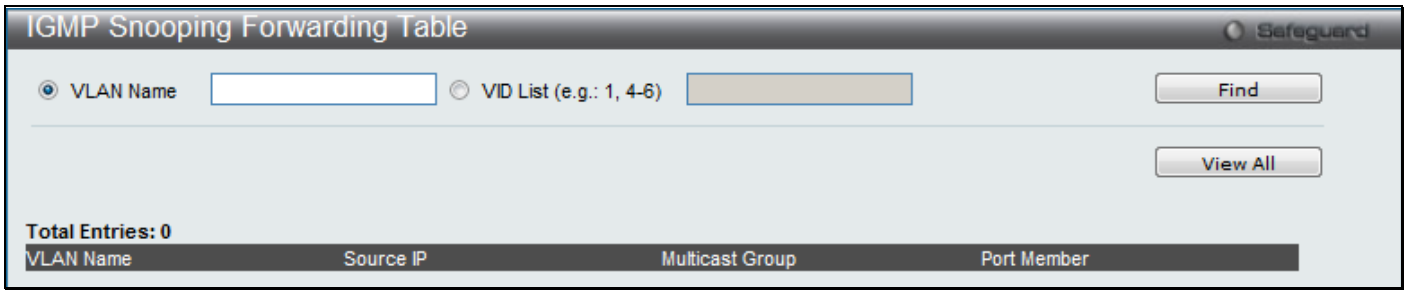


Figure 5-59 IGMP Snooping Forwarding Table window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.

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

Click the **View All** button to display all the existing entries.

IGMP Snooping Counter

Users can view the switch's IGMP Snooping counter table.

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

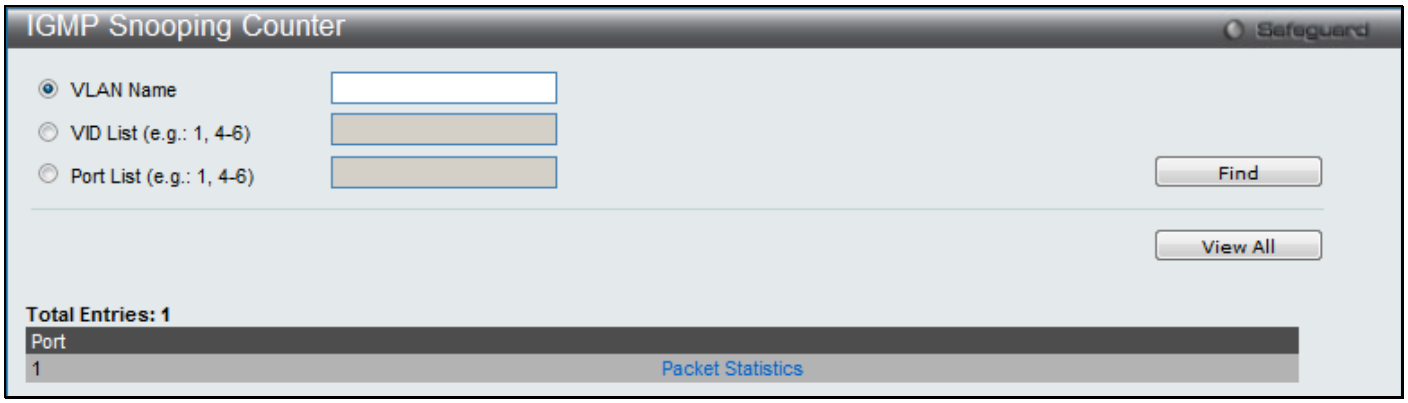


Figure 5-60 IGMP Snooping Counter window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	The *Port List* of the multicast group.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the Packet Statistics link to view the IGMP Snooping Counter Table.

After clicking the Packet Statistics link, the following page will appear:

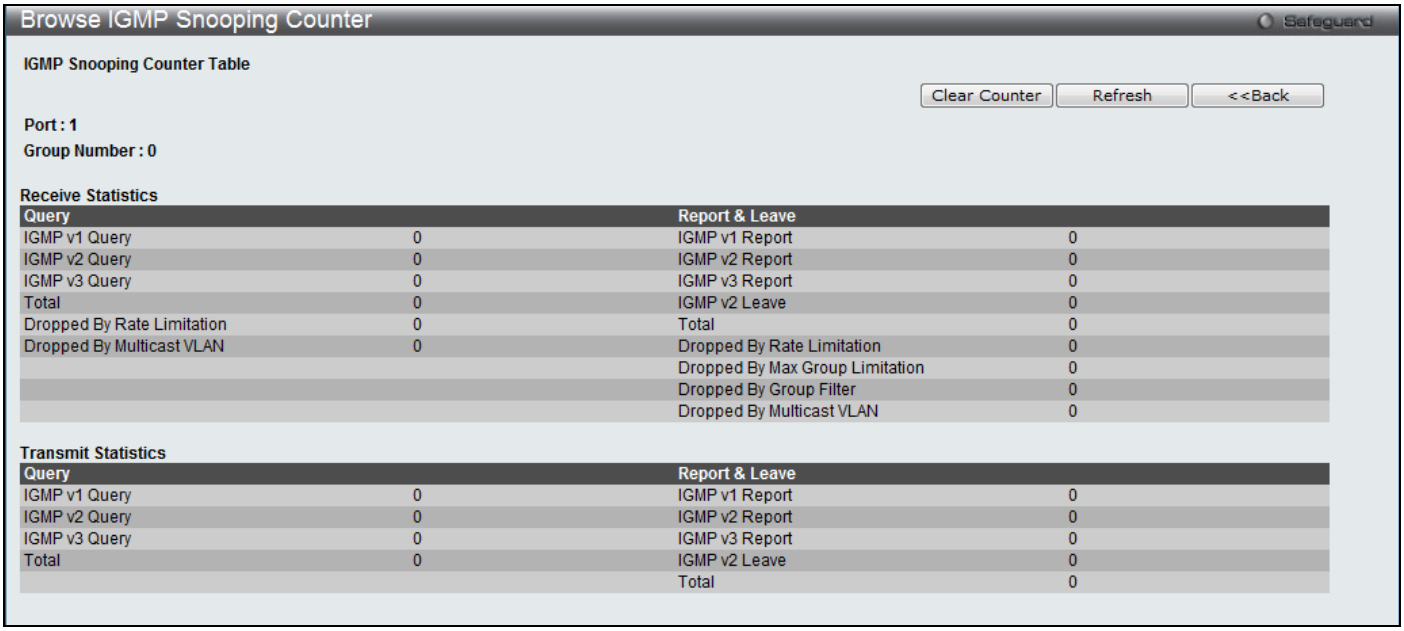


Figure 5-61 Browse IGMP Snooping Counter window

Click the **Clear Counter** button to clear all the information displayed in the fields.
Click the **Refresh** button to refresh the display table so that new information will appear.
Click the **<<Back** button to return to the previous page.

IGMP Host Table

On this page the user can view the IGMP host table.

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

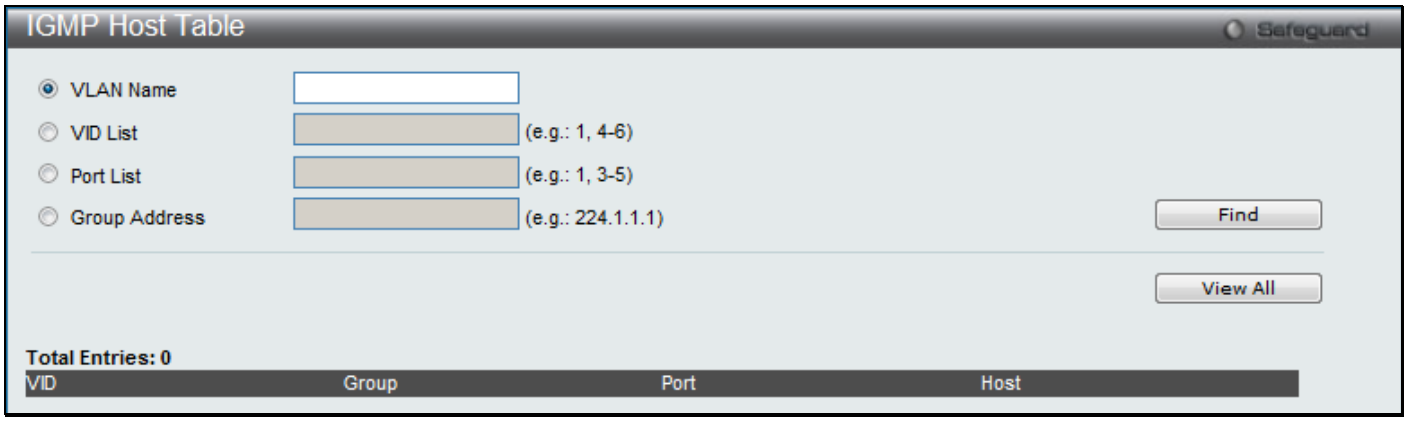


Figure 5-62 IGMP Host Table window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	The *Port List* of the multicast group.
Group Address	The *Group Address* of the multicast group.

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

Click the **View All** button to display all the existing entries.

CPU Filter L3 Control Packet Settings

Some Denial of Service (DoS) attacks are preceded by broadcasting bulk network control protocols. By default, the switch's CPU will process these protocols and update local databases. However, if hackers send faked or bulk control packets, switch CPU will overload and will not able to process the normal traffic.

The L3 control packet filtering will force the switch to drop those abnormal control packets received from the ports that shouldn't have them. (eg, UNI ports)

Users can enable or disable the port state for the layer 3 control packet filter. If enabled, the layer 3 control packet will be dropped.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > CPU Filter L3 Control Packet Settings**, as shown below:

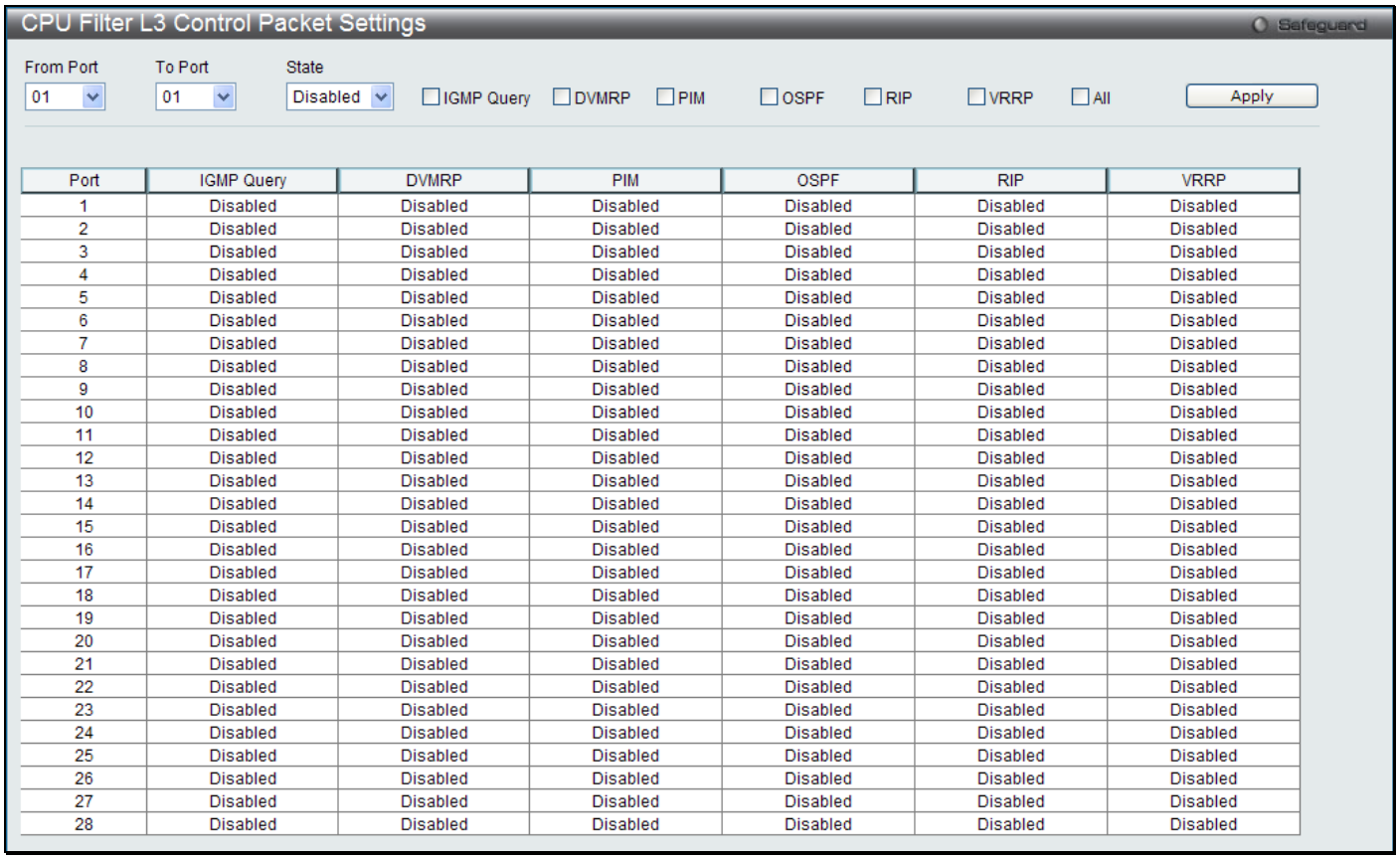


Figure 5-63 CPU Filter L3 Control Packet Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select the port range to use for the CPU Filter configuration.
State	Here the user can enable or disable the CPU Filtering.
IGMP Query	Select this option to include IGMP Query in the CPU Filtering.
DVMRP	Select this option to include DVMRP in the CPU Filtering.
PIM	Select this option to include PIM in the CPU Filtering.
OSPF	Select this option to include OSPF in the CPU Filtering.
RIP	Select this option to include RIP in the CPU Filtering.
VRRP	Select this option to include VRRP in the CPU Filtering.
All	Select this option to include all the information in the CPU Filtering.

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

NOTE: It's only recommended to enable these features when the CPU load is too high. An incorrect filtering rule might cause the system to behave abnormal.

MLD Proxy

MLD proxy plays the host role on the upstream interface. It will send MLD report packet to the router port. MLD proxy plays the router role on the downstream interfaces. It reduces the number of the MLD control packets transmitted to the core network.

MLD Proxy Settings

Users can configure the MLD proxy state and MLD proxy upstream interface in this page.

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

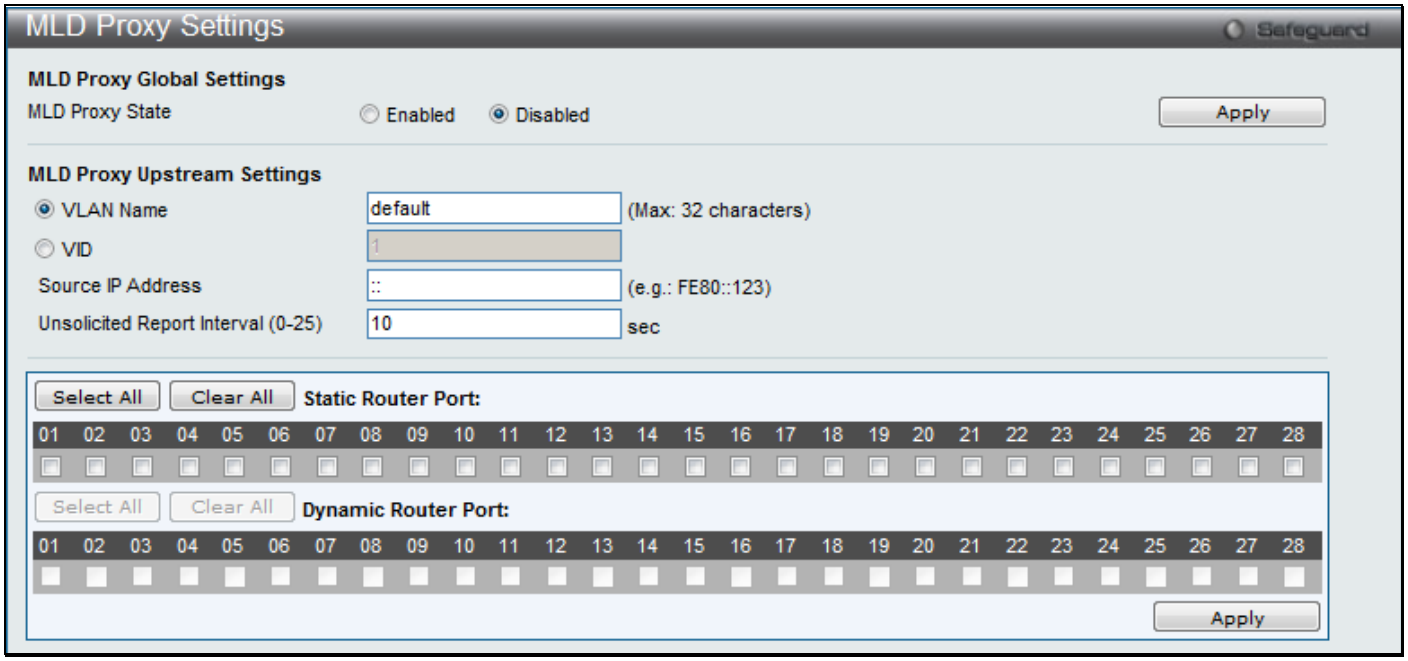


Figure 5-64 MLD Proxy Settings window

The fields that can be configured are described below:

Parameter	Description
MLD Proxy State	Here the user can enable or disable the MLD Proxy Global State.
VLAN Name	The VLAN name for the interface.
VID	The VID for the interface.
Source IP Address	The Source IP of the protocol packet. If it is unspecified, the zero IP will be used.
Unsolicited Report Interval (0-25)	The unsolicited report interval. It is the time between repetitions of the host's initial report of membership in a group. Default is 10 seconds. If set to 0, it means to send only one report packet.
Static Router Port	Select the static router ports that will be included in the configuration.
Dynamic Router Port	Display a list of ports that are connected to multicast-enabled routers.

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

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

MLD Proxy Downstream Settings

Users can configure the MLD proxy downstream interface in this page. The MLD proxy downstream interface must be a MLD snooping enabled VLAN.

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

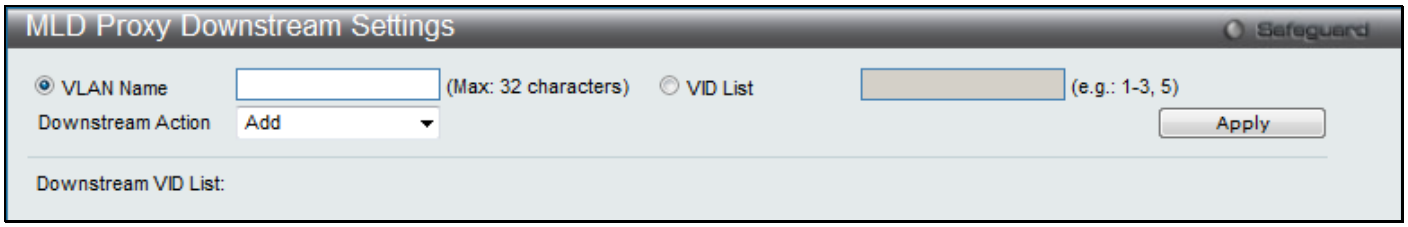


Figure 5-65 MLD Proxy Downstream Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN name for the interface.
VID List	The VID List for the interface.
Downstream Action	Here the user can select the appropriate action. Selecting **Add** will add a downstream interface. Selecting **Delete** will remove a downstream interface.

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

MLD Proxy Group

On this page the user can view the MLD Proxy Group.

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

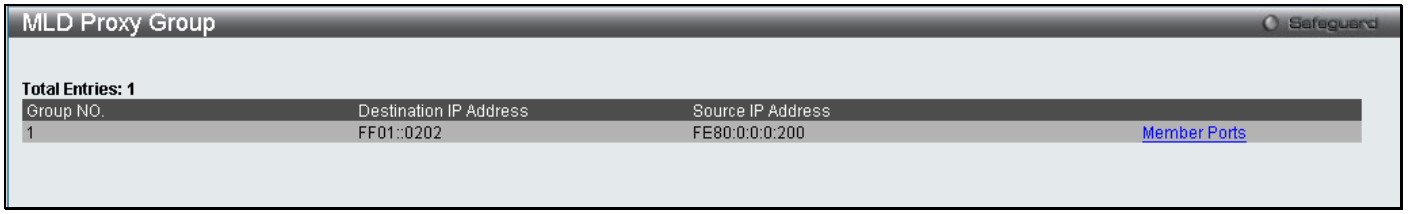


Figure 5-66 MLD Proxy Group window

Click the Member Ports link to view the MLD proxy member port information.

After clicking the Member Ports option, the following window will appear.

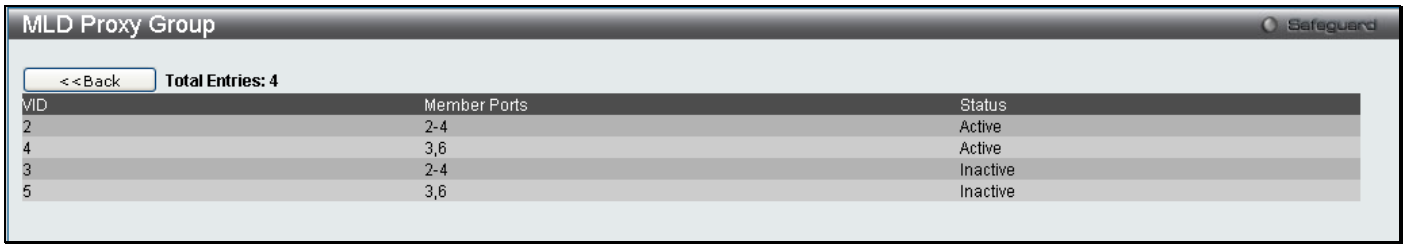


Figure 5-67 MLD Proxy Group window

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

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds

the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

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

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

Data Driven Learning

The Switch allows you to implement data driven learning for MLD snooping groups. If data-driven learning, also known as dynamic IP multicast learning, is enabled for a VLAN, when the Switch receives IP multicast traffic on the VLAN, an MLD snooping group is created. Learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to age out or to age out by a timer.

When the data driven learning State is enabled, the multicast filtering mode for all ports is ignored. This means multicast packets will be flooded as a forwarding table.

NOTE: If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. In other words, the aging out mechanism will follow the conditions of an ordinary MLD snooping entry.

Data driven learning is useful on a network which has video cameras connected to a Layer 2 switch that is recording and sending IP multicast data. The switch needs to forward IP data to a data centre without dropping or flooding any packets. Since video cameras do not have the capability to run MLD protocols, the IP multicast data will be dropped with the original MLD snooping function.

MLD Snooping Settings

Users can configure the settings for MLD snooping.

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

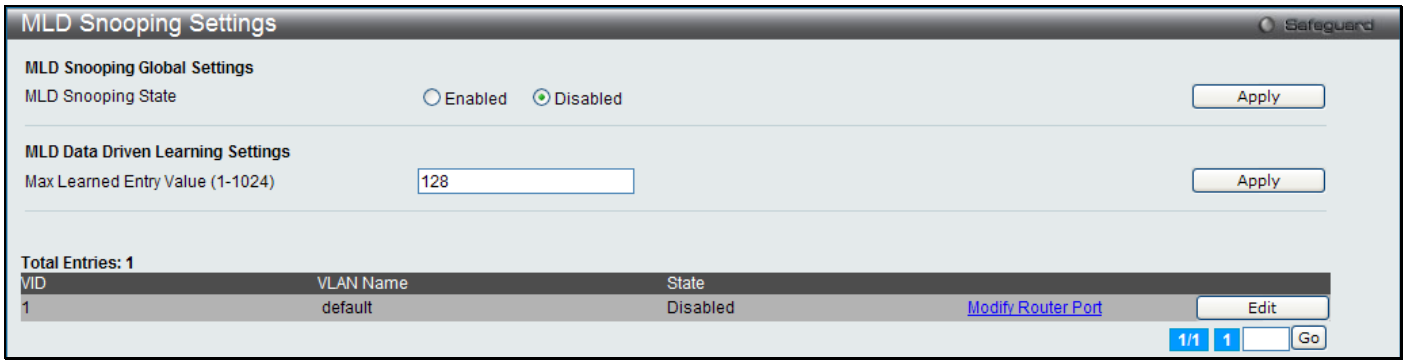


Figure 5-68 MLD Snooping Settings window

The fields that can be configured are described below:

Parameter	Description
MLD Snooping State	Here the user can enable or disable the MLD snooping state.
Max Learning Entry Value (1-1024)	Here the user can enter the maximum learning entry value.

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

Click the Modify Router Port link to configure the MLD Snooping Router Port Settings for a specific entry.

Click the **Edit** button to configure the MLD Snooping Parameters Settings for a specific entry.

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

After clicking the **Edit** button, the following page will appear:

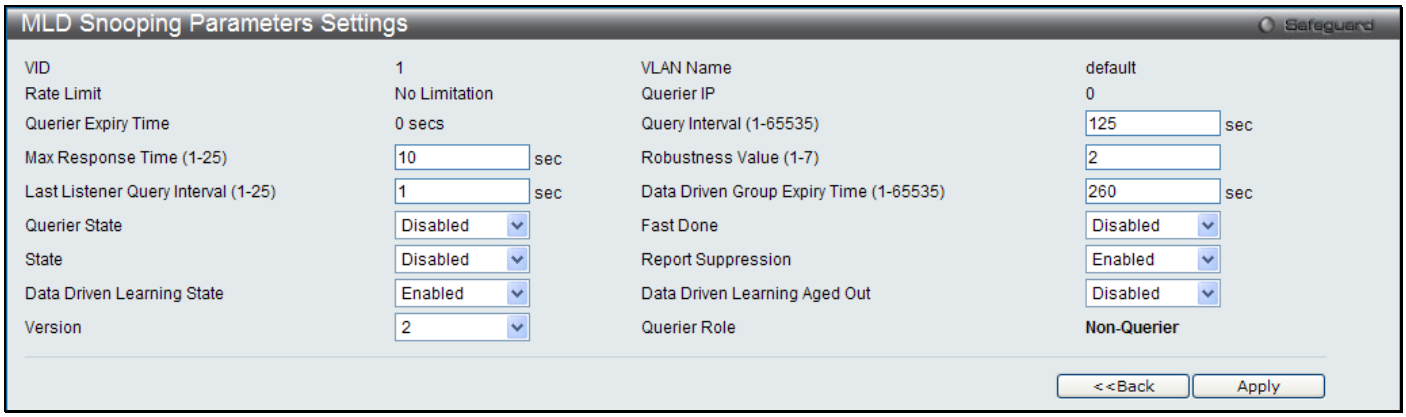


Figure 5-69 MLD Snooping Parameters Settings window

The fields that can be configured are described below:

Parameter	Description
Query Interval (1-65535)	Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
Max Response Time (1-25)	The maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.
Robustness Value (1-7)	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: • *Group listener interval* - Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). The default value is 260 seconds. • *Other Querier present interval* - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the Querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). The default is 255 seconds.

	• *Last listener query count* - Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.
Last Listener Query Interval (1-25)	The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group. This interval is calculated as follows: (last listener query interval * robustness variable).
Data Driven Group Expiry Time (1-65535)	Here the user can enter the data driven group expiry time value.
Querier State	This allows the switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.
Fast Done	Here the user can enable or disable the fast done feature.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
Report Suppression	Here the user can enable or disable the report suppression features. This feature prevents duplicate reports from being sent to the multicast devices. If you disable MLD report suppression, all MLD reports are forwarded to the multicast routers.
Data Driven Learning State	Enable or disable data driven learning of MLD snooping groups.
Data Driven Learning Aged Out	Enable or disable the age out function for data driven entries.
Version	Specifies the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be forwarded from the router ports or VLAN flooding.

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

After clicking the Modify Router Port link, the following page will appear:

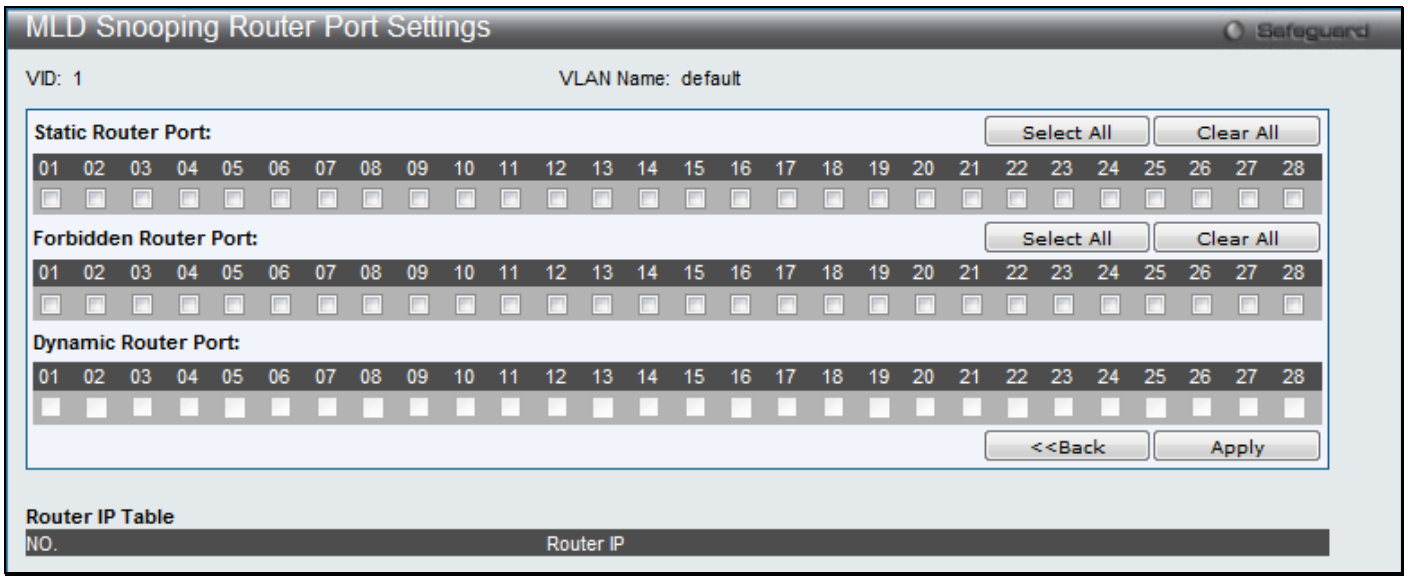


Figure 5-70 MLD Snooping Router Port Settings window

The fields that can be configured are described below:

Parameter	Description
Static Router Port	This section is used to designate a range of ports as being connected to multicast-

	enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.
Forbidden Router Port	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Dynamic Router Port	Displays router ports that have been dynamically configured.
Ports	Select the appropriate ports individually to include them in the Router Port configuration.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

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

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

MLD Snooping Rate Limit Settings

Users can configure the rate limit of the MLD control packet that the switch can process on a specific port or VLAN in this page. This configuration is used to limit the maximum packet number within a port or a VLAN per second.

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

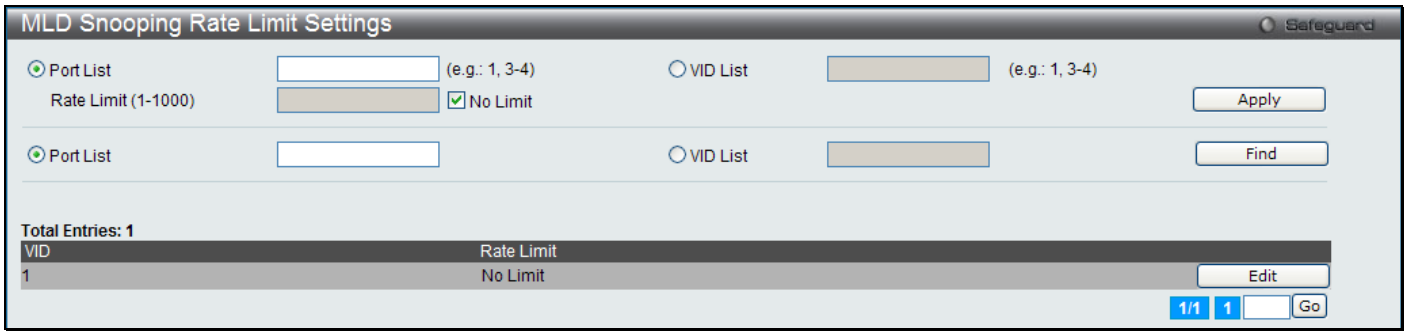


Figure 5-71 MLD Snooping Rate Limit Settings window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter the Port List here.
VID List	Enter the VID List value here.
Rate Limit	Configure the rate limit of MLD control packet that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packet that exceeds the limited rate will be dropped. Selecting the **No Limit** option lifts the rate limit requirement.

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

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.

MLD Snooping Static Group Settings

This page used to configure the MLD snooping multicast group static members.

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

Figure 5-72 MLD Snooping Static Group Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The name of the VLAN on which the static group resides.
VID List	The ID of the VLAN on which the static group resides.
IPv6 Address	Specifies the multicast group IPv6 address.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Create** button to add a static group.
Click the **Delete** button to delete a static group.
Click the **View All** button to display all the existing 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.

After clicking the **Edit** button, the following page will appear:

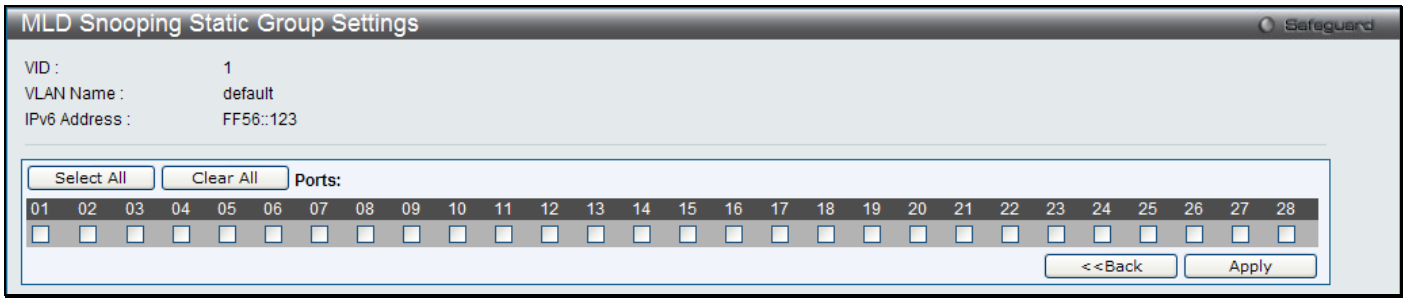


Figure 5-73 MLD Snooping Static Group Settings window

Click the **Select All** button to select all the ports for configuration.
Click the **Clear All** button to unselect all the ports for configuration.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Apply** button to accept the changes made.

MLD Router Port

Users can display which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.

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

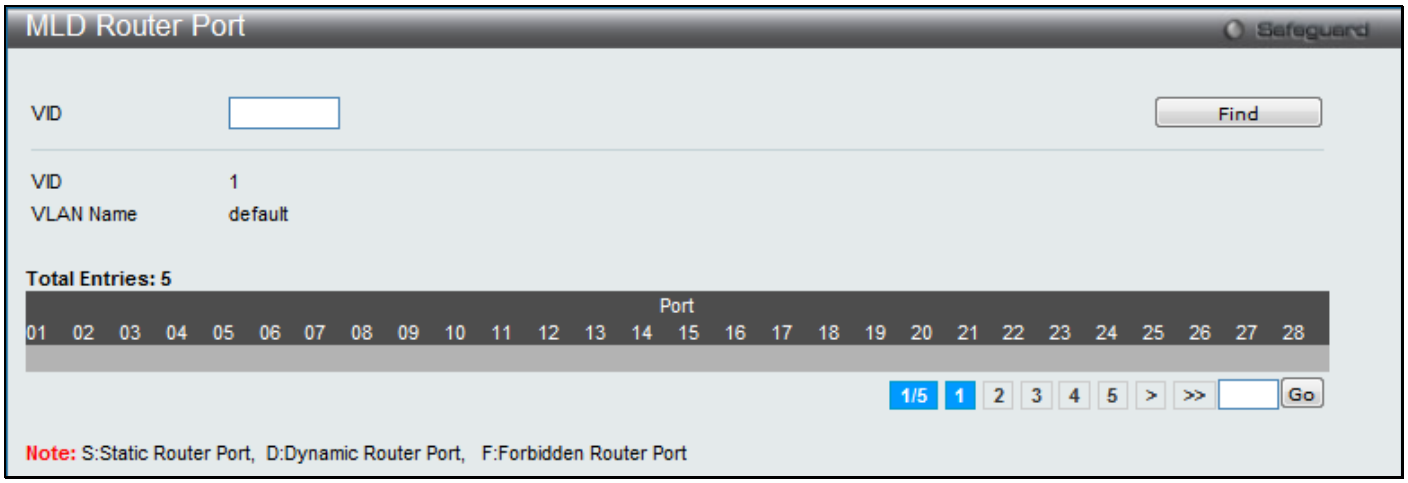


Figure 5-74 MLD Router Port window

The fields that can be configured are described below:

Parameter	Description
VID	Enter a VLAN ID to be displayed.

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.

NOTE: The abbreviations used in this window are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

MLD Snooping Group

Users can view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4.

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

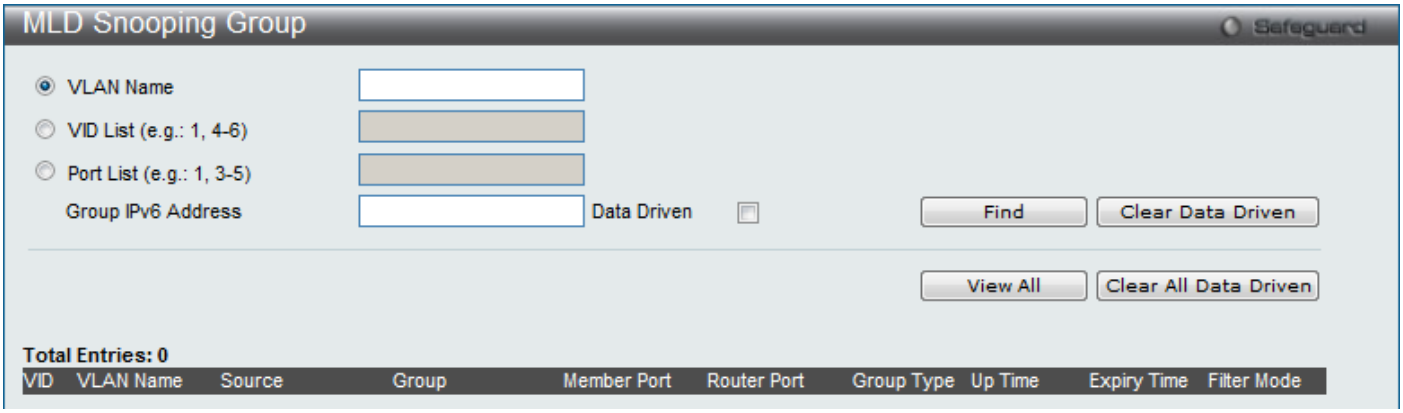


Figure 5-75 MLD Snooping Group window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	Specifies the port number(s) used to find a multicast group.

Group IPv6 Address	Enter the group IPv6 address used here.
Data Driven	If Data Drive is selected, only data driven groups will be displayed.

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

Click the **Clear Data Driven** button to delete the specific MLD snooping group which is learned by the Data Driven feature of the specified VLAN.

Click the **View All** button to display all the existing entries.

Click the **Clear All Data Driven** button to delete all MLD snooping groups which is learned by the Data Driven feature of specified VLANs.

MLD Snooping Forwarding Table

This page displays the switch's current MLD snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The MLD snooping further restricts the forwarding ports.

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

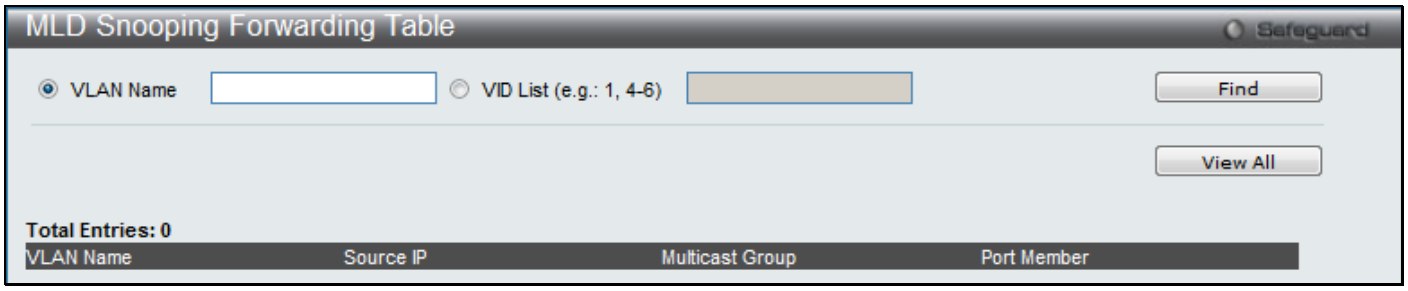


Figure 5-76 MLD Snooping Forwarding Table window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The name of the VLAN for which you want to view MLD snooping forwarding table information.
VID List	The ID of the VLAN for which you want to view MLD snooping forwarding table information.

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

Click the **View All** button to display all the existing entries.

MLD Snooping Counter

This page displays the statistics counter for MLD protocol packets that are received by the switch since MLD Snooping is enabled.

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

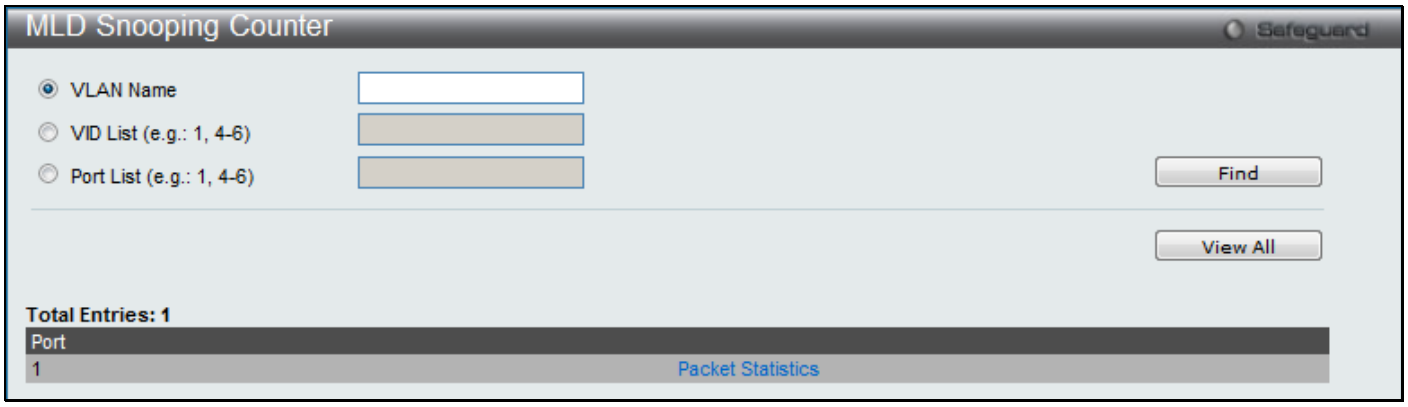


Figure 5-77 MLD Snooping Counter window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Specifies a VLAN name to be displayed.
VID List	Specifies a list of VLANs to be displayed.
Port List	Specifies a list of ports to be displayed.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the Packet Statistics link to view the MLD Snooping Counter Settings for the specific entry.

After clicking the Packet Statistics link, the following page will appear:

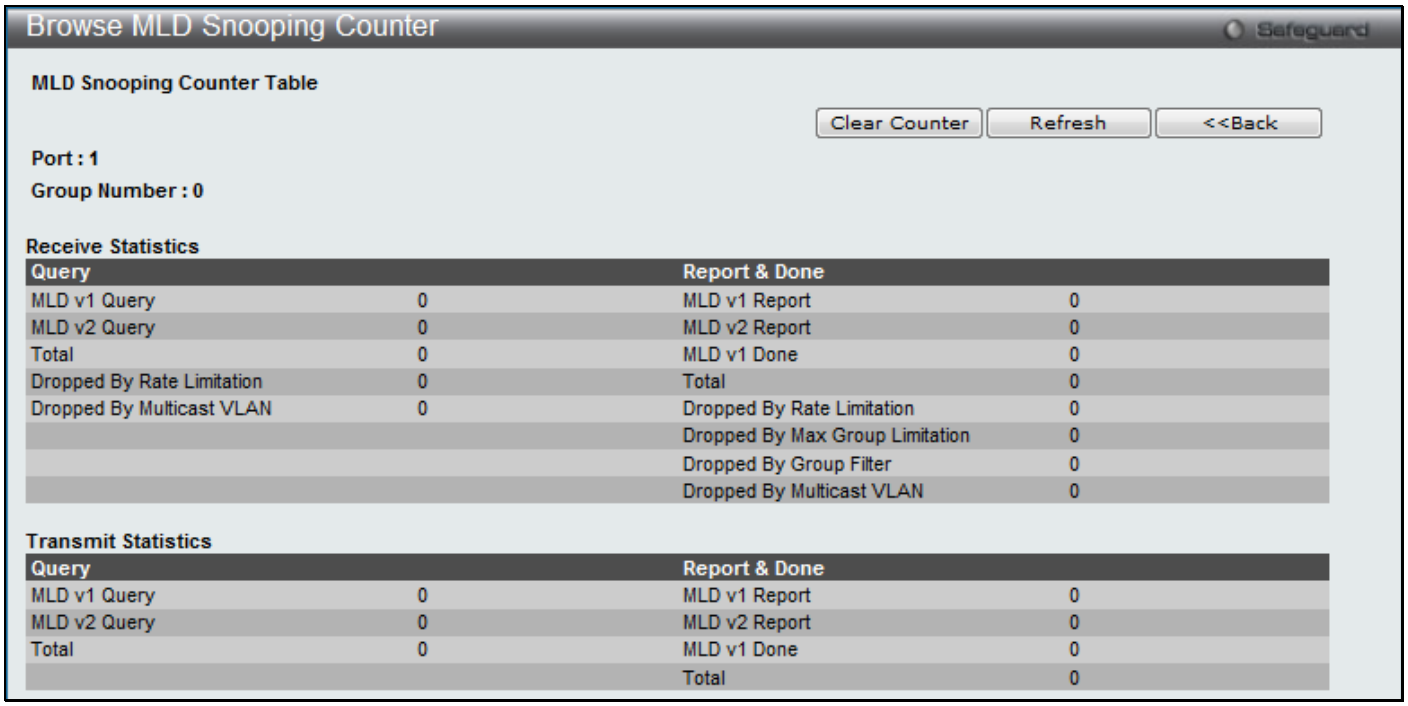


Figure 5-78 Browse MLD Snooping Counter window

Click the **Clear Counter** button to clear all the information displayed in the fields.
Click the **Refresh** button to refresh the display table so that new information will appear.
Click the **<<Back** button to return to the previous page.

MLD Host Table

This page displays the current host of VLAN, port or group on the switch. The hosts only take effect when fast leave is enabled. If no parameter is specified, it will display all hosts in the switch.

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

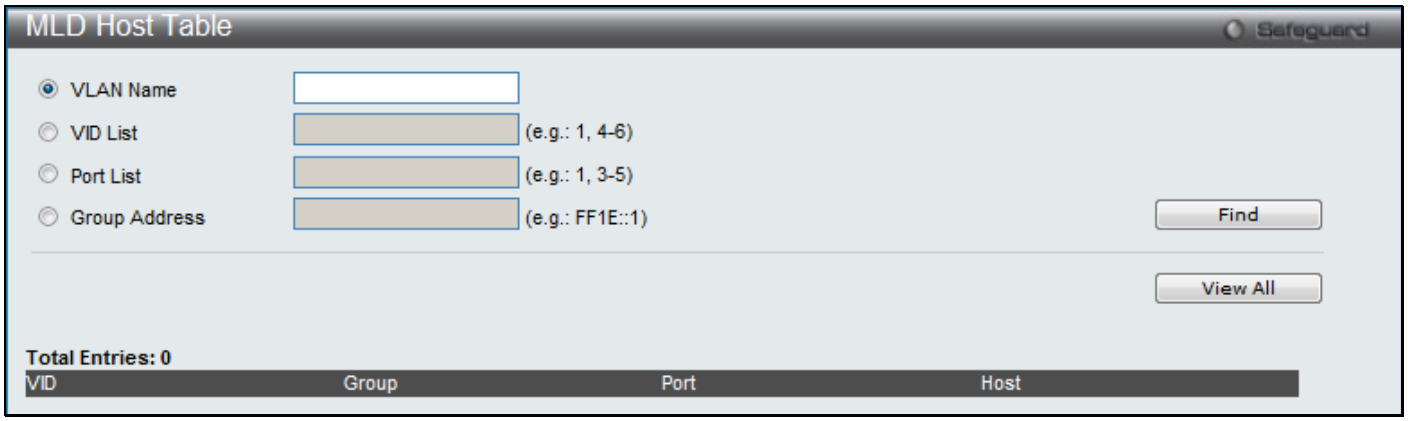


Figure 5-79 MLD Host Table window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Specifies VLAN name, belong to which hosts information is to be displayed.
VID List	Specifies VLAN ID, belong to which hosts information is to be displayed.
Port List	Specifies ports range, belong to which hosts information is to be displayed.
Group Address	Specifies the group's IPv6 address, belong to which hosts information is to be displayed.

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

Click the **View All** button to display all the existing entries.

Multicast VLAN

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

Restrictions and Provisos:

The Multicast VLAN feature of this Switch does have some restrictions and limitations, such as:

1. Multicast VLANs can be implemented on edge and non-edge switches.
2. Member ports and source ports can be used in multiple ISM VLANs. But member ports and source ports cannot be the same port in a specific ISM VLAN.
3. The Multicast VLAN is exclusive with normal 802.1q VLANs, which means that VLAN IDs (VIDs) and VLAN Names of 802.1q VLANs and ISM VLANs cannot be the same. Once a VID or VLAN Name is chosen for any VLAN, it cannot be used for any other VLAN.
4. The normal display of configured VLANs will not display configured Multicast VLANs.
5. Once an ISM VLAN is enabled, the corresponding IGMP snooping state of this VLAN will also be enabled. Users cannot disable the IGMP feature for an enabled ISM VLAN.
6. One IP multicast address cannot be added to multiple ISM VLANs, yet multiple Ranges can be added to one ISM VLAN.

IGMP Multicast Group Profile Settings

Users can add a profile to which multicast address reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP Multicast address or range of IP Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

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

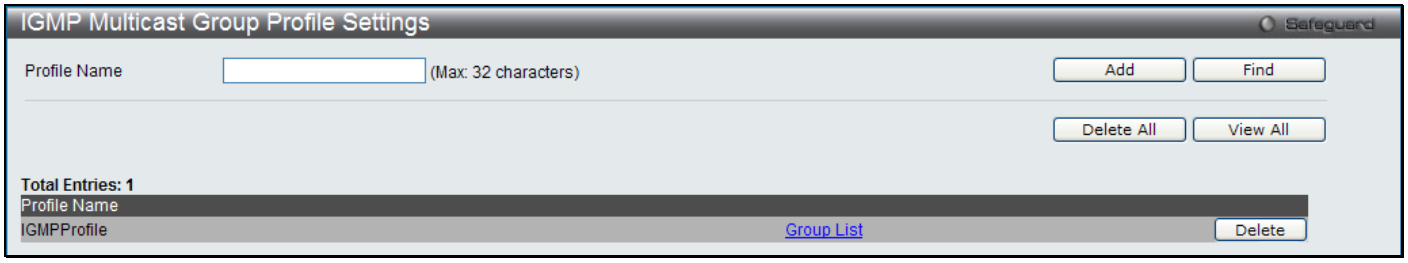


Figure 5-80 IGMP Multicast Group Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.
Click the **View All** button to display all the existing entries.
Click the Group List link to configure the Multicast Group Profile Address Settings for the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:

Figure 5-81 Multicast Group Profile Multicast Address Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Here the user can enter the multicast address list value.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Delete** button to remove the specific entry.

IGMP Snooping Multicast VLAN Settings

On this page the user can configure the IGMP snooping multicast VLAN parameters.

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

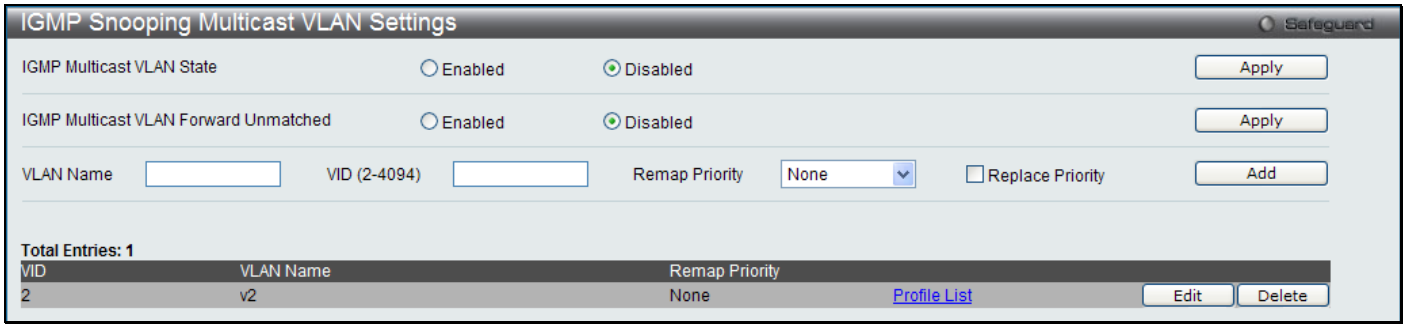


Figure 5-82 IGMP Snooping Multicast VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
IGMP Multicast VLAN State	Here the user can enable or disable the IGMP Multicast VLAN state.
IGMP Multicast VLAN Forward Unmatched	Here the user can enable or disable the IGMP Multicast VLAN Forwarding state.
VLAN Name	Here the user can enter the VLAN Name used.
VID (2-4094)	Here the user can enter the VID used.
Remap Priority	*0-7* – The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. *None* – If specified, the packet's original priority is used. The default setting is *None*.
Replace Priority	Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.

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

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

Click the Profile List link to configure the IGMP Snooping Multicast VLAN Settings for the specific entry.

Click the **Edit** button to configure the IGMP Snooping Multicast VLAN Settings for the specific entry.

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

After clicking the **Edit** button, the following page will appear:

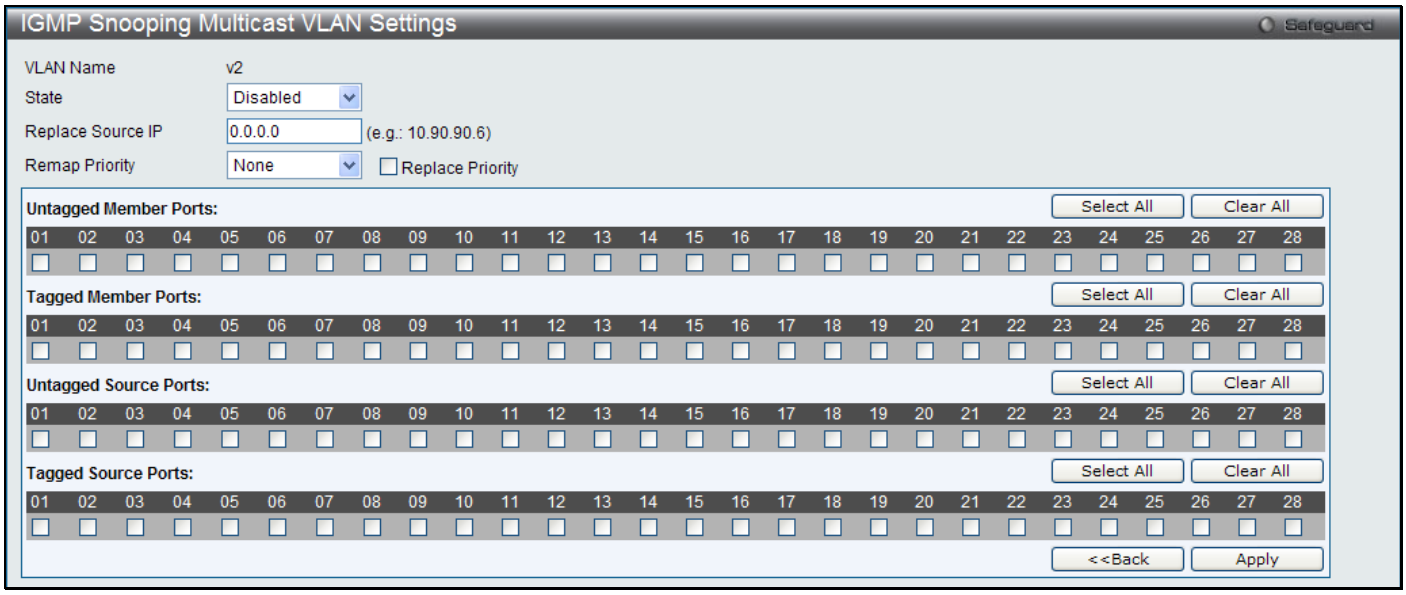


Figure 5-83 IGMP Snooping Multicast VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
State	Here the user can enable or disable the state.
Replace Source IP	With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will be replaced by "0".
Remap Priority	*0-7* – The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. *None* – If **None** is specified, the packet's original priority is used. The default setting is None.
Replace Priority	Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.
Untagged Member Ports	Specify the untagged member port of the multicast VLAN.
Tagged Member Ports	Specify the tagged member port of the multicast VLAN.
Untagged Source Ports	Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.
Tagged Source Ports	Specify the source port or range of source ports as tagged members of the multicast VLAN.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

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

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

After clicking the Profile List link, the following page will appear:

Figure 5-84 IGMP Snooping Multicast VLAN Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Here the user can select the IGMP Snooping Multicast VLAN Group Profile name.

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

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

Click the Show IGMP Snooping Multicast VLAN Entries link to view the IGMP Snooping Multicast VLAN Settings.

MLD Multicast Group Profile Settings

Users can add, delete, or configure the MLD multicast group profile on this page.

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

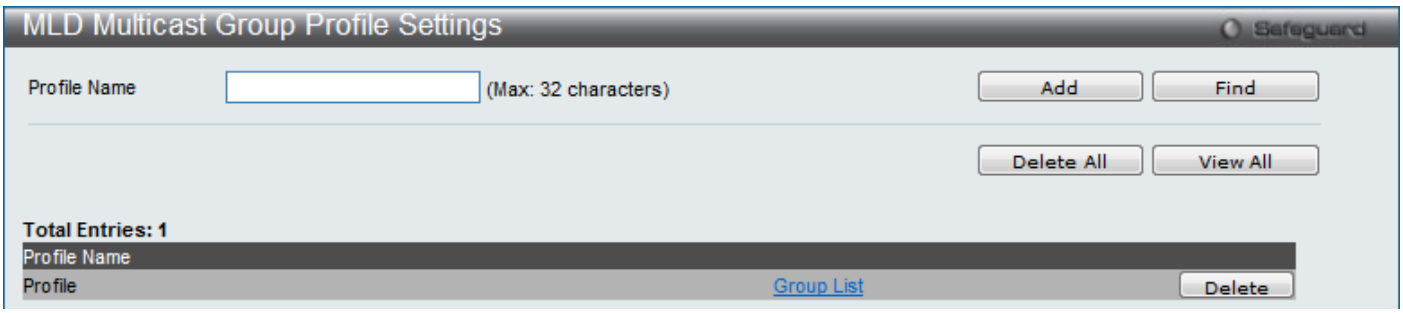


Figure 5-85 MLD Multicast Group Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Here the user can enter the MLD Multicast Group Profile name.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.
Click the **View All** button to display all the existing entries.
Click the Group List link to configure the Multicast Group Profile Multicast Address Settings for the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:

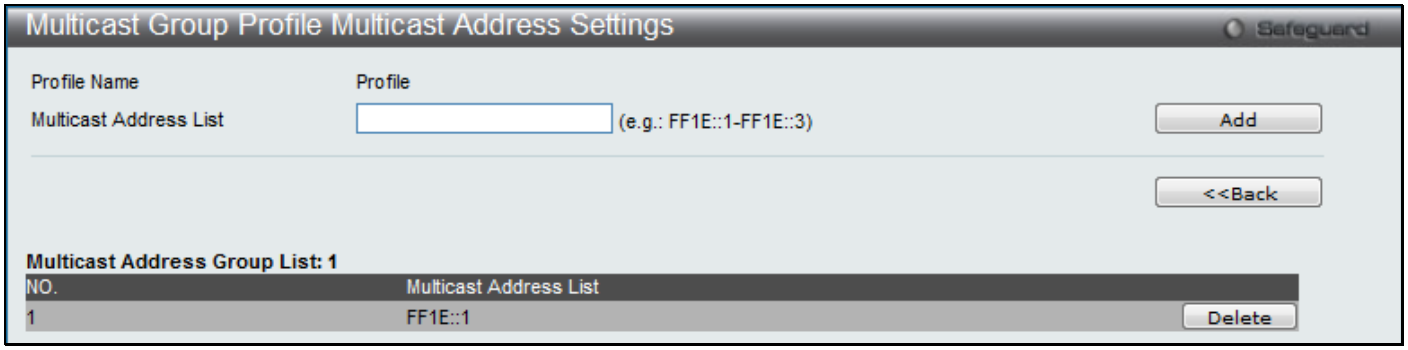


Figure 5-86 Multicast Group Profile Multicast Address Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Here the user can enter the multicast address list.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Delete** button to remove the specific entry.

MLD Snooping Multicast VLAN Settings

Users can add, delete, or configure the MLD snooping multicast VLAN on this page.

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

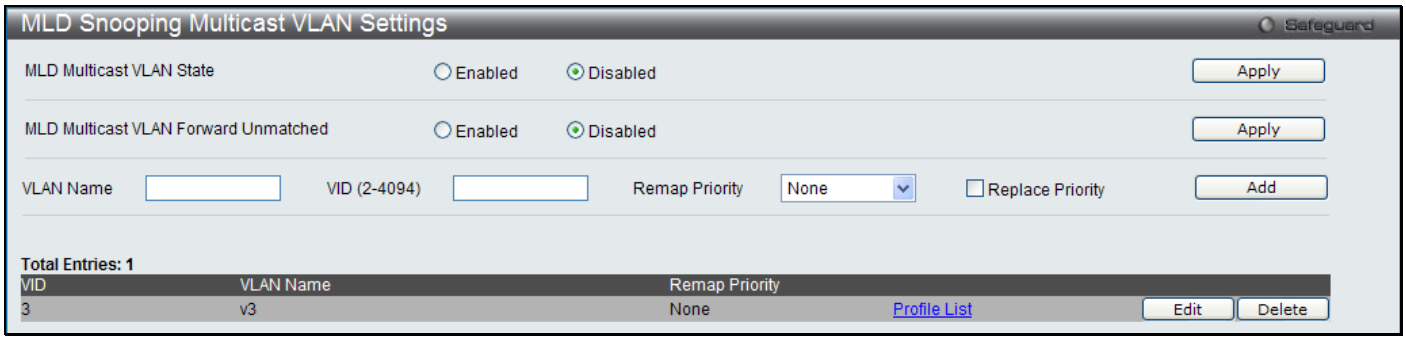


Figure 5-87 MLD Snooping Multicast VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
MLD Multicast VLAN State	Here user can enable or disable the MLD multicast VLAN state.
MLD Multicast VLAN Forward Unmatched	Here user can enable or disable the MLD multicast VLAN Forward Unmatched state.
VLAN Name	Here the user can enter the VLAN name used.
VID (2-4094)	Here the user can enter the VID value used.
Remap Priority	The user can select this option to enable the Remap Priority feature. Specify the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If *None* is specified, the packet's original priority will be used. The default setting is None.
Replace Priority	Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Click the **Apply** button to accept the changes made for each individual section.
Click the **Add** button to add a new entry based on the information entered.
Click the Profile List link to configure the MLD Snooping Multicast VLAN Settings for the specific entry.
Click the **Edit** button to configure the MLD Snooping Multicast VLAN Settings for the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the **Edit** button, the following page will appear:

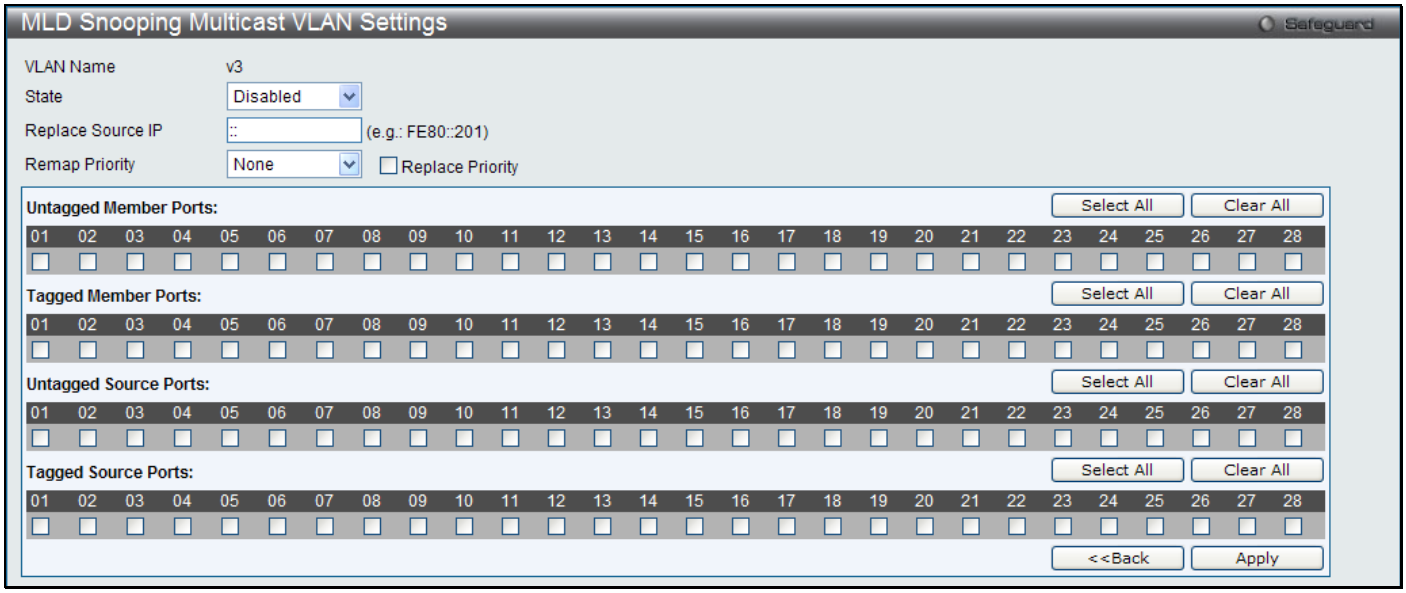


Figure 5-88 MLD Snooping Multicast VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
State	Here the user can enable or disable the state.
Replace Source IP	With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will be replaced by "::".
Remap Priority	*0-7* – The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. *None* – If **None** is specified, the packet's original priority is used. The default setting is **None**.
Replace Priority	Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.
Untagged Member Ports	Specify the untagged member port of the multicast VLAN. Click the **Select All** button to select all the ports or click the **Clear All** button to unselect all the ports.
Tagged Member Ports	Specify the tagged member port of the multicast VLAN. Click the **Select All** button to select all the ports or click the **Clear All** button to unselect all the ports.
Untagged Source Ports	Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN
Tagged Source Ports	Specify the source port or range of source ports as tagged members of the multicast VLAN.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

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

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

After clicking the Profile List link, the following page will appear:

Figure 5-89 MLD Snooping Multicast VLAN Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Here the user can select the MLD Snooping Multicast VLAN Group Profile name.

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

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

Click the Show MLD Snooping Multicast VLAN Entries link to view the MLD Snooping Multicast VLAN Settings.

IP Multicast VLAN Replication

IP Multicast VLAN Replication Global Settings

The window is used to configure the IP multicast VLAN replication parameters.

To view the following window, click **L2 Features > L2 Multicast Control > IP Multicast VLAN Replication > IP Multicast VLAN Replication Global Settings**, as shown below:

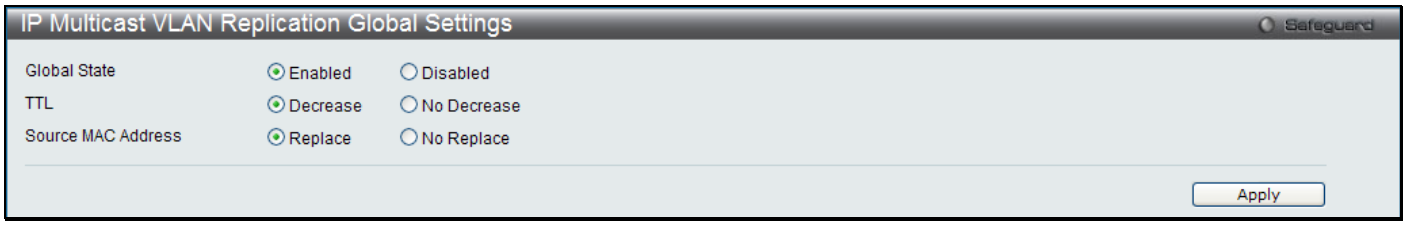


Figure 5-90 IP Multicast VLAN Replication Global Settings window

The fields that can be configured are described below:

Parameter	Description
Global State	Here the user can enable or disable the global state feature.
TTL	Here the user can select to decrease or no decrease the Time to live (TTL) value in the packets.
Source MAC Address	Here the user can select to replace or not to replace the Source MAC Address of the packet.

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

IP Multicast VLAN Replication Settings

This window is used to add and view the IP multicast VLAN replication table.

To view the following window, click **L2 Features > L2 Multicast Control > IP Multicast VLAN Replication > IP Multicast VLAN Replication Settings**, as shown below:

Figure 5-91 IP Multicast VLAN Replication Settings window

The fields that can be configured are described below:

Parameter	Description
Entry Name	Here the user can enter a Multicast VLAN Replication entry name.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find by Hardware** the find an entry based on the hardware.
Click the **View All** button to display all the existing entries.
Click the **Edit** button under **Source** to re-configure the specific entry.
Click the **Edit** button under **Destination** to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the **Edit** button under **Source**, the following page will appear:

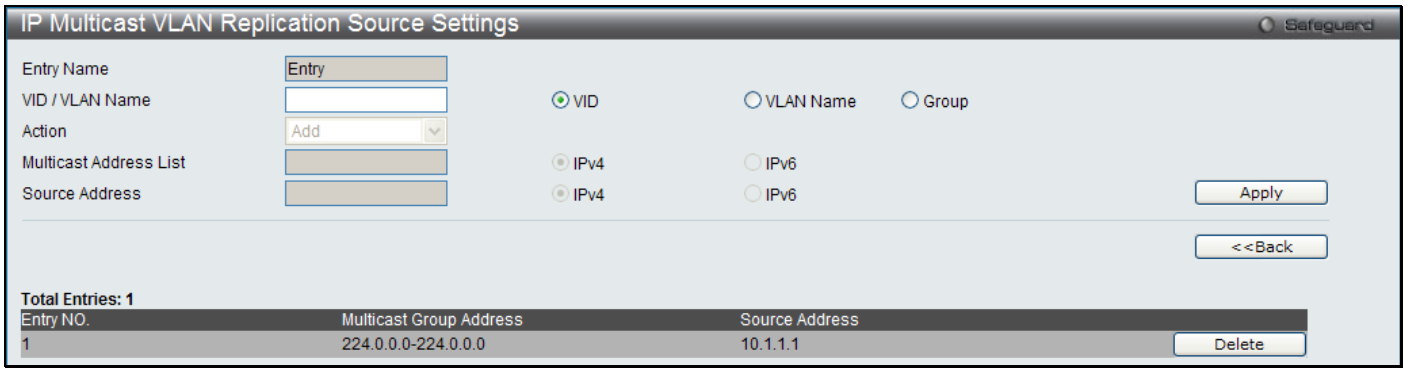


Figure 5-92 IP Multicast VLAN Replication Source Settings window

The fields that can be configured are described below:

Parameter	Description
VID / VLAN Name	Here the user can choose to enter a VLAN Name, VID value or Group value.
Action	Here the user can select the action to be taken.
Multicast Address List	Here the user can enter the multicast address list.
Source Address	Here the user can enter the source address.

Click the **Apply** button to accept the changes made.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Delete** button to remove the specific entry.

After clicking the **Edit** button under **Destination**, the following page will appear:

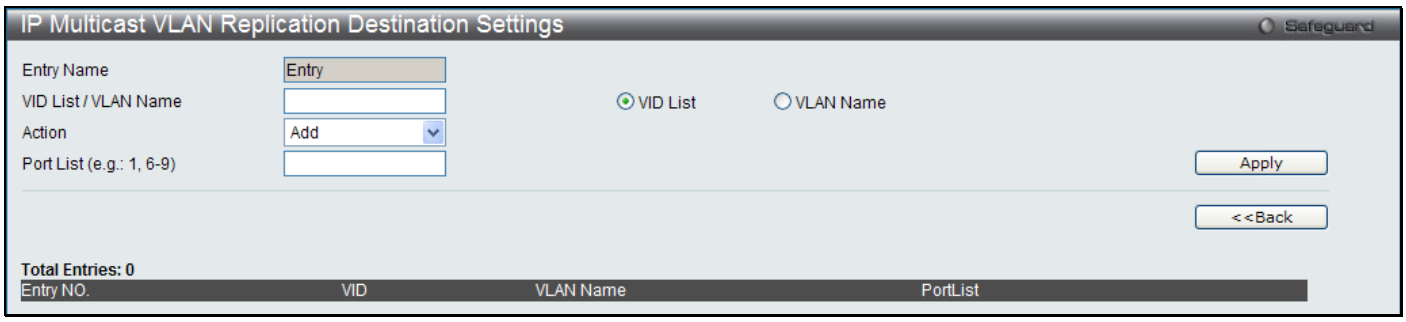


Figure 5-93 IP Multicast VLAN Replication Destination Settings window

The fields that can be configured are described below:

Parameter	Description
VID / VLAN Name	Here the user can choose to enter a VLAN Name, VID value or Group value.
Action	Here the user can select the action to be taken.
Port List	Here the user can enter the port list.

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

Multicast Filtering

IPv4 Multicast Filtering

IPv4 Multicast Profile Settings

Users can add a profile to which multicast address(s) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IPv4 Multicast address or range of IPv4 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Multicast Profile Settings**, as shown below:

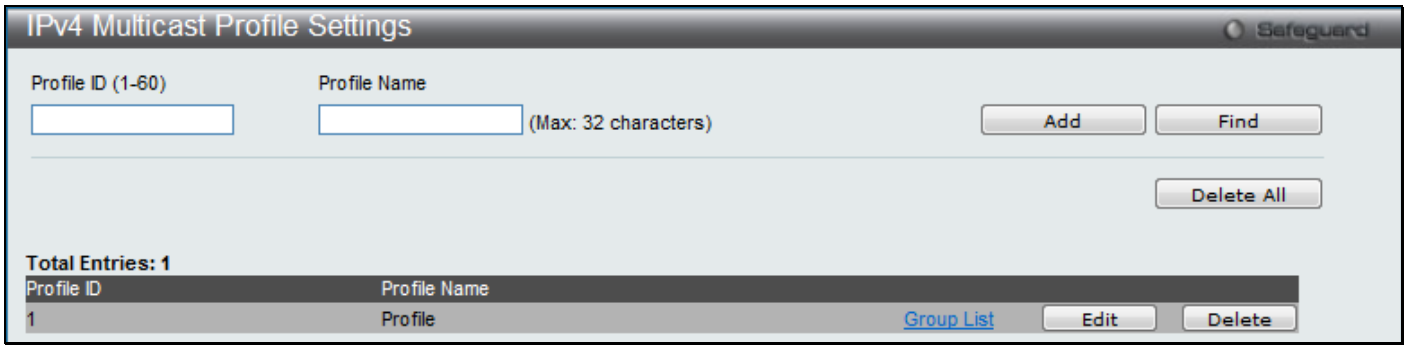


Figure 5-94 IPv4 Multicast Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-60)	Enter a Profile ID between *1* and *60*.
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.
Click the Group List link to configure the multicast address group list settings for the specific entry.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:

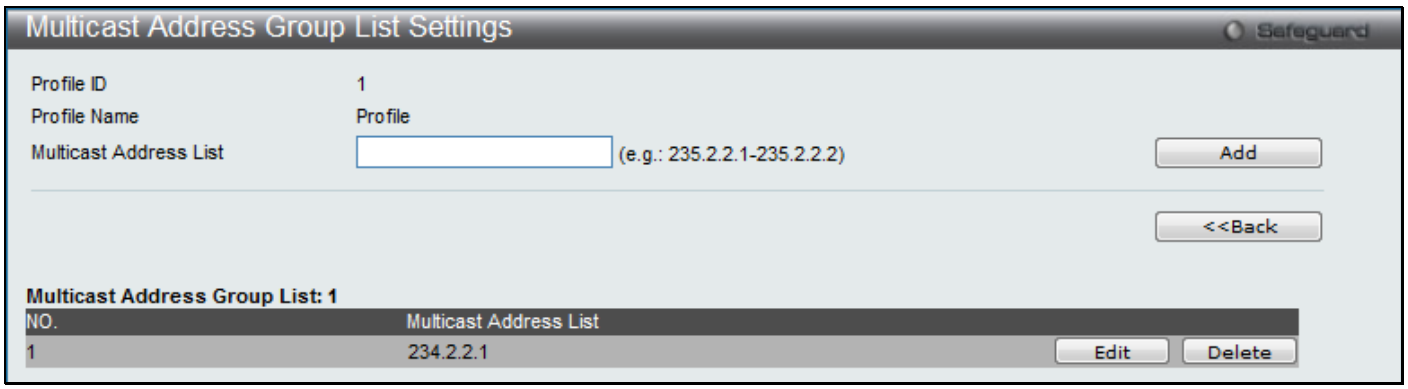


Figure 5-95 Multicast Address Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Enter the multicast address list here.

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

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

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

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

IPv4 Limited Multicast Range Settings

Users can configure the ports and VLANs on the Switch that will be involved in the Limited IPv4 Multicast Range. The user can configure the range of multicast ports that will be accepted by the source ports to be forwarded to the receiver ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Limited Multicast Range Settings**, as shown below:

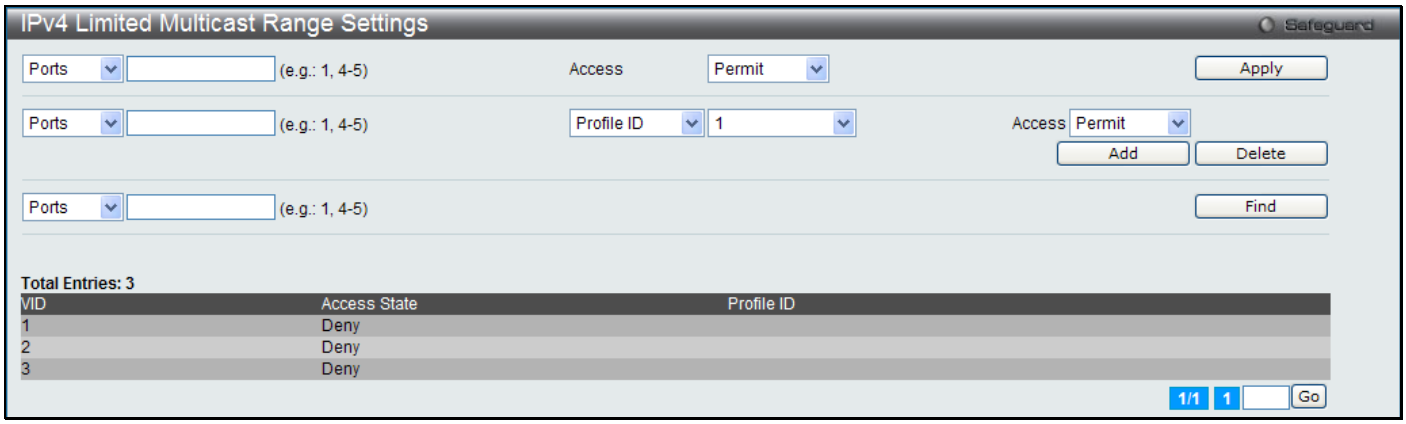


Figure 5-96 IPv4 Limited Multicast Range Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Please select the appropriate port(s) or VLAN IDs used for the configuration here.
Access	Here the user can assign access permissions to the ports selected. Options listed are **Permit** and **Deny**.
Profile ID / Profile Name	Here the user can select the profile ID or profile name used and then assign **Permit** or **Deny** access to them.

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 specific entry based on the information entered.

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.

IPv4 Max Multicast Group Settings

Users can configure the ports and VLANs on the switch that will be a part of the maximum filter group, up to a maximum of 1024.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Max Multicast Group Settings**, as shown below:

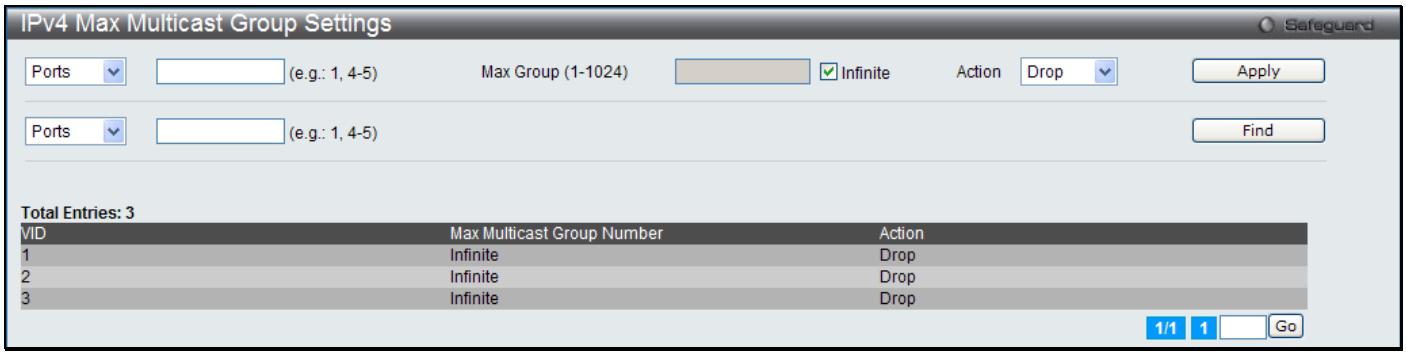


Figure 5-97 IPv4 Max Multicast Group Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Please select the appropriate port(s) or VLAN IDs used for the configuration here.
Max Group (1-1024)	Deselect the **Infinite** check box to enter a **Max Group** value here.
Infinite	Here the user can enable or disable the use of the Infinite value.
Action	Here the user can select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

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

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 Multicast Filtering

Users can add a profile to which multicast address(s) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IPv6 Multicast address or range of IPv6 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

IPv6 Multicast Profile Settings

Users can add, delete, and configure the IPv6 multicast profile on this page.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Multicast Profile Settings**, as shown below:

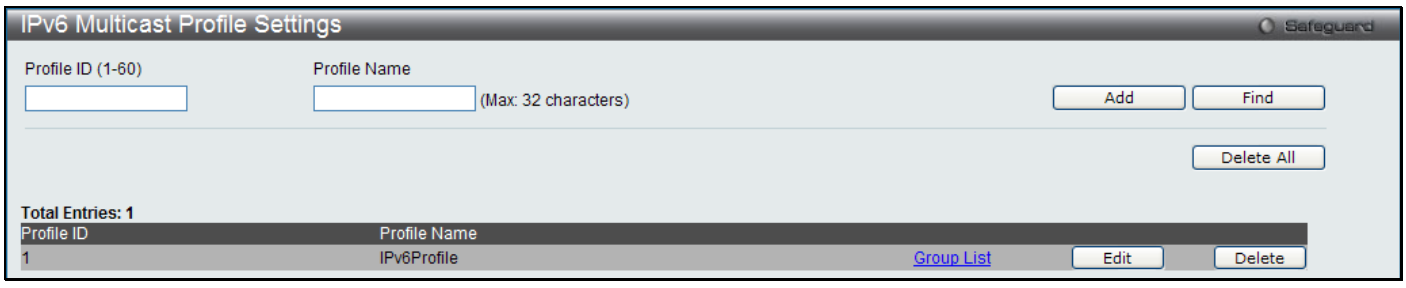


Figure 5-98 IPv6 Multicast Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-60)	Enter a Profile ID between *1* and *60*.
Profile Name	Enter a name for the IP Multicast Profile.

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

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

Click the **Delete All** button to remove all the entries listed.
Click the Group List link to configure the multicast address group list settings for the specific entry.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:

Figure 5-99 Multicast Address Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Enter the multicast address list here.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

IPv6 Limited Multicast Range Settings

Users can configure the ports and VLANs on the Switch that will be involved in the Limited IPv6 Multicast Range.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Limited Multicast Range Settings**, as shown below:

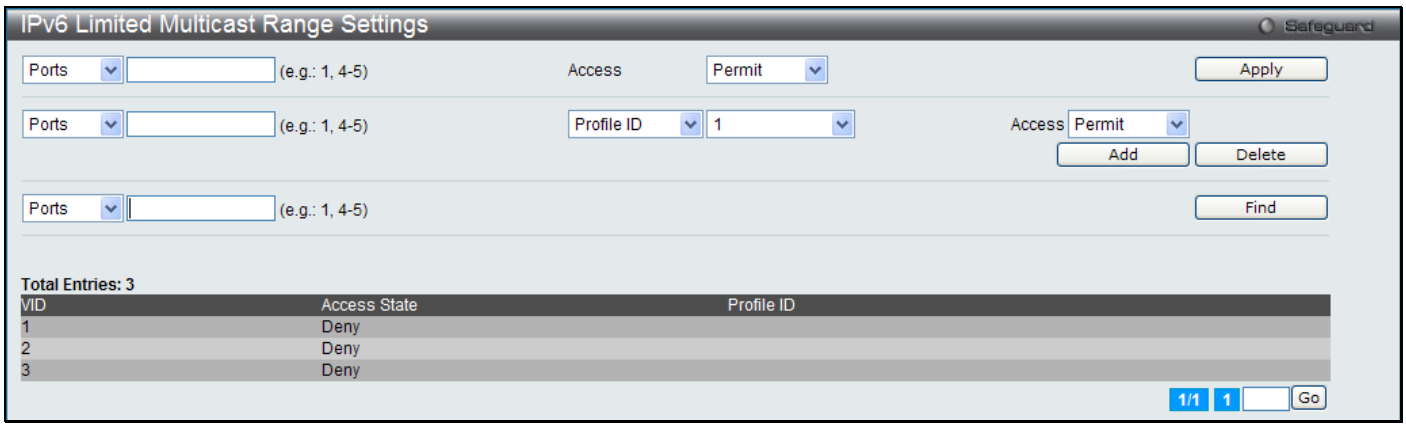


Figure 5-100 IPv6 Limited Multicast Range Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Please select the appropriate port(s) or VLAN IDs used for the configuration here.
Access	Here the user can assign access permissions to the ports selected. Options listed are **Permit** and **Deny**.
Profile ID / Profile Name	Here the user can select the profile ID or profile name used and then assign **Permit** or **Deny** access to them.

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 specific entry.

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 Max Multicast Group Settings

Users can configure the ports and VLANs on the switch that will be a part of the maximum filter group, up to a maximum of 1024.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Max Multicast Group Settings**, as shown below:

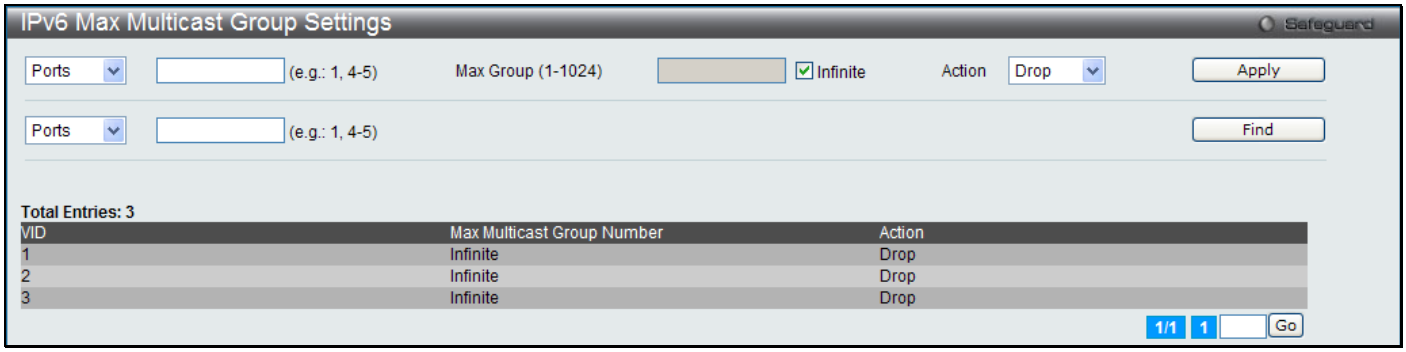


Figure 5-101 IPv6 Max Multicast Group Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Please select the appropriate port(s) or VLAN IDs used for the configuration here.
Max Group	Deselect the **Infinite** check box to enter a **Max Group** value in here.
Infinite	Here the user can enable or disable the use of the Infinite value.
Action	Here the user can select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

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

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.

Multicast Filtering Mode

Users can configure the multicast filtering mode.

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

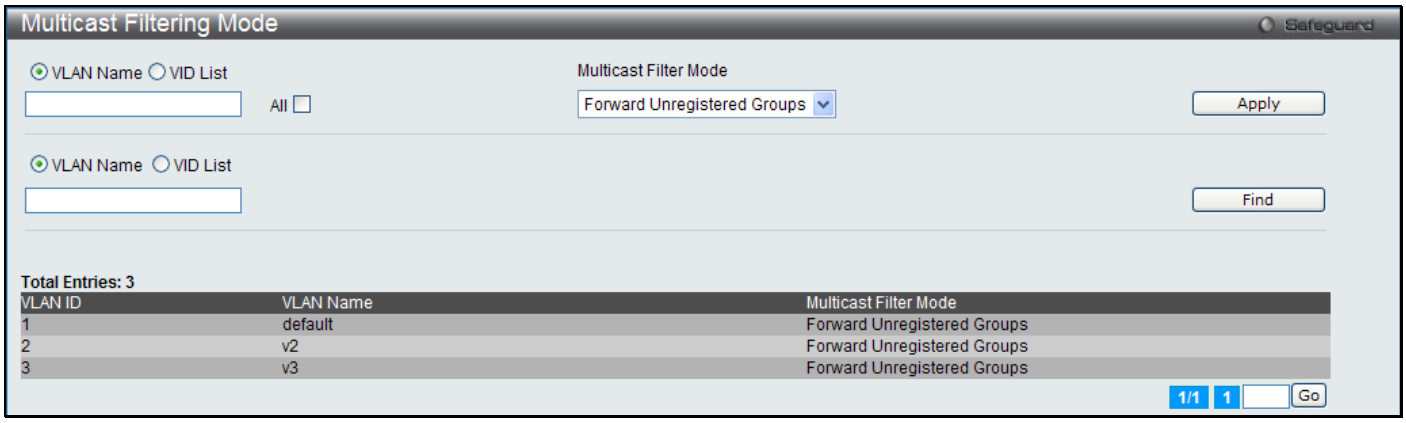


Figure 5-102 Multicast Filtering Mode window

The fields that can be configured are described below:

Parameter	Description
VLAN Name / VID List	The VLAN to which the specified filtering action applies. Tick the **All** option to apply this feature to all the VLANs.
Multicast Filtering Mode	This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN. *Forward Unregistered Groups* – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. *Filter Unregistered Groups* – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above.

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

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

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

ERPS Settings

The first industry standard is called ITU-T G.8032 for Ethernet Ring Protection Switching (ERPS). It is achieved by integrating mature Ethernet operations, administration, and maintenance (OAM) functions and a simple automatic protection switching (APS) protocol for Ethernet ring networks. ERPS provides sub-50ms protection for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

One link within a ring will be blocked to avoid Loop (RPL, Ring Protection Link). When the failure happens, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

G.8032 Terms and Concepts

RPL (Ring Protection Link) – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring

RPL Owner – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protected state

R-APS (Ring – Automatic Protection Switching) - Protocol messages defined in Y.1731 and G.8032 used to coordinate the protection actions over the ring through RAPS VLAN (R-APS Channel).

RAPS VLAN (R-APS Channel) – A separate ring-wide VLAN for transmission of R-APS messages

Protected VLAN – The service traffic VLANs for transmission of normal network traffic

This page is used to enable the ERPS function on the switch.

NOTE: STP and LBD should be disabled on the ring ports before enabling ERPS. The ERPS cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when ERPS is enabled.

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

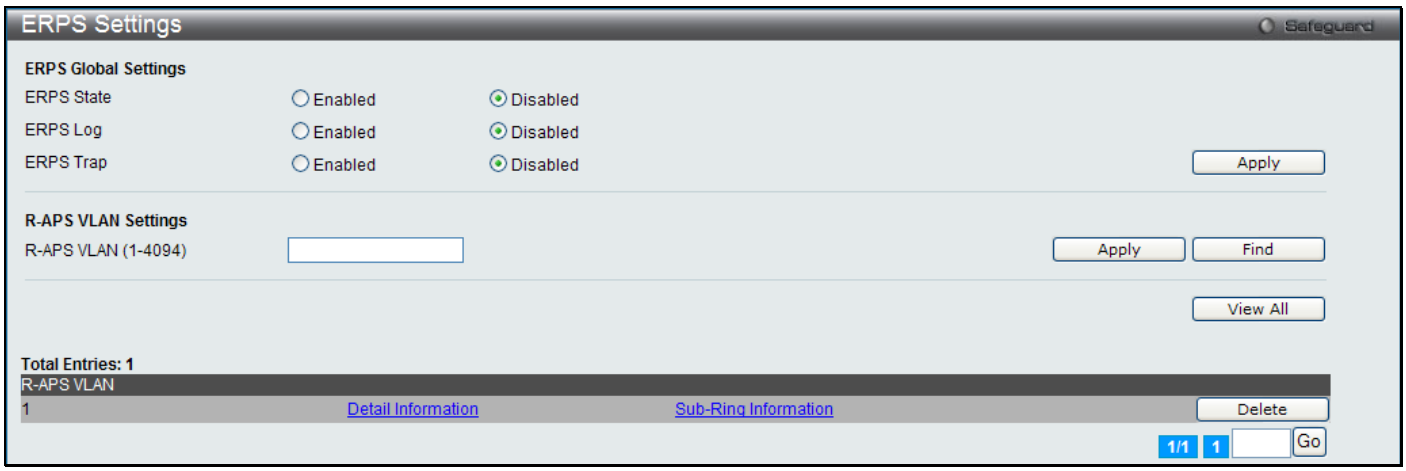


Figure 5-103 ERPS Settings window

The fields that can be configured are described below:

Parameter	Description
ERPS State	Here the user can enable or disable the ERPS State.
ERPS Log	Here the user can enable or disable the ERPS Log.
ERPS Trap	Here the user can enable or disable the ERPS Trap.
R-APS VLAN (1-4094)	Specifies the VLAN which will be the R-APS VLAN.

Click the **Apply** button to accept the changes made.
Click the **Find** button to find a specific entry based on the information entered.
Click the **View All** button to view all the entries configured.
Click the Detail Information link to view detailed information of the R-APS entry.
Click the Sub-Ring Information link to view the Sub-Ring information of the R-APS entry.
Click the **Delete** button to remove the specific entry.

After clicking the Detail Information link, the following window will appear:

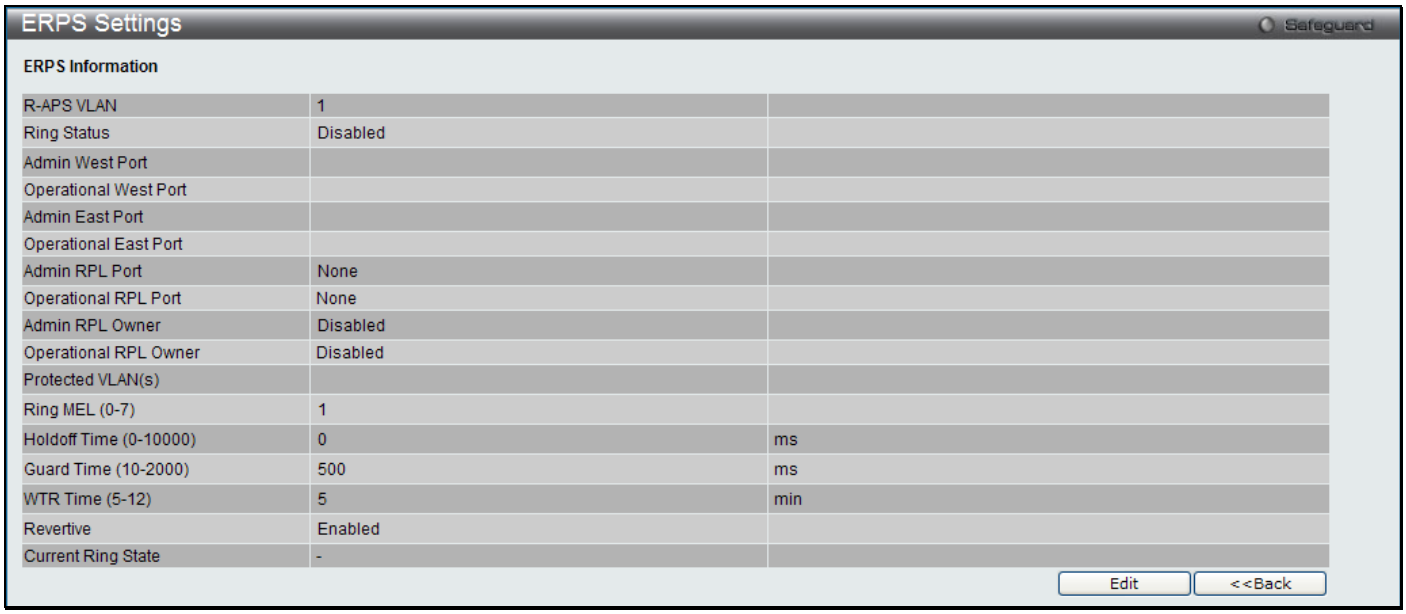


Figure 5-104 ERPS Settings - Detail Information window

Click the **Edit** button to re-configure the specific entry.
Click the **<<Back** button to return to the ERPS settings page.

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

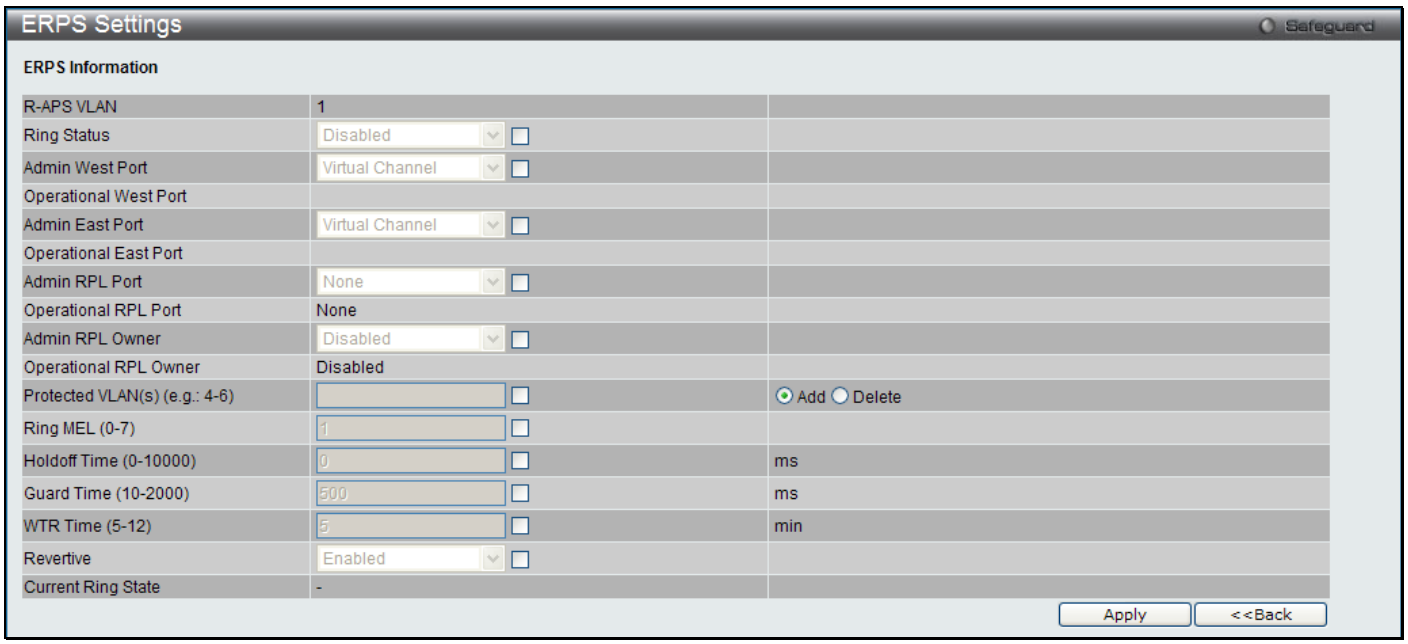


Figure 5-105 ERPS Settings - Detail Information Edit window

The fields that can be configured or displayed are described below:

Parameter	Description
R-APS VLAN	Display the R-APS VLAN ID.
Ring Status	Tick the check box and use the drop-down menu to enable or disable the specified ring.
Admin West Port	Tick the check box and use the drop-down menu to specify the port as the west ring port and also the virtual port channel used.
Operational West Port	The operational west port value is displayed.
Admin East Port	Tick the check box and use the drop-down menu to specify the port as the east ring port and also the virtual port channel used.
Operational East Port	Display the operational east port value.
Admin RPL Port	Tick the check box and use the drop-down menu to specify the RPL port used. Options to choose from are *West Port*, *East Port*, and *None*.
Operational RPL Port	Display the operational RPL port value.
Admin RPL Owner	Tick the check box and use the drop-down menu to enable or disable the RPL owner node.
Operational RPL Owner	Display the operational RPL owner value.
Protected VLAN(s)	Tick the check box, click the **Add** or **Delete** radio button, and enter the protected VLAN group.
Ring MEL (0-7)	Tick the check box and enter the ring MEL of the R-APS function. The default ring MEL is 1.
Holdoff Time (0-10000)	Tick the check box and enter the hold-off time of the R-APS function. The default hold-off time is 0 milliseconds.
Guard Time (10-2000)	Tick the check box and enter the guard time of the R-APS function. The default guard time is 500 milliseconds.
WTR Time (5-12)	Tick the check box and enter the WTR time of the R-APS function.
Revertive	Tick the check box and use the drop-down menu to enable or disable the state of the R-

	APS revertive option.
Current Ring State	Display the current Ring state.

Click the **Apply** button to accept the changes made.
Click the **<<Back** button to return to the previous window.

After clicking the Sub-Ring Information link, the following window will appear:

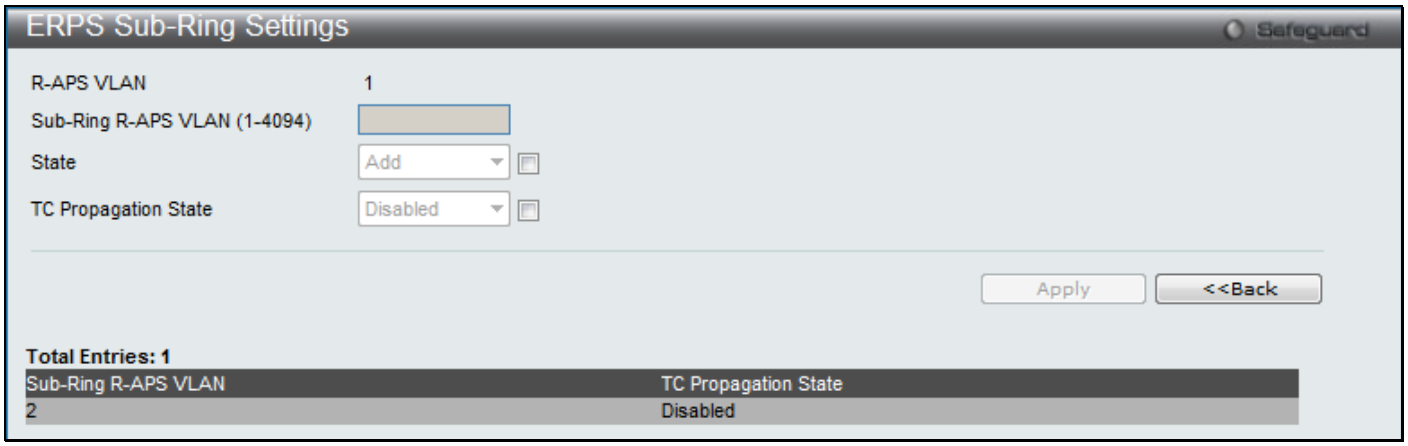


Figure 5-106 ERPS Sub-Ring Settings window

The fields that can be configured are described below:

Parameter	Description
Sub-Ring R-APS VLAN (1-4094)	Enter the Sub-Ring R-APS VLAN ID used here.
State	Tick the check box and use the drop-down menu to add or delete the ERPS Sub-Ring state.
TC Propagation State	Tick the check box and use the drop-down menu to enable or disable the TC Propagation state.

Click the **Apply** button to accept the changes made.
Click the **<<Back** button to return to the previous window.

Local Loopback Port Settings

On this page the user can configure the local loopback port parameters.

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

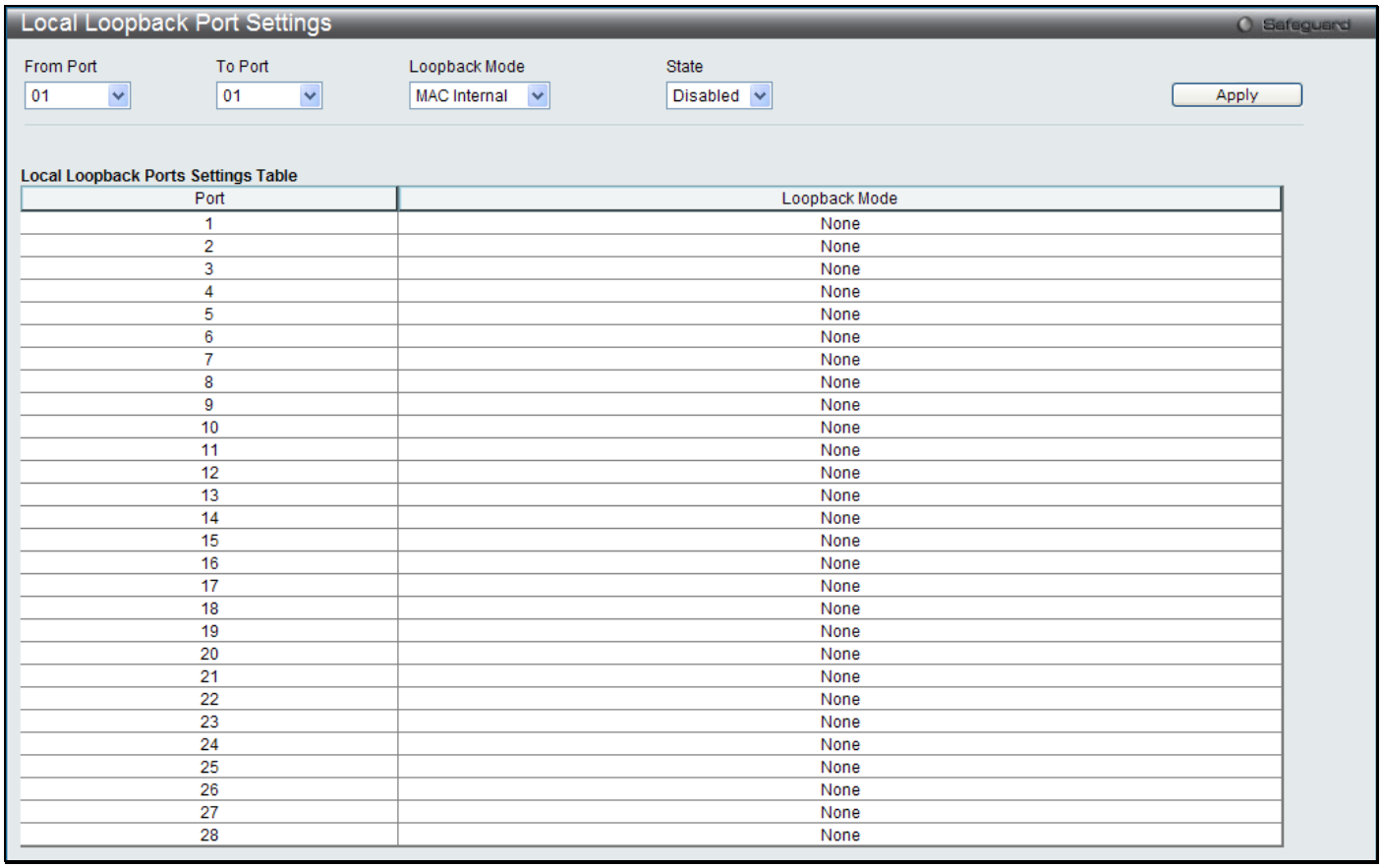


Figure 5-107 Local Loopback Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select the port range to use for this configuration.
Loopback Mode	Here the user can select the Loopback mode used. Modes to choose from are **MAC Internal, MAC External, PHY Internal** and **PHY External**. When the user chooses to use the physical (PHY) mode then the user will be able to set the **Medium Type**.
State	Here the user can choose to enable or disable the state.
Medium Type	Here the user can set the medium type to **Copper** or to **Fiber**.

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

LLDP

The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) through a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP

LLDP Global Settings

On this page the user can configure the LLDP global parameters.

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

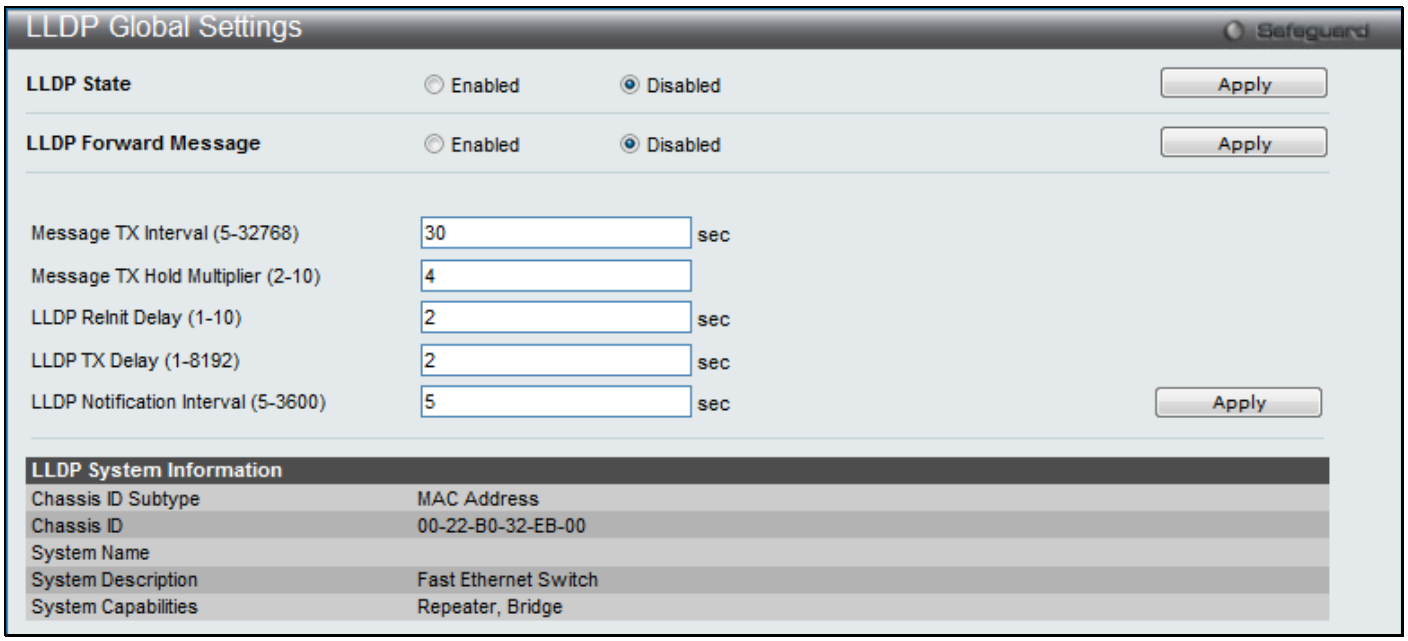


Figure 5-108 LLDP Global Settings window

The fields that can be configured are described below:

Parameter	Description
LLDP State	Here the user can enable or disable the LLDP feature.
LLDP Forward Message	When LLDP is disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message TX Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (5 to 32768).
Message TX Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP Relnit Delay (1-10)	The LLDP re-initialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP re-init delay, enter a value in seconds (1 to 10).
LLDP TX Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (1 to 8192).
LLDP Notification interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (5 to 3600).

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

LLDP Port Settings

On this page the user can configure the LLDP port parameters.

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

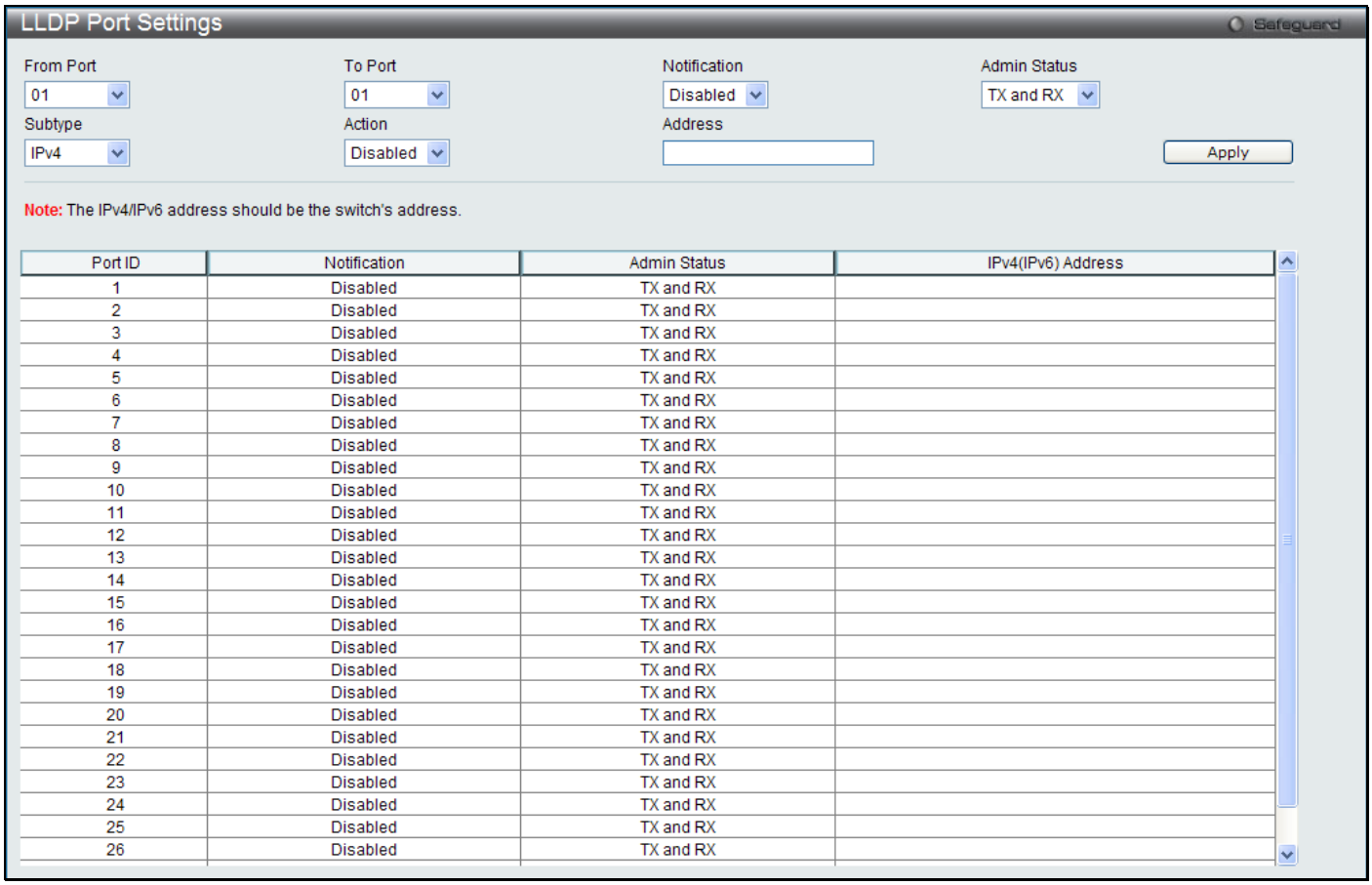


Figure 5-109 LLDP Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select the ports used for this configuration.
Notification	Use the pull-down menu to enable or disable the status of the LLDP notification. This function controls the SNMP trap however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This function controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains **TX**, **RX**, **TX And RX** or **Disabled**. *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. *Disabled*: the local LLDP agent can neither transmit nor receive LLDP frames. The default value is TX And RX.
Subtype	Here the user can select the type of the IP address information will be sent.
Action	Here the user can enable or disable the action field.
Address	Here the user can enter the IP address will that 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

On this page the user can view the LLDP management address list.

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

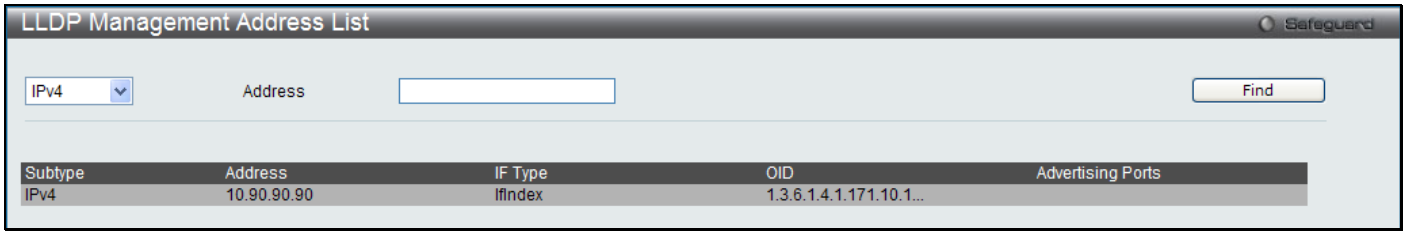


Figure 5-110 LLDP Management Address List window

The fields that can be configured are described below:

Parameter	Description
IPv4 / IPv6	Here the user can select either IPv4 or IPv6.
Address	Enter the management IP address or the IP address of the entity you wish to advertise to here. The IPv4 address is a management IP address, so the IP information will be sent with the frame when the management address configuration is enabled.

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

LLDP Basic TLVs Settings

TLV stands for Type-length-value, which 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 > LLDP Basic TLVs Settings**, as shown below:

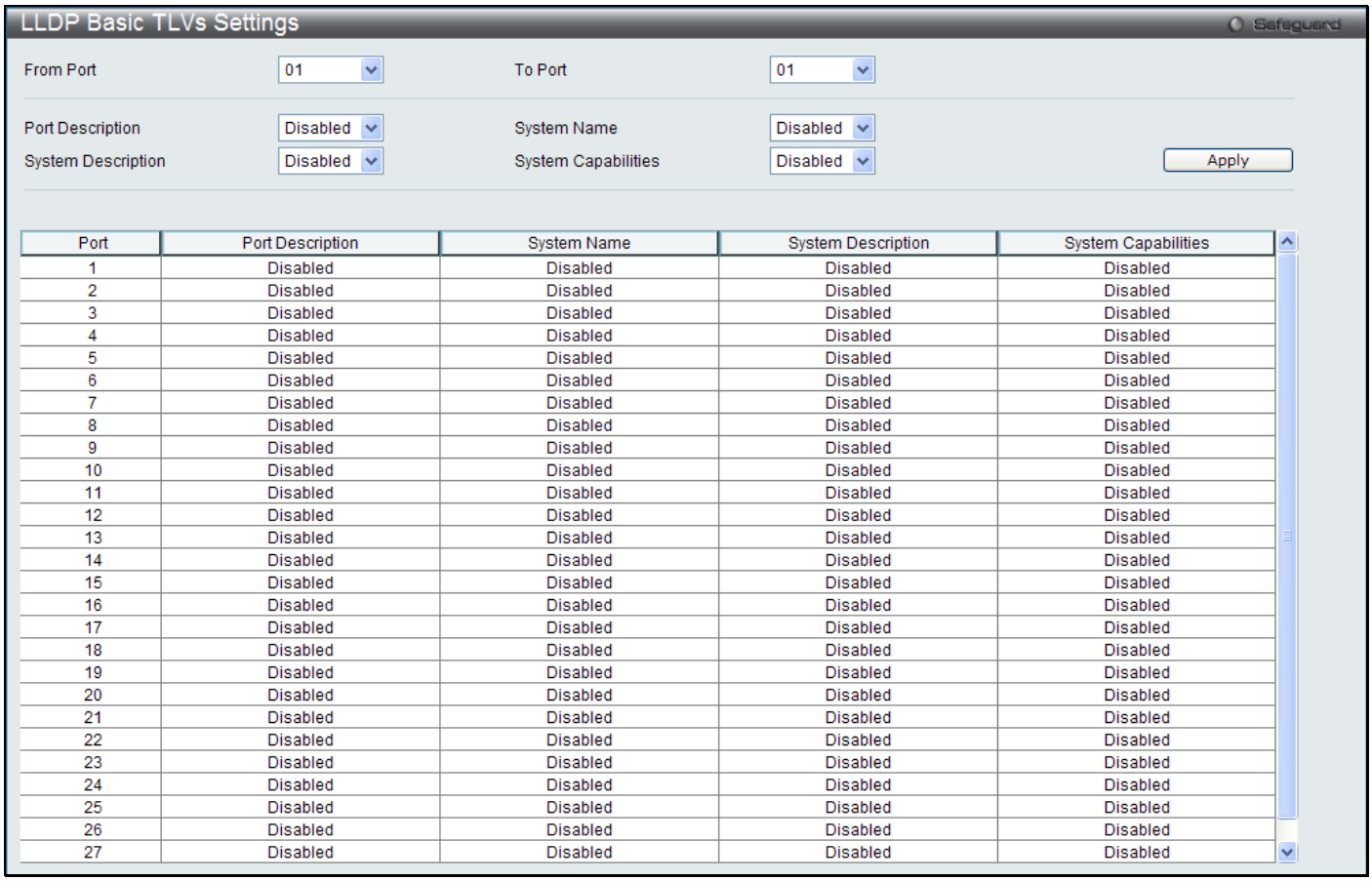


Figure 5-111 LLDP Basic TLVs Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can enter the port range to use for this configuration.
Port Description	Here the user can enable or disable the Port Description option.
System Name	Here the user can enable or disable the System Name option.
System Description	Here the user can enable or disable the System Description option.
System Capabilities	Here the user can 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 > LLDP Dot1 TLVs Settings**, as shown below:

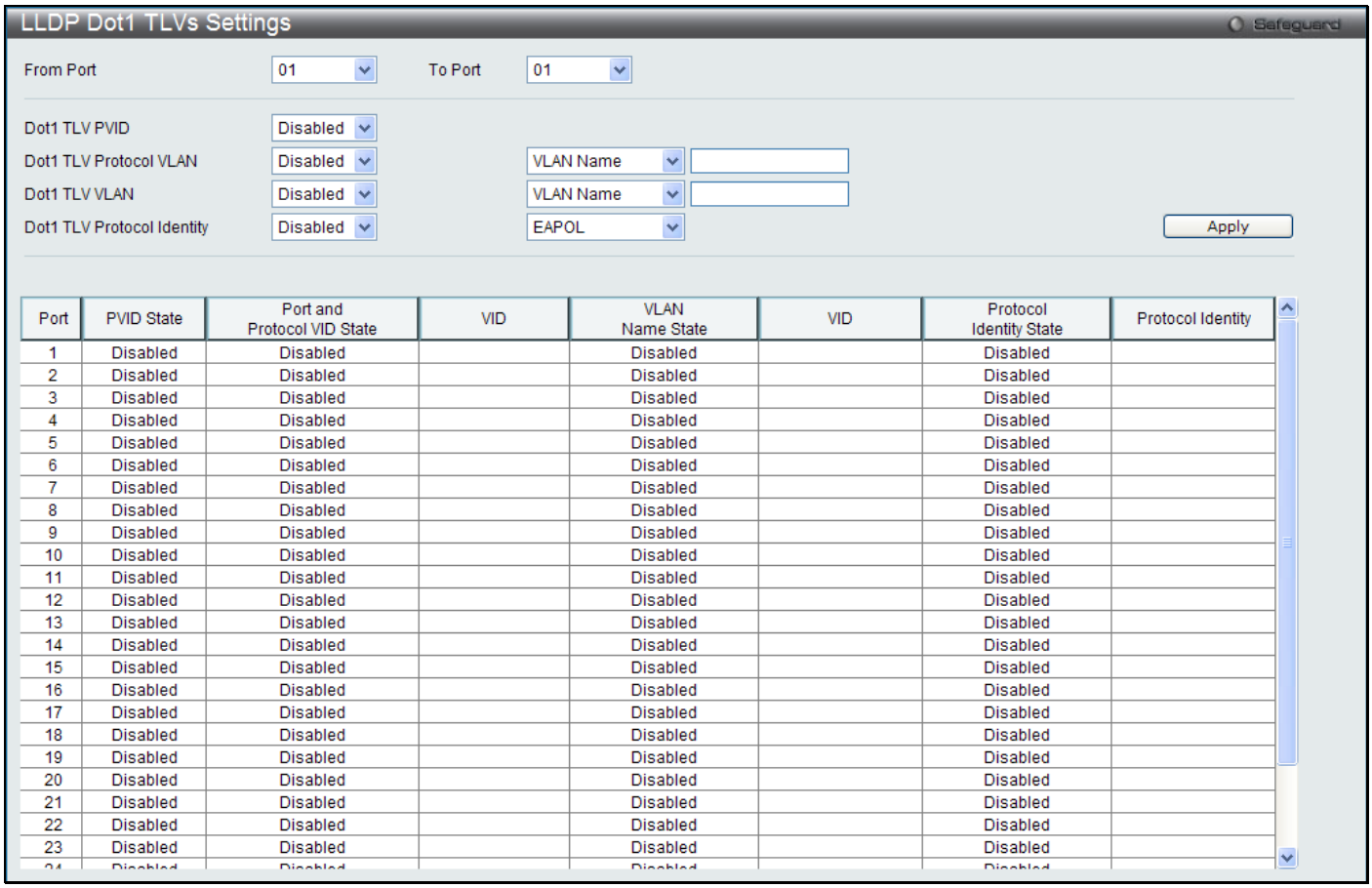


Figure 5-112 LLDP Dot1 TLVs Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can enter the port range to use for this configuration.
Dot1 TLV PVID	Here the user can enable or disable and configure the Dot1 TLV PVID option.
Dot1 TLV Protocol VLAN	Here the user can enable or disable and configure the Dot1 TLV Protocol VLAN option. After enabling this option to the user can select to use either **VLAN Name**, **VID List** or **All** in the next drop-down menu. After selecting this, the user can enter either the **VLAN Name** or **VID List** value in the space provided.
Dot1 TLV VLAN	Here the user can enable or disable and configure the Dot1 TLV VLAN option. After enabling this option to the user can select to use either **VLAN Name**, **VID List** or **All** in the next drop-down menu. After selecting this, the user can enter either the **VLAN Name** or **VID List** value in the space provided.
Dot1 TLV Protocol Identity	Here the user can enable or disable and configure the Dot1 TLV Protocol Identity option. After enabling this option the user can select to either use **EAPOL**, **LACP**, **GVRP**, **STP**, or **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 > LLDP Dot3 TLVs Settings**, as shown below:

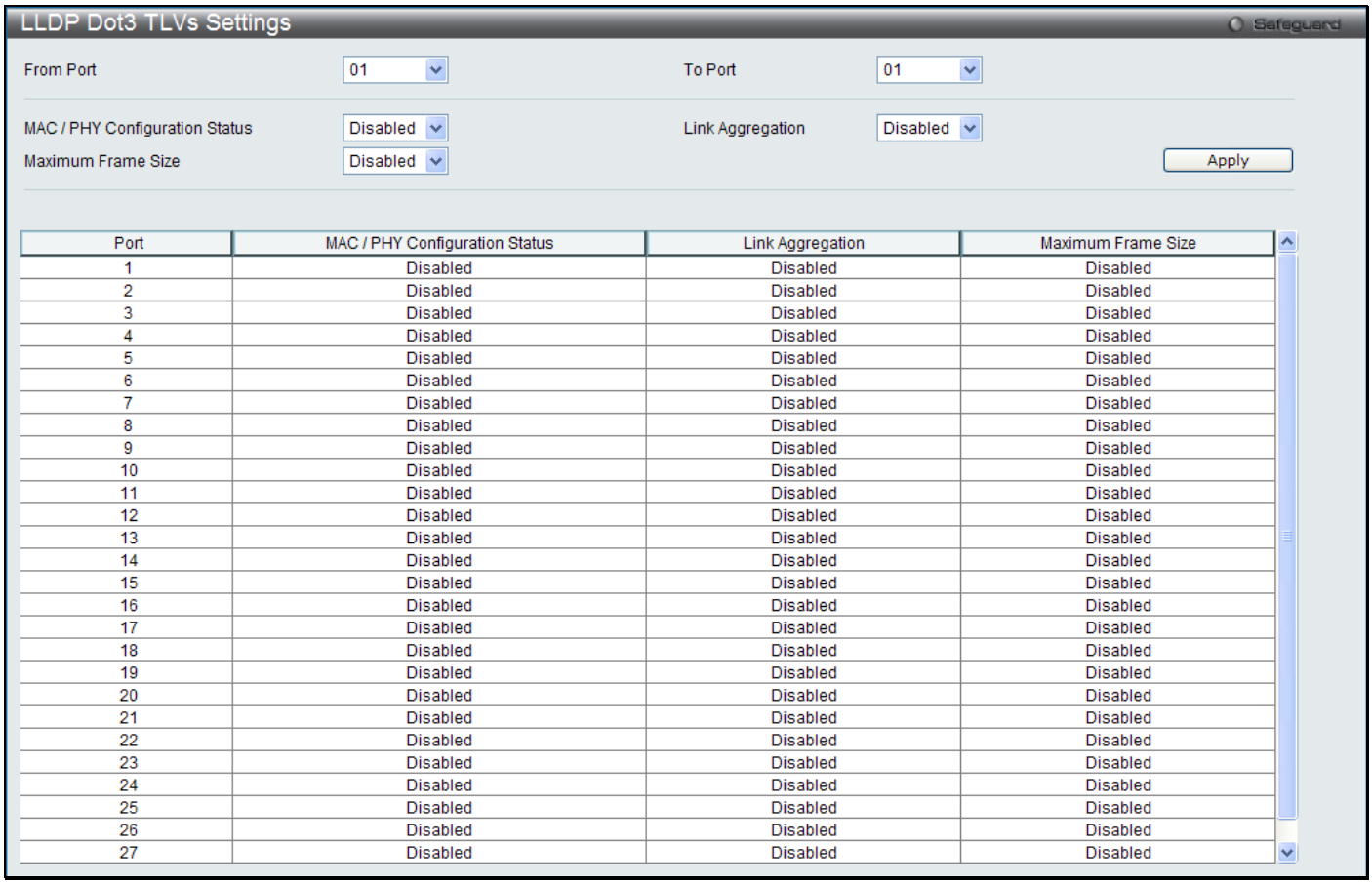


Figure 5-113 LLDP Dot3 TLVs Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can enter the port range to use for this configuration.
MAC / PHY Configuration Status	This TLV optional data type indicates that the LLDP agent should transmit the MAC/PHY configuration/status TLV. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is Disabled.
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is Disabled.
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is Disabled.

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

LLDP Statistics System

The LLDP Statistics System page allows you an overview of the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch. Select a **Port** number and click the **Find** button to view statistics for a certain port.

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

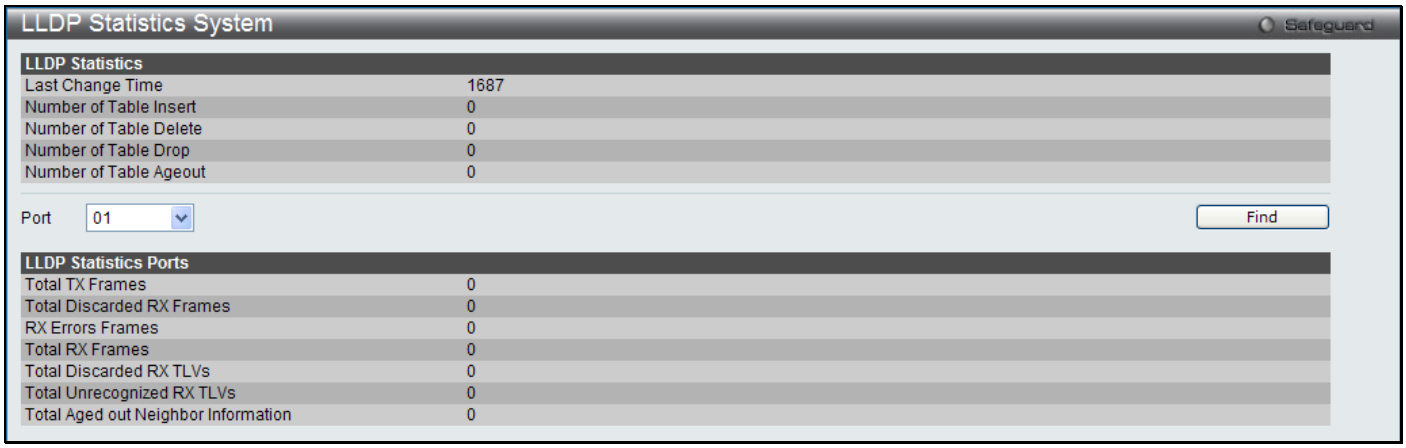


Figure 5-114 LLDP Statistics System window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port.

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

LLDP Local Port Information

The LLDP Local Port Information page displays 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 > LLDP Local Port Information**, as shown below:

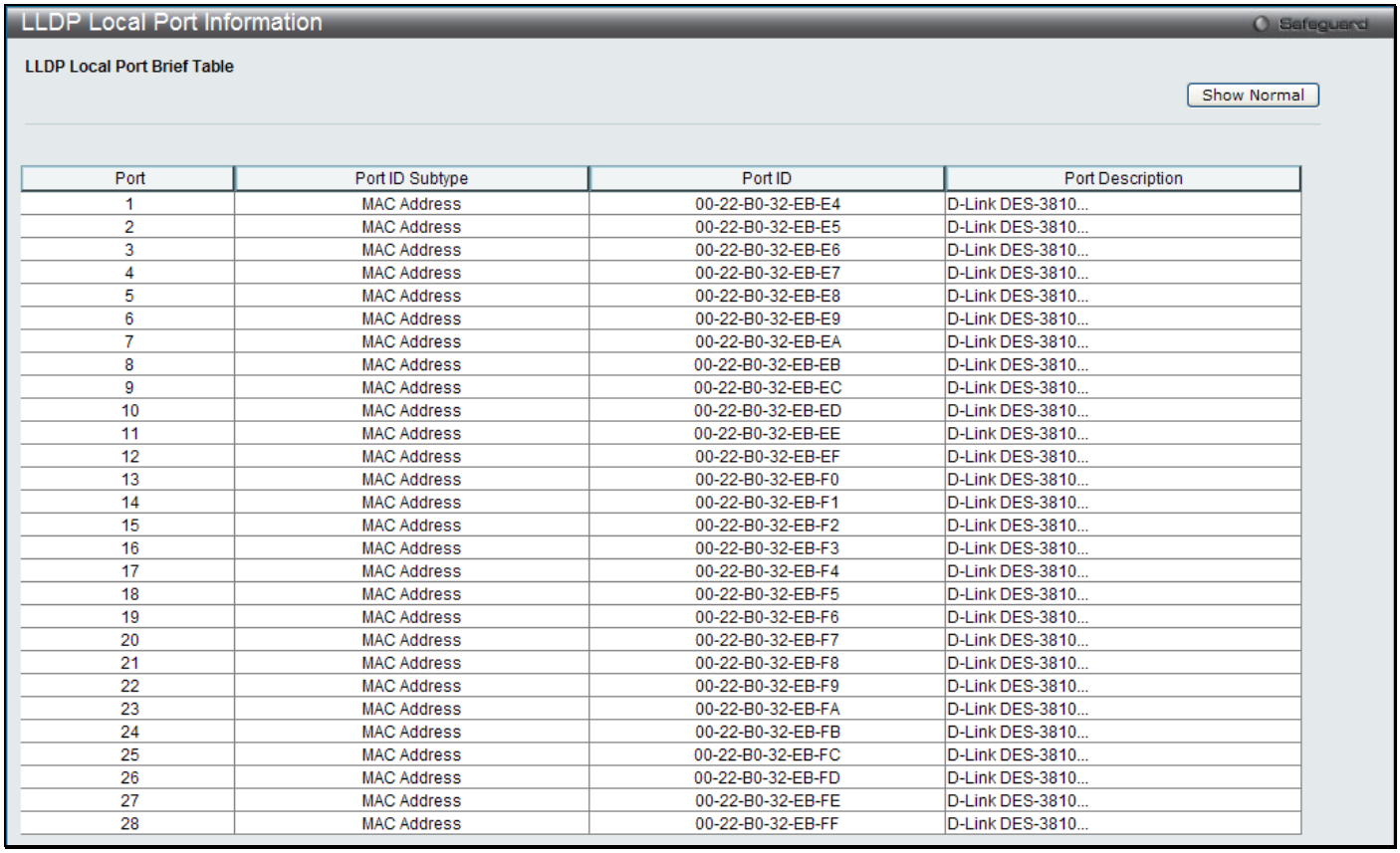


Figure 5-115 LLDP Local Port Information window

To view the normal LLDP Local Port information page per port, click the **Show Normal** button.

After clicking the **Show Normal** button, the following page will appear:

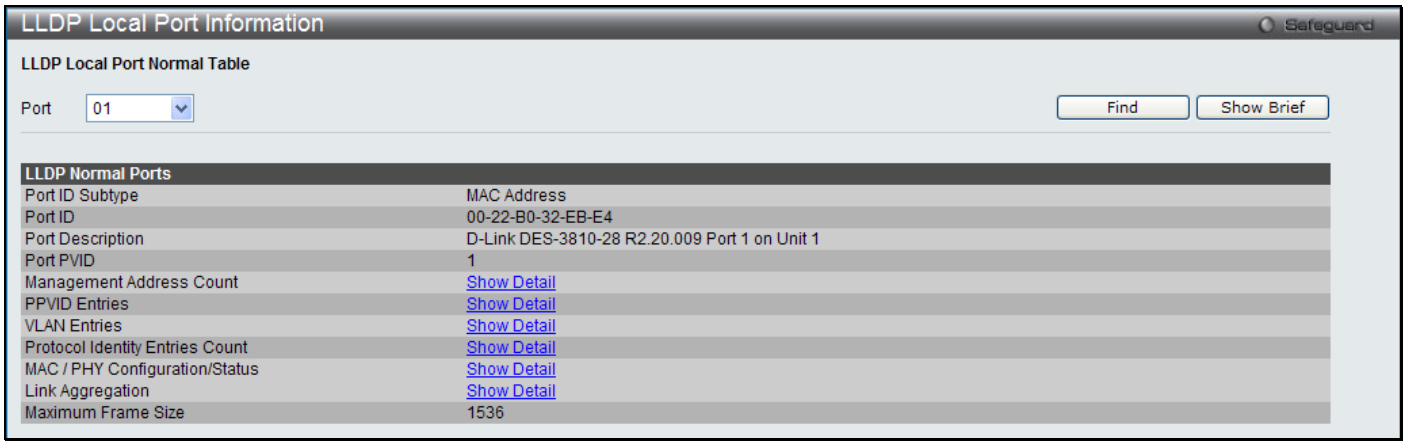


Figure 5-116 LLDP Local Port Information - Show Normal window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port.

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

To view more details about, for example, the **Management Address Count**, click on the Show Detail hyperlink.

To view the brief LLDP Local Port information window per port, click the **Show Brief** button.

After clicking the Show Detail hyperlink under the Management Address Count, the following page will appear:

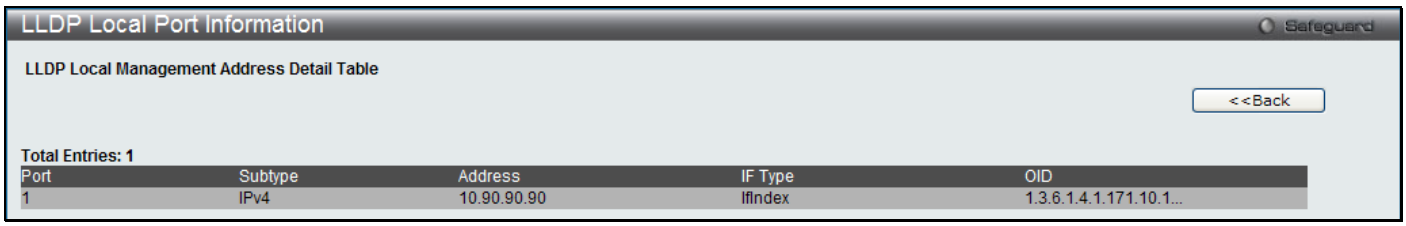


Figure 5-117 LLDP Local Port Information window

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

LLDP Remote Port Information

This page displays port 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 > LLDP Remote Port Information**, as shown below:

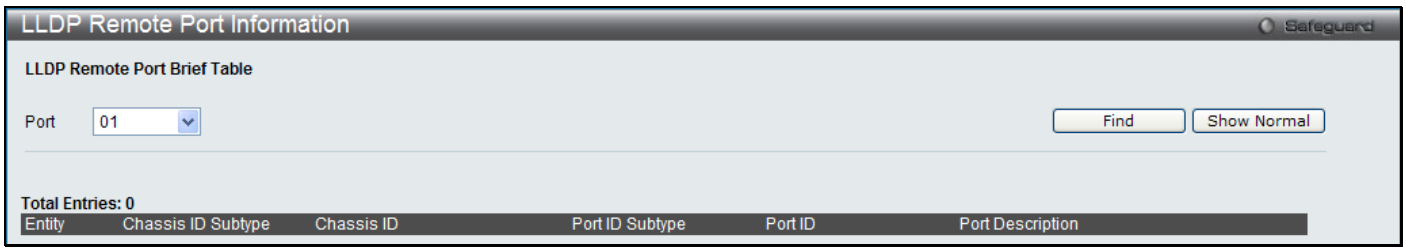


Figure 5-118 LLDP Remote Port Information window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port.

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

To view the normal LLDP Remote Port information page per port, click the **Show Normal** button.

After clicking the **Show Normal** button, the following page will appear:

Figure 5-119 LLDP Remote Port Information window

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

LLDP-MED

LLDP-MED (Media-Endpoint-Discovery) extends the LLDP industry standard to support advanced features on the network edges with specialized capabilities and LLDP-MED standards-based functionality.

LLDP-MED System Settings

On this page the user can configure the fast start repeat count.

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

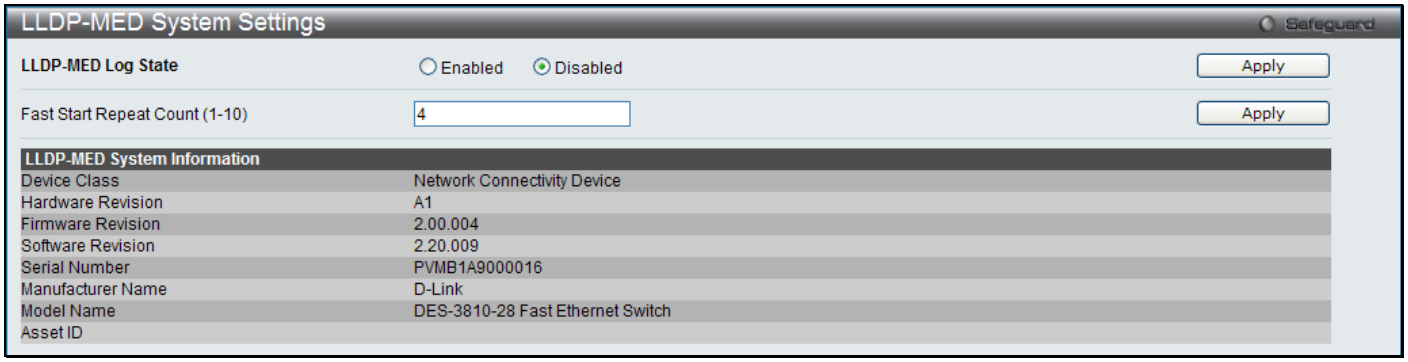


Figure 5-120 LLDP-MED System Settings window

The fields that can be configured are described below:

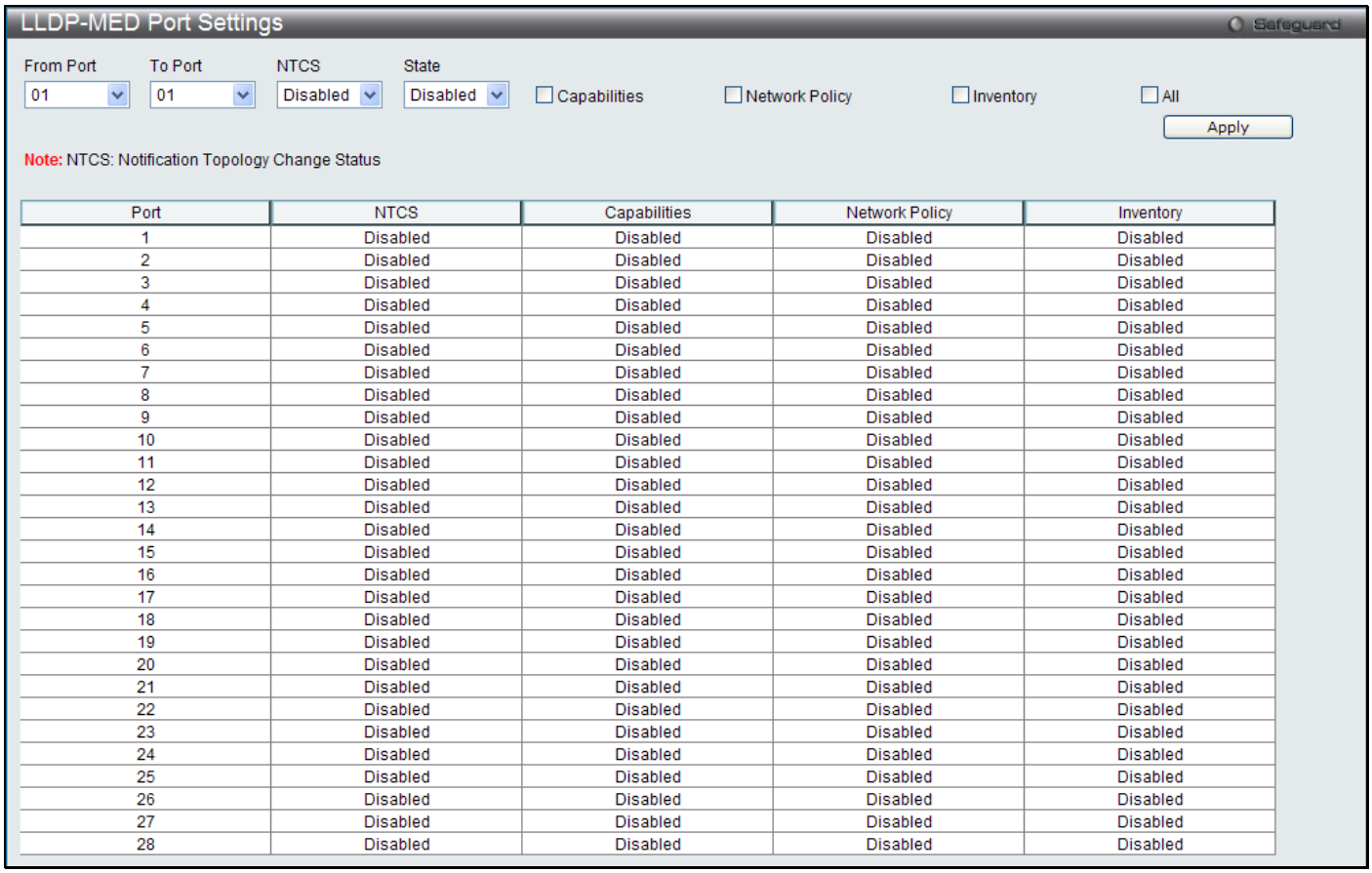
Parameter	Description
LLDP-MED Log State	Here the user can enable or disable the LLDP-MED Log State.
Fast Start Repeat Count (1-10)	The repeat count range is from 1 to 10. The default value is 4.

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

LLDP-MED Port Settings

On this page the user can enable or disable transmit LLDP-MED TLVs. Setting non-supported capability shall have no functional effect and will result in an inconsistent value error returned to the management application. It effectively disables LLDP-MED on a per-port basis by disabling transmission of capabilities TLV. In this case the remote table's objects in the LLDP-MED MIB corresponding to the respective port will not be populated.

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



Port	NTCS	Capabilities	Network Policy	Inventory
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled
25	Disabled	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled	Disabled

Figure 5-121 LLDP-MED Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Specified a range of ports to be configured.
NTCS	Here the user can enable or disable the notification topology change status.
State	Here the user can enable or disable TLVs.
Capabilities	This TLV type indicates that LLDP agent should transmit 'LLDP-MED capabilities TLV'. If user wants to transmit LLDP-MED PDU, this TLV type should be enabled. Otherwise, this port cannot transmit LLDP-MED PDU.
Network Policy	This TLV type indicates that LLDP agent should transmit 'LLDP-MED network policy TLV'.
Inventory	This TLV type indicates that LLDP agent should transmit 'LLDP-MED inventory TLV'.
All	Select this option to include **Capabilities, Network Policy** and **Inventory** in the configuration.

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

LLDP-MED Local Port Information

On this page the LLDP-MED local port information will be displayed per port.

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

Figure 5-122 LLDP-MED Local Port Information window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port.

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

LLDP-MED Remote Port Information

On this page the LLDP-MED Remote Port Information will be displayed.

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

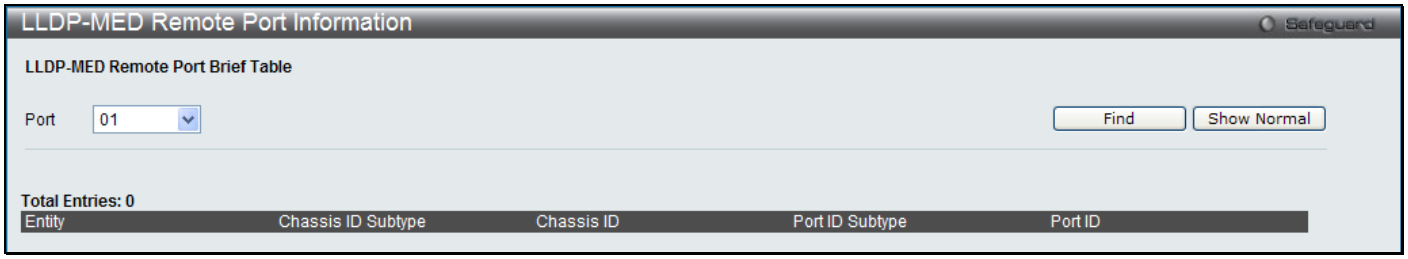


Figure 5-123 LLDP-MED Remote Port Information window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port.

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

To view the normal LLDP Remote Port information page per port, click the **Show Normal** button.

After clicking the **Show Normal** button, the following page will appear:

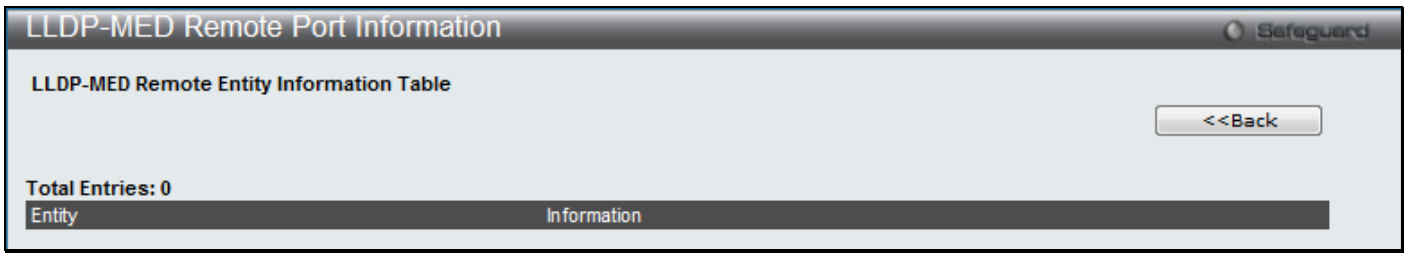


Figure 5-124 LLDP-MED Remote Port Information window

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

NLB FDB Settings

The Switch supports Network Load Balancing (NLB). This is a MAC forwarding control for supporting the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. In multicast mode, the client uses a multicast MAC address as the destination MAC to reach the server. Regardless of the mode, the destination MAC is the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. The NLB multicast FDB entry will be mutually exclusive with the L2 multicast entry.

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

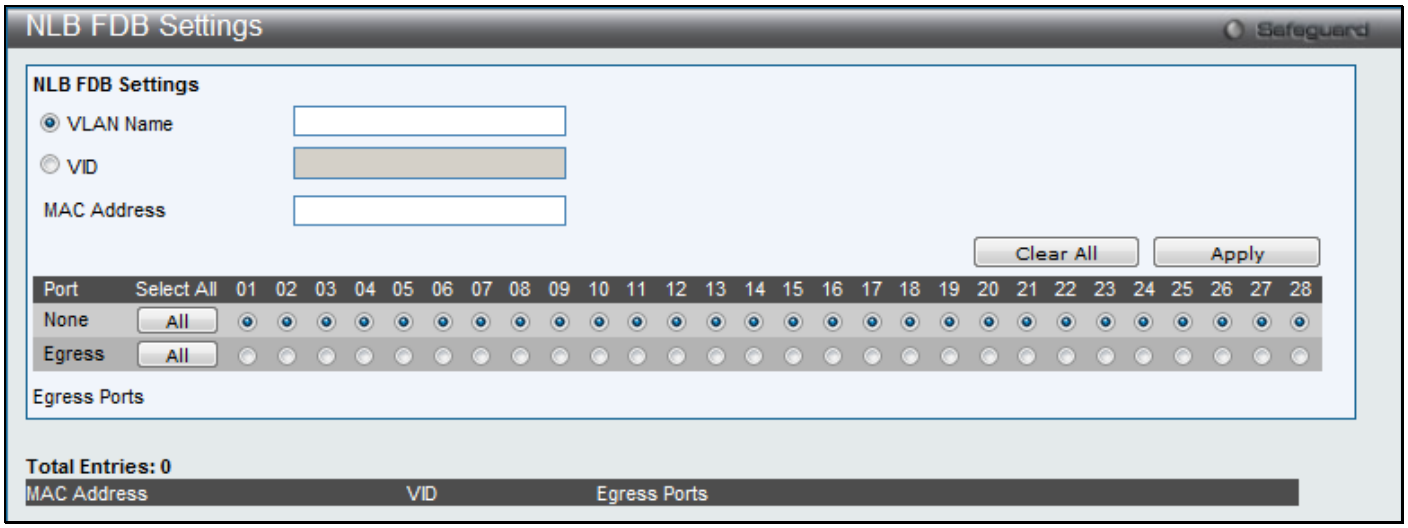


Figure 5-125 NLB FDB Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN name of the NLB multicast FDB entry to be created.
VID	Click the radio button and enter the VLAN by the VLAN ID.
MAC Address	Enter the MAC address of the NLB multicast FDB entry to be created.
Ports	Choose the forwarding ports for the specified NLB multicast FDB entry. *None* – The port is not the forwarding port. Click the **All** button to select all the ports. *Egress* - The port is the forwarding port. Click the **All** button to select all the ports.

Click the **Clear All** button to clear out all the information entered.

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

Chapter 6 L3 Features

IPv4 Static/Default Route Settings

The Switch supports static routing for IPv4 and IPv6 formatted addressing. Users can create up to 256 static route entries for IPv4 and 128 static route entries for IPv6. 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 response 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 Settings**, as shown below:

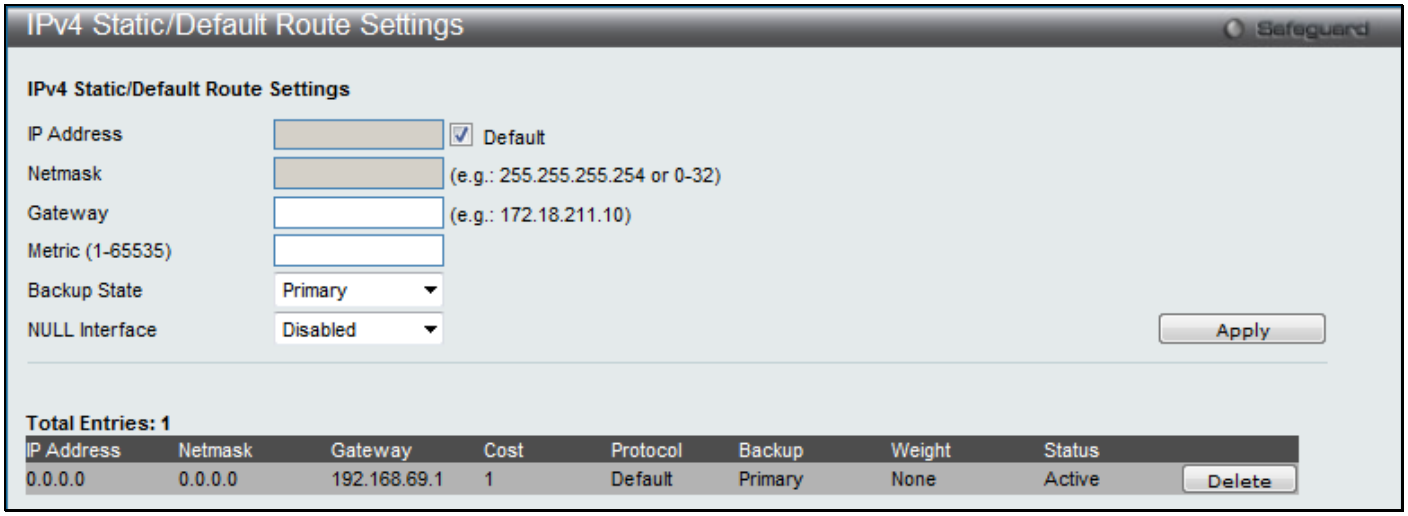


Figure 6-1 IPv4 Static/Default Route Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	This field allows the entry of an IPv4 address to be assigned to the Static or Default route.
Netmask	This field allows the entry of a subnet mask to be applied to the corresponding subnet

	mask of the IP address.
Gateway	This field allows the entry of a Gateway IP Address to be applied to the corresponding gateway of the IP address.
Metric (1-65535)	Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.
Backup State	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, switch will try the backup routes according to the order learnt by the routing table until route success. The field represents the Backup state that the Static and Default Route is configured for.
NULL Interface	Specify to enable or disable the NULL function for the routes. The null interface provides an alternative method of filtering traffic. Packets send to null interface will be dropped by the switch.

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

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

IPv4 Route Table

The IPv4 routing table stores all the external routes information of the switch. On this page the user can view all the external route information on the switch.

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

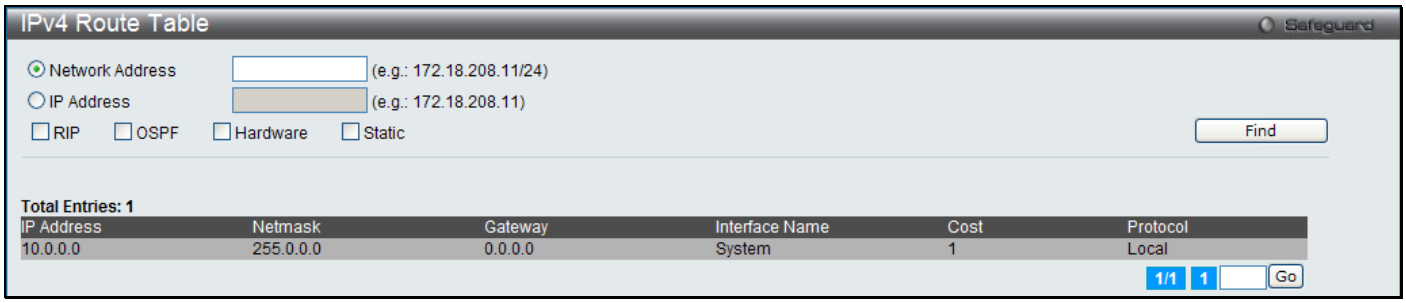


Figure 6-2 IPv4 Route Table window

The fields that can be configured are described below:

Parameter	Description
Network Address	Specifies the IPv4 network address used for this search. The network address should be followed by the CIDR notation for the subnet mask used.
IP Address	Specifies the specific IPv4 address used for this search without the CIDR notation.
RIP	Specifies to display routes that are related to RIP.
OSPF	Specifies to display routes that are related to OSPF.
Hardware	Select the Hardware option to display only the routes that have been written into the chip.
Static	Specifies to display only static routes.

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

IPv6 Static/Default Route Settings

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses.

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

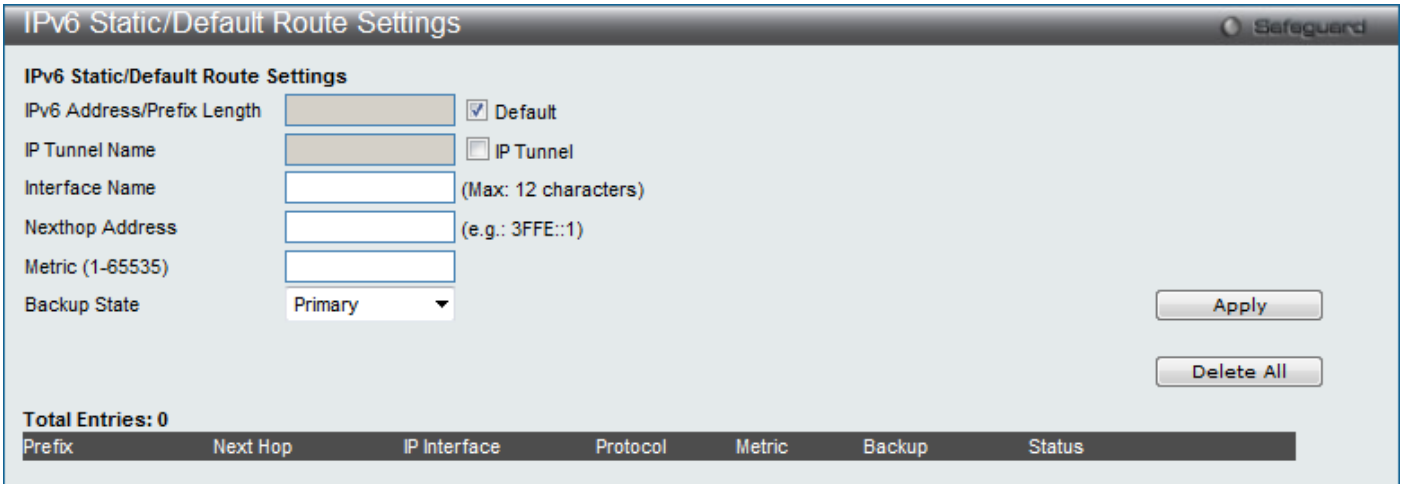


Figure 6-3 IPv6 Static/Default Route Settings window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	The IPv6 address and corresponding Prefix Length of the IPv6 Static or Default Route entry.
IP Tunnel Name	Tick the **IP Tunnel** option and enter the IP tunnel name used here.
Interface Name	The IP Interface where the static IPv6 route is created.
Nexthop Address	The corresponding IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric of the IPv6 interface entered into the table representing the number of routers between the Switch and the IPv6 address above. Metric values allowed are between 1 and 65535.
Backup State	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, the switch will try the backup routes according to the order learnt by the routing table until route success. This field represents the backup state for the IPv6 configured. This field may be Primary or Backup.

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

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

IPv6 Route Table

The IPv6 routing table stores all the external routes information of the switch. On this page the user can view all the external route information on the switch.

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

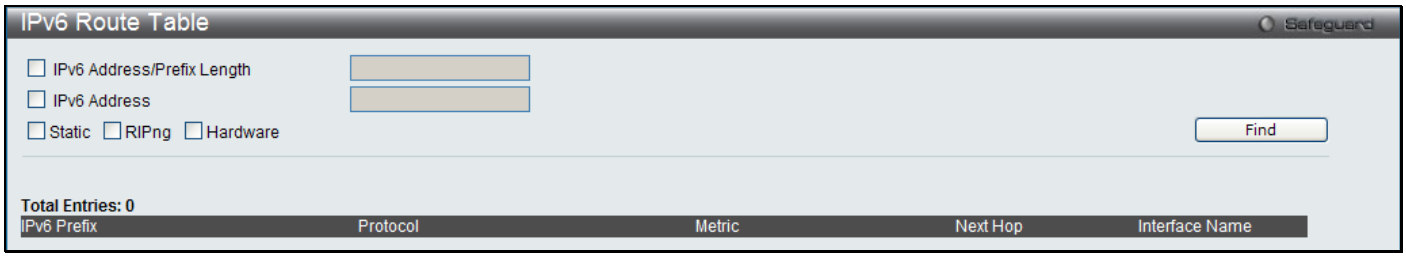


Figure 6-4 IPv6 Route Table window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix	Tick the check box and enter a 128-bit length IPv6 address.

Length	
IPv6 Address	Tick the check box and enter the destination IPv6 address of the route to be displayed.
Static	Tick the check box to display the static route.
RIPng	Tick the check box to display routes that are related to RIPng.
Hardware	Tick the check box to display only the routes that have been written into the chip.

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

Policy Route Settings

Policy Based routing is a method used by the Switch to give specified devices a cleaner path to the Internet. Used in conjunction with the Access Profile feature, the Switch will identify traffic originating from a device using the Access Profile feature and forward it on to a next hop router that has a more direct connection to the Internet than the normal routing scheme of your network.

Take the example adjacent picture. Let's say that the PC with IP address 10.1.1.1 belongs to the manager of a company while the other PCs belong to employees. The network administrator hopes to circumvent network traffic by configuring the Policy Routing Switch to make a more direct connection to the Internet using a next hop router (10.2.2.2) that is directly attached to a Gateway router (10.3.3.3), thus totally avoiding the normal network and its related traffic. To accomplish this, the user must configure the Access Profile feature of the Switch to have the PC, with IP address 10.1.1.1 as the Source IP address and the Internet address as the destination IP address (learned through routing protocols), along with other pertinent information. Next, the administrator must configure the Policy Route window to be enabled for this Access Profile and its associated rule, and the Next Hop Router's IP address (10.2.2.2) must be set. Finally, this Policy Route entry must be enabled.

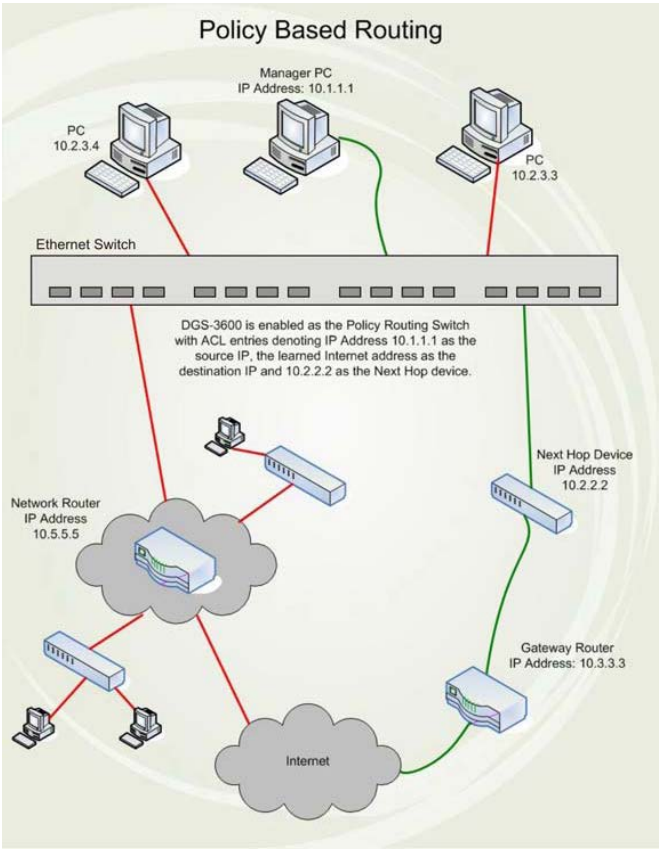


Figure 6-5 Policy Base Routing Example window

Once completed, the Switch will identify the IP address using the Access Profile function, recognize that is has a Policy Based route, and then forward the information on to the specified next hop router, that will, in turn, relay packets to the gateway router. Thus, the new, cleaner path to the Internet has been formed.

There are some restrictions and cautions when implementing this feature:

1. The access profile must first be created, along with the accompanying rule. If the administrator attempts to enable this feature without the access profile, an error message will be produced.
2. If the access profile is configured as Deny, the packet will be dropped and not forwarded to the next hop destination.
3. If the administrator deletes a rule or profile that is directly linked to a configured policy route, and error message will be prompted to the administrator.

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

Figure 6-6 Policy Route Settings window

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

After clicking the **Edit** button, the following page will appear:

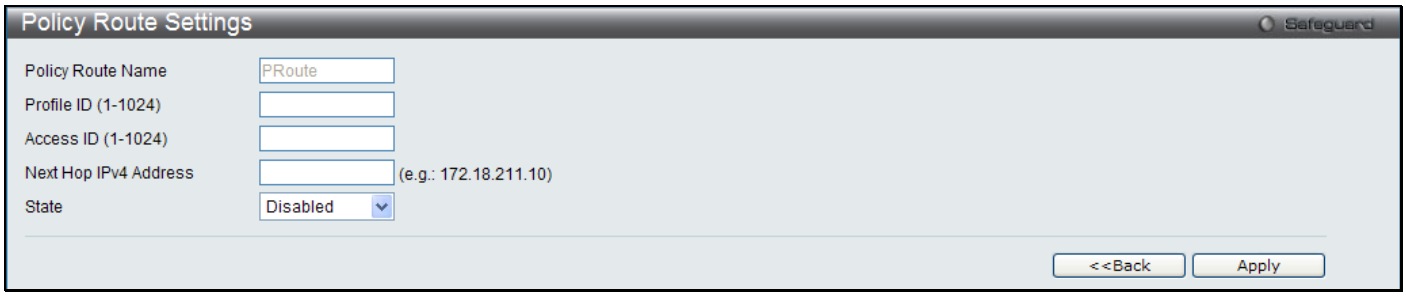


Figure 6-7 Policy Route Settings window

The fields that can be configured are described below:

Parameter	Description
Policy Route Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this policy route.
Profile ID (1-1024)	Enter the Profile ID number of the Access Profile, previously created, which will be used to identify packets as following this Policy Route. This access profile, along with the access rule, must first be constructed before this policy route can be created.
Access ID (1-1024)	Enter the Access ID number of the Access Rule, previously created, which will be used to identify packets as following this Policy Route. This access rule, along with the access profile, must first be constructed before this policy route can be created.
Next Hop IPv4 Address	This is the IP address of the Next Hop router that will have a direct connection to the Gateway router connected to the Internet.
State	Use the pull-down menu to enable or disable this Policy Route.

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

IP Forwarding Table

The IP forwarding table stores all the direct connected IP information. On this page the user can view all the direct connected IP information.

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

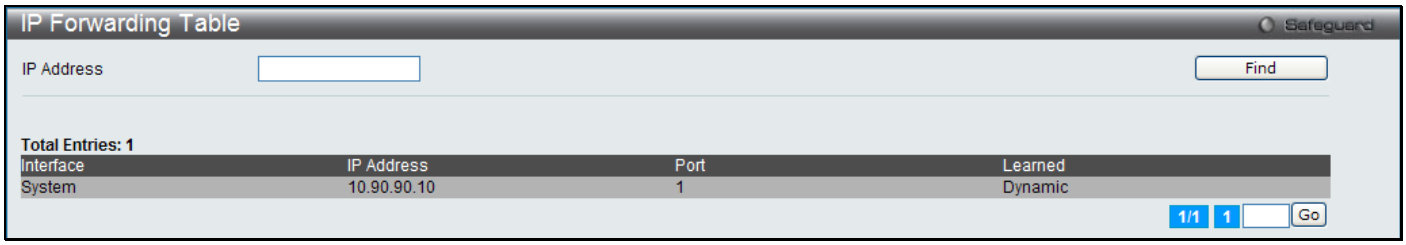


Figure 6-8 IP Forwarding Table window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IP address of the Interface 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.

IP Multicast Forwarding Table

This window will show current IP multicasting information on the Switch.

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

Figure 6-9 IP Multicast Forwarding Table window

The fields that can be configured are described below:

Parameter	Description
Group Address	Enter the group address.
Network Address	Enter the network address.

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

Click the **View All** button to display all the existing entries.

IP Multicast Interface Table

This window displays the current IP multicasting interfaces located on the Switch. To search for a specific entry, enter a multicast interface name into the **Interface Name** field and click **Find**. To search for entries using the same Multicast Routing, choose **Protocol** from the drop down list and click **Find**.

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

Figure 6-10 IP Multicast Interface Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the interface name
Protocol	Use the drop-down menu to select the protocol.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Route Preference Settings

This page is used to configure the route preference settings for this Switch.

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

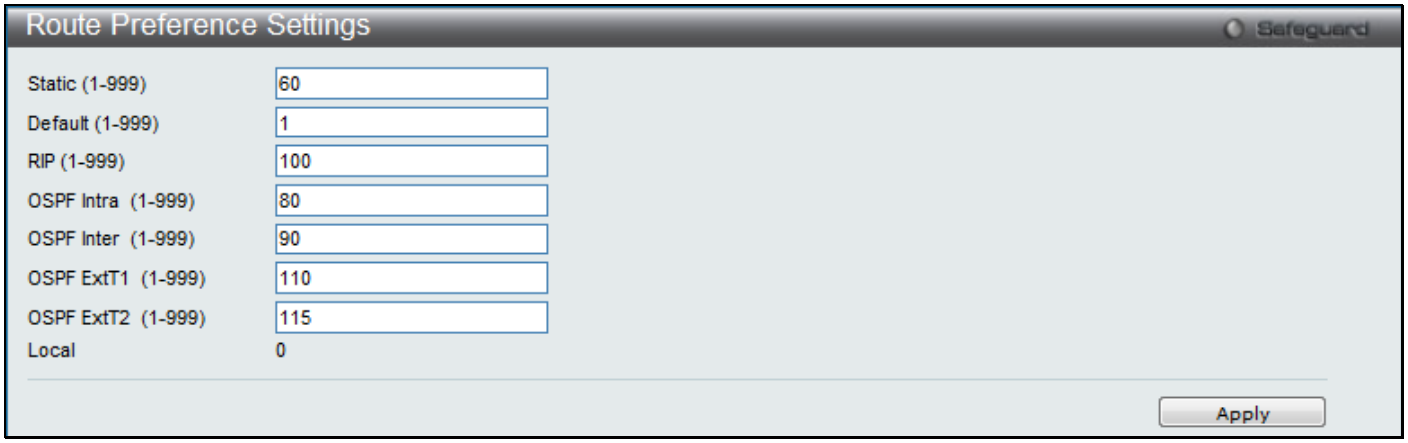


Figure 6-11 Route Preference Settings window

The fields that can be configured are described below:

Parameter	Description
Static (1-999)	Configure the preference of static route. The default value is 60.
Default (1-999)	Configure the preference of default route. The default value is 1.
RIP (1-999)	Configure the preference of RIP route. The default value is 100.
OSPF Intra (1-999)	Configure the preference of OSPF intra-area route. The default value is 80.
OSPF Inter (1-999)	Configure the preference of OSPF inter-area route. The default value is 90.
OSPF ExtT1 (1-999)	Configure the preference of OSPF external type-1 route. The default value is 110.
OSPF ExtT2 (1-999)	Configure the preference of OSPF external type-2 route. The default value is 115.

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

ECMP Algorithm Settings

This page is used to configure the ECMP OSPF state for this Switch.

To view the following window, click **L3 Features > ECMP Algorithm Settings**, as shown below:

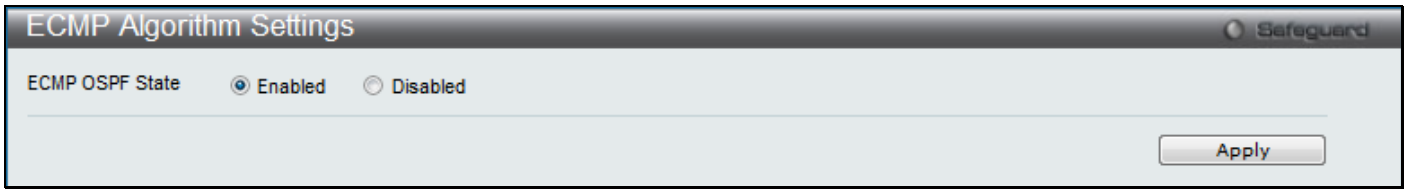


Figure 6-12 ECMP Algorithm Settings window

The fields that can be configured are described below:

Parameter	Description
ECMP OSPF State	Specifies whether the ECMP OSPF State is enable or disabled.

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

Route Redistribution Settings

This page is used to configure redistribute routing information from one routing protocols to another.

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

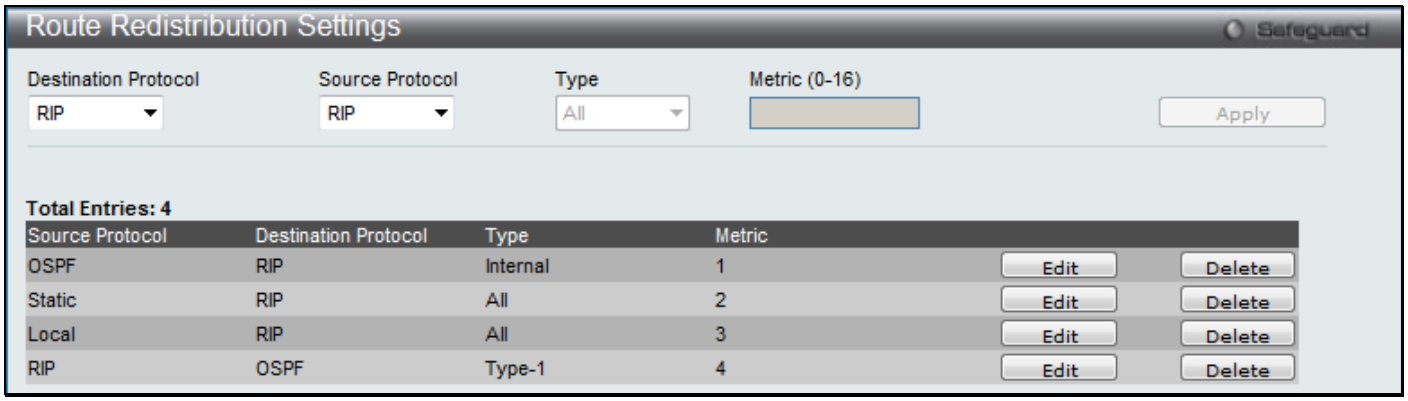


Figure 6-13 Route Redistribution Settings window

The fields that can be configured are described below:

Parameter	Description
Destination Protocol	Specifies the destination protocol. Options to choose from are **RIP** and **OSPF**.
Source Protocol	Specifies the source protocol. Options to choose from are **RIP**, **OSPF**, **Static** and **Local**.
Type	Specifies the type of route to be redistributed. Options to choose from are **All, Internal, External, Ext Type1, Ext Type2, Inter-E1, Inter-E2, Type-1,** and **Type-2**. To redistribute all types of route select the **All** option.
Metric (0-16)	Specifies the metric value for the redistributed routes.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the specified entry.
Click the **Delete** button to remove the specified entry.

IP Tunnel

IP Tunnel Settings

This window is used to configure IP Tunnel Settings.

To view the following window, click **L3 Features > IP Tunnel > IP Tunnel Settings**, as shown below:

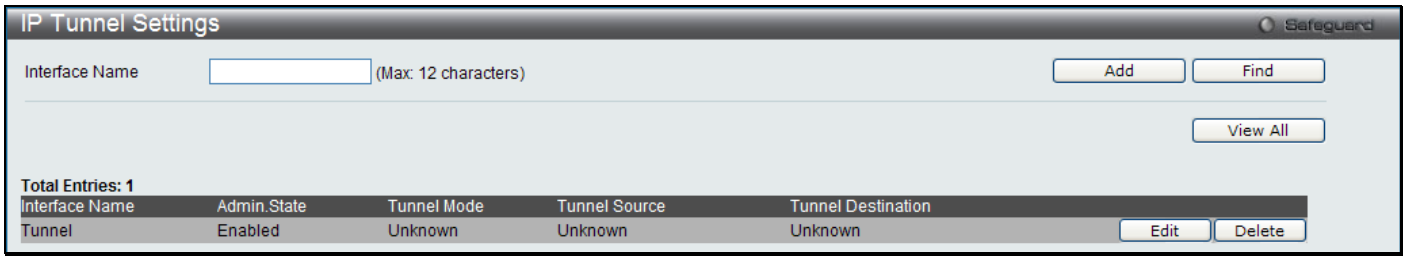


Figure 6-14 IP Tunnel Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP tunnel interface name.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

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

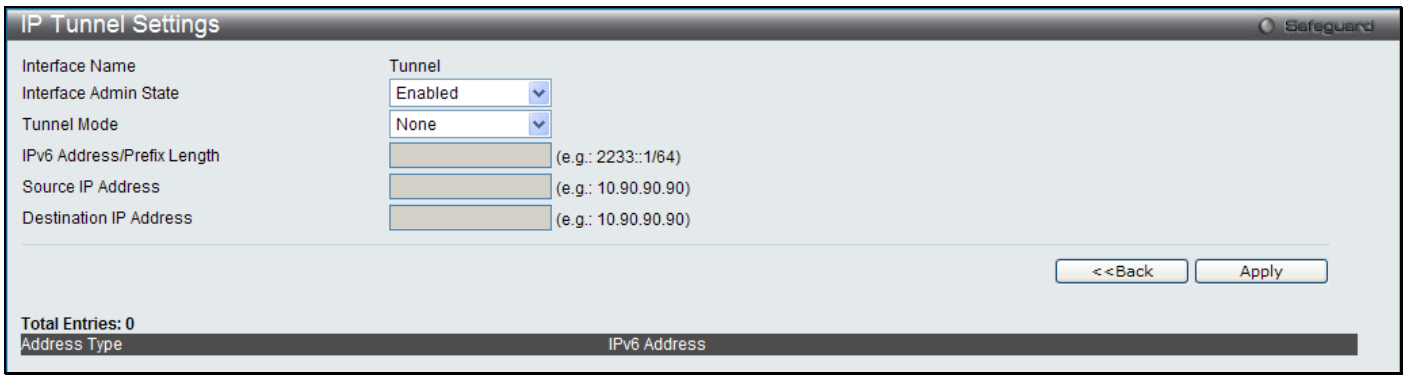


Figure 6-15 IP Tunnel Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Interface Admin State	Use the drop-down menu to enable or disable the interface admin state.
Tunnel Mode	Use the drop-down menu to select the tunnel modes. Available selections are *None*, *Manual*, *6to4*, and *ISATAP*.
IPv6 Address/Prefix Length	Enter the IPv6 network address.
Source IP Address	Enter the source IP address.
Destination IP Address	Enter the destination IP address.

Click the **<<Back** button to return to the previous window.
Click the **Apply** button to accept the changes made for each individual section.

IP Tunnel GRE Settings

This window is used to configure an existing tunnel as a GRE tunnel (IPv6-in-IPv4) on the Switch. If this tunnel has been configured in another mode before, the tunnel's information will still exist in the database. However, whether the tunnel's former information is valid or not, it depends on the current mode.

To view the following window, click **L3 Features > IP Tunnel > IP Tunnel GRE Settings**, as shown below:

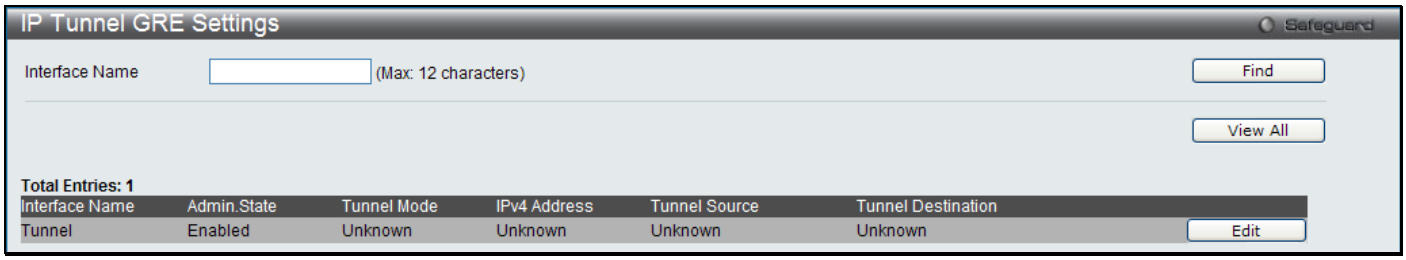


Figure 6-16 IP Tunnel GRE Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP tunnel interface name.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Edit** button to re-configure the specific entry.

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

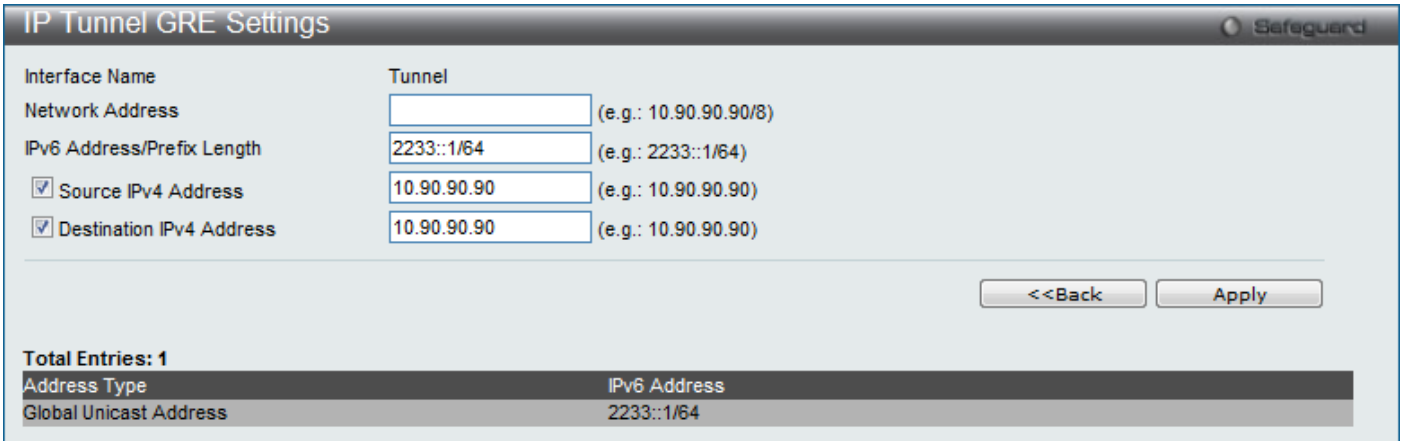


Figure 6-17 IP Tunnel GRE Settings (Edit) window

The fields that can be configured are described below:

Parameter	Description
Network Address	Enter the IPv4 network address assigned to the GRE tunnel interface. IPv4 processing will be enabled on the IPv4 tunnel interface when an IPv4 address is configured. This IPv4 address is not connected with the tunnel source or destination IPv4 address.
IPv6 Address/Prefix Length	Enter the IPv6 network address assigned to the GRE tunnel interface. IPv6 processing will be enabled on the IPv6 tunnel interface when an IPv6 address is configured. This IPv6 address is not connected with the tunnel source or destination IPv4 address.
Source IPv4 Address	Click the radio button and enter the source IPv4 address of the GRE tunnel interface. It is used as the source address for packets in the tunnel.
Destination IPv4 Address	Click the radio button and enter the destination IPv4 address of the GRE tunnel interface. It is used as the destination address for packets in the tunnel.

Click the **<<Back** button to return to the previous window.
Click the **Apply** button to accept the changes made for each individual section.

OSPF

The Open Shortest Path First (OSPF) routing protocol uses a link-state algorithm to determine routes to network destinations. A “link” is an interface on a router and the “state” is a description of that interface and its relationship to

neighboring routers. The state contains information such as the IP address, subnet mask, type of network the interface is attached to, other routers attached to the network, etc. The collection of link-states is then collected in a link-state database that is maintained by routers running OSPF.

OSPF specifies how routers will communicate to maintain their link-state database and defines several concepts about the topology of networks that use OSPF.

To limit the extent of link-state update traffic between routers, OSPF defines the concept of Area. All routers within an area share the exact same link-state database, and a change to this database once one router triggers an update to the link-state database of all other routers in that area. Routers that have interfaces connected to more than one area are called Border Routers and take the responsibility of distributing routing information between areas.

One area is defined as Area 0 or the Backbone. This area is central to the rest of the network in that all other areas have a connection (through a router) to the backbone. Only routers have connections to the backbone and OSPF is structured such that routing information changes in other areas will be introduced into the backbone, and then propagated to the rest of the network.

When constructing a network to use OSPF, it is generally advisable to begin with the backbone (area 0) and work outward

Link-State Algorithm

An OSPF router uses a link-state algorithm to build a shortest path tree to all destinations known to the router. The following is a simplified description of the algorithm's steps:

1. When OSPF is started, or when a change in the routing information changes, the router generates a link-state advertisement. This advertisement is a specially formatted packet that contains information about all the link-states on the router.
2. This link-state advertisement is flooded to all routers in the area. Each router that receives the link-state advertisement will store the advertisement and then forward a copy to other routers.
3. When the link-state database of each router is updated, the individual routers will calculate a Shortest Path Tree to all destinations □ with the individual router as the root. The IP routing table will then be made up of the destination address, associated cost, and the address of the next hop to reach each destination.
4. Once the link-state databases are updated, Shortest Path Trees calculated, and the IP routing tables written □ if there are no subsequent changes in the OSPF network (such as a network link going down) there is very little OSPF traffic.

Shortest Path Algorithm

The Shortest Path to a destination is calculated using the Dijkstra algorithm. Each router is placed at the root of a tree and then calculates the shortest path to each destination based on the cumulative cost to reach that destination over multiple possible routes. Each router will then have its own Shortest Path Tree (from the perspective of its location in the network area) even though every router in the area will have and use the exact same link-state database.

The following sections describe the information used to build the Shortest Path Tree.

OSPF Cost

Each OSPF interface has an associated cost (also called "metric") that is representative of the overhead required to send packets over that interface. This cost is inversely proportional to the bandwidth of the interface (i.e. a higher bandwidth interface has a lower cost). There is then a higher cost (and longer time delays) in sending packets over a 56 Kbps dial-up connection than over a 10 Mbps Ethernet connection. The formula used to calculate the OSPF cost is as follows:

Cost = 100,000,000 / bandwidth in bps

As an example, the cost of a 10 Mbps Ethernet line will be 10 and the cost to cross a 1.544 Mbps T1 line will be 64.

Shortest Path Tree

To build Router A's shortest path tree for the network diagramed below, Router A is put at the root of the tree and the smallest cost link to each destination network is calculated.

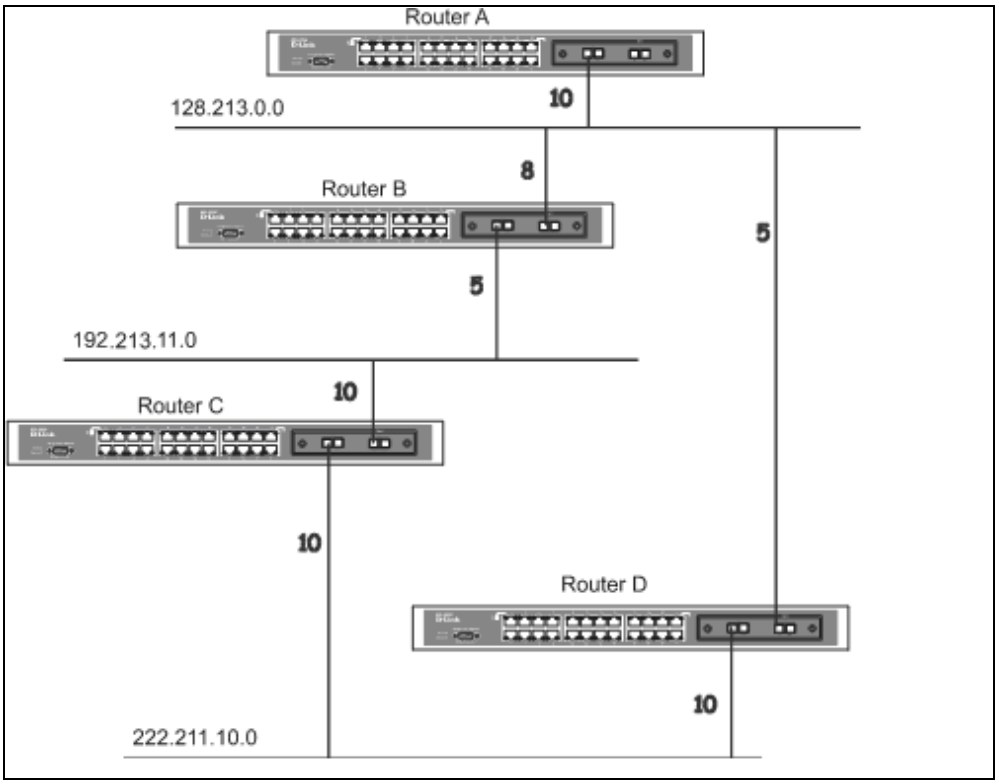


Figure 6-18 Constructing a Shortest Path Tree

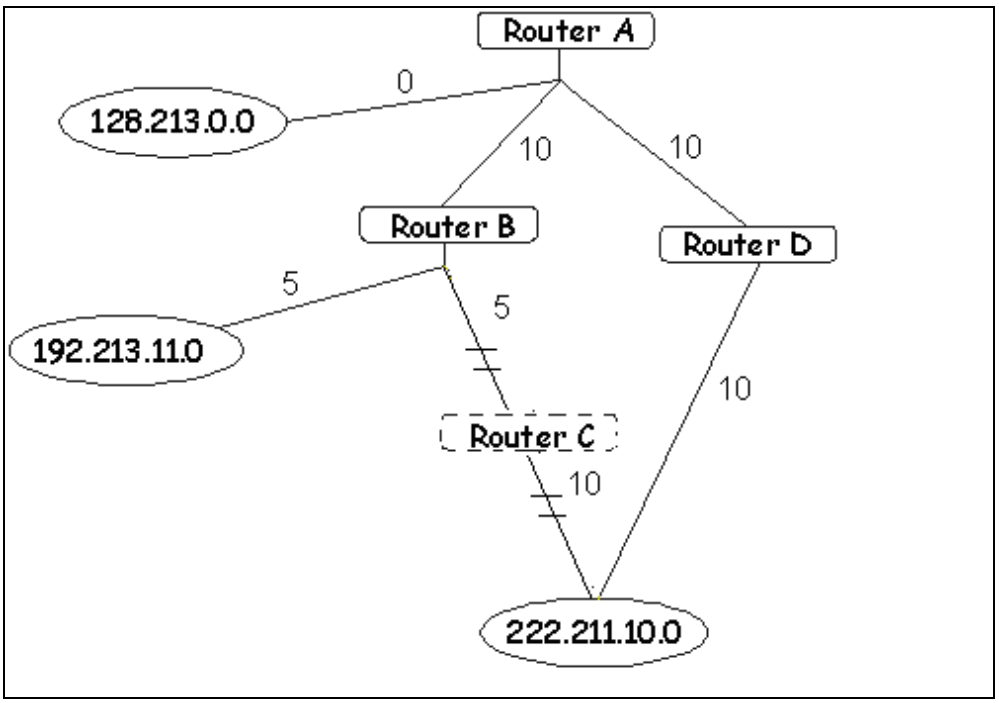


Figure 6-19 Constructing a Shortest Path Tree

The diagram above shows the network from the viewpoint of Router A. Router A can reach 192.213.11.0 through Router B with a cost of 10 + 5 = 15. Router A can reach 222.211.10.0 through Router C with a cost of 10 + 10 = 20. Router A can also reach 222.211.10.0 through Router B and Router D with a cost of 10 + 5 + 10 = 25, but the cost is higher than the route through Router C. This higher-cost route will not be included in the Router A's shortest path tree. The resulting tree will look like this:

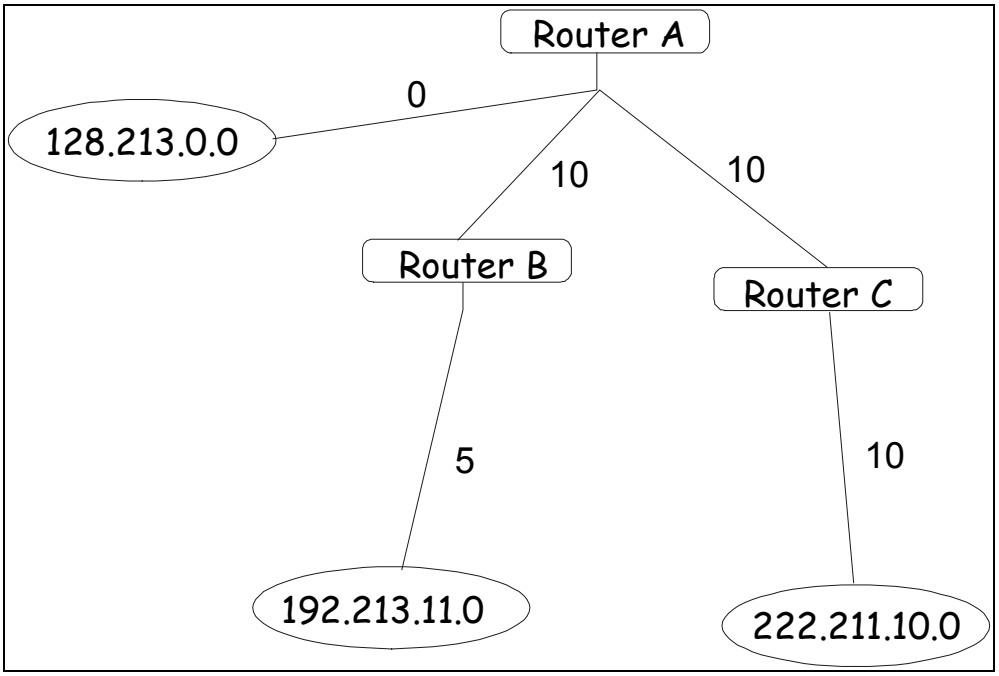


Figure 6-20 Constructing a Shortest Path Tree - Completed

Note that this shortest path tree is only from the viewpoint of Router A. The cost of the link from Router B to Router A, for instance is not important to constructing Router A's shortest path tree, but is very important when Router B is constructing its shortest path tree.

Note also that directly connected networks are reached at a cost of zero, while other networks are reached at the cost calculated in the shortest path tree.

Router A can now build its routing table using the network addresses and costs calculated in building the above shortest path tree.

Areas and Border Routers

OSPF link-state updates are forwarded to other routers by flooding to all routers on the network. OSPF uses the concept of areas to define where on the network routers that need to receive particular link-state updates are located. This helps ensure that routing updates are not flooded throughout the entire network and will reduce the amount of bandwidth consumed by updating the various router's routing tables.

Areas establish boundaries beyond which link-state updates do not need to be flooded. So the exchange of link-state updates and the calculation of the shortest path tree are limited to the area that the router is connected to.

Routers that have connections to more than one area are called Border Routers (BR). The Border Routers have the responsibility of distributing necessary routing information and changes between areas.

Areas are specific to the router interface. A router that has all of its interfaces in the same area is called an Internal Router. A router that has interfaces in multiple areas is called a Border Router. Routers that act as gateways to other networks (possibly using other routing protocols) are called Autonomous System Border Routers (ASBRs).

Link-State Packets

There are a number of different types of link-state packets, four of which are illustrated below:

1. **Router Link-State Updates** - These describe a router's links to destinations within an area.
2. **Summary Link-State Updates** - Issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).
3. **Network Link-State Updates** - Issued by multi-access areas that have more than one attached router. One router is elected as the Designated Router (DR) and this router issues the network link-state updates describing every router on the segment.
4. **External Link-State Updates** - Issued by an Autonomous System Border Router and describes routes to destinations outside the AS or a default route to the outside AS.

The format of these link-state updates is described in more detail below.

Router link-state updates are flooded to all routers in the current area. These updates describe the destinations reachable through all of the router's interfaces.

Summary link-state updates are generated by Border Routers to distribute routing information about other networks within the AS. Normally, all Summary link-state updates are forwarded to the backbone (area 0) and are then forwarded to all other areas in the network. Border Routers also have the responsibility of distributing routing information from the Autonomous System Border Router in order for routers in the network to get and maintain routes to other Autonomous Systems.

Network link-state updates are generated by a router elected as the Designated Router on a multi-access segment (with more than one attached router). These updates describe all of the routers on the segment and their network connections.

External link-state updates carry routing information to networks outside the Autonomous System. The Autonomous System Border Router is responsible for generating and distributing these updates.

OSPF Authentication

OSPF packets can be authenticated as coming from trusted routers by the use of predefined passwords. The default for routers is to use no authentication.

There are two other authentication methods: Simple Password Authentication (key) and Message Digest authentication (MD-5).

Simple Password Authentication

A password (or key) can be configured on a per-area basis. Routers in the same area that participate in the routing domain must be configured with the same key. This method is possibly vulnerable to passive attacks where a link analyzer is used to obtain the password.

Message Digest Authentication (MD-5)

MD-5 authentication is a cryptographic method. A key and a key-ID are configured on each router. The router then uses an algorithm to generate a mathematical "message digest" that is derived from the OSPF packet, the key and the key-ID. This message digest (a number) is then appended to the packet. The key is not exchanged over the wire and a non-decreasing sequence number is included to prevent replay attacks.

Backbone and Area 0

OSPF limits the number of link-state updates required between routers by defining areas within which a given router operates. When more than one area is configured, one area is designated as area 0, also called the backbone.

The backbone is at the center of all other areas, all areas of the network have a physical (or virtual) connection to the backbone through a router. OSPF allows routing information to be distributed by forwarding it into area 0, from which the information can be forwarded to all other areas (and all other routers) on the network.

In situations where an area is required, but is not possible to provide a physical connection to the backbone, a virtual link can be configured.

Virtual Links

Virtual links accomplish two purposes:

1. Linking an area that does not have a physical connection to the backbone.
2. Patching the backbone in case there is a discontinuity in area 0.

Areas Not Physically Connected to Area 0

All areas of an OSPF network should have a physical connection to the backbone, but in some cases it is not possible to physically connect a remote area to the backbone. In these cases, a virtual link is configured to connect the remote area to the backbone. A virtual path is a logical path between two border routers that have a common area, with one border router connected to the backbone.

Partitioning the Backbone

OSPF also allows virtual links to be configured to connect the parts of the backbone that are discontinuous. This is the equivalent to linking different area 0s together using a logical path between each area 0. Virtual links can also be added for redundancy to protect against a router failure. A virtual link is configured between two border routers that both have a connection to their respective area 0s.

Neighbors

Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers.

Any two routers must meet the following conditions before they become neighbors:

1. **Area ID** - Two routers having a common segment □ their interfaces have to belong to the same area on that segment. Of course, the interfaces should belong to the same subnet and have the same subnet mask.
2. **Authentication** - OSPF allows for the configuration of a password for a specific area. Two routers on the same segment and belonging to the same area must also have the same OSPF password before they can become neighbors.
3. **Hello and Dead Intervals** - The Hello interval specifies the length of time, in seconds, between the hello packets that a router sends on an OSPF interface. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the OSPF router down. OSPF routers exchange Hello packets on each segment in order to acknowledge each other's existence on a segment and to elect a Designated Router on multi-access segments. OSPF requires these intervals to be exactly the same between any two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
4. **Stub Area Flag** - Any two routers also must have the same stub area flag in their Hello packets in order to become neighbors.

Adjacencies

Adjacent routers go beyond the simple Hello exchange and participate in the link-state database exchange process. OSPF elects one router as the Designated Router (DR) and a second router as the Backup Designated Router (BDR) on each multi-access segment (the BDR is a backup in case of a DR failure). All other routers on the segment will then contact the DR for link-state database updates and exchanges. This limits the bandwidth required for link-state database updates.

Designated Router Election

The election of the DR and BDR is accomplished using the Hello protocol. The router with the highest OSPF priority on a given multi-access segment will become the DR for that segment. In case of a tie, the router with the highest Router ID wins. The default OSPF priority is 1. A priority of zero indicates a router that cannot be elected as the DR.

Building Adjacency

Two routers undergo a multi-step process in building the adjacency relationship. The following is a simplified description of the steps required:

- **Down** - No information has been received from any router on the segment.
- **Attempt** - On non-broadcast multi-access networks (such as Frame Relay or X.25), this state indicates that no recent information has been received from the neighbor. An effort should be made to contact the neighbor by sending Hello packets at the reduced rate set by the Poll Interval.
- **Init** - The interface has detected a Hello packet coming from a neighbor but bi-directional communication has not yet been established.
- **Two-way** - Bi-directional communication with a neighbor has been established. The router has seen its address in the Hello packets coming from a neighbor. At the end of this stage the DR and BDR election would have been done. At the end of the Two-way stage, routers will decide whether to proceed in building an adjacency or not. The decision is based on whether one of the routers is a DR or a BDR or the link is a point-to-point or virtual link.
- **Exstart** - (Exchange Start) Routers establish the initial sequence number that is going to be used in the information exchange packets. The sequence number insures that routers always get the most recent

information. One router will become the primary and the other will become secondary. The primary router will poll the secondary for information.

- **Exchange** - Routers will describe their entire link-state database by sending database description packets.
- **Loading** - The routers are finalizing the information exchange. Routers have link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated will be put on the request list. Any update that is sent will be put on the retransmission list until it gets acknowledged.
- **Full** - The adjacency is now complete. The neighboring routers are fully adjacent. Adjacent routers will have the same link-state database.

Adjacencies on Point-to-Point Interfaces

OSPF Routers that are linked using point-to-point interfaces (such as serial links) will always form adjacencies. The concepts of DR and BDR are unnecessary.

OSPF Packet Formats

All OSPF packet types begin with a standard 24-byte header and there are five packet types. The header is described first, and each packet type is described in a subsequent section.

All OSPF packets (except for Hello packets) forward link-state advertisements. Link-State Update packets, for example, flood advertisements throughout the OSPF routing domain.

- OSPF packet header
- Hello packet
- Database Description packet
- Link-State Request packet
- Link-State Update packet
- Link-State Acknowledgment packet

OSPF Packet Header

Every OSPF packet is preceded by a common 24-byte header. This header contains the information necessary for a receiving router to determine if the packet should be accepted for further processing.

The format of the OSPP packet header is shown below:

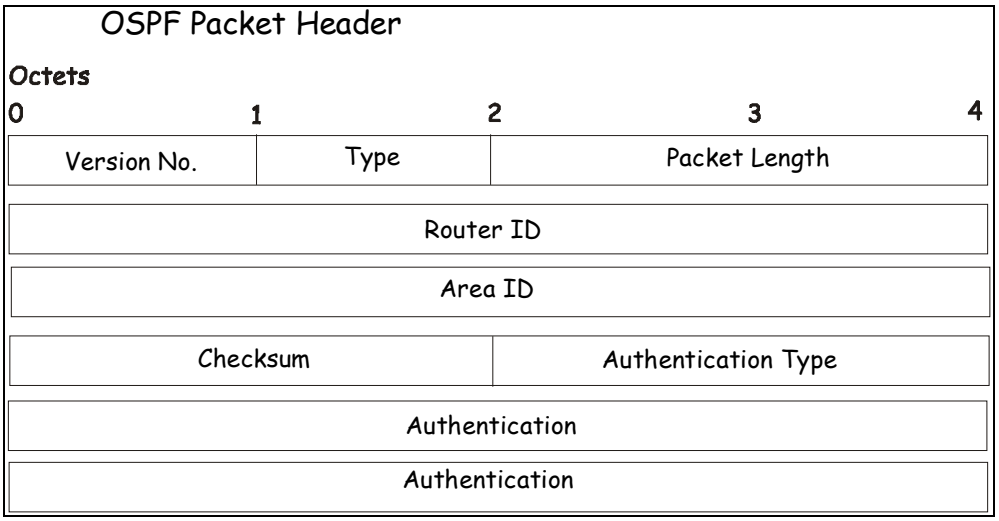


Figure 6-21 OSPF Packet Header Format

Parameter	Description
Version No.	The OSPF version number.
Type	The OSPF packet type. The OSPF packet types are as follows: Type Description Hello Database Description Link-State Request Link-State Update Link-State Acknowledgment.
Packet Length	The length of the packet in bytes. This length includes the 24-byte header.
Router ID	The Router ID of the packet's source.
Area ID	A 32-bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Packets traversing a virtual link are assigned the backbone Area ID of 0.0.0.0
Checksum	A standard IP checksum that includes all of the packet's contents except for the 64-bit authentication field.
Authentication Type	The type of authentication to be used for the packet.
Authentication	A 64-bit field used by the authentication scheme.

Hello Packet

Hello packets are OSPF packet type 1. They are sent periodically on all interfaces, including virtual links, in order to establish and maintain neighbor relationships. In addition, Hello Packets are multicast on those physical networks having a multicast or broadcast capability, enabling dynamic discovery of neighboring routers.

All routers connected to a common network must agree on certain parameters such as the Network Mask, the Hello Interval, and the Router Dead Interval. These parameters are included in the hello packets, so that differences can inhibit the forming of neighbor relationships. A detailed explanation of the receive process for Hello packets is necessary so that differences cannot inhibit the forming of neighbor relationships.

The format of the Hello packet is shown below:

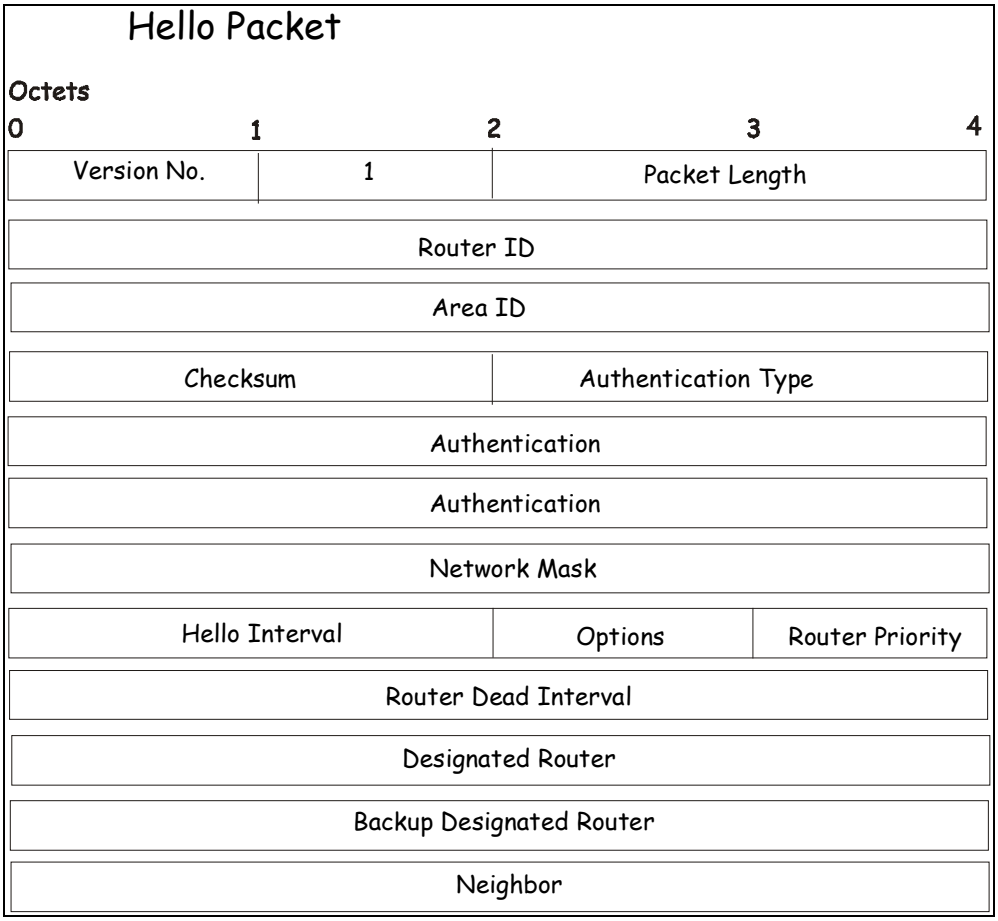


Figure 6-22 Hello Packet

Parameter	Description
Network Mask	The network mask associated with this interface.
Options	The optional capabilities supported by the router.
Hello Interval	The number of seconds between this router's Hello packets.
Router Priority	This router's Router Priority. The Router Priority is used in the election of the DR and BDR. If this field is set to 0, the router is ineligible to become the DR or the BDR.
Router Dead Interval	The number of seconds that must pass before declaring a silent router as down.
Designated Router	The identity of the DR for this network, in the view of the advertising router. The DR is identified here by its IP interface address on the network.
Backup Designated Router	The identity of the Backup Designated Router (BDR) for this network. The BDR is identified here by its IP interface address on the network. This field is set to 0.0.0.0 if there is no BDR.
Neighbor	The Router IDs of each router from whom valid Hello packets have been seen within the Router Dead Interval on the network.

Database Description Packet

Database Description packets are OSPF packet type 2. These packets are exchanged when an adjacency is being initialized. They describe the contents of the topological database. Multiple packets may be used to describe the database. For this purpose, a poll-response procedure is used. One of the routers is designated to be master, the other a slave. The master seconds Database Description packets (polls) that are acknowledged by Database Description packets sent by the slave (responses). The responses are linked to the polls via the packets' DD sequence numbers.

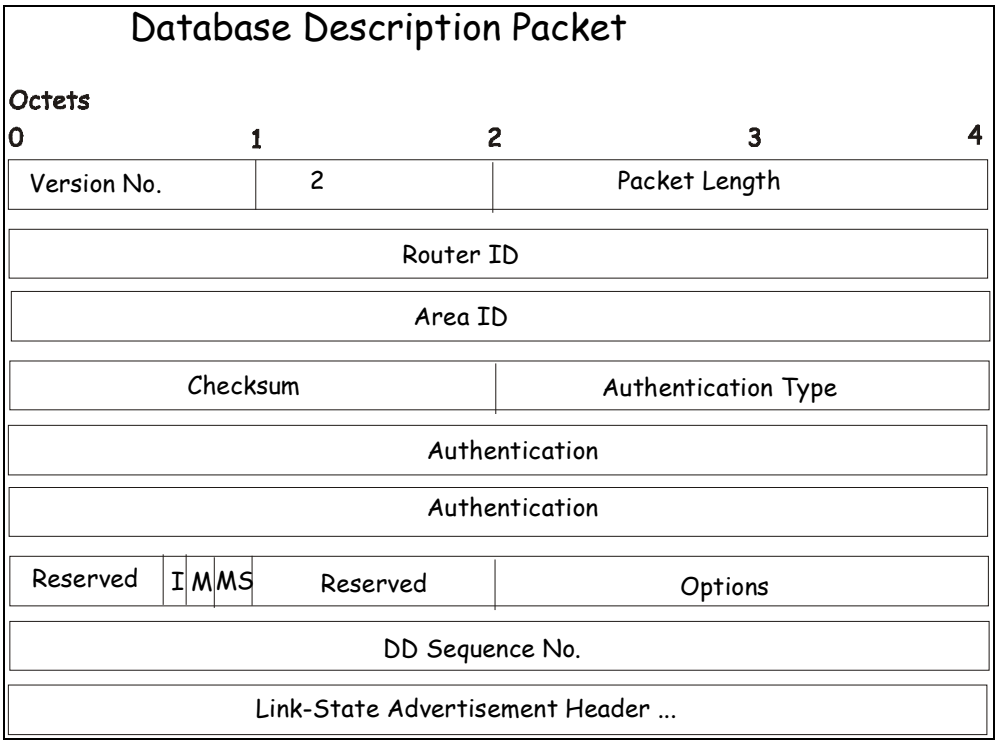


Figure 6-23 Database Description Packet

Parameter	Description
Options	The optional capabilities supported by the router.
I-bit	The Initial bit. When set to 1, this packet is the first in the sequence of Database Description packets.
M-bit	The More bit. When set to 1, this indicates that more Database Description packets will follow.
MS-bit	The Master Slave bit. When set to 1, this indicates that the router is the master during the Database Exchange process. A zero indicates the opposite.
DD Sequence Number	User to sequence the collection of Database Description Packets. The initial value (indicated by the Initial bit being set) should be unique. The DD sequence number then increments until the complete database description has been sent.

The rest of the packet consists of a list of the topological database's pieces. Each link state advertisement in the database is described by its link state advertisement header.

Link-State Request Packet

Link-State Request packets are OSPF packet type 3. After exchanging Database Description packets with a neighboring router, a router may find that parts of its topological database are out of date. The Link-State Request packet is used to request the pieces of the neighbor's database that are more up to date. Multiple Link-State Request packets may need to be used. The sending of Link-State Request packets is the last step in bringing up an adjacency.

A router that sends a Link-State Request packet has in mind the precise instance of the database pieces it is requesting, defined by LS sequence number, LS checksum, and LS age, although these fields are not specified in the Link-State Request packet itself. The router may receive even more recent instances in response.

The format of the Link-State Request packet is shown below:

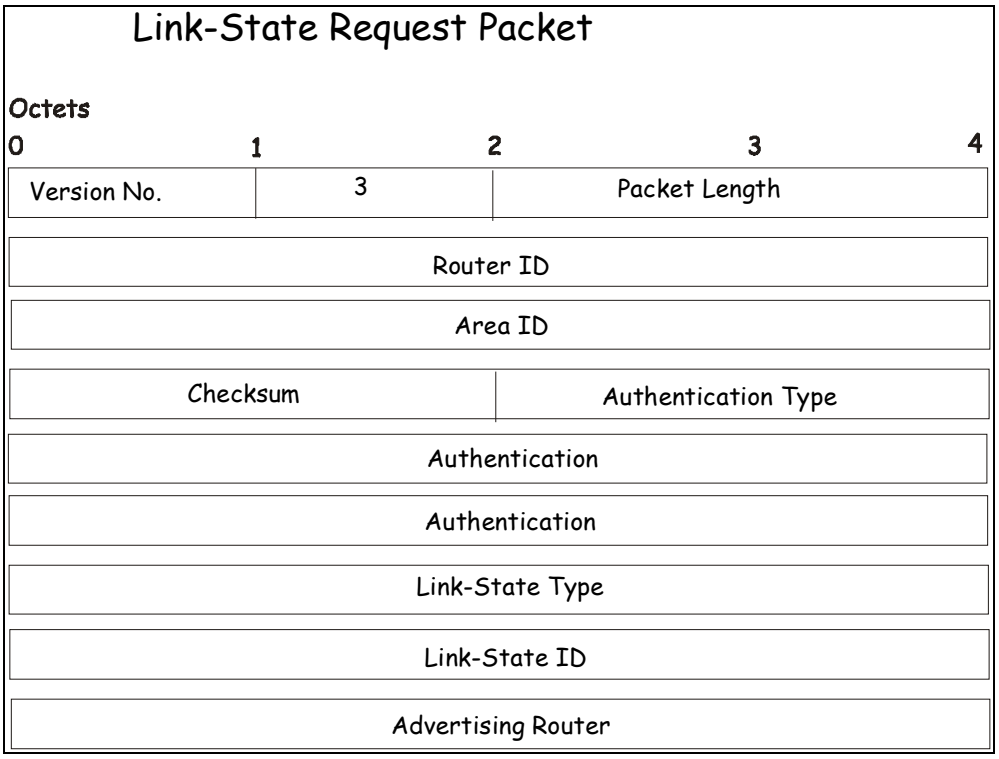


Figure 6-24 Link-State Request Packet

Each advertisement requested is specified by its Link-State Type, Link-State ID, and Advertising Router. This uniquely identifies the advertisement, but not its instance. Link-State Request packets are understood to be requests for the most recent instance.

Link-State Update Packet

Link-State Update packets are OSPF packet type 4. These packets implement the flooding of link-state advertisements. Each Link-State Update packet carries a collection of link-state advertisements one hop further from its origin. Several link-state advertisements may be included in a single packet.

Link-State Update packets are multicast on those physical networks that support multicast/broadcast. In order to make the flooding procedure reliable, flooded advertisements are acknowledged in Link-State Acknowledgment packets. If retransmission of certain advertisements is necessary, the retransmitted advertisements are always carried by unicast Link-State Update packets.

The format of the Link-State Update packet is shown below:

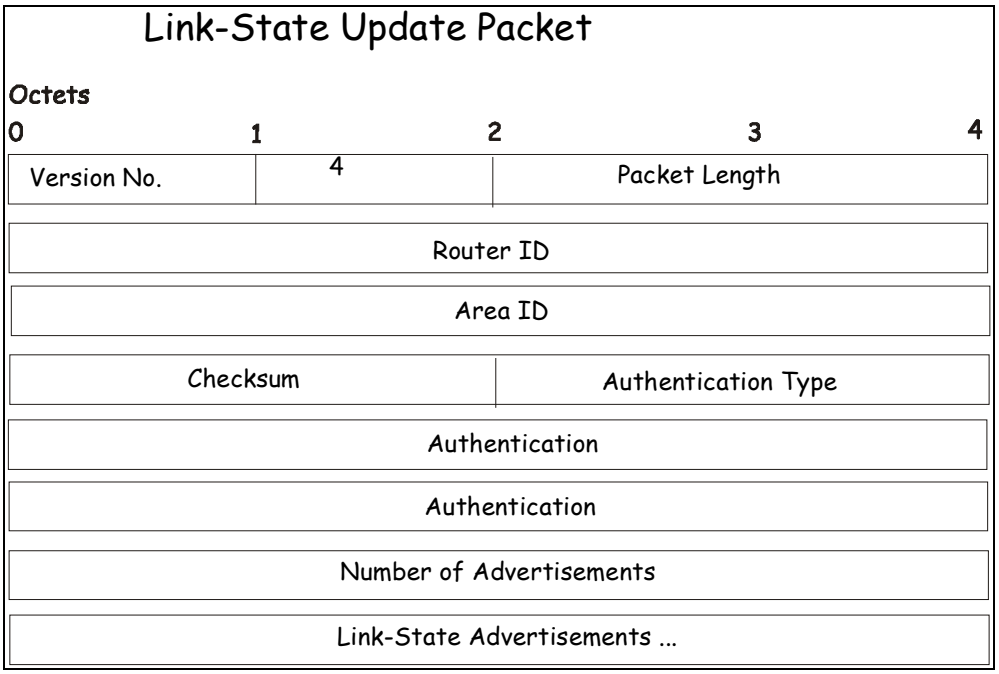


Figure 6-25 Link-State Update Packet

The body of the Link-State Update packet consists of a list of link-state advertisements. Each advertisement begins with a common 20-byte header, the link-state advertisement header. Otherwise, the format of each of the five types of link-state advertisements is different.

Link-State Acknowledgment Packet

Link-State Acknowledgment packets are OSPF packet type 5. To make the folding of link-state advertisements reliable, flooded advertisements are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link-State Acknowledgment packets. Multiple link-state advertisements can be acknowledged in a single Link-State Acknowledgment packet.

Depending on the state of the sending interface and the source of the advertisements being acknowledged, a Link-State Acknowledgment packet is sent either to the multicast address AllSPFRouters, to the multicast address AllDRouters, or as a unicast packet.

The format of this packet is similar to that of the Data Description packet. The body of both packets is simply a list of link-state advertisement headers.

The format of the Link-State Acknowledgment packet is shown below:

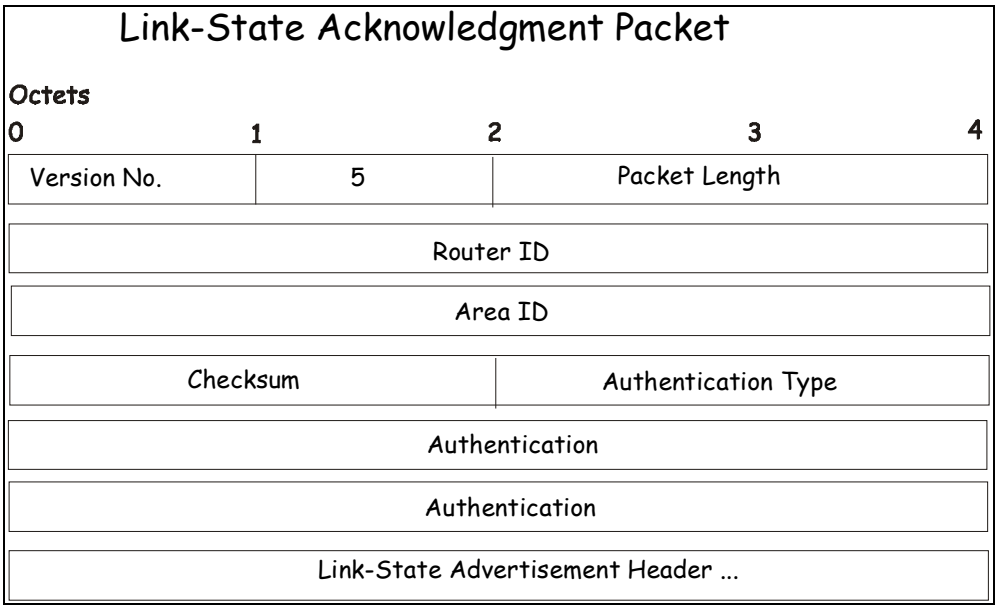


Figure 6-26 Link State Acknowledge Packet

Each acknowledged link-state advertisement is described by its link-state advertisement header. It contains all the information required to uniquely identify both the advertisement and the advertisement's current instance.

Link-State Advertisement Formats

There are five distinct types of link-state advertisements. Each link-state advertisement begins with a standard 20-byte link-state advertisement header. Succeeding sections then diagram the separate link-state advertisement types.

Each link-state advertisement describes a piece of the OSPF routing domain. Every router originates a router links advertisement. In addition, whenever the router is elected as the Designated Router, it originates a network links advertisement. Other types of link-state advertisements may also be originated. The flooding algorithm is reliable, ensuring that all routers have the same collection of link-state advertisements. The collection of advertisements is called the link-state (or topological) database.

From the link-state database, each router constructs a shortest path tree with itself as root. This yields a routing table. There are four types of link state advertisements, each using a common link state header. These are:

1. Router Links Advertisements
2. Network Links Advertisements
3. Summary Link Advertisements
4. Autonomous System Link Advertisements

Link State Advertisement Header

All link state advertisements begin with a common 20-byte header. This header contains enough information to uniquely identify the advertisements (Link State Type, Link State ID, and Advertising Router). Multiple instances of the link state advertisement may exist in the routing domain at the same time. It is then necessary to determine which instance is more recent. This is accomplished by examining the link state age, link state sequence number and link state checksum fields that are also contained in the link state advertisement header.

The format of the Link State Advertisement Header is shown below:

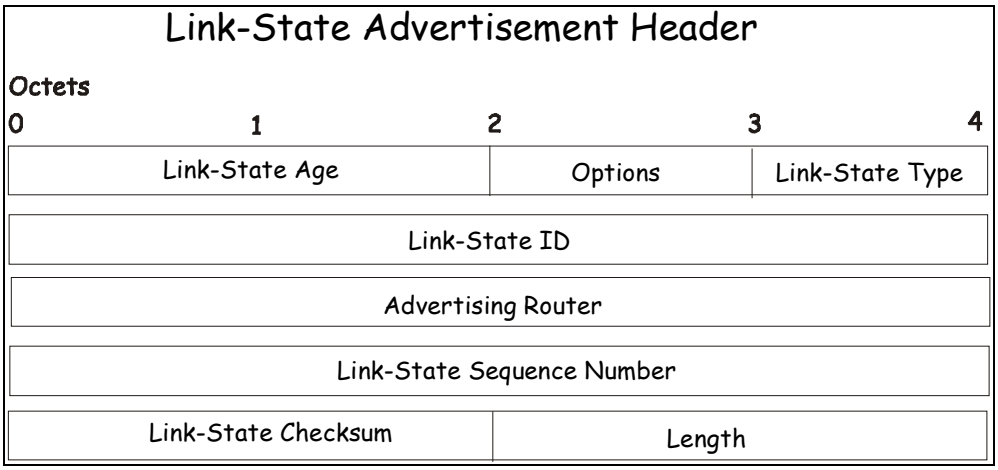


Figure 6-27 Link State Advertisement Header

Parameter	Description
Link State Age	The time is seconds since the link state advertisement was originated.
Options	The optional capabilities supported by the described portion of the routing domain.
Link State Type	The type of the link state advertisement. Each link state type has a separate advertisement format. The link state types are as follows: Router Links, Network Links, Summary Link (IP Network), Summary Link (ASBR), AS External Link.
Link State ID	This field identifies the portion of the internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's Link State Type.
Advertising Router	The Router ID of the router that originated the Link State Advertisement. For example, in network links advertisements this field is set to the Router ID of the network's Designated Router.
Link State Sequence Number	Detects old or duplicate link state advertisements. Successive instances of a link state advertisement are given successive Link State Sequence numbers.
Link State Checksum	The Fletcher checksum of the complete contents of the link state advertisement, including the link state advertisement header by accepting the Link State Age field.
Length	The length in bytes of the link state advertisement. This includes the 20-byte link state advertisement header.

Router Links Advertisements

Router links advertisements are type 1 link state advertisements. Each router in an area originates a routers links advertisement. The advertisement describes the state and cost of the router's links to the area. All of the router's links to the area must be described in a single router links advertisement.

The format of the Router Links Advertisement is shown below:

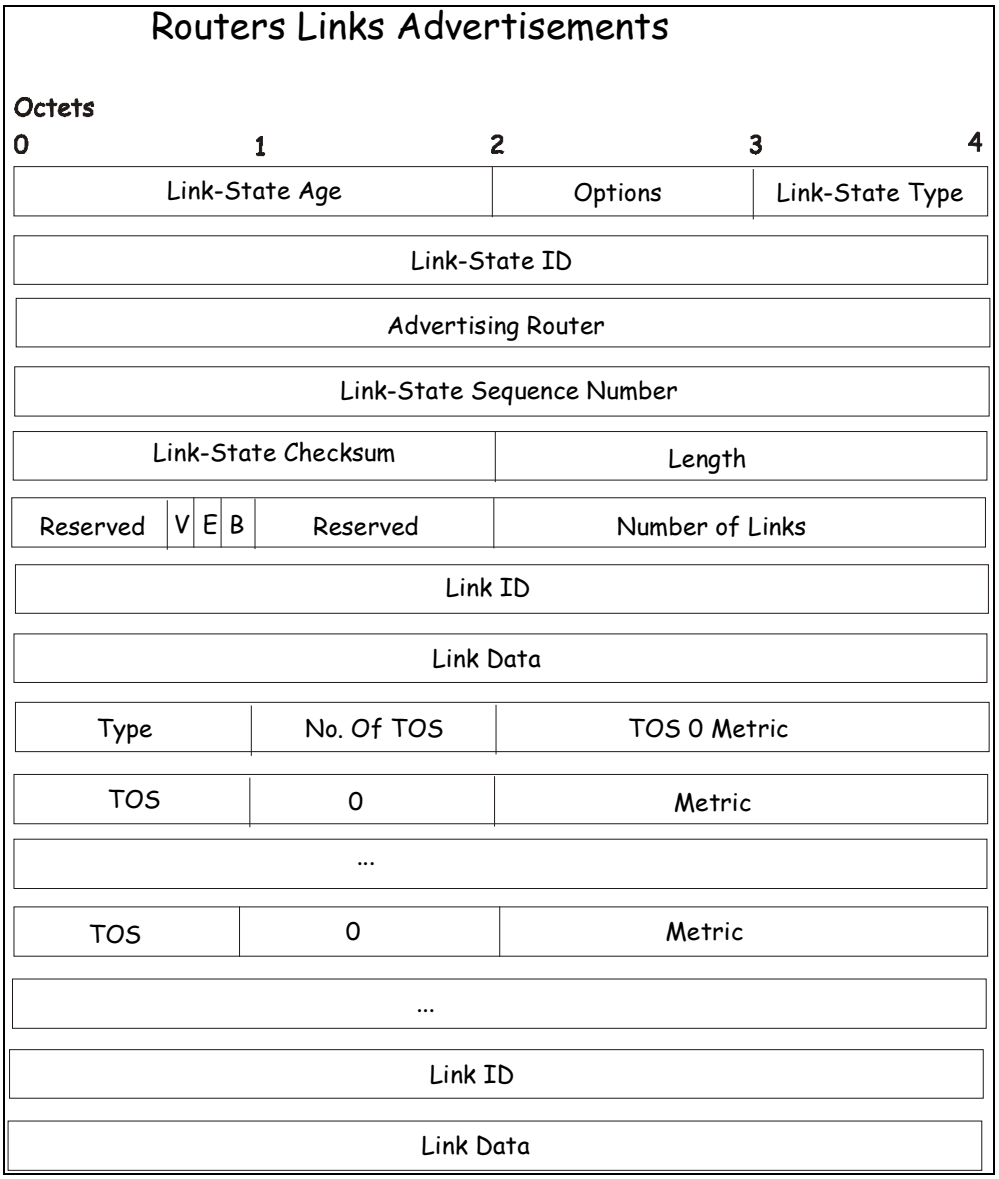


Figure 6-28 Routers Links Advertisements

In router links advertisements, the Link State ID field is set to the router's OSPF Router ID. The T-bit is set in the advertisement's Option field if and only if the router is able to calculate a separate set of routes for each IP Type of Service (TOS). Router links advertisements are flooded throughout a single area only.

Parameter	Description
V-bit	When set, the router is an endpoint of an active virtual link that is using the described area as a Transit area (V is for Virtual link endpoint).
E-bit	When set, the router is an Autonomous System (AS) boundary router (E is for External).
B-bit	When set, the router is an area border router (B is for Border).
Number of Links	The number of router links described by this advertisement. This must be the total collection of router links to the area.

The following fields are used to describe each router link. Each router link is typed. The Type field indicates the kind of link being described. It may be a link to a transit network, to another router or to a stub network. The values of all the other fields describing a router link depend on the link's Type. For example, each link has an associated 32-bit data field. For links to stub networks, this field specifies the network's IP address mask. For other link types, the Link Data specifies the router's associated IP interface address.

Parameter	Description
Type	A quick classification of the router link. One of the following: Type Description: Point-to-point connection to another router. Connection to a transit network. Connection to a stub network. Virtual link.
Link ID	Identifies the object that this router link connects to. Value depends on the link's Type. When connecting to an object that also originates a link state advertisement (i.e. another router or a transit network) the Link ID is equal to the neighboring advertisement's Link State ID. This provides the key for looking up an advertisement in the link state database. Type Link ID: Neighboring router's Router ID. IP address of Designated Router. IP network/subnet number. Neighboring router's Router ID
Link Data	Contents again depend on the link's Type field. For connections to stub networks, it specifies the network's IP address mask. For unnumbered point-to-point connection, it specifies the interface's MIB-II ifIndex value. For other link types it specifies the router's associated IP interface address. This latter piece of information is needed during the routing table build process, when calculating the IP address of the next hop.
No. of TOS	The number of different Type of Service (TOS) metrics given for this link, not counting the required metric for TOS 0. If no additional TOS metrics are given, this field should be set to 0.
TOS 0 Metric	The cost of using this router link for TOS 0.

For each link, separate metrics may be specified for each Type of Service (ToS). The metric for ToS 0 must always be included, and was discussed above. Metrics for non-zero TOS are described below. Note that the cost for non-zero ToS values that are not specified defaults to the ToS 0 cost. Metrics must be listed in order of increasing TOS encoding. For example, the metric for ToS 16 must always follow the metric for ToS 8 when both are specified.

Parameter	Description
ToS	IP Type of Service that this metric refers to.
Metric	The cost of using this outbound router link, for traffic of the specified TOS.

Network Links Advertisements

Network links advertisements are Type 2 link state advertisements. A network links advertisement is originated for each transit network in the area. A transit network is a multi-access network that has more than one attached router. The network links advertisement is originated by the network's Designated Router. The advertisement describes all routers attached to the network, including the Designated Router itself. The advertisement's Link State ID field lists the IP interface address of the Designated Router.

The distance from the network to all attached routers is zero, for all ToS. This is why the ToS and metric fields need not be specified in the network links advertisement.

The format of the Network Links Advertisement is shown below:

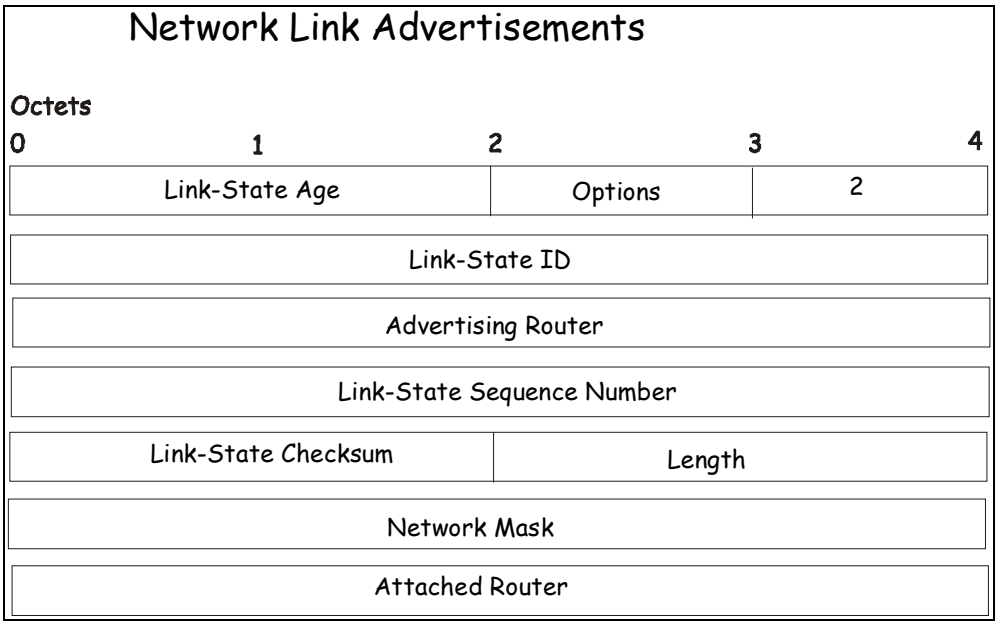


Figure 6-29 Network Link Advertisements

Parameter	Description
Network Mask	The IP address mask for the network.
Attached Router	The Router IDs of each of the routers attached to the network. Only those routers that are fully adjacent to the Designated Router (DR) are listed. The DR includes itself in this list.

Summary Link Advertisements

Summary link advertisements are Type 3 and 4 link state advertisements. These advertisements are originated by Area Border routers. A separate summary link advertisement is made for each destination known to the router that belongs to the Autonomous System (AS), yet is outside the area.

Type 3 link state advertisements are used when the destination is an IP network. In this case, the advertisement's Link State ID field is an IP network number. When the destination is an AS boundary router, a Type 4 advertisement is used, and the Link State ID field is the AS boundary router's OSPF Router ID. Other that the difference in the Link State ID field, the format of Type 3 and 4 link state advertisements are identical.

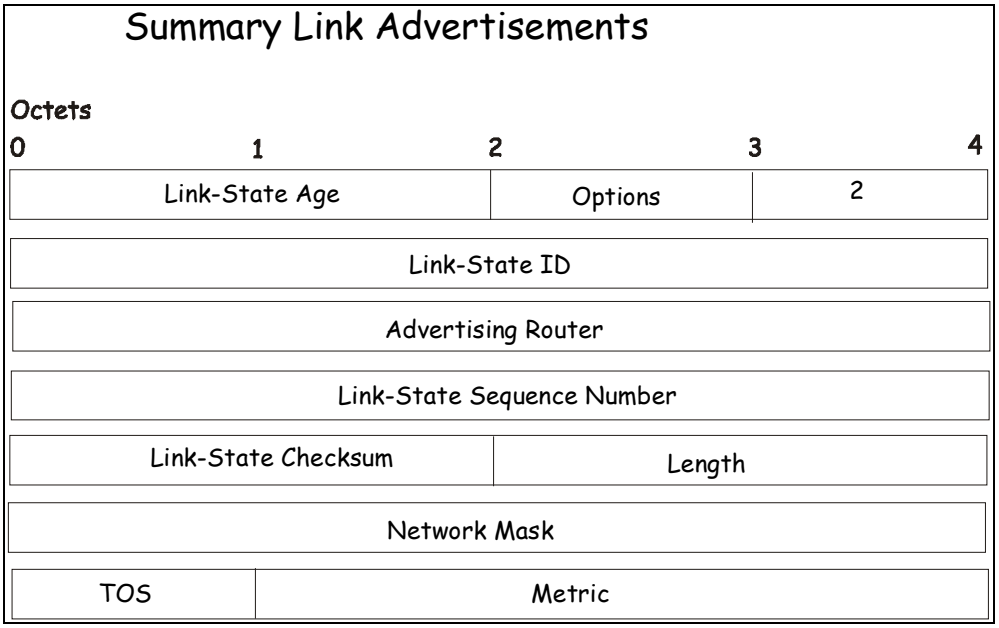


Figure 6-30 Summary Link Advertisements

For stub area, Type 3 summary link advertisements can also be used to describe a default route on a per-area basis. Default summary routes are used in stub area instead of flooding a complete set of external routes. When describing a default summary route, the advertisement' s Link State ID is always set to the Default Destination □ 0.0.0.0, and the Network Mask is set to 0.0.0.0.

Separate costs may be advertised for each IP Type of Service. Note that the cost for ToS 0 must be included, and is always listed first. If the T-bit is reset in the advertisement's Option field, only a route for ToS 0 is described by the advertisement. Otherwise, routes for the other ToS values are also described. If a cost for a certain ToS is not included, its cost defaults to that specified for ToS 0.

Parameter	Description
Network Mask	For Type 3 link state advertisements, this indicates the destination network's IP address mask. For example, when advertising the location of a class A network the value 0xff000000.
ToS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. Expressed in the same units as the interface costs in the router links advertisements.

Autonomous Systems External Link Advertisements

Autonomous Systems (AS) link advertisements are Type 5 link state advertisements. These advertisements are originated by AS boundary routers. A separate advertisement is made for each destination known to the router that is external to the AS.

AS external link advertisements usually describe a particular external destination. For these advertisements the Link State ID field specifies an IP network number. AS external link advertisements are also used to describe a default route. Default routes are used when no specific route exists to the destination. When describing a default route, the Link State ID is always set with the Default Destination address (0.0.0.0) and the Network Mask is set to 0.0.0.0.

The format of the AS External Link Advertisement is shown below:

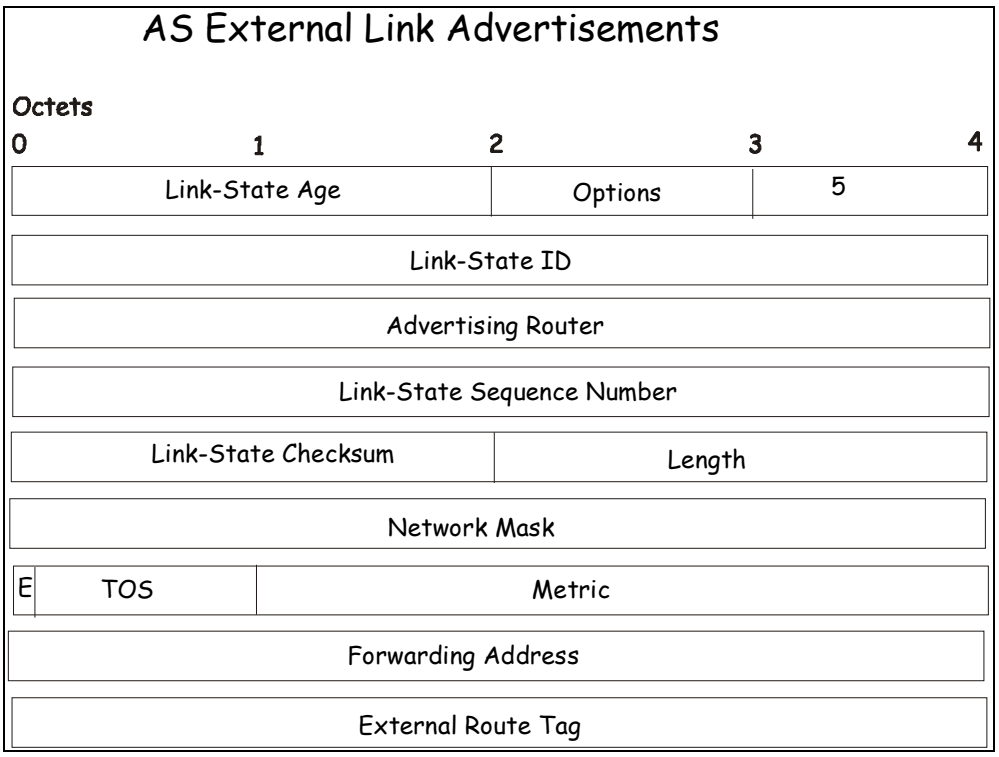


Figure 6-31 AS External Link Advertisements

Parameter	Description
Network Mask	The IP address mask for the advertised destination.
E-bit	The type of external metric. If the E-bit is set, the metric specified is a Type 2 external metric. This means the metric is considered larger than any link state path. If the E-bit is zero, the specified metric is a Type 1 external metric. This means that is comparable directly to the link state metric.
Forwarding Address	Data traffic for the advertised destination will be forwarded to this address. If the Forwarding Address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. The interpretation of this metric depends on the external type indication (the E - bit above).
External Route Tag	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

Including the NSSA

The NSSA or Not So Stubby Area is a feature that has been added to OSPF so external routes from ASs (Autonomous Systems) can be imported into the OSPF area. As an extension of stub areas, the NSSA feature uses a packet translation system used by BRs (Border Routers) to translate outside routes into the OSPF area.

Consider the following example:

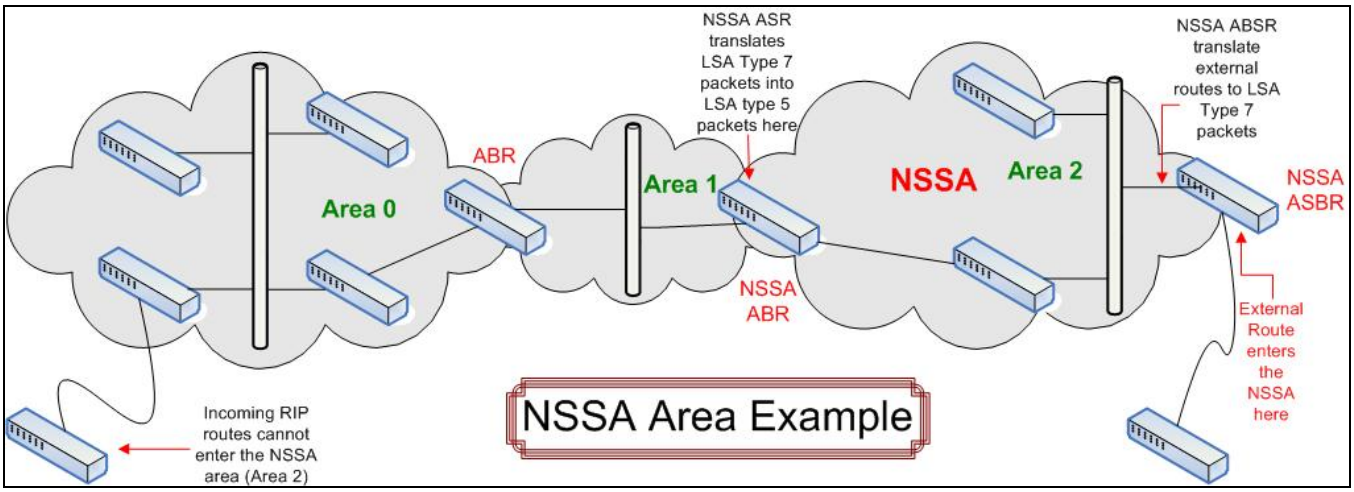


Figure 6-32 NSSA Area example

The NSSA ASBR (Not So Stubby Area Autonomous System Border Router) is receiving External Route information and translating it as an LSA Type-7 packet that will be distributed ONLY to switches within the NSSA (Area 2 in the example above). For this route's information to enter another area, the LSA Type-7 packet has to be translated into an LSA Type-5 packet by the NSSA ABR (Area Border Router) and then is distributed to other switches within the other OSPF areas (Area 1 and 2 in the example above). Once completed, new routes are learned and new shortest routes will be determined.

To alleviate any problems with OSPF summary routing due to new routes and packets, all NSSA area border routers (ABR) must support optional importing of LSA type-3 summary packets into the NSSA.

Type-7 LSA Packets

Type-7 LSA (Link State Advertisement) packets are used to import external routes into the NSSA. These packets can originate from NSSA ASBRs or NSSA ABRs and are defined by setting the P-Bit in the LSA type-7 packet header. Each destination network learned from external routes is converted into Type-7 LSA packets. These packets are specific for NSSA switches and the route information contained in these packets cannot leave the area unless translated into Type-5 LSA packets by Area Border Routers. See the following table for a better description of the LSA type-7 packet seen here.

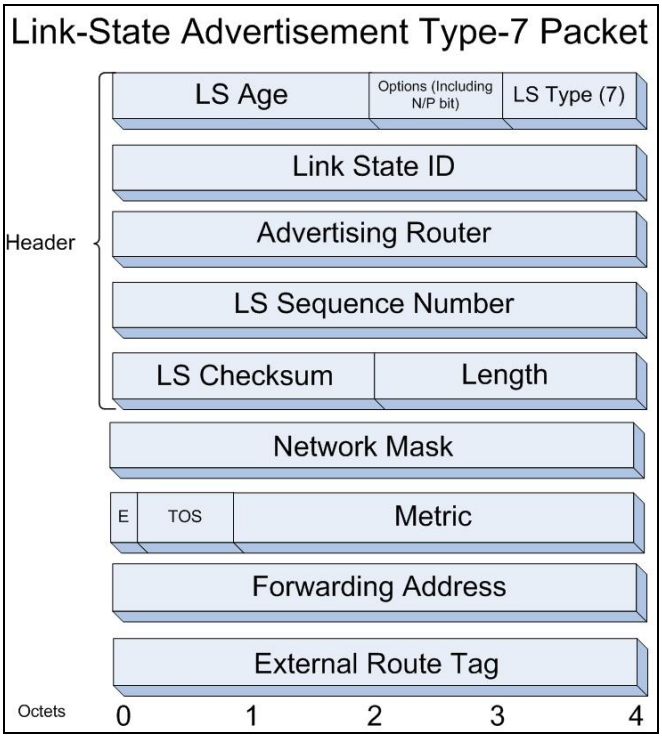


Figure 6-33 LSA Type-7 Packet

Parameter	Description
Link State Packet Header	This field will hold information concerning information regarding the LS Checksum, length, LS sequence number, Advertising Router, Link State ID, LS age, the packet type (Type-7), and the options field. The Options byte contains information regarding the N-Bit and the P-Bit, which will be described later in this section.
Network Mask	The IP address mask for the advertised destination.
E-bit	The type of external metric. If the E-bit is set, the metric specified is a Type 2 external metric. This means the metric is considered larger than any link state path. If the E-bit is zero, the specified metric is a Type 1 external metric. This means that is comparable directly to the link state metric.
Forwarding Address	Data traffic for the advertised destination will be forwarded to this address. If the Forwarding Address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator. Yet, if the network between the NSSA ASBR and the adjacent AS is advertised in the area as an internal OSFP route, this address will be the next hop address. Conversely, if the network is not advertised as internal, this field should be any of the router's active OSPF interfaces.
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. The interpretation of this metric depends on the external type indication (the E-bit above).
External Route Tag	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

The N-Bit

Contained in the options field of the Link State Packet header, the N-Bit is used to ensure that all members of an NSSA agree on the area configurations. Used in conjunction with the E-Bit, these two bits represent the flooding capability of an external LSA. Because type-5 LSAs cannot be flooded into the NSSA, the N-Bit will contain information for sending and receiving LSA type-7 packets, while the E-bit is to be cleared. An additional check must be created for the function that accepts these packets to verify these two bits (N and E-Bit). Bits matching the checking feature will be accepted, while other bit combinations will be dropped.

The P-Bit

Also included in the Options field of the LSA type-7 packet, the P-Bit (propagate) is used to define whether or not to translate the LSA type-7 packet into an LSA type-5 packet for distribution outside the NSSA.

LSA Type-7 Packet Features

- LSA Type-7 address ranges for OSPF areas are defined as a pair, consisting of an IP address and a mask. The packet will also state whether or not to advertise and it will also contain an external route tag.
- The NSSA ASBR will translate external routes into type-7 LSAs to be distributed on the NSSA. NSSA ABRs will optionally translate these type-7 packets into type-5 packets to be distributed among other OSPF areas. These type-5 packets are indiscernible from other type-5 packets. The NSSA does not support type-5 LSAs.
- Once border routers of the NSSA have finished translating or grouping type-7 LSAs into type-5 LSAs, type-5 LSAs should be flushed or reset as a translation or an aggregation of other type-7 LSAs.
- The forwarding addresses contained in translated type-5 LSAs must be set, with the exception of an LSA address range match.

OSPFv2

OSPF Global Settings

This window is used to configure the OSPF Global settings for this Switch.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Global Settings**, as shown below:

Figure 6-34 OSPF Global Settings window

The fields that can be configured are described below:

Parameter	Description
OSPF State	Specifies to enable or disable the OSPF global state.
OSPF Router ID	A 32-bit number (in the same format as an IP address - xxx.xxx.xxx.xxx) that uniquely identifies the Switch in the OSPF domain. It is common to assign the highest IP address assigned to the Switch (router).

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

OSPF Area Settings

This window is used to configure the OSPF Area settings for this Switch. OSPF allows collections of contiguous networks and hosts to be grouped together. Such a group, together with the routers having interfaces to any one of the included networks, is called an area.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Area Settings**, as shown below:

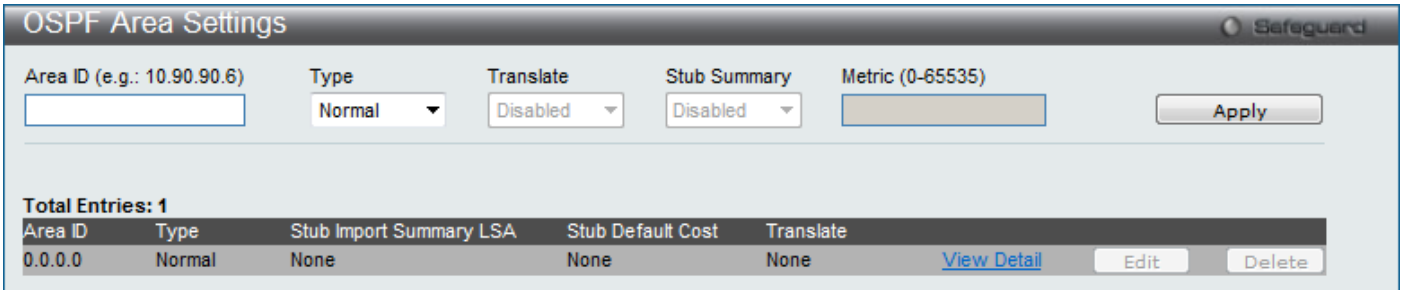


Figure 6-35 OSPF Area Settings window

The fields that can be configured are described below:

Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	OSPF area operation *Normal*, *Stub*, or *NSSA*. In some Autonomous Systems, the majority of the topological database may consist of AS external advertisements. An OSPF AS external advertisement is usually flooded throughout the entire AS. However, OSPF allows certain areas to be configured as "stub areas". AS external advertisements are not flooded into or throughout stub areas. Routing to AS external destinations in these areas is based on a (per-area) default only. This reduces the topological database size, and therefore the memory requirements, for a stub area's internal routers.
Translate	Use the pull-down menu to enable or disable the translating of Type-7 LSAs into Type-5 LSAs, so that they can be distributed outside of the NSSA. The default is Disabled. This field can only be configured if NSSA is chosen in the Type field.
Stub Summary	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Metric (0-65535)	Enter the metric (1 - 65535; 0 for auto cost) of this area. For NSSA areas, the metric field determines the cost of traffic entering the NSSA area.

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

Click the View Detail link to view a display of the OSPF Area settings.

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

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

After click the View Detail link, the following page will be displayed.

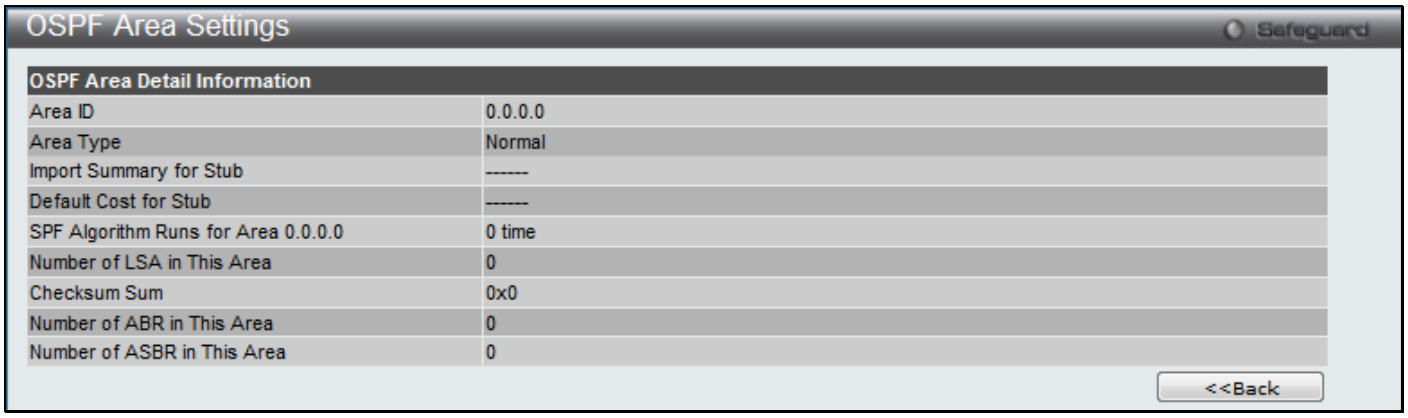


Figure 6-36 OSPF Area Settings – View Detail window

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

OSPF Interface Settings

This window is used to configure the OSPF Interface settings for this Switch.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Interface Settings**, as shown below:

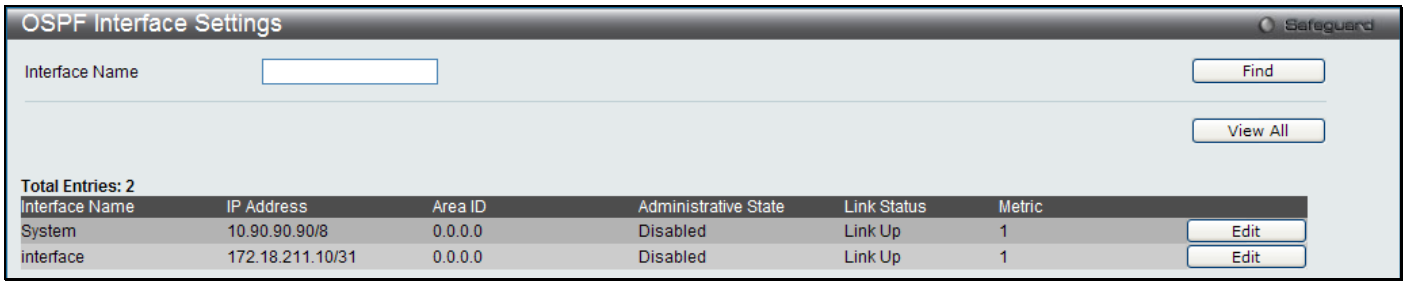


Figure 6-37 OSPF Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IP interface here

Click the **Find** button to find the interface entered.
Click the **View All** button to view all the interfaces configured on this switch.
Click the **Edit** button to re-configure the selected entry.

After clicking the **Edit** button, the following page with be displayed.

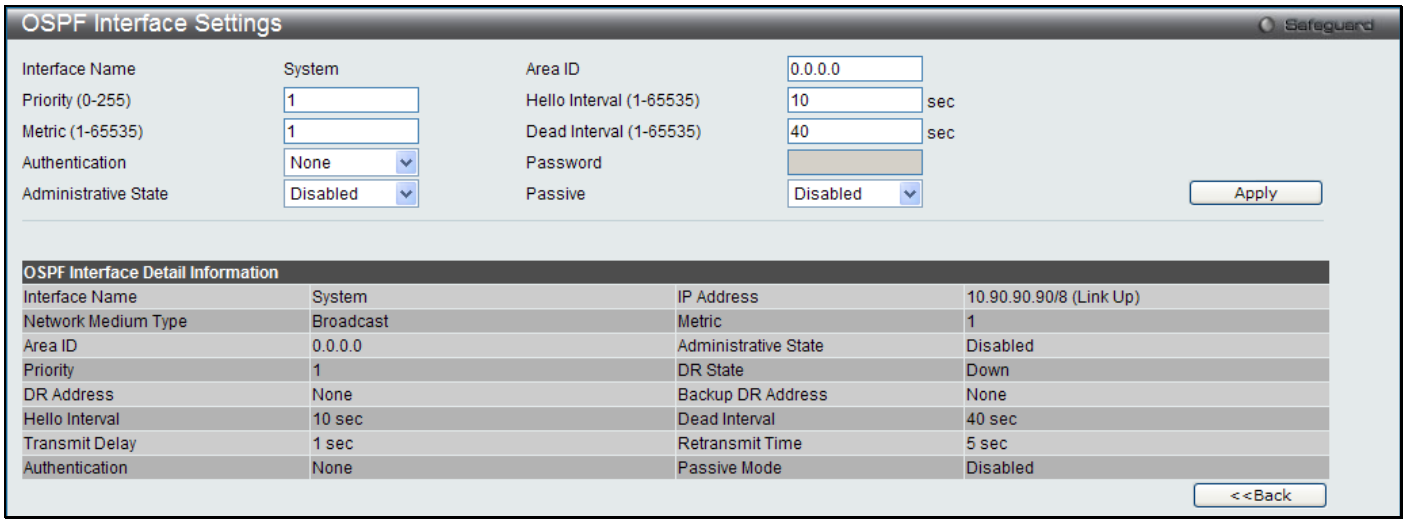


Figure 6-38 OSPF Interface Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Priority (0-255)	Specifies the priority for the Designated Router election. If a Router Priority of 0 is set, the Switch cannot be elected as the DR for the network.
Metric (1-65535)	Specifies the interface metric used.
Authentication	Select the authentication used. Options to choose from are *None*, *Simple* and *MD5*. When choosing *Simple* authentication, a **Password** must be entered. When choosing *MD5* authentication, a **Key ID** must be entered.
Administrative State	Specifies whether to enable or disable the administrative state.
Area ID	Specifies the area to which the interface is assigned. An Area ID is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Hello Interval (1-65535)	Allows the specification of the interval between the transmissions of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Dead Interval (1-65535)	Allows the specification of the length of time between the receipts of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.
Passive	Assign the designated entry to be a passive interface. A passive interface will not advertise to any other routers than those within its OSPF intranet.

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

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

OSPF Virtual Link Settings

This window is used to configure the OSPF virtual interface settings for this Switch.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Virtual Link Settings**, as shown below:

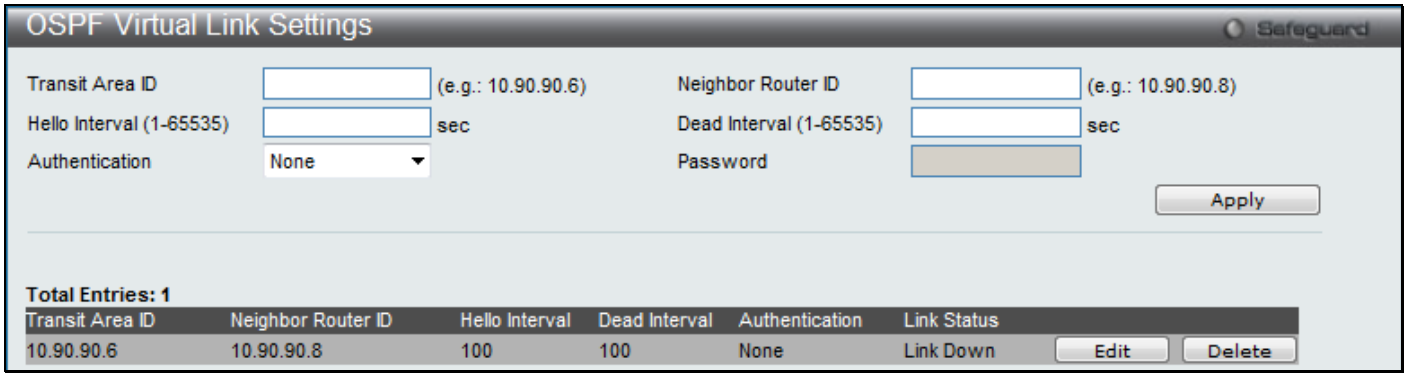


Figure 6-39 OSPF Virtual Link Settings window

The fields that can be configured are described below:

Parameter	Description
Transit Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Hello Interval (1-65535)	Allows the specification of the interval between the transmissions of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Neighbor Router ID	The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

Dead Interval (1-65535)	Allows the specification of the length of time between the receipts of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.
Authentication	Select the authentication used. Options to choose from are *None*, *Simple* and *MD5*. When choosing *Simple* authentication, a **Password** must be entered. When choosing *MD5* authentication, a **Key ID** must be entered.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the selected entry.
Click the **Delete** button to remove the selected entry.

After clicking the **Edit** button, the following page with be displayed.

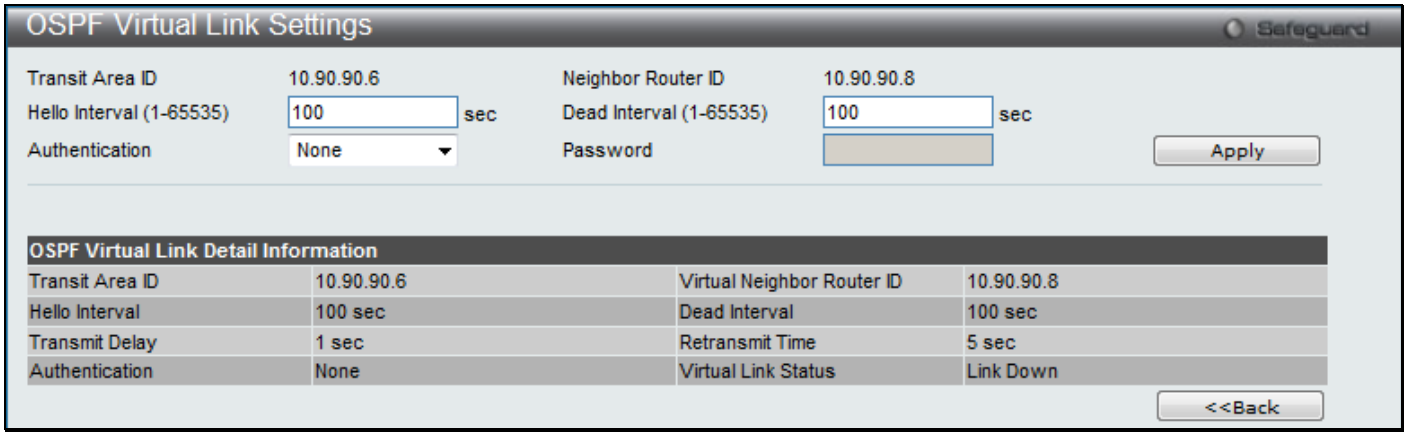


Figure 6-40 OSPF Virtual Link Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Hello Interval (1-65535)	Allows the specification of the interval between the transmissions of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Dead Interval (1-65535)	Allows the specification of the length of time between the receipts of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.
Authentication	Select the authentication used. Options to choose from are *None*, *Simple* and *MD5*. When choosing *Simple* authentication, a **Password** must be entered. When choosing *MD5* authentication, a **Key ID** must be entered.

Click the **Apply** button to accept the changes made.
Click on the **<<Back** button to return to the previous window.

OSPF Area Aggregation Settings

This window is used to configure the OSPF area aggregation settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Area Aggregation Settings**, as shown below:

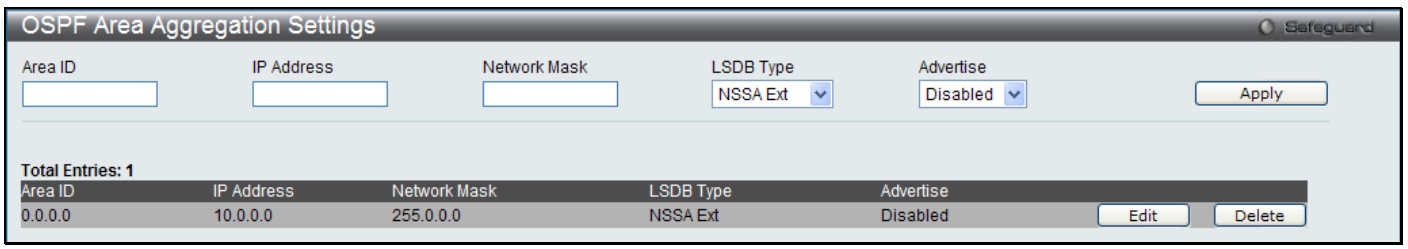


Figure 6-41 OSPF Area Aggregation Settings window

The fields that can be configured are described below:

Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
IP Address	The IP address that uniquely identifies the network that corresponds to the OSPF Area.
Network Mask	The network mask that uniquely identifies the network that corresponds to the OSPF Area.
LSDB Type	The type of address aggregation. Options to choose from are *NSSA Ext* and *Summary*.
Advertise	Allows for the advertisement trigger to be enabled or disabled.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the selected entry.
Click the **Delete** button to remove the selected entry.

OSPF Host Route Settings

This window is used to configure OSPF host route settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Host Route Settings**, as shown below:

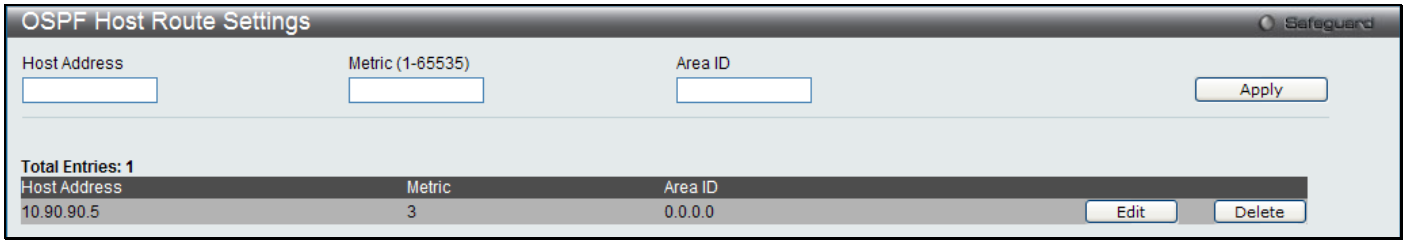


Figure 6-42 OSPF Host Route Settings window

The fields that can be configured are described below:

Parameter	Description
Host Address	Specifies the host's IP address used.
Metric (1-65535)	Enter a metric between 1 and 65535, which will be advertised.
Area ID	Enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the selected entry.
Click the **Delete** button to remove the selected entry.

OSPF Default Information Originate Settings

This window will change the status of the originating OSPF default external route.

To view this window, click **L3 Features > OSPF > OSPFv2 > OSPF Default Information Originate Settings** as shown below:

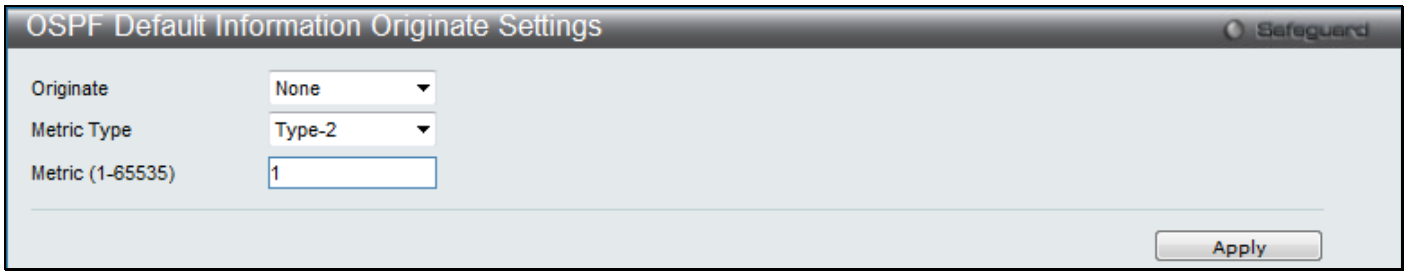


Figure 6-43 OSPF Default Information Originate Settings window

The fields that can be configured are described below:

Parameter	Description
Originate	Select the status of the originating default information here. Selecting *Default* specifies that the external default route will be originated only when one default route already exists. Selecting *Always* specifies that the external default route will be originated, whether a default route exists or not. Selecting *None* specifies that the external default route will never be originated. This is the default option.
Metric Type	Select the type of LSA that contains the default external route imported into OSPF. Selecting *Type-1* specifies that this default external route will be calculated using the metric by adding the interface cost to the metric entered in the metric field. Selecting *Type-2* specifies that this default external route will be calculated using the metric entered in the metric field without change. This is the default option.
Metric (1-65535)	Enter the metric value used by the originating default external route here. This value must be between 1 and 65535.

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

OSPF LSDB Table

This window is used to display the OSPF Link State Database (LSDB).

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF LSDB Table**, as shown below:

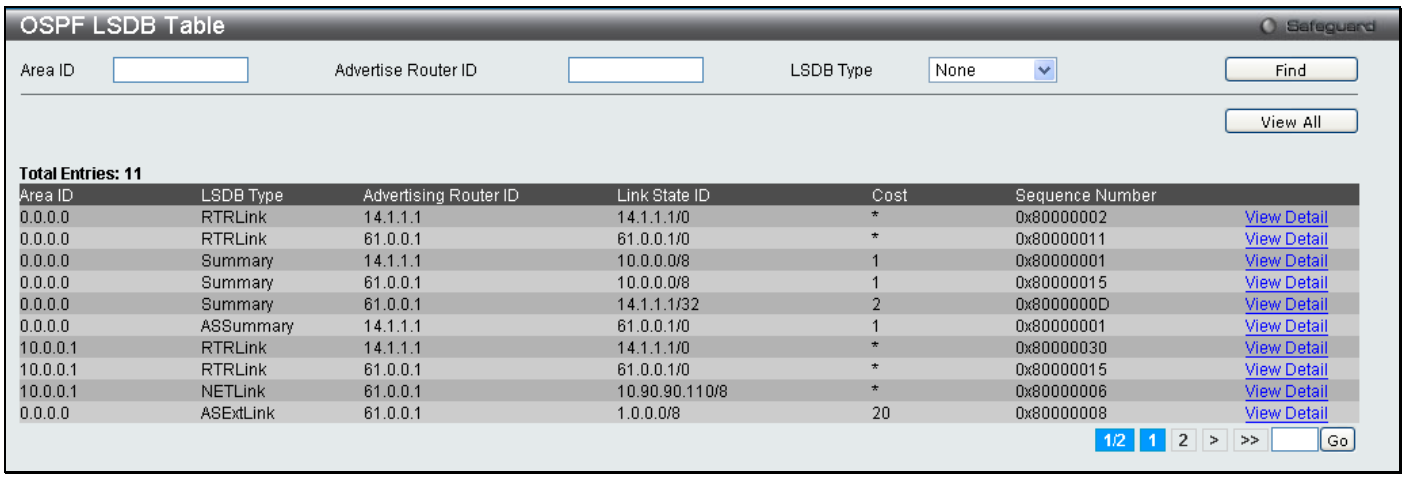


Figure 6-44 OSPF LSDB Table window

The fields that can be configured are described below:

Parameter	Description
Area ID	Enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Advertise Router ID	Enter the router ID of the advertising router.
LSDB Type	Specifies the LSDB type to be displayed. Options to choose from are *None*, *RTRLink*, *NETLink*, *Summary*, *ASSummary*, *ASExtLink*, *NSSA Ext* and *Stub*.

Click the **Find** button to find the specified entry.

Click the **View All** button to view all the OSPF Link State Database entries.

Click the View Detail link to view the OSPF LSDB details of the specific entry.

After clicking the View Detail link, the following window will appear:

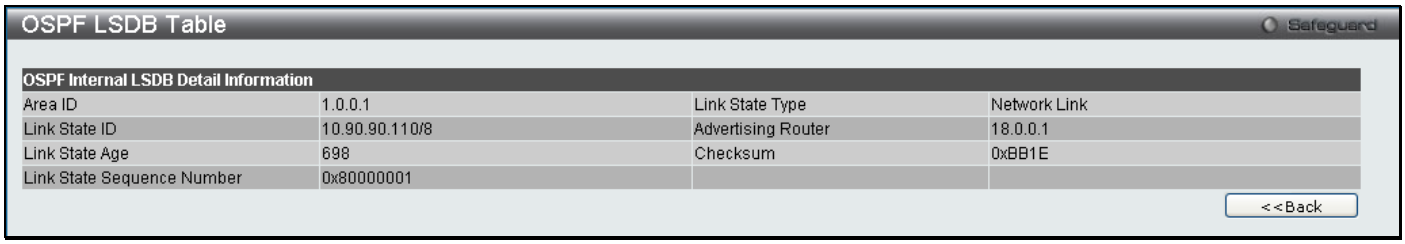


Figure 6-45 OSPF LSDB Table – View Detail window

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

OSPF Neighbor Table

This window is used to display OSPF-neighbor information on a per-interface basis.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Neighbor Table**, as shown below:

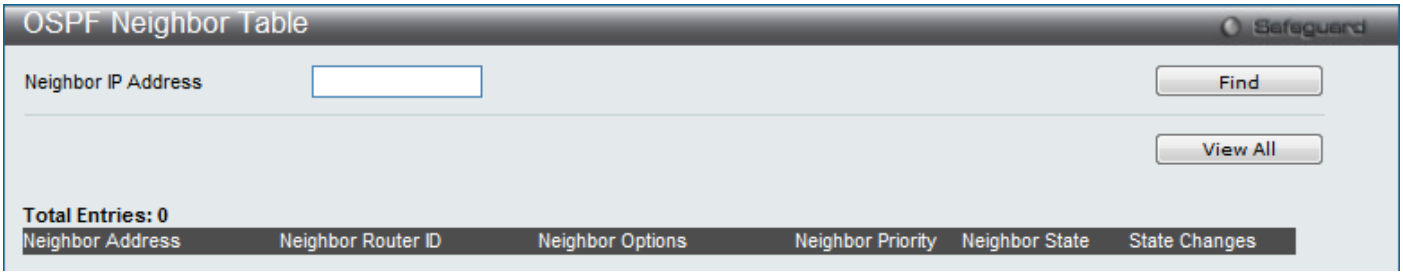


Figure 6-46 OSPF Neighbor Table window

The fields that can be configured are described below:

Parameter	Description
Neighbor IP Address	Enter the IP address of the neighbor router.

Click the **Find** button to find the specified entry.

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

OSPF Virtual Neighbor Table

This window is used to display OSPF-neighbor information of OSPF virtual links.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPF Virtual Neighbor Table**, as shown below:

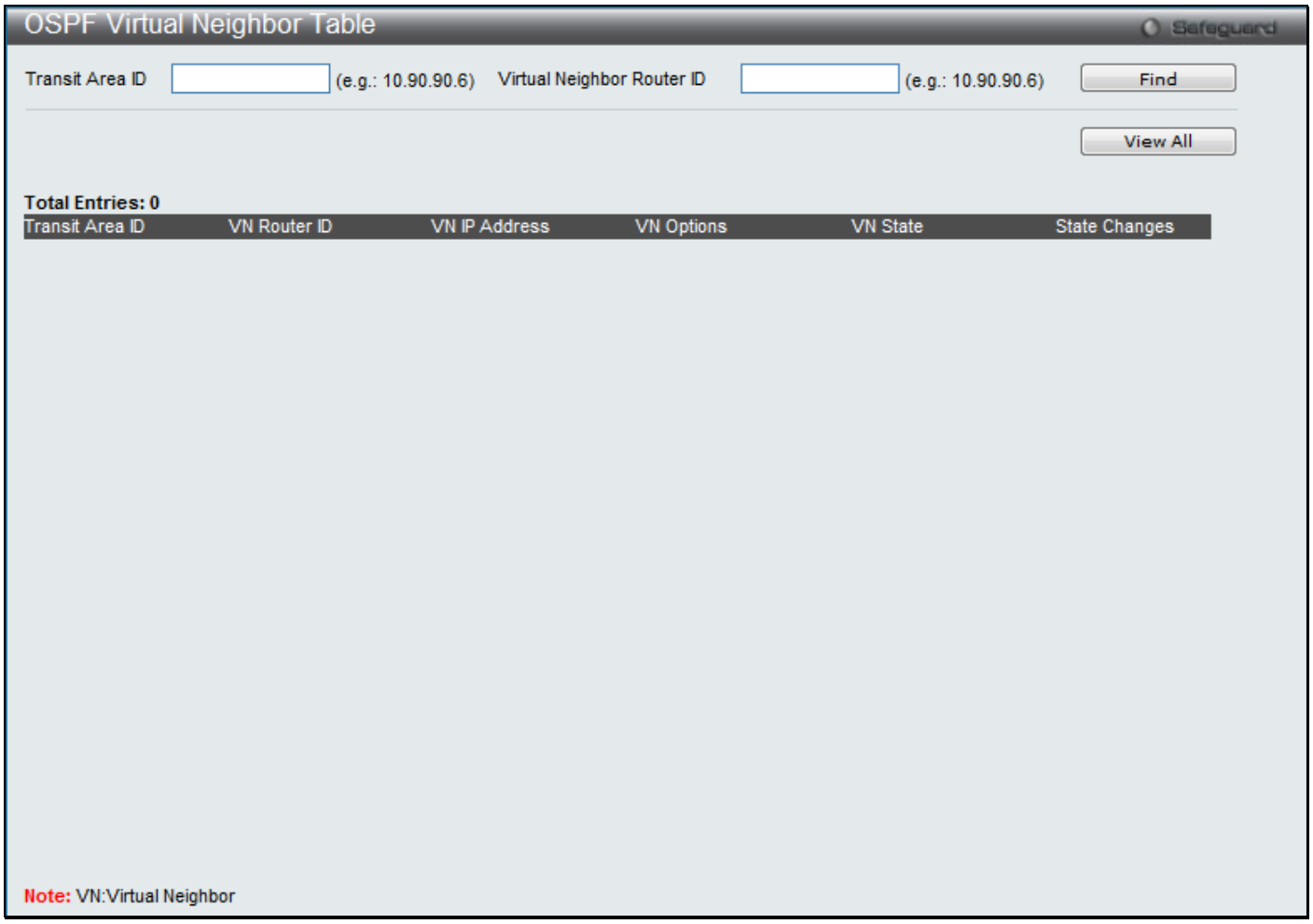


Figure 6-47 OSPF Virtual Neighbor Table window

The fields that can be configured are described below:

Parameter	Description
Transit Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Virtual Neighbor Router ID	The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.

Click the **Find** button to find the specified entry.

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

RIP

The Routing Information Protocol is a distance-vector routing protocol. There are two types of network devices running RIP - active and passive. Active devices advertise their routes to others through RIP messages, while passive devices listen to these messages. Both active and passive routers update their routing tables based upon RIP messages that active routers exchange. Only routers can run RIP in the active mode.

Every 30 seconds, a router running RIP broadcasts a routing update containing a set of pairs of network addresses and a distance (represented by the number of hops or routers between the advertising router and the remote network). So, the vector is the network address and the distance is measured by the number of routers between the local router and the remote network.

RIP measures distance by an integer count of the number of hops from one network to another. A router is one hop from a directly connected network, two hops from a network that can be reached through a router, etc. The more routers between a source and a destination, the greater the RIP distance (or hop count).

There are a few rules to the routing table update process that help to improve performance and stability. A router will not replace a route with a newly learned one if the new route has the same hop count (sometimes referred to as 'cost'). So learned routes are retained until a new route with a lower hop count is learned.

When learned routes are entered into the routing table, a timer is started. This timer is restarted every time this route is advertised. If the route is not advertised for a period of time (usually 180 seconds), the route is removed from the routing table.

RIP does not have an explicit method to detect routing loops. Many RIP implementations include an authorization mechanism (a password) to prevent a router from learning erroneous routes from unauthorized routers.

To maximize stability, the hop count RIP uses to measure distance must have a low maximum value. Infinity (that is, the network is unreachable) is defined as 16 hops. In other words, if a network is more than 16 routers from the source, the local router will consider the network unreachable.

RIP can also be slow to converge (to remove inconsistent, unreachable or looped routes from the routing table) because RIP messages propagate relatively slowly through a network.

Slow convergence can be solved by using split horizon update, where a router does not propagate information about a route back to the interface on which it was received. This reduces the probability of forming transient routing loops.

Hold down can be used to force a router to ignore new route updates for a period of time (usually 60 seconds) after a new route update has been received. This allows all routers on the network to receive the message.

A router can 'poison reverse' a route by adding an infinite (16) hop count to a route's advertisement. This is usually used in conjunction with triggered updates, which force a router to send an immediate broadcast when an update of an unreachable network is received.

RIP Version 1 Message Format

There are two types of RIP messages: routing information messages and information requests. Both types use the same format.

The Command field specifies an operation according the following table:

Command	Description
1	Request for partial or full routing information.
2	Response containing network-distance pairs from sender's routing table.
3	Turn on trace mode.
4	Turn off trace mode.
5	Reserved for Sun Microsystems internal use.
9	Update Request.
10	Update Response.
11	Update Acknowledgement

RIP Command Codes

The field VERSION contains the protocol version number (1 in this case), and is used by the receiver to verify which version of RIP the packet was sent.

RIP 1 Message

RIP is not limited to TCP/IP. Its address format can support up to 14 octets (when using IP, the remaining 10 octets must be zeros). Other network protocol suites can be specified in the Family of Source Network field (IP has a value of 2). This will determine how the address field is interpreted.

RIP specifies that the IP address, 0.0.0.0, denotes a default route.

The distances, measured in router hops are entered in the Distance to Source Network, and Distance to Destination Network fields.

RIP 1 Route Interpretation

RIP was designed to be used with classed address schemes, and does not include an explicit subnet mask. An extension to version 1 does allow routers to exchange subnet addresses, but only if the subnet mask used by the network is the same as the subnet mask used by the address. This means the RIP version 1 cannot be used to propagate classless addresses.

Routers running RIP version 1 must send different update messages for each IP interface to which it is connected. Interfaces that use the same subnet mask as the router's network can contain subnet routes, other interfaces cannot. The router will then advertise only a single route to the network.

RIP Version 2 Extensions

RIP version 2 includes an explicit subnet mask entry, so RIP version 2 can be used to propagate variable length subnet addresses or CIDR classless addresses. RIP version 2 also adds an explicit next hop entry, which speeds convergence and helps prevent the formation of routing loops.

RIP2 Message Format

The message format used with RIP2 is an extension of the RIP1 format. RIP version 2 also adds a 16-bit route tag that is retained and sent with router updates. It can be used to identify the origin of the route. Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

RIP Settings

This window is used to configure the RIP settings for one or more IP interfaces.

To view the following window, click **L3 Features > RIP > RIP Settings**, as shown below:

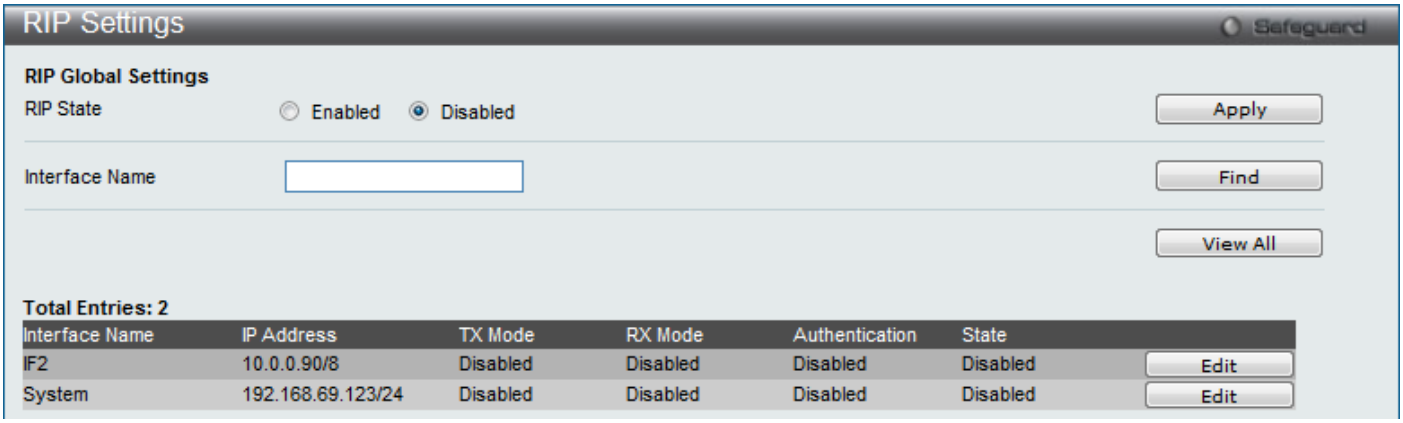


Figure 6-48 RIP Settings window

The fields that can be configured are described below:

Parameter	Description
RIP State	Specifies that the RIP state will be enabled or disabled. If the state is disabled, then RIP packets will not be either transmitted or received by the interface. The network configured on this interface will not be in the RIP database.
Interface Name	Specifies the IP interface name used for this configuration.

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

Click the **Find** button to find the specified entry.

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

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

After clicking the **Edit** button, the following page with be displayed.

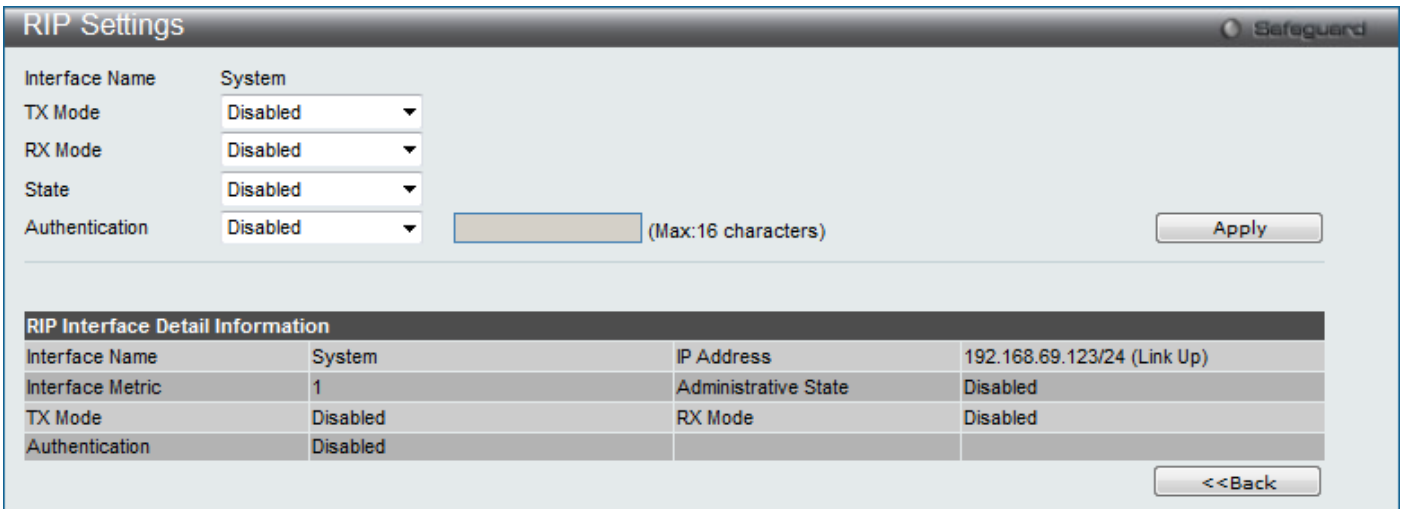


Figure 6-49 RIP Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Specifies the IP interface name used for this configuration.
TX Mode	Specifies the RIP transmission mode. Options to choose from are **v1 Only**, **v1 Compatible** and **v2 Only**. Select **Disable** to disable this option.
RX Mode	Specifies the RIP receive mode Options to choose from are **v1 Only**, **v2 Only** and **v1 or v2**. Select **Disable** to disable this option.
State	Specifies that the RIP state will be enabled or disabled. If the state is disabled, then RIP packets will not be either transmitted or received by the interface. The network configured on this interface will not be in the RIP database.
Authentication	Specifies to set the state of authentication. When the authentication state is enabled, enter the password used in the space provided.

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

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

RIPng (EI Mode Only)

RIPng Global Settings

This window is used to configure the RIPng global settings.

To view the following window, click **L3 Features > RIP > RIPng > RIPng Global Settings**, as shown below:

Figure 6-50 RIPng Global Settings window

The fields that can be configured are described below:

Parameter	Description
RIPng State	Click to enable or disable the RIPng state.
Method	Use the drop-down menu to select the method of RIPng. No Horizon – Select for not using any horizon. Split Horizon – Select to use basic split horizon. Poison Reverse – Select to use poison-reverse.
Update Time (5-65535)	Specifies the update timer.
Expire Time (1-65535)	Specifies when to expire the update.
Garbage Collection Time (1-65535)	Specifies the garbage-collection timer.

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

RIPng Interface Settings

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

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

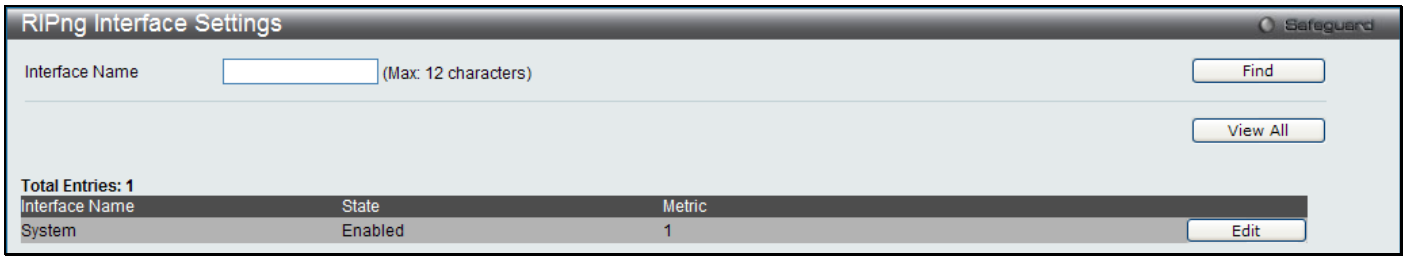


Figure 6-51 RIPng Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IPv6 interface name.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the configure entries.
Click the **Edit** button to re-configure the specific entry.

After clicking the **Edit** button, the following page with be displayed.

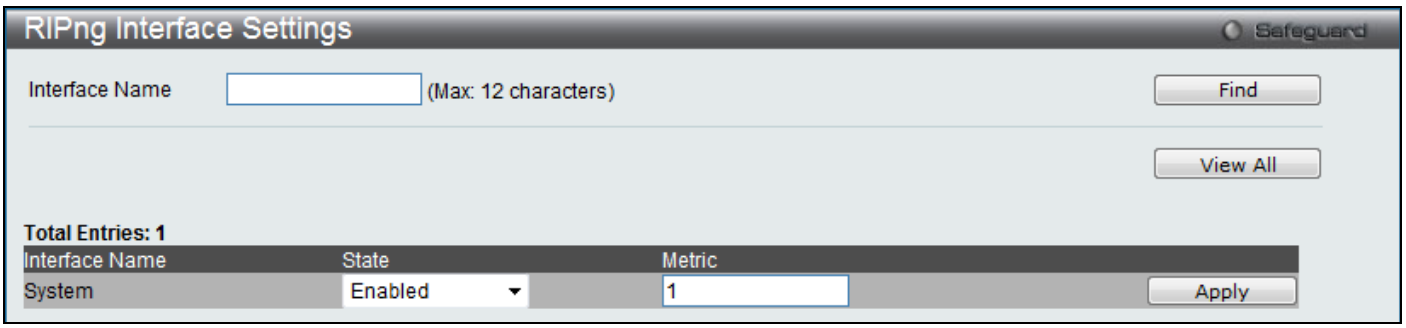


Figure 6-52 RIPng Interface Settings (Edit) window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the RIPng state on the selected interfaces.
Metric	Enter the metric value used here. The RIPng route that was learned from the interface will add this value as a new route metric. The default value is 1. This value must be between 1 and 15.

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

IP Multicast Routing Protocol

IGMP

IGMP Interface Settings

The Internet Group Management Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. Each IP interface configured on the Switch is displayed in the below IGMP Interface Settings window.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface Settings**, as shown below:

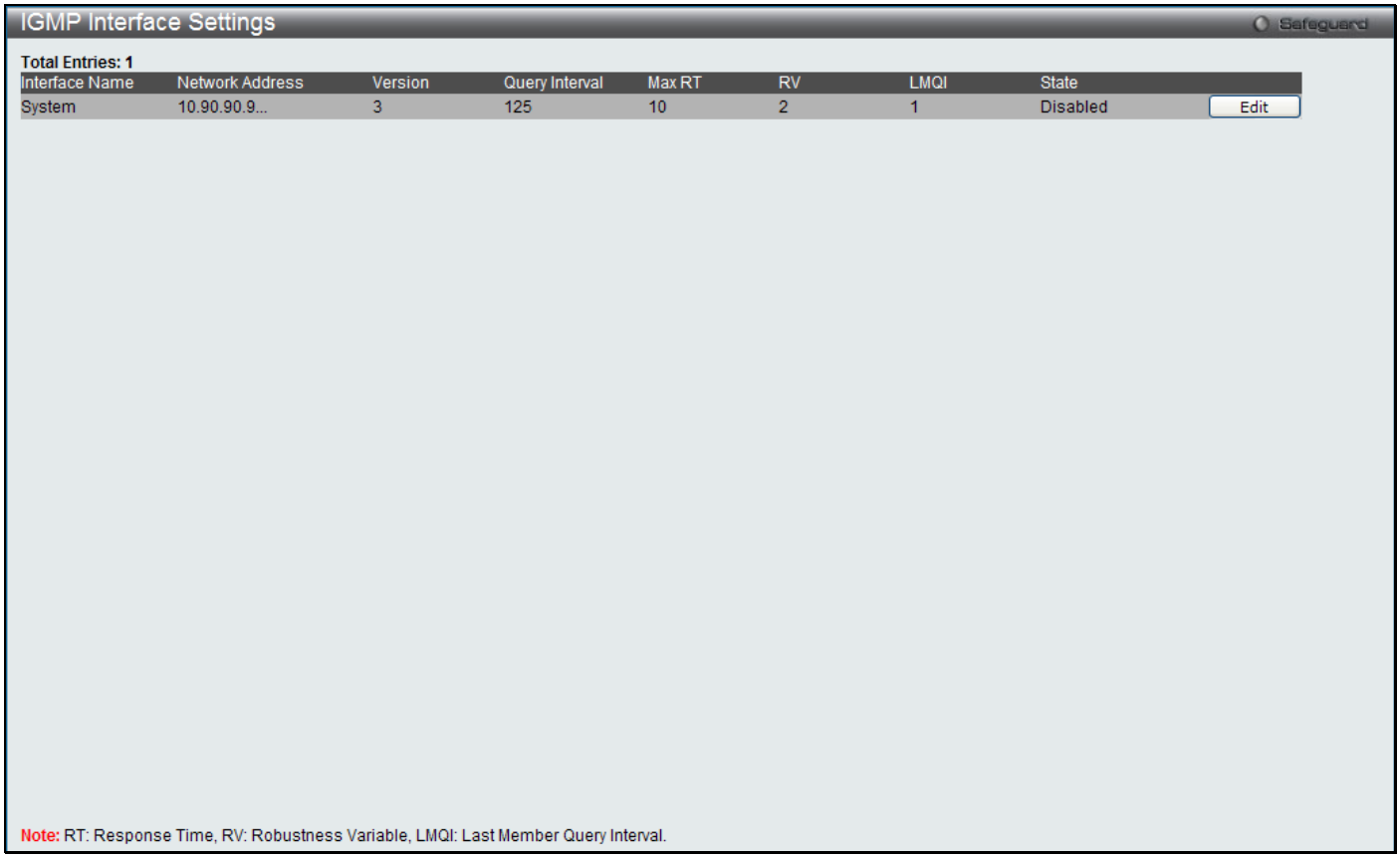


Figure 6-53 IGMP Interface Settings window

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

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

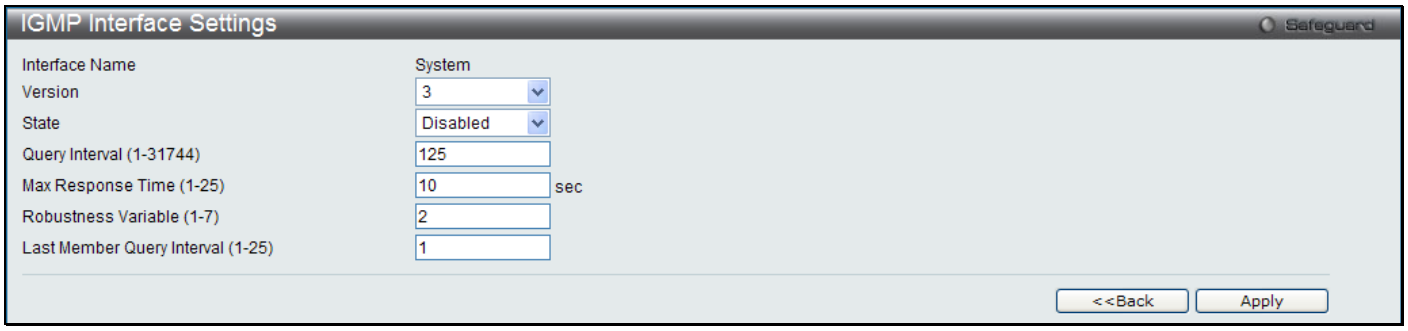


Figure 6-54 IGMP Interface Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Version	Use the drop-down menu to select the IGMP version that will be used to interpret IGMP queries on the interface.
State	Use the drop-down menu to enables or disables IGMP for the IP interface. The default is Disabled.
Query Interval (1-31744)	Enter a value between 1 and 31744 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time (1-25)	Enter a value between 1 and 25 to specify the maximum amount of time allowed before sending an IGMP response report. The default time is 10 seconds.
Robustness Variable (1-7)	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 1 and 7 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets. The default setting is 2.
Last Member Query Interval (1-25)	Enter a value between 1 and 25 to specify the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is 1 second.

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

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

IGMP Check Subscriber Source Network Settings

This window is used to configure the flag that determines whether or not to check the subscriber source IP when an IGMP report or leave message is received. When this option is enabled on an interface, any IGMP report or leave messages received by the interface will be checked to determine whether its source IP is in the same network as the interface. If the check failed for a received report or leave message, the message won't be processed by IGMP protocol. If the check is disabled, the IGMP report or leave message with any source IP will be processed by the IGMP protocol.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Check Subscriber Source Network Settings**, as shown below:

Figure 6-55 IGMP Check Subscriber Source Network Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP interface name, used for this search, here.
Subscriber Source Network Check	Click the **Edit** button and choose to enable or disable the flag that determines whether or not to check the subscriber source IP when an IGMP report or leave message is received.

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

Click the **View All** button to display all the configure entries.

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

IGMP Group Table

The window is used to display the dynamic IGMP groups on the Switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Group Table**, as shown below:

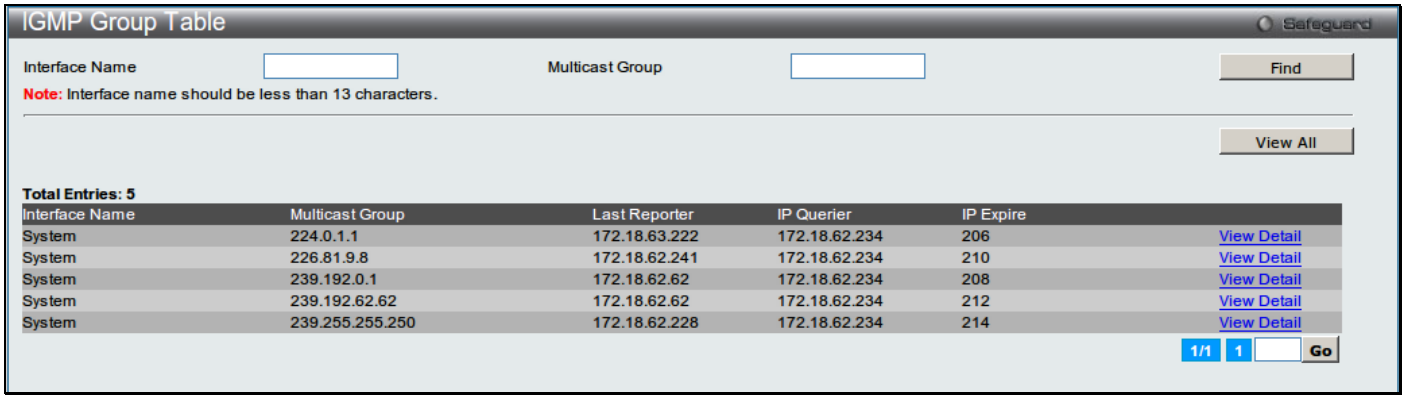


Figure 6-56 IGMP Group Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP interface name used for this configuration.
Multicast Group	Enter the multicast group IP address.

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

Click the **View All** button to view all the interfaces configured on this switch.

Click the View Detail link to view more information regarding the specific entry.

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

Click the View Detail link to see the following window.

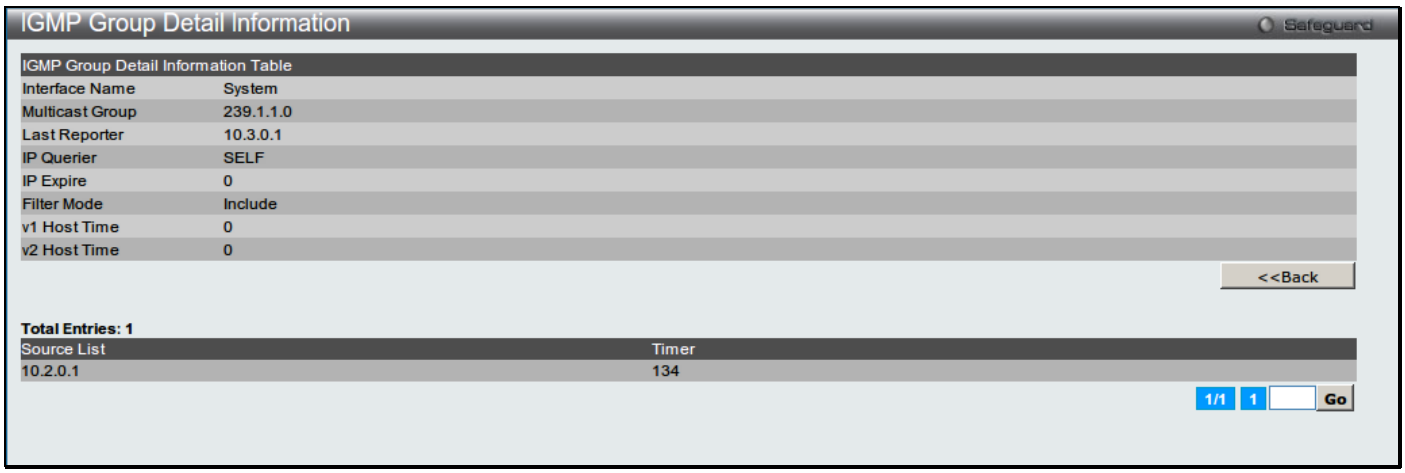


Figure 6-57 IGMP Group Detail Information window

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

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

IGMP Static Group Settings

This window is used to create an IGMP static group on the switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Static Group Settings**, as shown below:

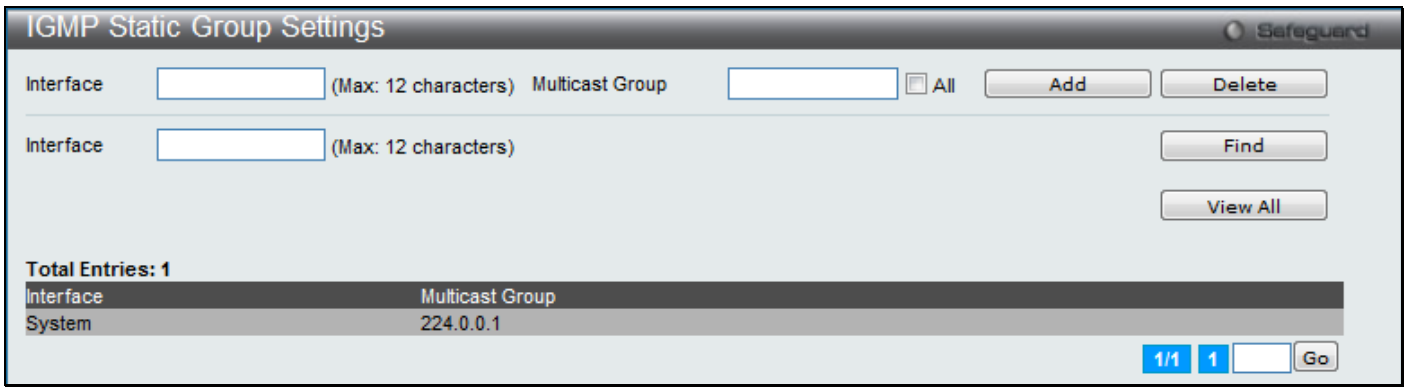


Figure 6-58 IGMP Static Group Settings window

The fields that can be configured are described below:

Parameter	Description
Interface	Enter the IP interface on which the IGMP static group resides. The IP interface must be the primary IP interface.
Multicast Group	Enter the multicast IP address.

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

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

Click the **Find** button to find the information entered.

Click the **View 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.

DVMRP

The Distance Vector Multicast Routing Protocol (DVMRP) is a hop-based method of building multicast delivery trees from multicast sources to all nodes of a network. Because the delivery trees are 'pruned' and 'shortest path', DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) relatively low bandwidth networks, and can be considered as a 'best-effort' multicasting protocol.

DVMRP resembles the Routing Information Protocol (RIP), but is extended for multicast delivery. DVMRP builds a routing table to calculate 'shortest paths' back to the source of a multicast message, but defines a 'route cost' (similar to the hop count in RIP) as a relative number that represents the real cost of using this route in the construction of a multicast delivery tree to be 'pruned' - once the delivery tree has been established.

When a sender initiates a multicast, DVMRP initially assumes that all users on the network will want to receive the multicast message. When an adjacent router receives the message, it checks its routing table to determine the interface that gives the shortest path (lowest cost) back to the source. If the multicast was received over the shortest path, then the adjacent router enters the information into its tables and forwards the message. If the message is not received on the shortest path back to the source, the message is dropped.

Route cost is a relative number that is used by DVMRP to calculate which branches of a multicast delivery tree should be 'pruned'. The 'cost' is relative to other costs assigned to other DVMRP routes throughout the network.

The higher the route cost, the lower the probability that the current route will be chosen to be an active branch of the multicast delivery tree (not 'pruned') - if there is an alternative route.

DVMRP Interface Settings

This window is used to configure the DVMRP global state and allow the DVMRP to be configured for each IP interface defined on the Switch. Each IP interface configured on the Switch is displayed in the below DVMRP Interface Settings window.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Interface Settings**, as shown below:

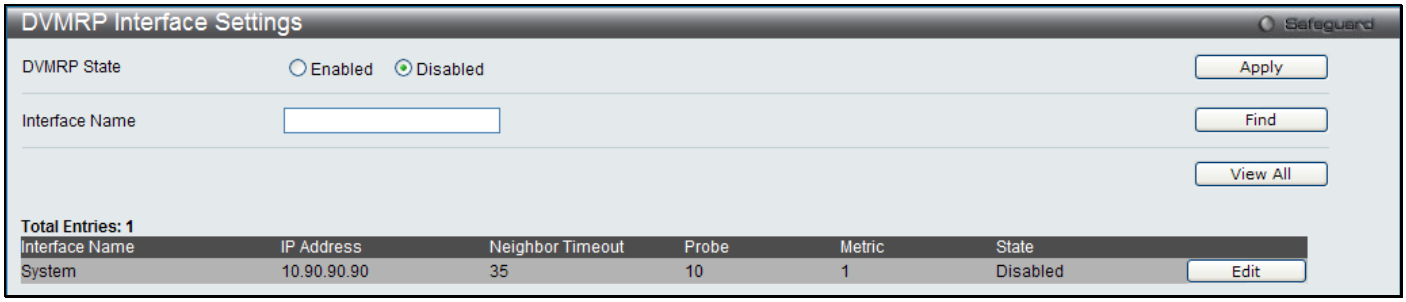


Figure 6-59 DVMRP Interface Settings window

The fields that can be configured are described below:

Parameter	Description
DVMRP State	Click the radio buttons to enable or disable the DVMRP state.
Interface Name	Enter the IP interface name of DVMRP to search for a specific entry. This must be a previously defined IP interface.

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

Click the **Find** button to find the interface entered.

Click the **View All** button to view all the interfaces configured on this switch.

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

DVMRP Routing Table

This window is used to display DVMRP routing table on the Switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Table**, as shown below:

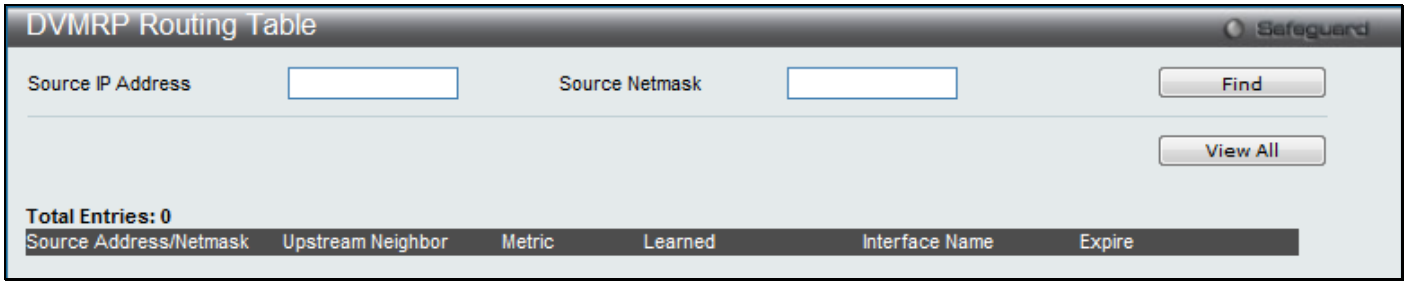


Figure 6-60 DVMRP Routing Table window

The fields that can be configured are described below:

Parameter	Description
Source IP Address	Enter the IP address of the Source.
Source Netmask	Enter the Netmask of the Source IP address.

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

Click the **View All** button to view all the interfaces configured on this switch.

DVMRP Neighbor Table

This window is used to display DVMRP neighbor table on the Switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Neighbor Table**, as shown below:

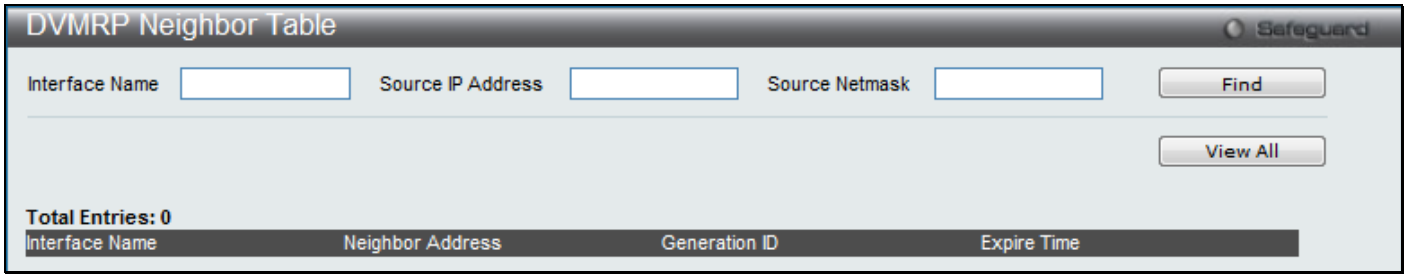


Figure 6-61 DVMRP Neighbor Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the interface.
Source IP Address	Enter the IP address of the Source.
Source Netmask	Enter the Netmask of the Source IP address.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to view all the interfaces configured on this switch.

DVMRP Routing Next Hop Table

This window is used to display DVMRP routing next hop table on the Switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Next Hop Table**, as shown below:

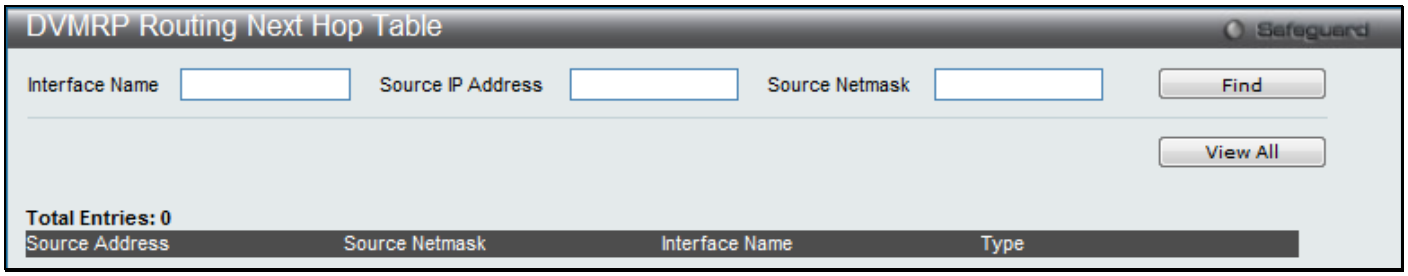


Figure 6-62 DVMRP Routing Next Hop Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the interface.
Source IP Address	Enter the IP address of the Source IP Address.
Source Netmask	Enter the netmask of the Source IP Address.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to view all the interfaces configured on this switch.

PIM

Protocol Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. PIM is protocol-independent as it does not include its own topology discovery mechanism, but uses routing information supplied by other traditional routing protocols, such as RIP or OSPF. The Switch supports four types of PIM, Dense Mode (PIM-DM), Sparse Mode (PIM-SM), PIM Source Specific multicast (PIM-SSM), and Sparse-Dense Mode (PIM-SM-DM).

PIM-SM

Protocol Independent Multicast - Sparse Mode (PIM-SM) is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) per group, and optionally creates shortest-path trees per source. Unlike most multicast routing protocols which flood the network with multicast packets, PIM-SM will forward traffic to routers who are explicitly a part of the multicast group through the use of a Rendezvous Point (RP). This RP will take all requests from PIM-SM enabled routers, analyze the information and then returns multicast information it receives from the source, to requesting routers within its configured network. Through this method, a distribution tree is created, with the RP as the root. This distribution tree holds all PIM-SM enabled routers within which information collected from these routers are stored by the RP.

When many routers are a part of a multiple access network, a Designated Router (DR) will be elected. The DR's primary function is to send Join/Prune messages to the RP. The router with the highest priority on the LAN will be selected as the DR. If there is a tie for the highest priority, the router with the higher IP address will be chosen.

The third type of router created in the PIM-SM configuration is the Boot Strap Router (BSR). The goal of the Boot Strap Router is to collect and relay RP information to PIM-SM enabled routers on the LAN. Although the RP can be statically set, the BSR mechanism can also determine the RP. Multiple Candidate BSRs (C-BSR) can be set on the network but only one BSR will be elected to process RP information. If it is not explicitly apparent which C-BSR is to be the BSR, all C-BSRs will emit Boot Strap Messages (BSM) out on the PIM-SM enabled network to determine which C-BSR has the higher priority and once determined, will be elected as the BSR. Once determined, the BSR will collect RP data emanating from candidate RPs on the PIM-SM network, compile it and then send it out on the land using periodic Boot Strap Messages (BSM). All PIM-SM Routers will get the RP information from the Boot Strap Mechanism and then store it in their database.

Discovering and Joining the Multicast Group

Although Hello packets discover PIM-SM routers, these routers can only join or be "pruned" from a multicast group through the use of Join/Prune Messages exchanged between the DR and RP. Join/Prune Messages are packets relayed between routers that effectively state which interfaces are, or are not to be receiving multicast data. These messages can be configured for their frequency to be sent out on the network and are only valid to routers if a Hello packet has first been received. A Hello packet will simply state that the router is present and ready to become a part of the RP's distribution tree. Once a router has accepted a member of the IGMP group and it is PIM-SM enabled, the interested router will then send an explicit Join/Prune message to the RP, which will in turn route multicast data from the source to the interested router, resulting in a unidirectional distribution tree for the group. Multicast packets are then sent out to all nodes on this tree. Once a prune message has been received for a router that is a member of the RP's distribution tree, the router will drop the interface from its distribution tree.

Distribution Trees

Two types of distribution trees can exist within the PIM-SM protocol, a Rendezvous-Point Tree (RPT) and a Shortest Path Tree (SPT). The RP will send out specific multicast data that it receives from the source to all outgoing interfaces enabled to receive multicast data. Yet, once a router has determined the location of its source, an SPT can be created, eliminating hops between the source and the destination, such as the RP. This can be configured by the switch administrator by setting the multicast data rate threshold. Once the threshold has been passed, the data path will switch to the SPT. Therefore, a closer link can be created between the source and destination, eliminating hops previously used and shortening the time a multicast packet is sent from the source to its final destination.

Register and Register-stop Messages

Multicast sources do not always join the intended receiver group. The first hop router (DR) can send multicast data without being the member of a group or having a designated source, which essentially means it has no information about how to relay this information to the RP distribution tree. This problem is alleviated through Register and Register-Stop messages. The first multicast packet received by the DR is encapsulated and sent on to the RP, which in turn removes the encapsulation and sends the packet on down the RP distribution tree. When the route has been established, a SPT can be created to directly connect routers to the source, or the multicast traffic flow can begin, traveling from the DR to the RP. When the latter occurs, the same packet may be sent twice, one type encapsulated,

one not. The RP will detect this flaw and then return a Register-stop message to the DR requesting it to discontinue sending encapsulated packets.

Assert Messages

At times on the PIM-SM enabled network, parallel paths are created from source to receiver, meaning some receivers will receive the same multicast packets twice. To improve this situation, Assert messages are sent from the receiving device to both multicast sources to determine which single router will send the receiver the necessary multicast data. The source with the shortest metric (hop count) will be elected as the primary multicast source. This metric value is included within the Assert message.

PIM-SSM

The Source Specific Multicast (SSM) feature is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups in SSM range, only source-specific multicast distribution trees (no shared trees) are created.

The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 to 232.255.255.255 for SSM applications and protocols. The Switch allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 to 239.255.255.255.

PIM-DM

The Protocol Independent Multicast - Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth as PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

The PIM-DM multicast routing protocol is assumes that all downstream routers want to receive multicast messages and relies upon explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit ‘join’ messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the Join/Prune Interval) or for the downstream routers to transmit explicit ‘prune’ messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches (‘prunes’ them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the ‘prune’ information from its database and floods multicast messages to all interfaces on that branch. The interval for removing ‘prune’ information is the Join/Prune Interval.

PIM-SM-DM

In the PIM-SM, RP is a key point for the first hop of the sender. If the first hop does not have RP information when the sender sends data out, it will drop the packet and do nothing. Sparse-Dense mode will be useful in this condition. In Sparse-Dense mode, the packets can be flooded to all the outgoing interfaces and pruning/joining (prune/graft) can be used to control the outgoing interface list if RP is not found. In other words, the PIM Sparse-Dense mode is treated in either the sparse mode or dense mode of the operation; it depends on which mode the multicast group operates. When an interface receives multicast traffic, if there is a known RP for the group, then the current operation mode on the interface is sparse mode, otherwise the current operation mode on the interface will be dense mode.

PIM for IPv4

PIM Global Settings

This window is used to configure PIM global state and the parameter settings for the PIM distribution tree on the Switch.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Global Settings**, as shown below:

Figure 6-63 PIM Global Settings window

The fields that can be configured are described below:

Parameter	Description
PIM Global State	Click the radio buttons to enable or disable PIM global state.
Register Probe Time (1-127)	Enter a time to send a NULL register message from the DR to the RP before the Register Suppression time expires. If a Register Stop message is received by the DR, the Register Suppression Time will be restarted. If no Register Stop message is received within the probe time, Register Packets will be resent to the RP. The user may configure a time between 1 and 127 seconds with a default setting of 5 seconds.
Register Suppression Time (3-255)	This field is to be configured for the first hop router from the source. After this router sends out a Register message to the RP, and the RP replies with a Register stop message, it will wait for the time configured here to send out another register message to the RP. The user may set a time between 3 and 255 with a default setting of 60 seconds.
Last Hop SPT Switchover	The drop-down menu is used by the last hop router to decide whether to receive multicast data from the shared tree or switch over to the shortest path tree. When the switchover mode is set to never, the last hope router will always receive multicast data from the shared tree. When the mode is set to immediately, the last hop router will always receive data from the shortest path tree.

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

PIM Interface Settings

This window is used to configure the settings for the PIM protocol per IP interface.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Interface Settings**, as shown below:

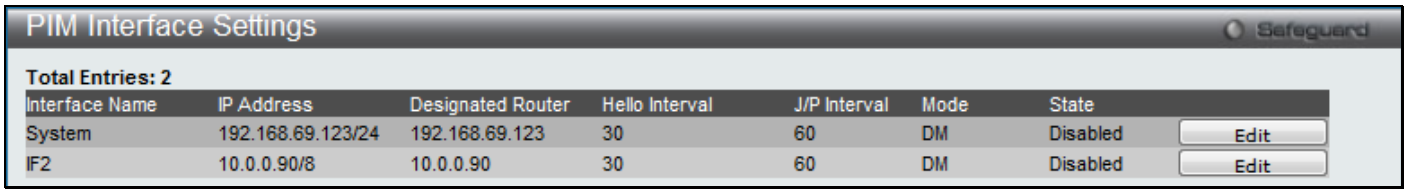


Figure 6-64 PIM Interface Settings window

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

After clicking the **Edit** button, the following page with be displayed.

Figure 6-65 PIM Interface Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Hello Interval (1-18724)	This field will set the interval time between the sending of Hello Packets from this IP interface to neighboring routers one hop away. These Hello packets are used to discover other PIM enabled routers and state their priority as the Designated Router (DR) on the PIM enabled network. The user may enter an interval time between 1 and 18724 seconds with a default interval time of 30 seconds.
Join/Prune Interval (1-18724)	This field will set the interval time between the sending of Join/Prune packets stating which multicast groups are to join the PIM enabled network and which are to be removed or "pruned" from that group. The user may enter an interval time between 1 and 18724 seconds with a default interval time of 60 seconds.
DR Priority (0-4294967294)	Enter the priority of this IP interface to become the Designated Router for the multiple access network. The user may enter a DR priority between 0 and 4,294,967,294 with a default setting of 1.
Mode	Use the drop-down menu to select the type of PIM protocol to use, Sparse Mode (*SM*), Dense Mode (*DM*), or Sparse-Dense Mode (*SM-DM*). The default setting is DM.
State	Use the drop-down menu to enable or disable PIM for this IP interface. The default is Disabled.

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

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

PIM Candidate BSR Settings

The following windows are used to configure the Candidate Boot Strap Router settings for the switch and the priority of the selected IP interface to become the Boot Strap Router (BSR) for the PIM enabled network. The Boot Strap Router holds the information which determines which router on the network is to be elected as the RP for the multicast group and then to gather and distribute RP information to other PIM-SM enabled routers.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Candidate BSR Settings**, as shown below:

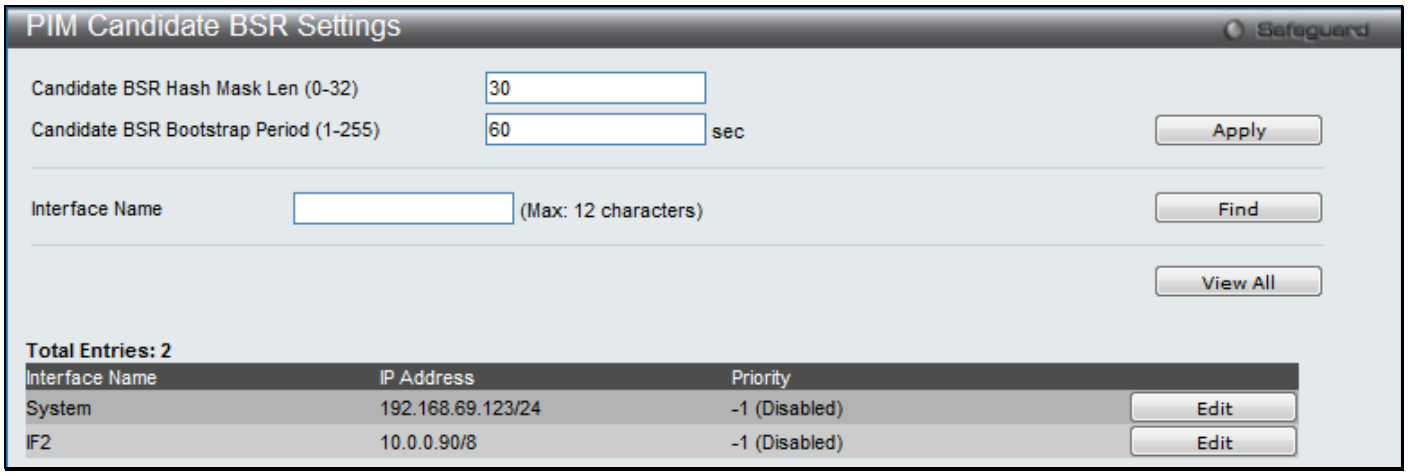


Figure 6-66 PIM Candidate BSR Settings

The fields that can be configured are described below:

Parameter	Description
Candidate BSR Hash Mask Len (0-32)	Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which C-RP on the PIM-SM enabled network will be the RP. The user may select a length between 0 and 32 with a default setting of 30.
Candidate BSR Bootstrap Period (1-255)	Enter a time period between 1 and 255 to determine the interval the Switch will send out Boot Strap Messages (BSM) to the PIM enabled network. The default setting is 60 seconds.
Interface name	Enter the interface name.

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 **View All** button to view all the interfaces configured on this switch.

Click the **Edit** button to configure the specific BSR priority.

After clicking the **Edit** button, the following page with be displayed.

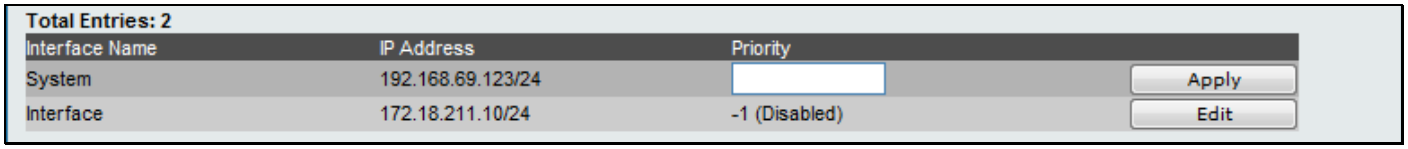


Figure 6-67 PIM Candidate BSR Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
Priority	Enter a value -1 or from 0 to 255. The default value is -1 which means the BSR state is disabled.

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

PIM Candidate RP Settings

The following window is used to set the Parameters for this Switch to become a candidate RP.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Candidate RP Settings**, as shown below:

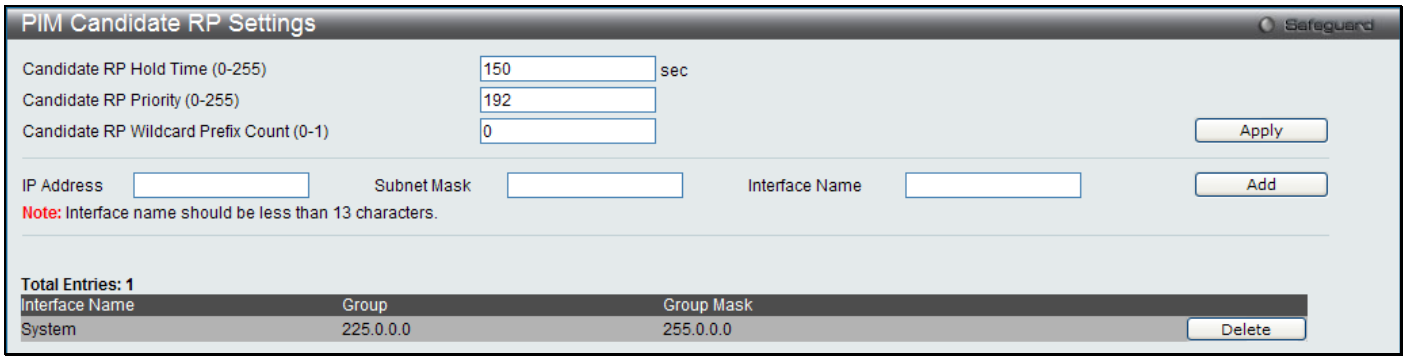


Figure 6-68 PIM Candidate RP Settings window

The fields that can be configured are described below:

Parameter	Description
Candidate RP Hold Time (0-255)	This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. The user may set a time between 0 and 255 seconds with a default setting of 150 seconds. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network.
Candidate RP Priority (0-255)	Enter a priority value to determine which CRP will become the RP for the distribution tree. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP. The user may set a priority between 0 and 255 with a default setting of 192.
Candidate RP Wildcard Prefix Count (0-1)	The user may set the Prefix Count value of the wildcard group address here by choosing a value between 0 and 1 with a default setting of 0.
IP Address	Enter the IP address of the device to be added as a Candidate RP.
Subnet mask	Enter the corresponding subnet mask of the device to be added as a Candidate RP.
Interface Name	Enter the IP interface where this device is located.

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 specific entry.

PIM Static RP Settings

The following window will allow the user to configure and display the parameters for the Switch to become a static RP.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Static RP Settings**, as shown below:

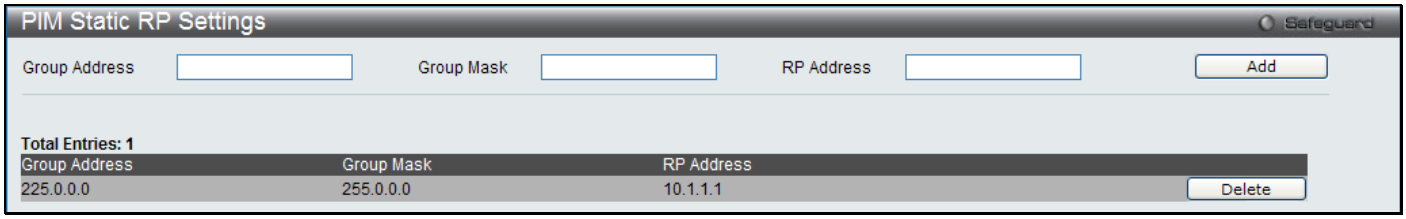


Figure 6-69 PIM Static RP Settings window

The fields that can be configured are described below:

Parameter	Description
Group Address	Enter the multicast group address for this Static RP. This address must be a class D address.
Group Mask	Enter the mask for the multicast group address stated above.
RP Address	Enter the IP address of the Rendezvous Point.

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

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

PIM Register Checksum Settings

This window is used to configure the IP address of the RP, for which the data part will be included when calculating the checksum for registering packets to the RP. The data part is included when calculating the checksum for a PIM register message to the RP on the first hop router.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Register Checksum Settings**, as shown below:

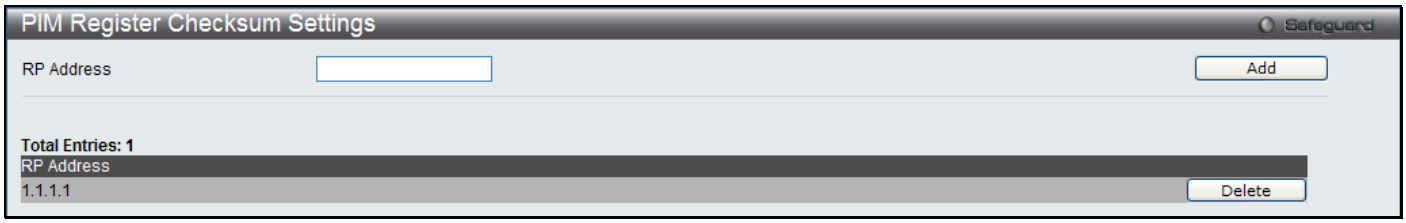


Figure 6-70 PIM Register Checksum Settings window

The fields that can be configured are described below:

Parameter	Description
RP Address	Enter the IP address of the RP for which the data part will be included when calculating checksum for registering packets to the RP.

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

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

PIM Neighbor Table

This window is used to display the current PIM neighbor router table.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Neighbor Table**, as shown below:

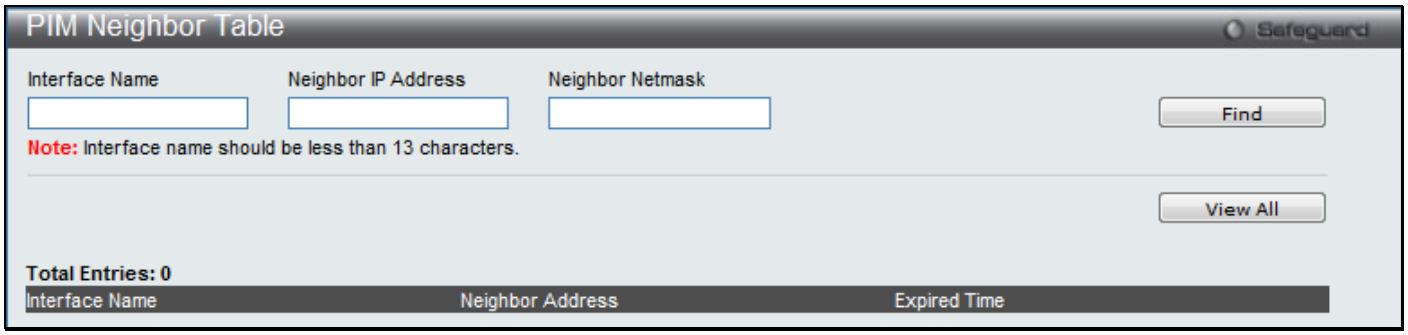


Figure 6-71 PIM Neighbor Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IP interface for which you want to display the current PIM neighbor routing table.

Neighbor IP Address	Enter the IP address of the destination.
Neighbor Netmask	Enter the netmask of the destination.

Click the **Find** button to find the interface entered.

Click the **View All** button to view all the interfaces configured on this switch.

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

PIM Multicast Route Table

This window is used to display the current PIM multicast route table.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Multicast Route Table**, as shown below:

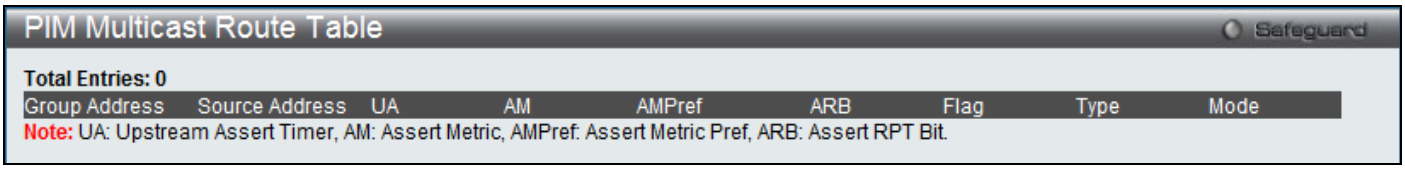


Figure 6-72 PIM Multicast Route Table window

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

PIM RP-Set Table

This window is used to display a list of all the RP-Set information.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP-Set Table**, as shown below:

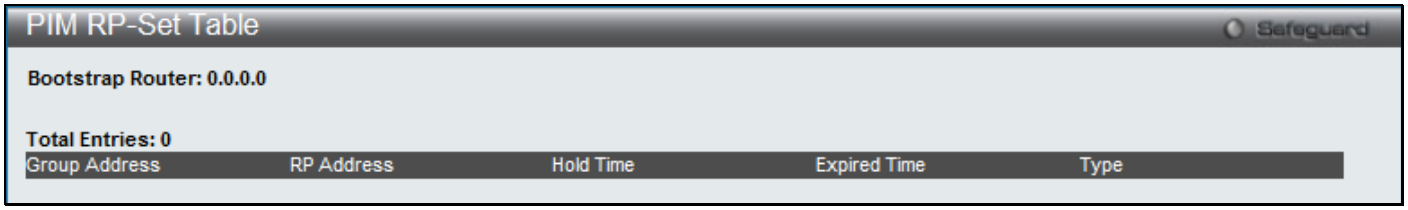


Figure 6-73 PIM RP-Set Table window

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

PIM SSM Settings

This window is used to enable the SSM (Source-Specific Multicast) service model in PIM-SM on the Switch. The PIM-SSM function will take active only when SSM service model and PIM-SM state both enabled.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SSM Settings**, as shown below:

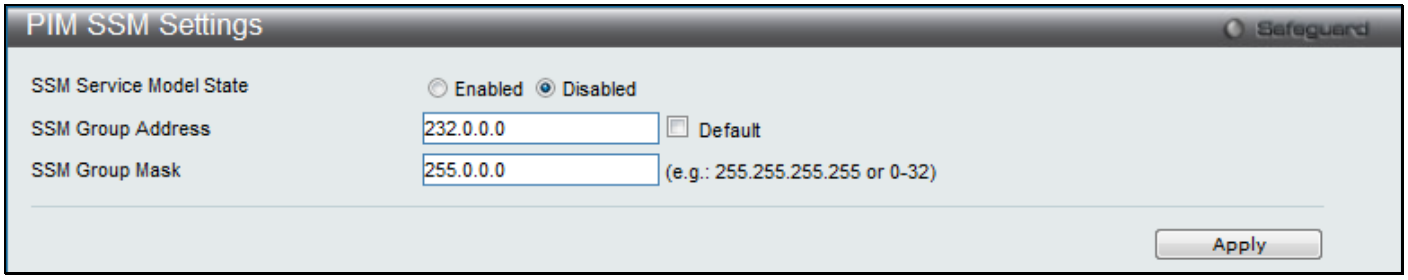


Figure 6-74 PIM SSM Settings window

The fields that can be configured are described below:

Parameter	Description

SSM Service Model State	Click the radio buttons to enable or disable the SSM service model on the Switch.
SSM Group Address	Enter the group address range for the SSM service in IPv4. Tick the Default check box to indicate that the group address range is 232.0.0.0/8.
SSM Group Mask	Enter the netmask of the SSM group.

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

VRRP

VRRP or Virtual Routing Redundancy Protocol is a function on the Switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the Switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the Switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

VRRP Global Settings

This window is used to configure the VRRP Global settings for this switch.

To view the following window, click **L3 Features > VRRP > VRRP Global Settings**, as shown below:

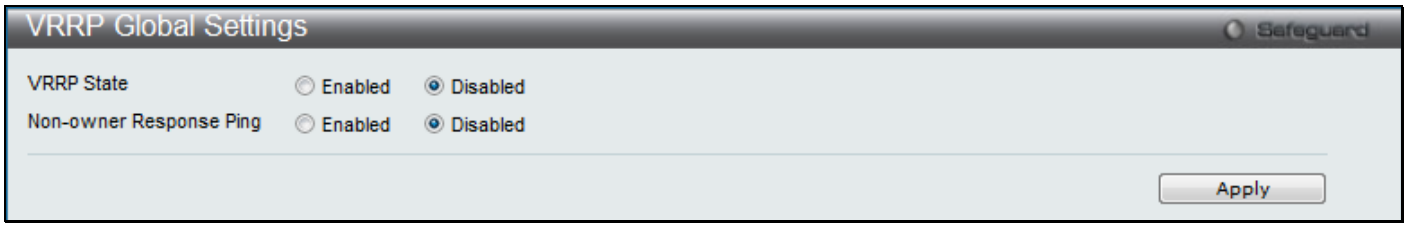


Figure 6-75 VRRP Global Settings window

The fields that can be configured are described below:

Parameter	Description
VRRP State	Specifies whether the VRRP Global state is enabled or disabled.
Non-owner Response Ping	Specifies that the virtual IP address is allowed to be pinged from other host end nodes to verify connectivity.

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

VRRP Virtual Router Settings

This window is used to configure the VRRP virtual router settings.

To view the following window, click **L3 Features > VRRP > VRRP Virtual Router Settings**, as shown below:

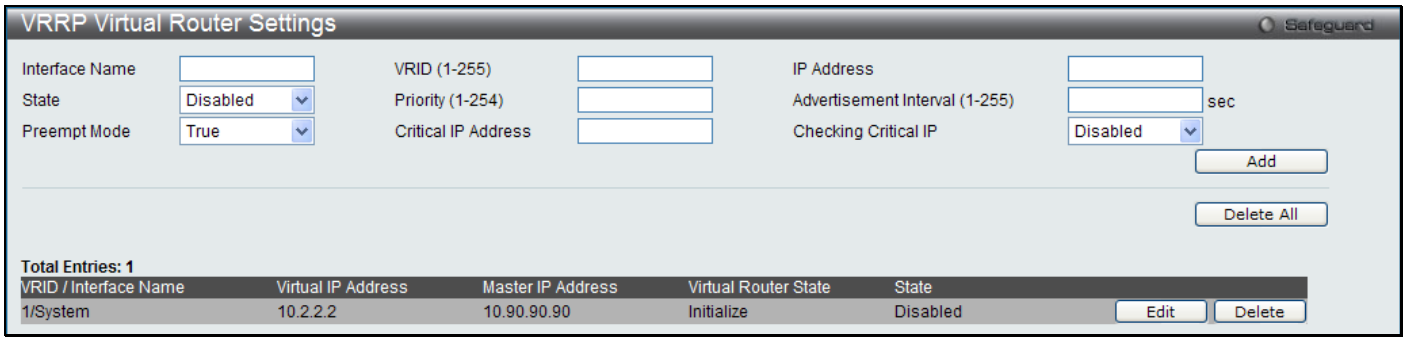


Figure 6-76 VRRP Virtual Router Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Specifies the IP interface name used to create a VRRP entry.
State	Specifies the state of the virtual router function of the interface.
Preempt Mode	This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A True entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A False entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group.
VRID (1-255)	Specifies the ID of the Virtual Router used. All routers participating in this group must be assigned the same VRID value. This value must be different from other VRRP groups set on the Switch.
Priority (1-254)	Specifies the priority to be used for the Virtual Router Master election process. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router.
Critical IP Address	Specifies an IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.
IP Address	Specifies the virtual router's IP address used. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.
Advertisement Interval (1-255)	Specifies the time interval used between sending advertisement messages.
Checking Critical IP	Specifies the state of checking the status (active or inactive) of a critical IP address. Options to choose from are **Enabled** and **Disabled**.

Click the **Add** button to add a new entry.

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

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

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

After clicking the **Edit** button, the following page with be displayed.

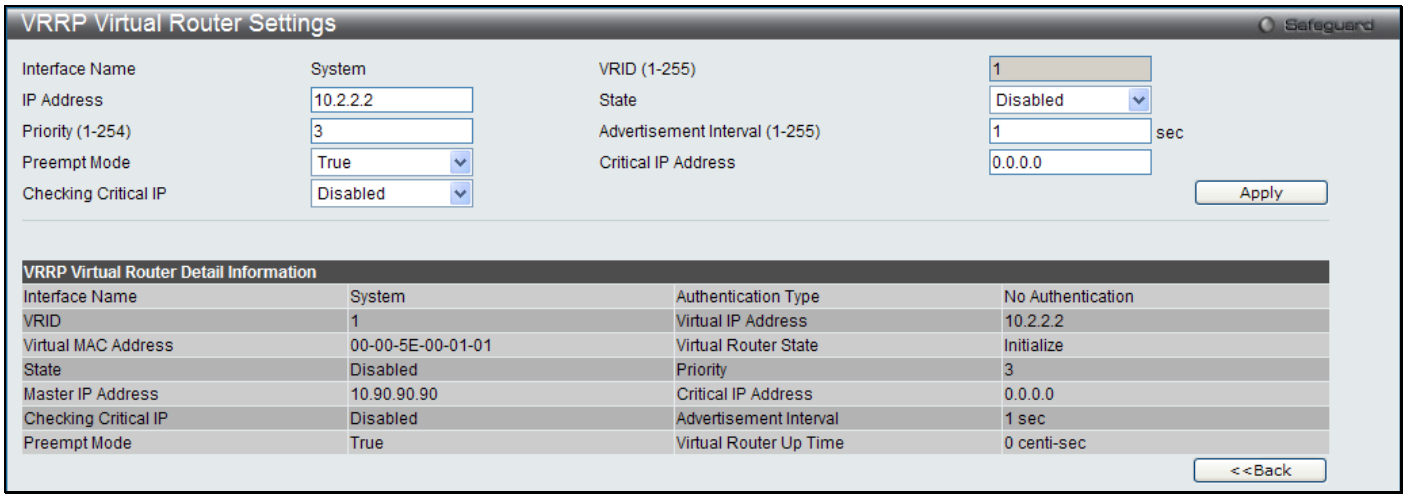


Figure 6-77 VRRP Virtual Router Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Displays the IP interface used to create a VRRP entry.
IP Address	Specifies the virtual router's IP address used. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.
Priority	Specifies the priority to be used for the Virtual Router Master election process
Preempt Mode	This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A True entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A False entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group.
Checking Critical IP	Specifies the state of checking the status (active or inactive) of a critical IP address. Options to choose from are **Enabled** and **Disabled**.
VRID	Specifies the ID of the Virtual Router used. All routers participating in this group must be assigned the same VRID value. This value must be different from other VRRP groups set on the Switch.
State	Specifies the state of the virtual router function of the interface.
Advertisement Interval	Specifies the time interval used between sending advertisement messages.
Critical IP Address	Specifies an IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.

Click the **Apply** button to accept the changes made.
Click on the **<<Back** button to return to the previous window.

VRRP Authentication Settings

This window is used to configure a virtual router authentication type on an interface.

To view the following window, click **L3 Features > VRRP > VRRP Authentication Settings**, as shown below:

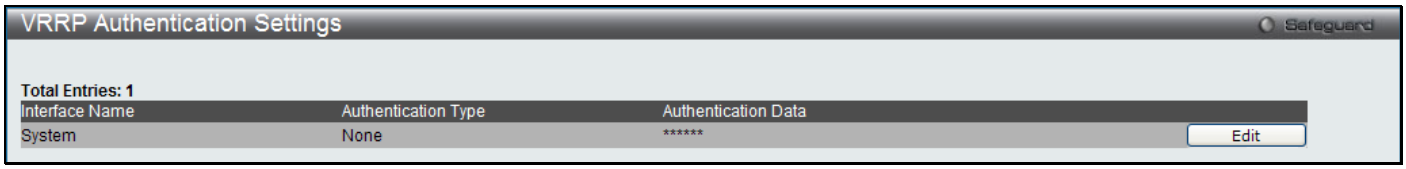


Figure 6-78 VRRP Authentication Settings window

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

The fields that can be configured are described below:

Parameter	Description
Authentication Type	Specifies the VRRP's authentication type. Options to choose from are **None**, **Simple** and **IP**. **None** - Selecting this parameter indicates that VRRP protocol exchanges will not be authenticated. **Simple** - Selecting this parameter will require the user to set a simple password in the Auth. Data field for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped. **IP** - Selecting this parameter will require the user to set an IP for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
Authentication Data	Specifies the authentication data used in the **Simple** and **IP** authentication algorithm. This entry must be consistent with all routers participating in the same IP interface. **Simple** - Simple will require the user to enter an alphanumeric string of no more than eight characters to identify VRRP packets received by a router. **IP** - IP will require the user to enter an alphanumeric string of no more than sixteen characters to identify VRRP packets received by a router.

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

MD5 Settings

The MD5 Configuration allows the entry of a 16 character Message Digest version 5 (MD5) key which can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain. This page is used to configure an MD5 key and password.

To view the following window, click **L3 Features > MD5 Settings**, as shown below:

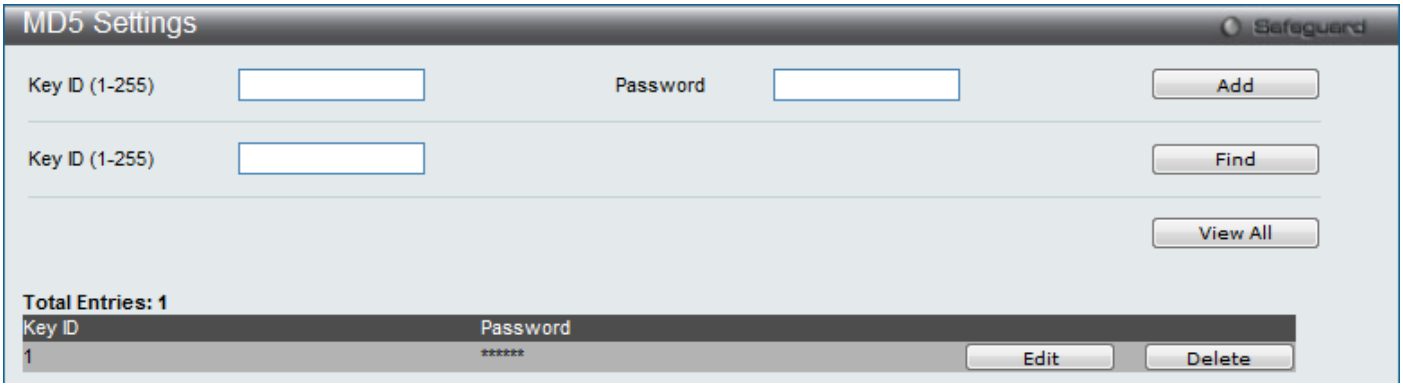


Figure 6-79 MD5 Settings window

The fields that can be configured are described below:

Parameter	Description
Key ID (1-255)	Specifies a number from 1 to 255 used to identify the MD5 Key.

Password	Specifies an alphanumeric string of between 1 and 16 case-sensitive characters used to generate the Message Digest which is in turn, used to authenticate OSPF packets within the OSPF routing domain.

Click the **Add** button to add a new Key ID with its corresponding password.

Click the **Find** button to search for the Key ID entered.

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

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

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

Chapter 7 QoS

802.1p Settings
Bandwidth Control
Traffic Control Settings
DSCP
HOL Blocking Prevention
Scheduling Settings

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements basic 802.1P priority queuing.

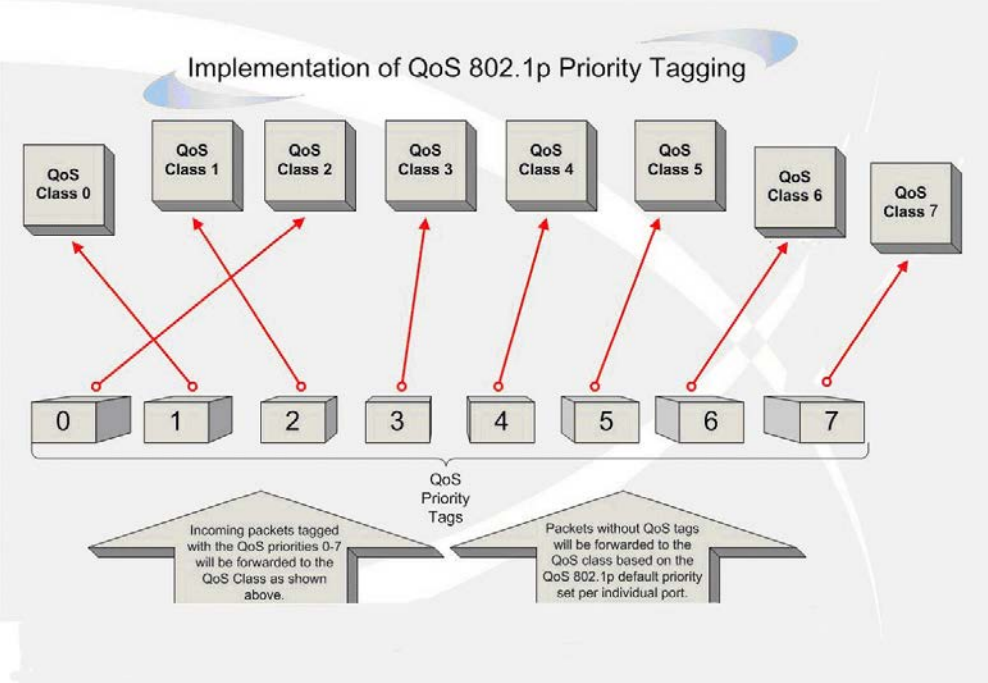


Figure 7-1 Implementation of QoS 802.1p Priority Tagging window

The picture above shows the default priority setting for the Switch. Class-7 has the highest priority of the seven priority classes of service on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, let's say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch supports 802.1p priority queuing. The Switch has eight priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.

- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of eight CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the Switch has eight configurable priority queues (and eight Classes of Service) for each port on the Switch.

NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the eight classes of service that may be used and configured by the administrator.

802.1p Settings

802.1p Default Priority Settings

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. This page allows the user to assign a default 802.1p priority to any given port on the switch that will insert the 802.1p priority tag to untagged packets received. The priority and effective priority tags are numbered from *0*, the lowest priority, to *7*, the highest priority. The effective priority indicates the actual priority assigned by RADIUS. If the RADIUS assigned value exceeds the specified limit, the value will be set at the default priority. For example, if the RADIUS assigns a limit of 8 and the default priority is 0, the effective priority will be 0.

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

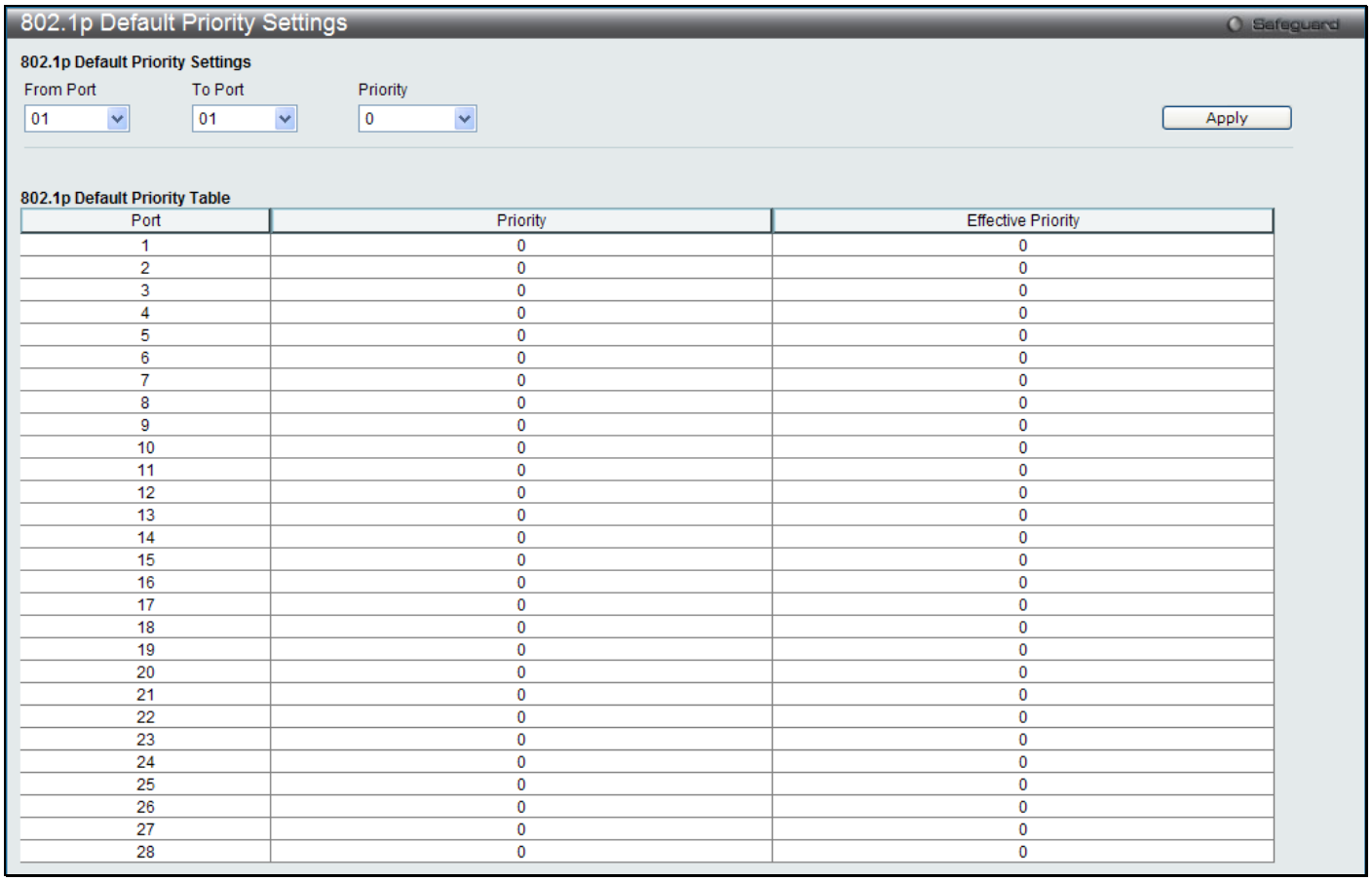


Figure 7-2 802.1p Default Priority Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Specifies the list of ports, to be used for this configuration, here.
Priority	Specifies the priority value that will be applied to the selected ports. Options to choose from are between 0 and 7.

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

802.1p User Priority Settings

The Switch allows the assignment of a class of service to each of the 802.1p priorities.

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

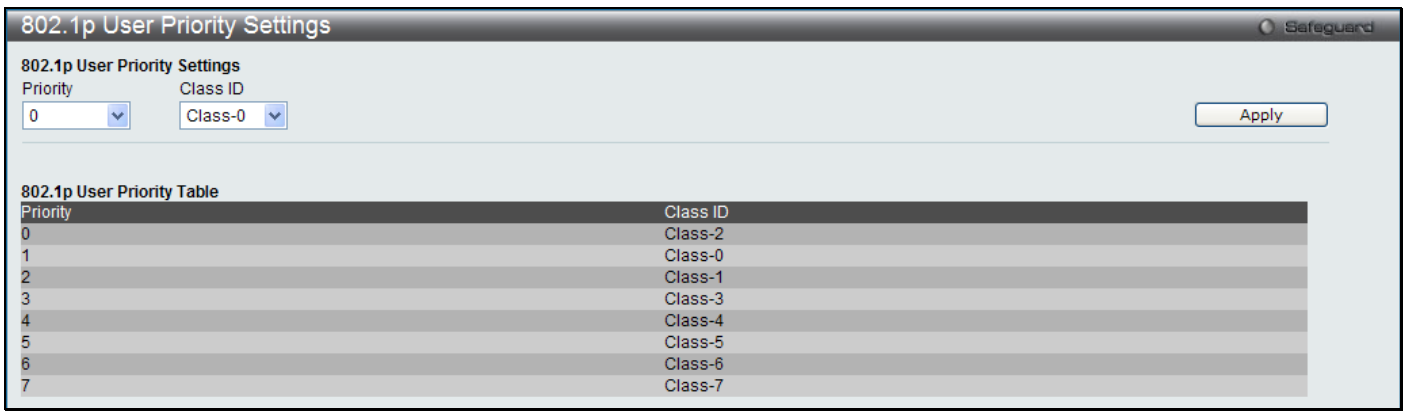


Figure 7-3 802.1p User Priority Settings window

The fields that can be configured are described below:

Parameter	Description
Priority	Specifies the priority value that will be applied to the selected Class ID.
Class ID	Specifies the Class ID used here. Once a priority has been assigned to the port groups on the Switch, then a Class may be assigned to each of the eight levels of 802.1p priorities. User priority mapping is not only for the default priority configured in the last page, but also for all the incoming tagged packets with 802.1p tag.

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

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

Bandwidth Control Settings

The Effective RX/TX Rate refers to the actual bandwidth of the switch port, if it does not match the configured rate. This usually means that the bandwidth has been assigned by a higher priority resource, such as a RADIUS server.

To view the following window, click **QoS > Bandwidth Control > Bandwidth Control Settings**, as shown below:

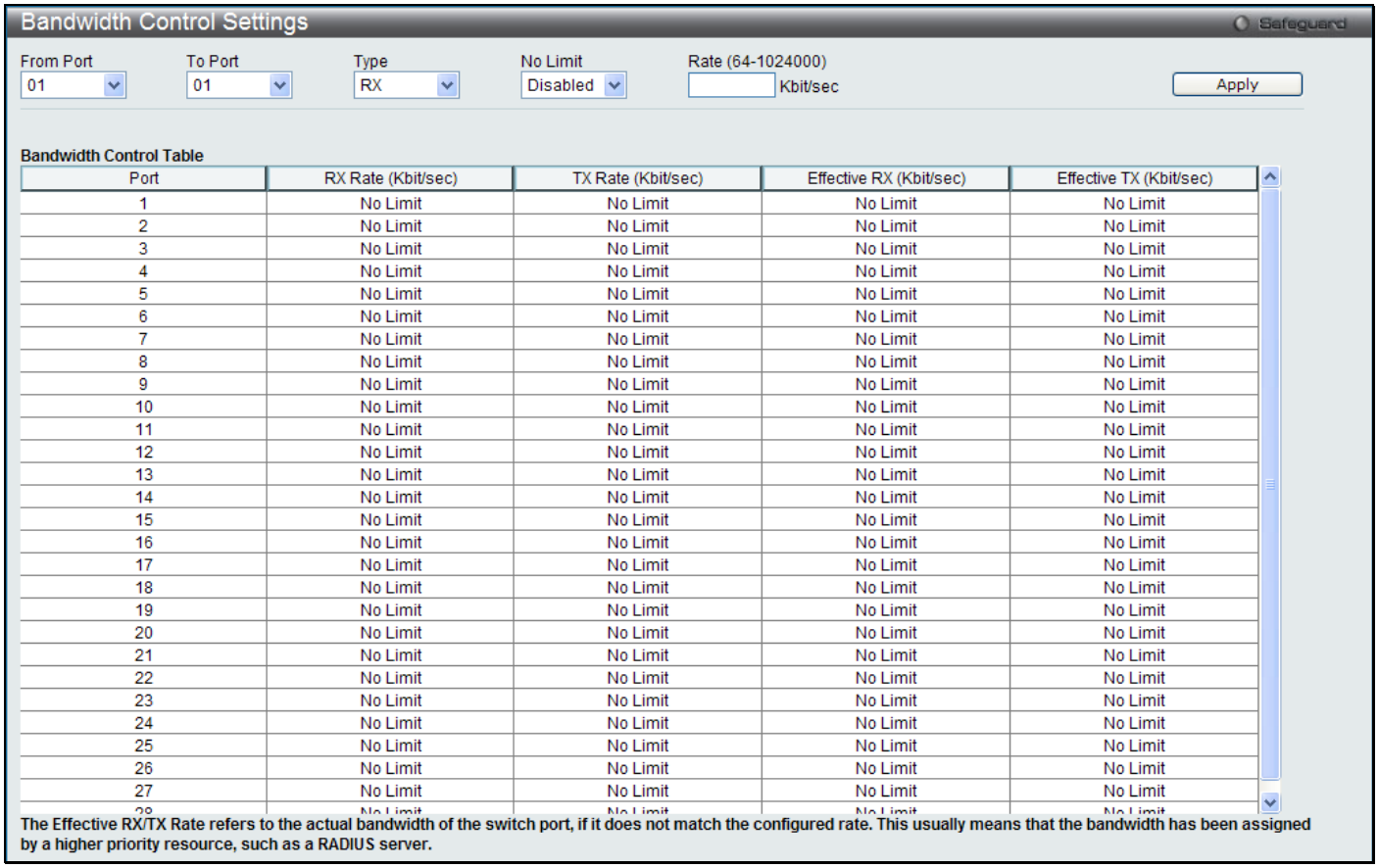


Figure 7-4 Bandwidth Control Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
Type	This drop-down menu allows a selection between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit	This drop-down menu allows the user to specify that the selected port will have no bandwidth limit or not. **NOTE:** If the configured number is larger than the port speed, it means no bandwidth limit.
Rate (64-1024000)	This field allows the input of the data rate that will be the limit for the selected port. The user may choose a rate between *64* and *1024000* Kbits per second.

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

Queue Bandwidth Control Settings

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

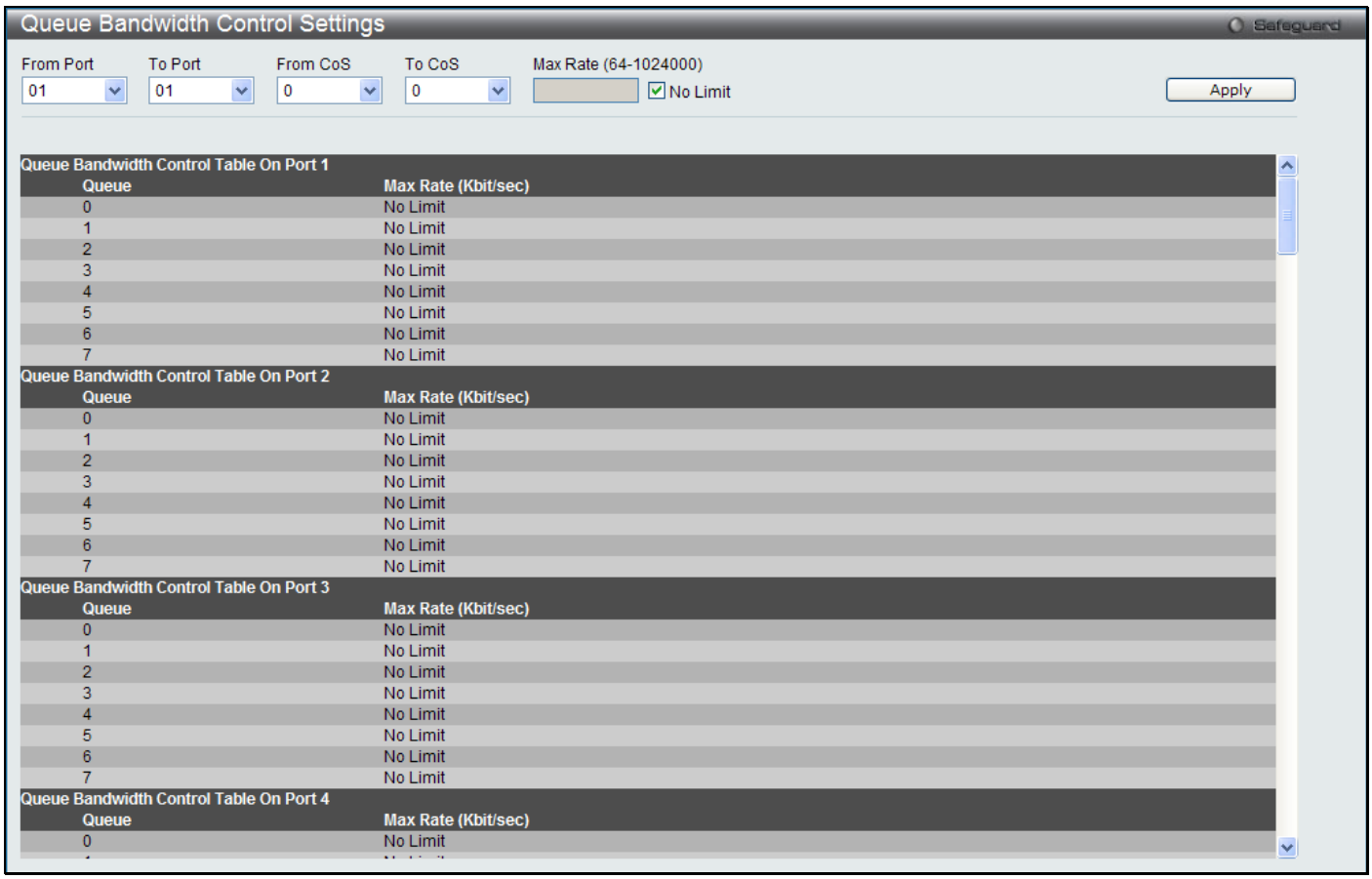


Figure 7-5 Queue Bandwidth Control Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select the port range to use for this configuration.
From CoS / To CoS	Here the user can select the queue range to use for this configuration.
Max Rate (64-1024000)	Here the user can enter the maximum rate for the queue. Tick the **No Limit** check box to have unlimited rate.

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

NOTE: The minimum granularity of queue bandwidth control is 1.85MBps. The system will adjust the number to the multiple of 1850 automatically.

Traffic Control Settings

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious end station on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

Packet storms are monitored to determine if too many packets are flooding the network based on threshold levels provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the *Drop* option of the Action parameter in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shut down the port to all incoming traffic, with the exception of STP BPDU packets, for a time period specified using the Count Down parameter.

If a Time Interval parameter times-out for a port configured for traffic control and a packet storm continues, that port will be placed in Shutdown Forever mode, which will cause a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the method of recovering the port is to manually recoup it using the **Port Settings** window in the **Configuration** folder or automatic recovering after 5 minutes. Select the disabled port and return its State to *Enabled* status. To utilize this method of Storm Control, choose the *Shutdown* option of the Action parameter in the window below.

Use this window to enable or disable storm control and adjust the threshold for multicast and broadcast storms.

To view the following window, click **QoS > Traffic Control Settings**, as shown below:

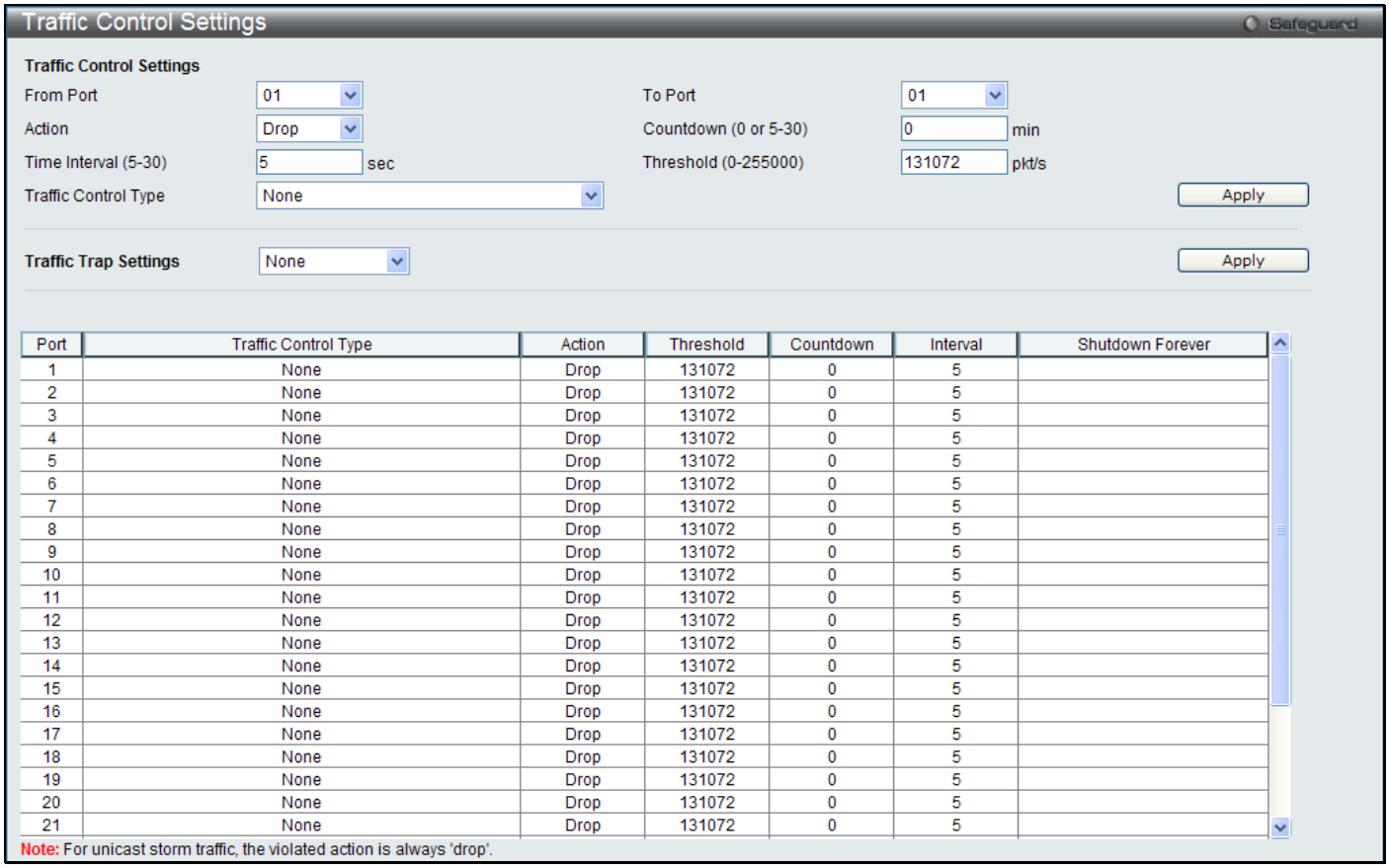


Figure 7-6 Traffic Control Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
Action	Select the method of traffic control from the pull-down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *Shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Count Down timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the port recovers after 5 minutes automatically or the user manually resets the port using the **Port Settings** window (**Configuration> Port Configuration> Port Settings**). Choosing this option obligates the user to configure the Time Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Count Down (0 or 5-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as *Shutdown* in their Action field and therefore will not operate for hardware-based Traffic Control implementations. The possible time settings for this field are *0* and *5* to *30* minutes.
Time Interval (5-30)	The Time Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Time Interval may be set between *5* and *30* seconds, with a default setting of *5* seconds.
Threshold (0-255000)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from *0-255000* with a default setting of *130560* packets per second.
Traffic Control Type	Specifies the desired Storm Control Type: *None*, *Broadcast*, *Multicast*, *Unknown Unicast*, *Broadcast + Multicast*, *Broadcast + Unknown Unicast*, *Multicast + Unknown Unicast*, and *Broadcast + Multicast + Unknown Unicast*.
Traffic Trap Settings	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: *None* – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. *Storm Occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. *Storm Cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. *Both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. This function cannot be implemented in the hardware mode. (When *Drop* is chosen for the Action parameter)

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

NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).

NOTE: Ports that are in the Shutdown Forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

NOTE: Ports that are in Shutdown Forever mode will be seen as link down in all windows and screens until the user recovers these ports.

NOTE: The minimum storm control threshold granularity: FE port 500pps, GE port 640pps.

DSCP

DSCP Trust Settings

This page is to configure the DSCP trust state of ports. When ports are under the DSCP trust mode, the switch will insert the priority tag to untagged packets by using the DSCP Map settings instead of the default port priority.

To view the following window, click **QoS > DSCP > DSCP Trust Settings**, as shown below:

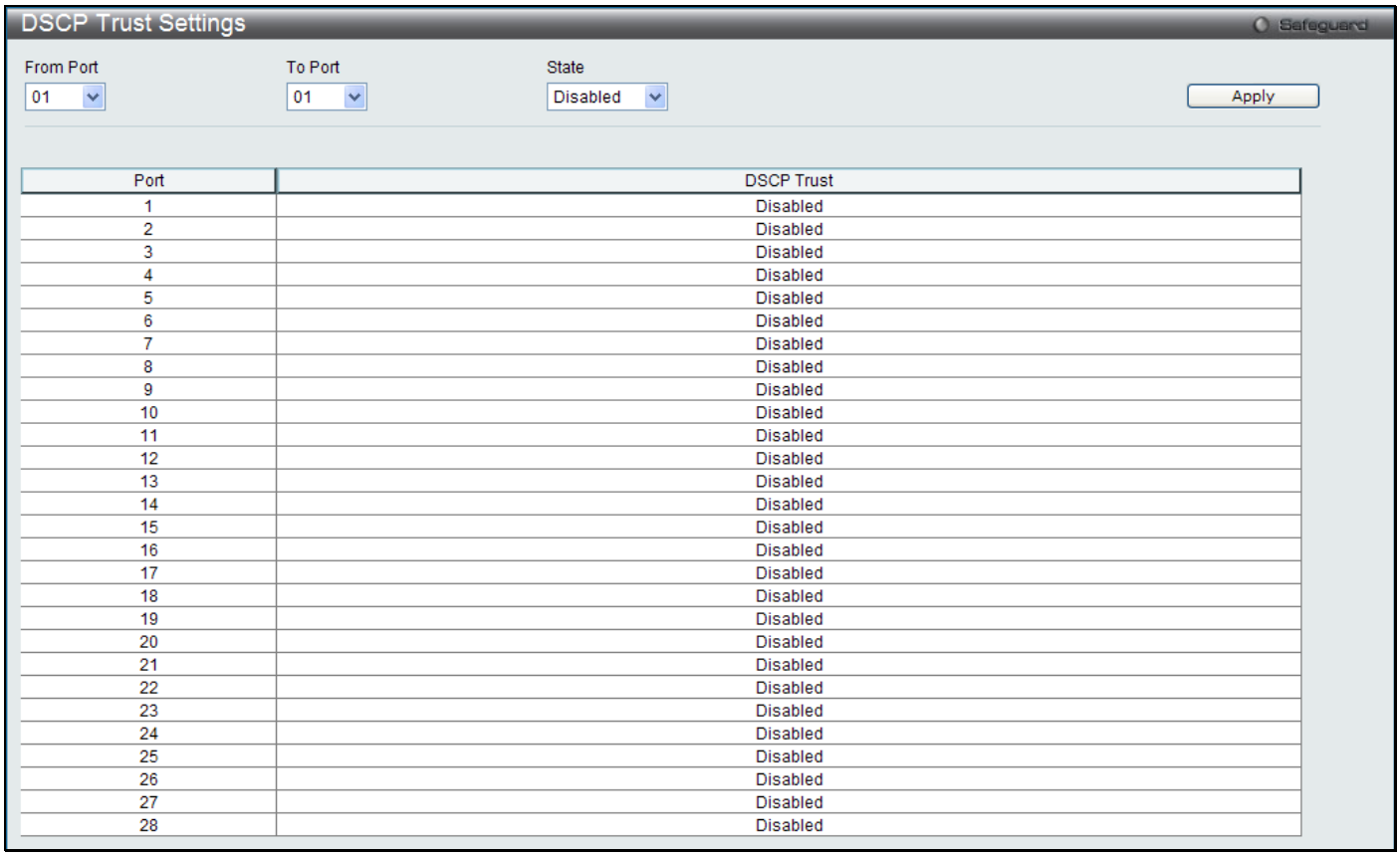


Figure 7-7 DSCP Trust Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of port to configure.
State	Enable/disable to trust DSCP. By default, DSCP trust is disabled.

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

DSCP Map Settings

The mapping of DSCP to queue will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

To view the following window, click **QoS > DSCP > DSCP Map Settings**, as shown below:

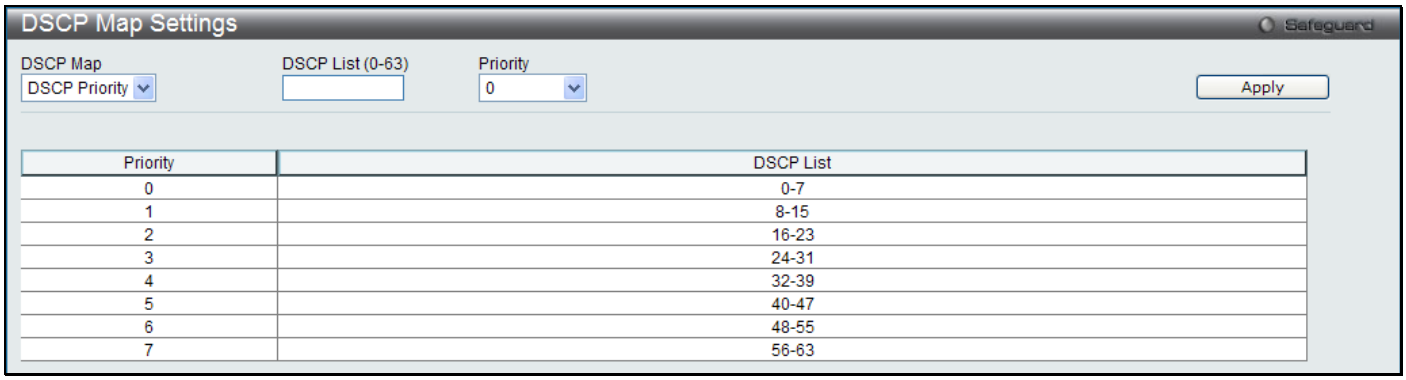


Figure 7-8 DSCP Map Settings – DSCP Priority window

To view the following window, click **QoS > DSCP > DSCP Map Settings** and select **DSCP DSCP** from the DSCP Map drop-down menu, as show below:

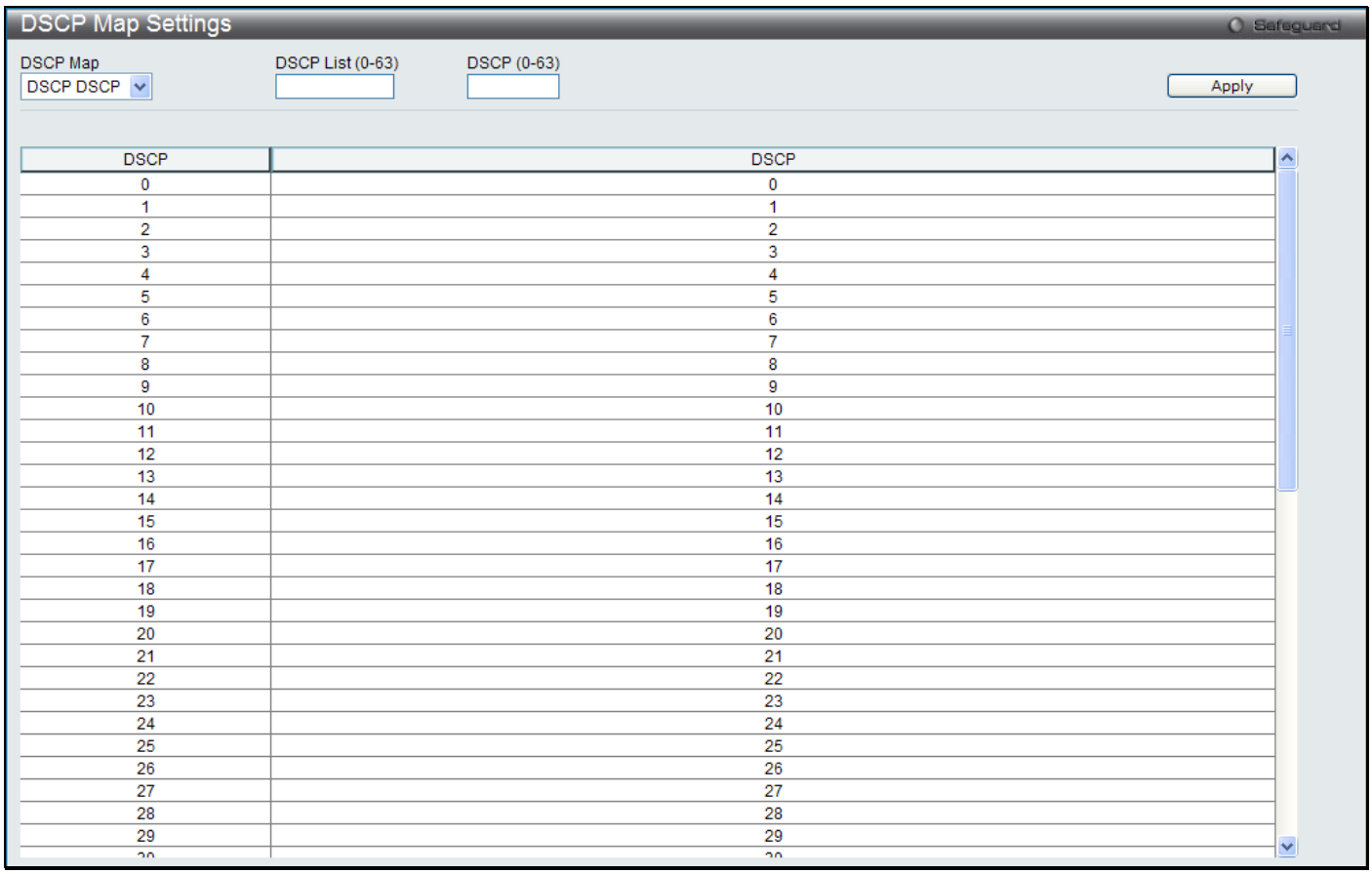


Figure 7-9 DSCP Map Settings – DSCP DSCP window

The fields that can be configured are described below:

Parameter	Description
DSCP Map	Here the user can select one of two options: *DSCP Priority* – Specifies a list of DSCP values to be mapped to a specific priority. *DSCP DSCP* – Specifies a list of DSCP value to be mapped to a specific DSCP.
DSCP List	Here the user can enter a DSCP List value.
Priority	Here the user can select a Priority value.
DSCP (0-63)	Enter a DSCP value. This appears when selecting *DSCP DSCP* in the **DSCP Map** drop-down menu.

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

HOL Blocking Prevention

HOL (Head of Line) Blocking happens when one of the destination ports of a broadcast or multicast packet are busy. The switch will hold this packet in the buffer while the other destination port will not transmit the packet even they are not busy. The HOL Blocking Prevention will ignore the busy port and forward the packet directly to have lower latency and better performance.

On this page the user can enable or disable HOL Blocking Prevention.

To view the following window, click **QoS > HOL Blocking Prevention**, as shown below:

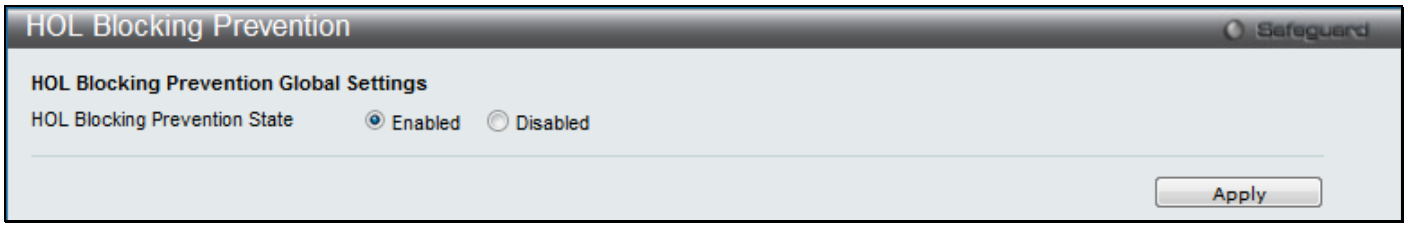


Figure 7-10 HOL Blocking Prevention window

The fields that can be configured are described below:

Parameter	Description
HOL Blocking Prevention Global Settings	Here the user can enable of disable the HOL blocking prevention global settings.

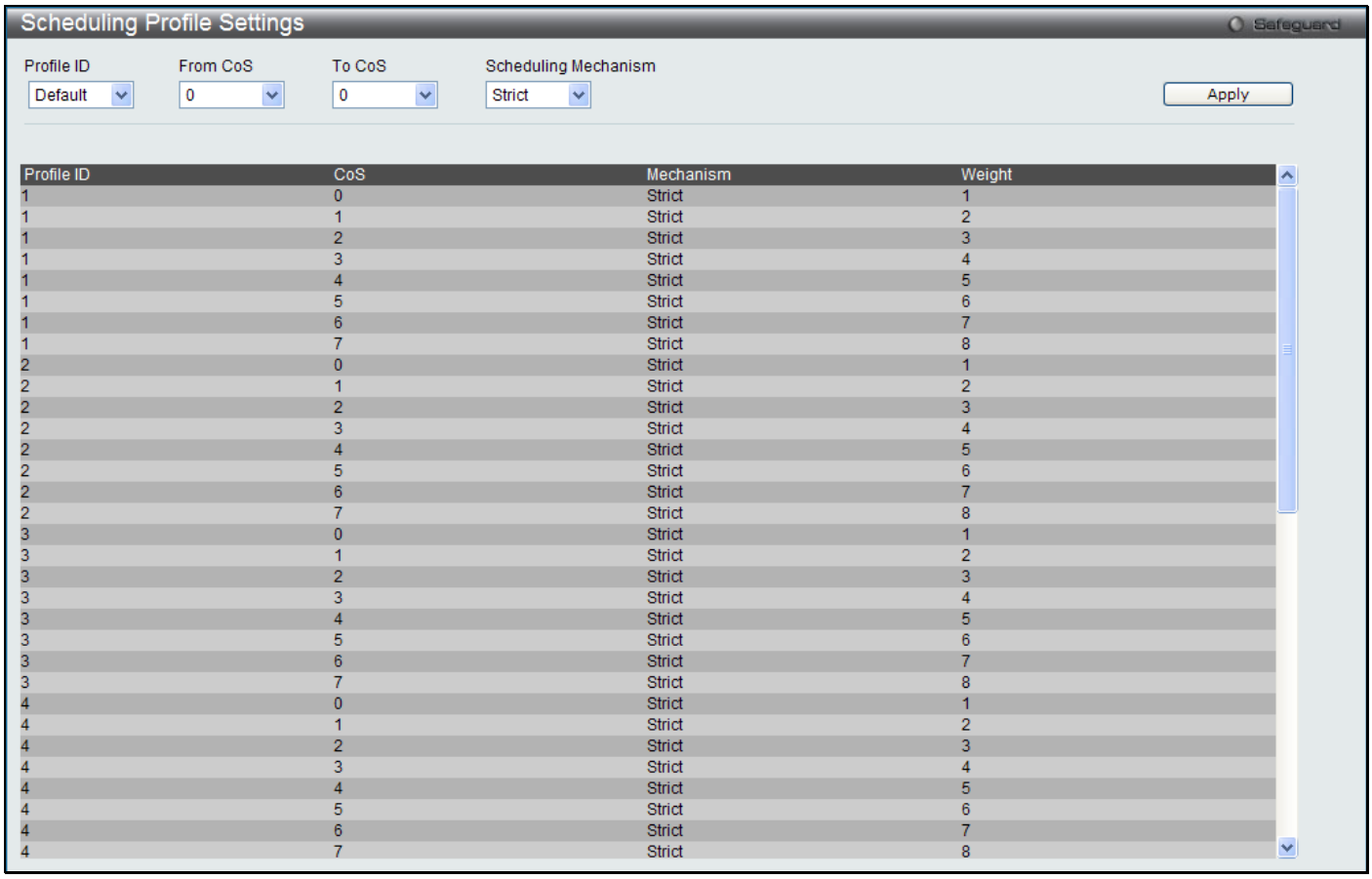
Click the **Apply** button to accept the changes made.

Scheduling Settings

Scheduling Profile Settings

Changing the output scheduling used for the hardware queues in the Switch can customize the QoS. As with any changes to the QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to the monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view the following window, click **QoS > Scheduling Settings > Scheduling Profile Settings**, as shown below:



Profile ID	CoS	Mechanism	Weight
1	0	Strict	1
1	1	Strict	2
1	2	Strict	3
1	3	Strict	4
1	4	Strict	5
1	5	Strict	6
1	6	Strict	7
1	7	Strict	8
2	0	Strict	1
2	1	Strict	2
2	2	Strict	3
2	3	Strict	4
2	4	Strict	5
2	5	Strict	6
2	6	Strict	7
2	7	Strict	8
3	0	Strict	1
3	1	Strict	2
3	2	Strict	3
3	3	Strict	4
3	4	Strict	5
3	5	Strict	6
3	6	Strict	7
3	7	Strict	8
4	0	Strict	1
4	1	Strict	2
4	2	Strict	3
4	3	Strict	4
4	4	Strict	5
4	5	Strict	6
4	6	Strict	7
4	7	Strict	8

Figure 7-11 Scheduling Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can select the profile ID to configure.
From CoS / To CoS	Here the user can select the range on CoS to configure.
Scheduling Mechanism	Here the user can select one of two Scheduling Mechanisms: *Strict* – The queue will operate in strict mode. The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weight* – Specifies the weights for weighted round robin. A value between 1 and n can be specified. The queue will operate in WRR mode if port mode is WRR. It will operate in strict mode if port mode is strict. Determination of n is project dependent.

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

Scheduling Group Settings

On this page the user can configure the scheduling group parameters.

To view the following window, click **QoS > Scheduling Settings > Scheduling Group Settings**, as shown below:

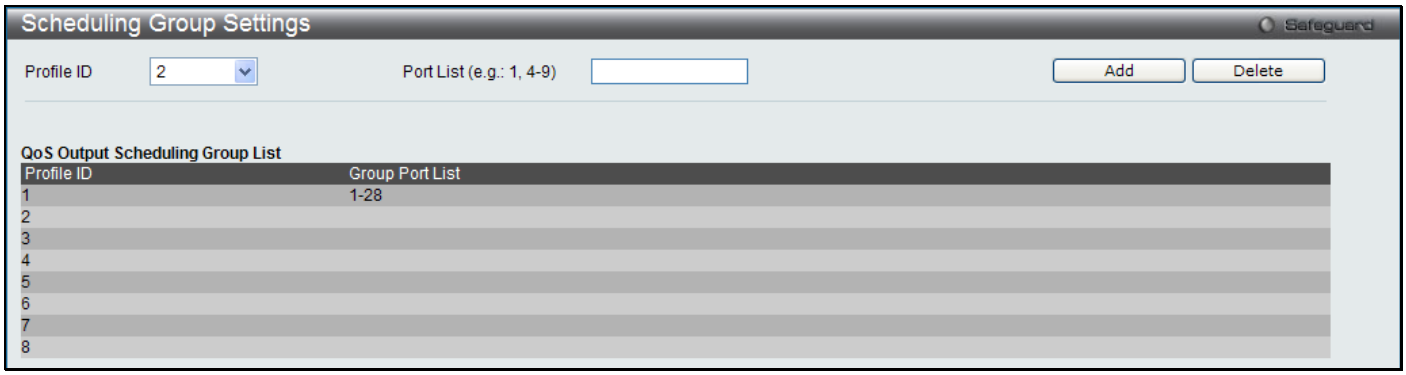


Figure 7-12 Scheduling Group Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can select the profile ID to configure.
Port List	Here the user can enter the port range to configure.

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

Chapter 8 ACL

ACL Configuration Wizard
Access Profile List
CPU Access Profile List
ACL Finder
ACL Flow Meter
Egress Access Profile List
Egress ACL Flow Meter

ACL Configuration Wizard

The ACL Configuration Wizard will aid the user in the creation of access profiles and ACL Rules automatically by simply inputting the address or service type and the action needed. It saves administrators a lot of time.

To view the following window, click **ACL > ACL Configuration Wizard**, as shown below:

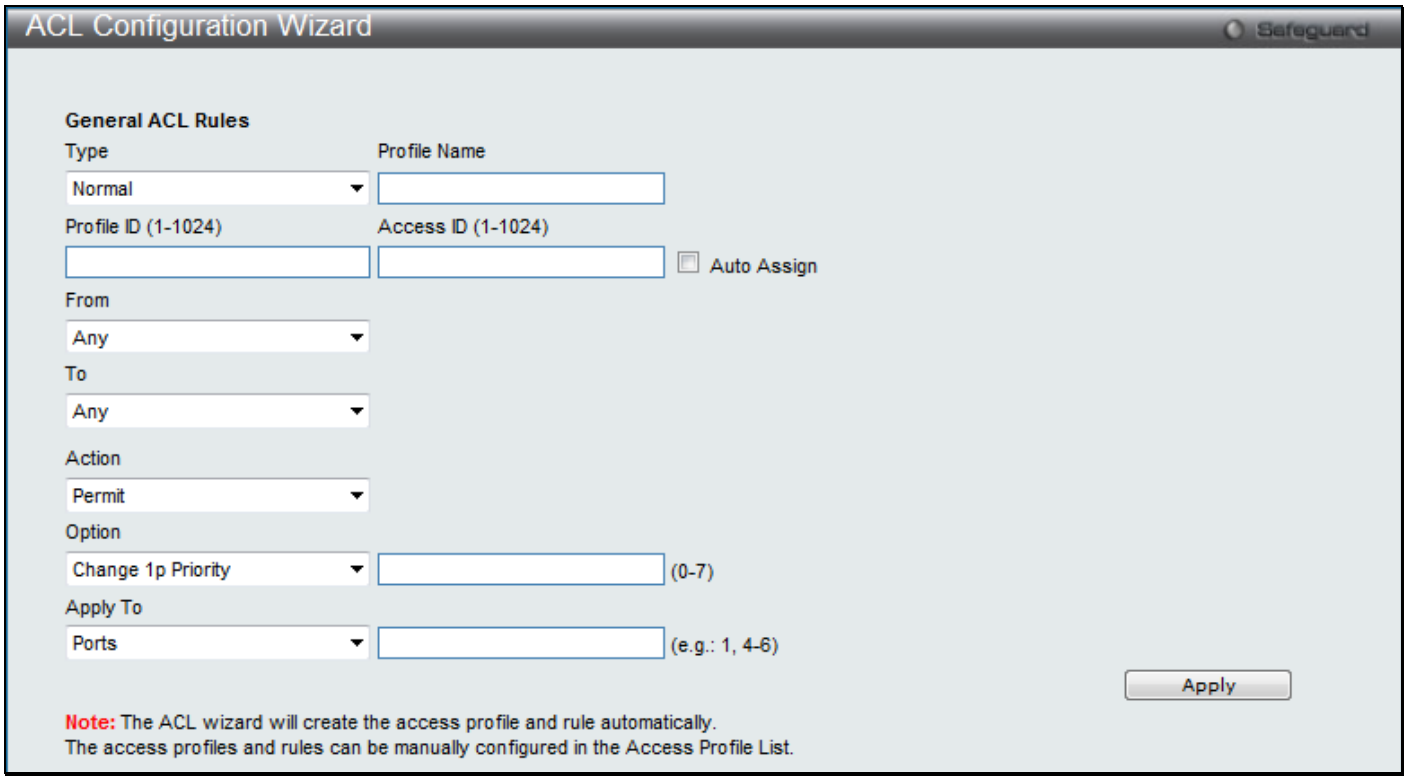


Figure 8-1 ACL Configuration Wizard window

The fields that can be configured are described below:

Parameter	Description
Type	Here the user can select one of three general ACL Rule types: *Normal* – Selecting this option will create a Normal ACL Rule. *CPU* – Selecting this option will create a CPU ACL Rule. *Egress* - Selecting this option will create an Egress ACL Rule.
Profile Name	After selecting to configure a **Normal** or **Egress** type rule, the user can enter the Profile Name for the new rule here.
Profile ID (1-1024)	Here the user can enter the Profile ID for the new rule.
Access ID (1-1024)	Here the user can enter the Access ID for the new rule. Selecting the **Auto Assign** option will allow the switch to automatically assign an unused access ID to this rule.

From / To	This rule can be created to apply to four different categories: *Any* – Selecting this option will include any starting category to this rule. *MAC Address* – Selecting this option will allow the user to enter a range of MAC addresses for this rule. *IPv4 Address* – Selecting this option will allow the user to enter a range of IPv4 addresses for this rule. *IPv6* – Selecting this option will allow the user to enter a range of IPv6 addresses for this rule.
Service Type	After selecting a subject in the **From** or **To** field, the user can select one of the following services: *Any* – Selecting this option will apply this rule to all service types. *ICMP All* – Selecting this option will apply this rule to all ICMP traffic used in this rule. *IGMP* – Selecting this option will apply this rule to IGMP traffic used in this rule. *TCP All* – Selecting this option will apply this rule to all TCP traffic used in this rule. *TCP Source Port* – Selecting this option will apply this rule to TCP traffic used in this rule from the source port only. *TCP Destination Port* – Selecting this option will apply this rule to TCP traffic used in this rule from the destination port only. *UDP All* – Selecting this option will apply this rule to all UDP traffic used in this rule. *UDP Source Port* – Selecting this option will apply this rule to UDP traffic used in this rule from the source port only. *UDP Destination Port* – Selecting this option will apply this rule to UDP traffic used in this rule from the destination port only. *VLAN Mask (Name)* – Selecting this option will apply this rule to the VLAN name used in this rule.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the mirror port section. Port Mirroring must be enabled and a target port must be set.
Option	After selecting the **Permit** action, the user can select one of the following options: *Change 1p Priority* – Here the user can enter the 1p priority value. *Replace DSCP* – Here the user can enter the DSCP value. *Replace ToS Precedence* – Here the user can enter the ToS Precedence value.
Apply To	Here the user can select and enter the object that this rule will be applied to. *Ports* – Here the user can enter a port number or a port range. *VLAN Name* – Here the user can enter the VLAN name. *VLAN ID* – Here the user can enter the VID.

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

NOTE: The Switch will use one minimum mask to cover all the terms that user input, however, some extra bits may also be masked at the same time. To optimize the ACL profile and rules, please use manual configuration.

Access Profile List

Access profiles allow you to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header.

The Switch supports four Profile Types, Ethernet ACL, IPv4 ACL, IPv6 ACL, and Packet Content ACL.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

Users can display the currently configured Access Profiles on the Switch.

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

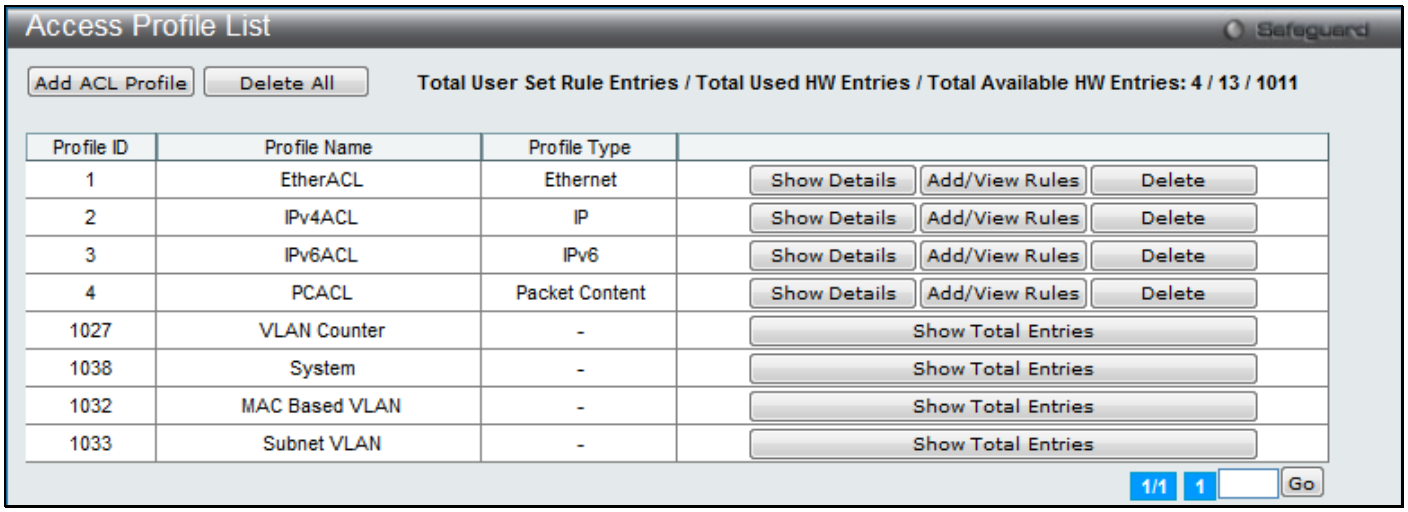


Figure 8-2 Access Profile List window

Click the **Add ACL Profile** button to add an entry to the **Access Profile List**.

Click the **Delete All** button to remove all access profiles from this table.

Click the **Show Details** button to display the information of the specific profile ID entry.

Click the **Add/View Rules** button to view or add ACL rules within the specified profile ID.

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

Click the **Show Total Entries** button to view the total amount of consumed hardware entries.

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

There are four **Add Access Profile** windows;

- one for Ethernet (or MAC address-based) profile configuration,
- one for IPv6 address-based profile configuration,
- one for IPv4 address-based profile configuration, and
- one for packet content profile configuration.

Adding an Ethernet ACL Profile

The window shown below is the **Add ACL Profile** window for Ethernet. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

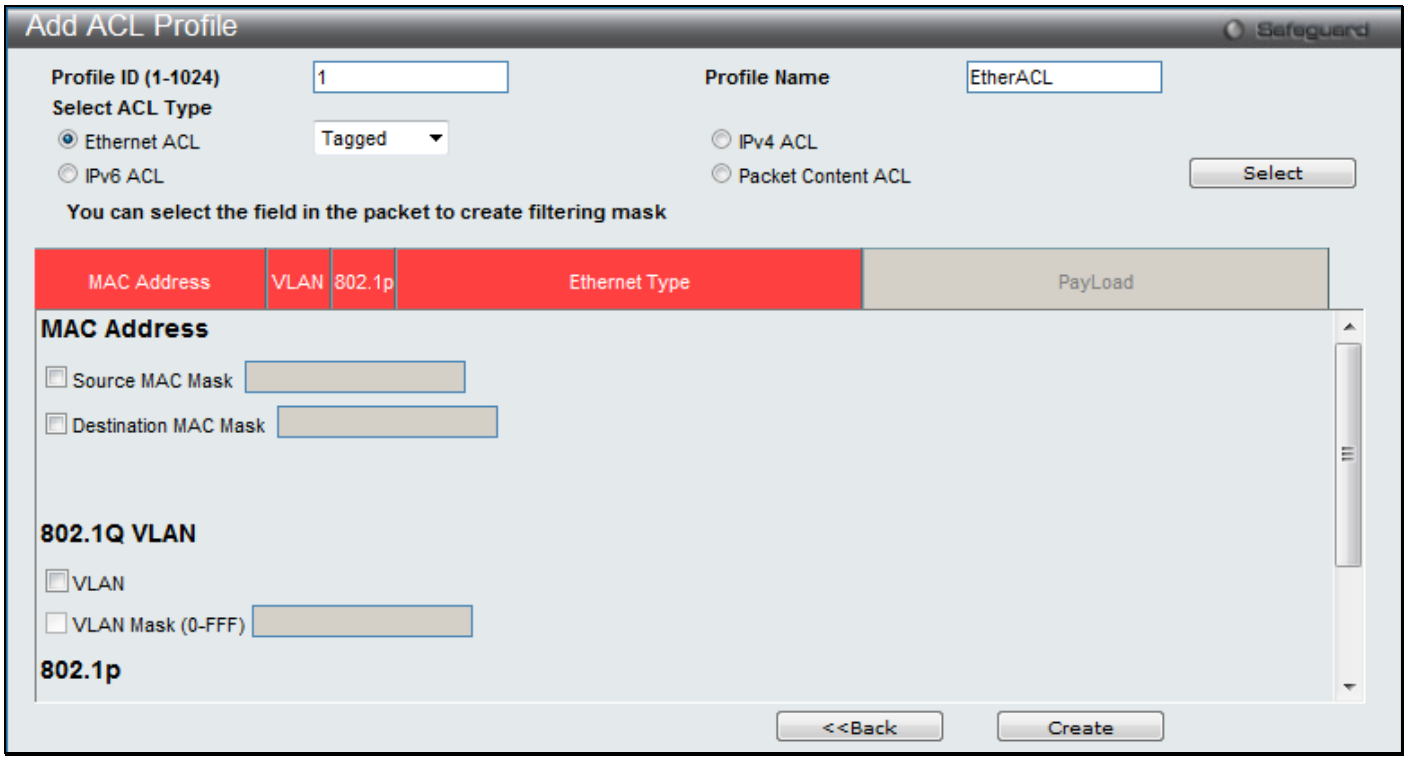


Figure 8-3 Add ACL Profile window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-1024)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *1024*
Profile Name	Here the user can enter a profile name for the profile created.
Select ACL Type	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

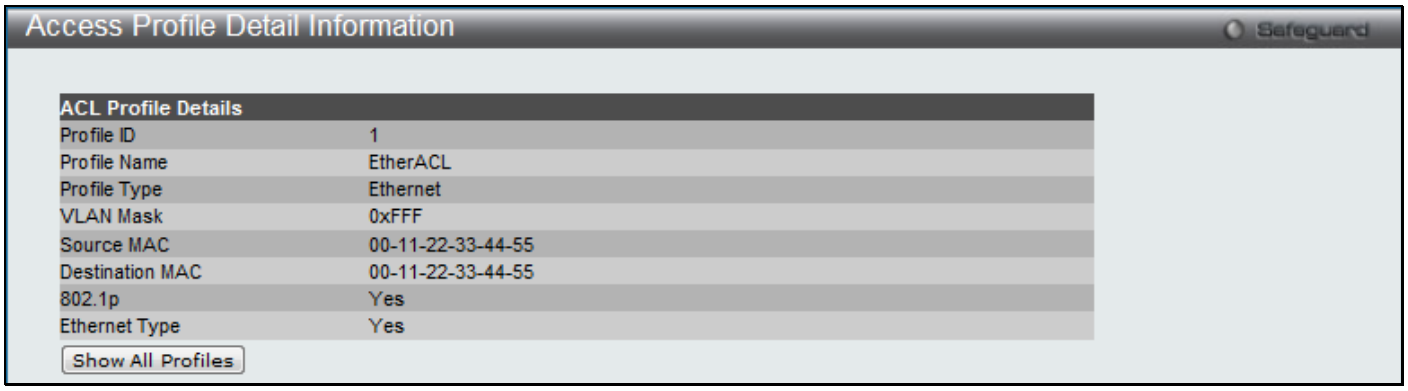


Figure 8-4 Access Profile Detail Information window (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

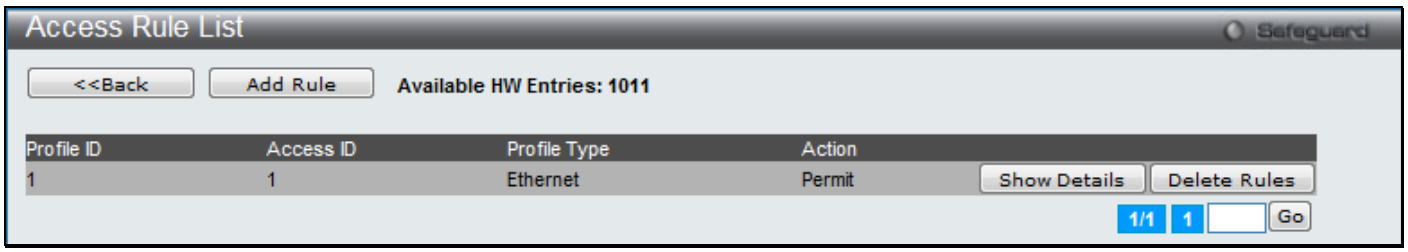


Figure 8-5 Access Rule List window (Ethernet ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

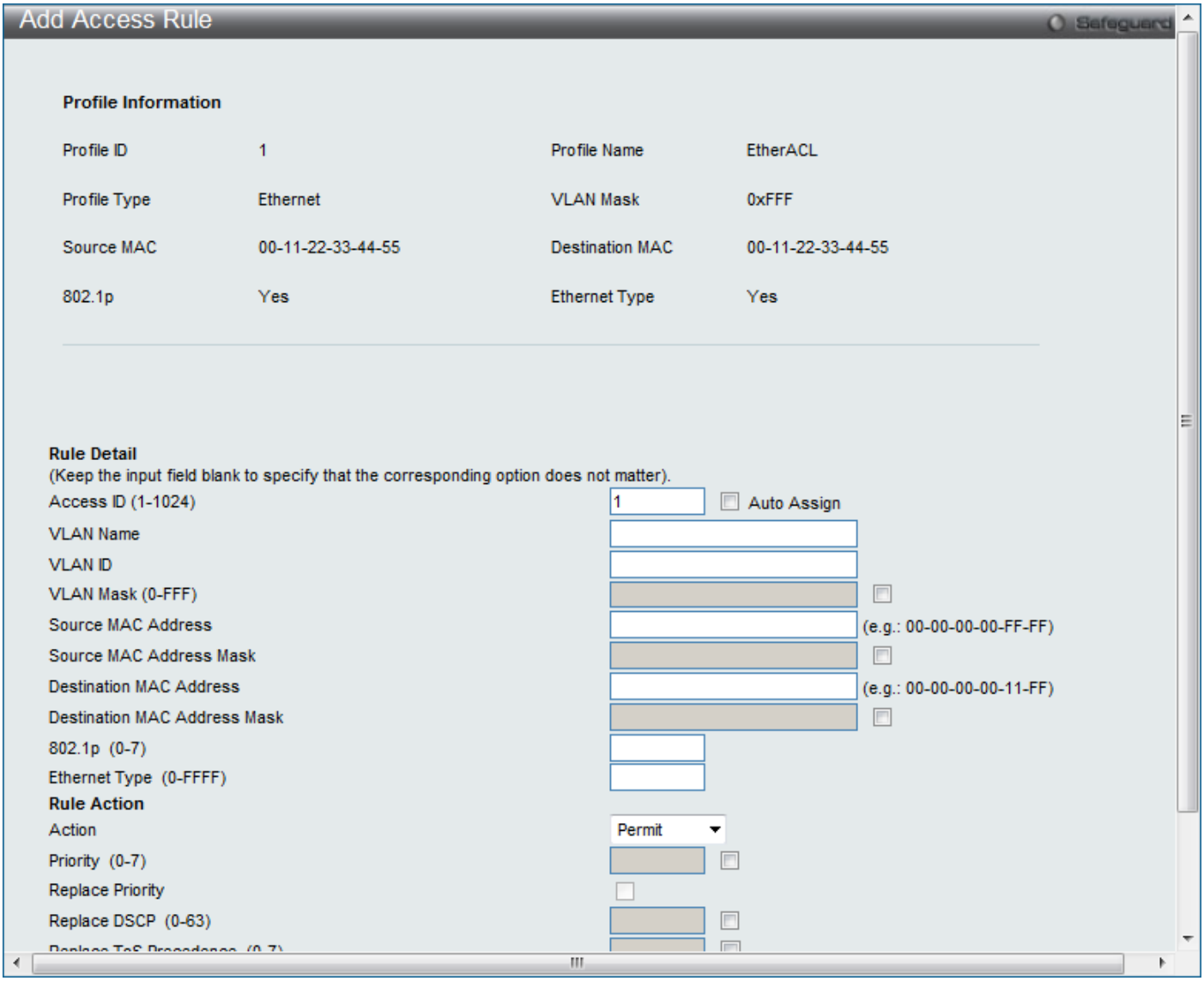


Figure 8-6 Add Access Rule window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-1024)	Enter the access ID for this rule here. This ID must be between 1 and 1024. *Auto Assign* – Select this option to instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	Enter the VLAN name used here.
VLAN ID	Enter the VLAN ID used here.
VLAN Mask	Select and enter the VLAN mask value used here.
Source MAC Address	Enter the source MAC address used here.
Source MAC Address Mask	Select and enter the source MAC address mask used here.
Destination MAC Address	Enter the destination MAC address used here.
Destination MAC Address Mask	Select and enter the destination MAC address mask used here.
802.1p	Enter the 802.1p priority tag value used here. This value must be between 0 and 7.
Ethernet Type	Enter the Ethernet type value used here.

Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the port mirror section. Port Mirroring must be enabled and a target port must be set.
Priority	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace Priority	Select and enter the replace priority value used here.
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified. This value must be between 0 and 63.
Replace ToS Precedence	Specifies that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC. This value must be between 0 and 7.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	Enter the list of ports, used for this rule, here.

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

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

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

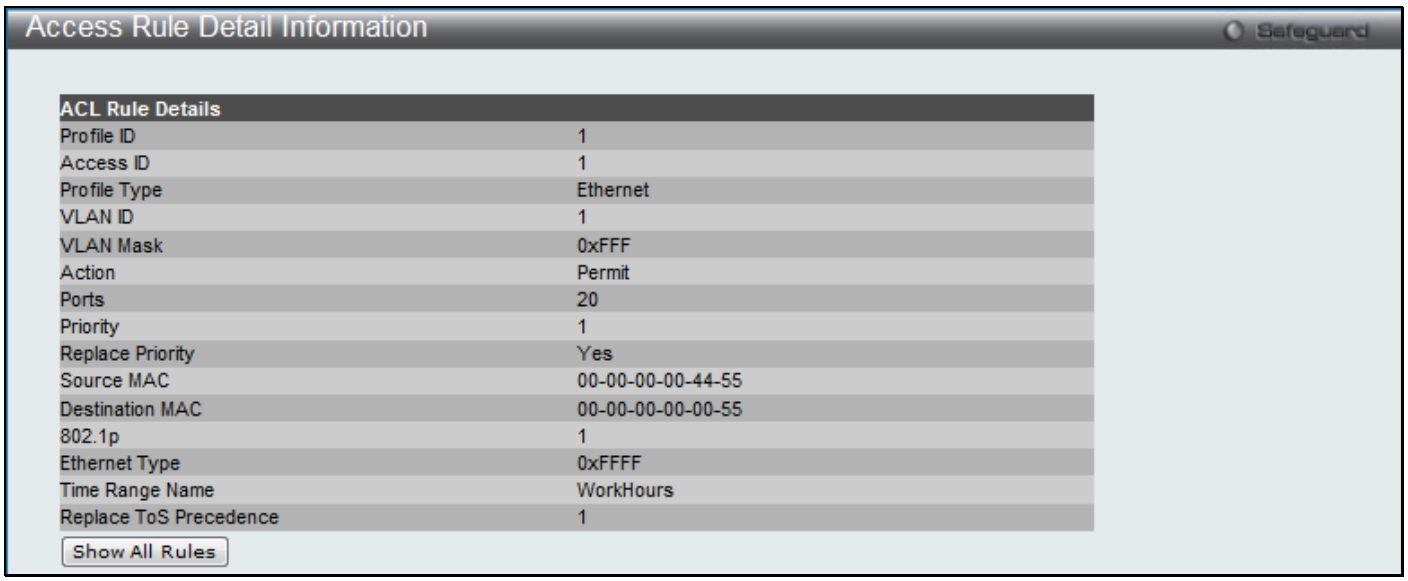


Figure 8-7 Access Rule Detail Information window (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv4 ACL Profile

The window shown below is the **Add ACL Profile** window for IPv4. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

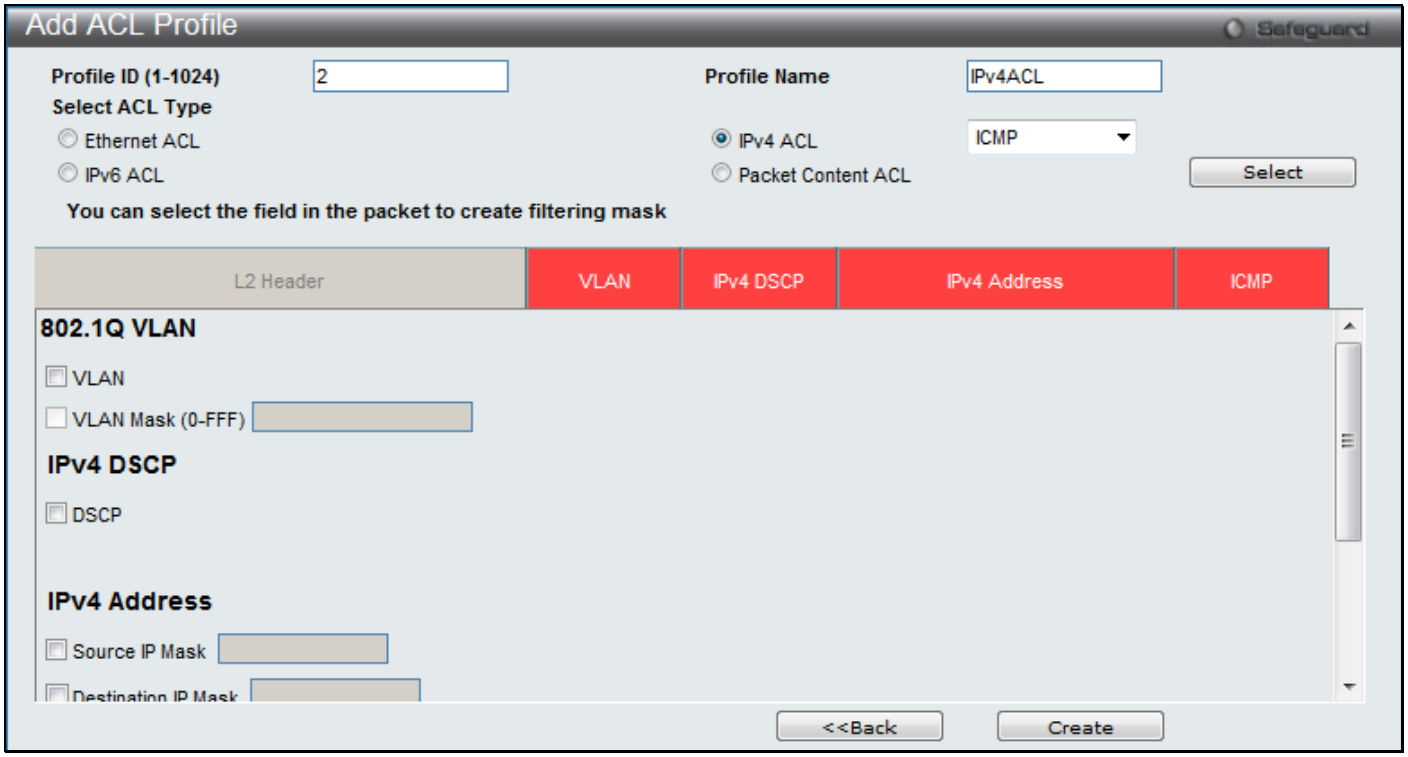


Figure 8-8 Adding ACL Profile window (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-1024)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *1024.*
Select ACL Type	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask	Enter an IP address mask for the source IP address.
IPv4 Destination IP Mask	Enter an IP address mask for the destination IP address.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.

	Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. *flag bit* - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff. *Protocol ID Mask* - Specify that the rule applies to the IP protocol ID traffic. *User Define* - Specify the Layer 4 part mask

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

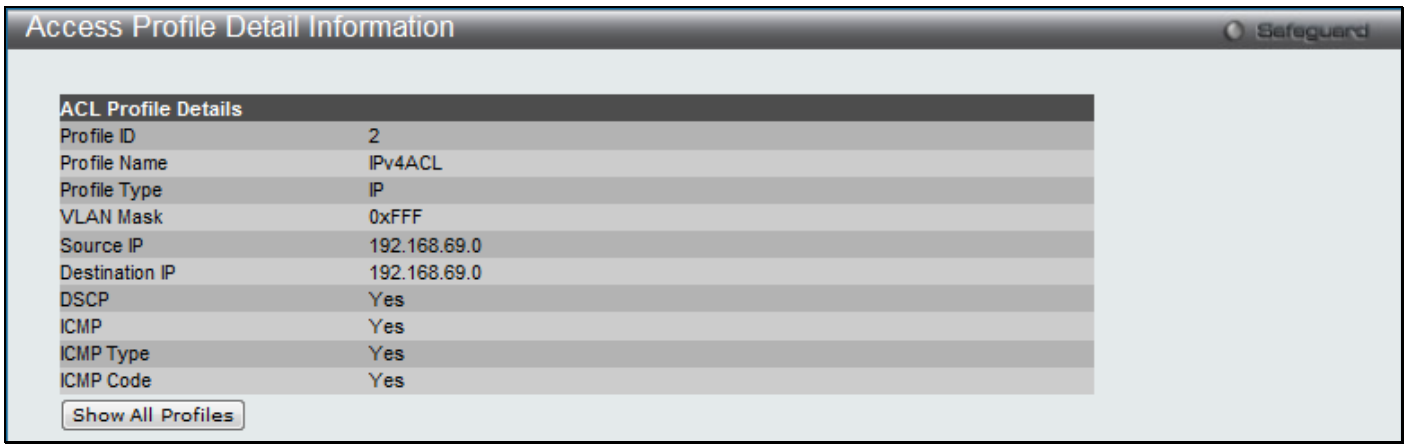


Figure 8-9 Access Profile Detail Information window (IPv4 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

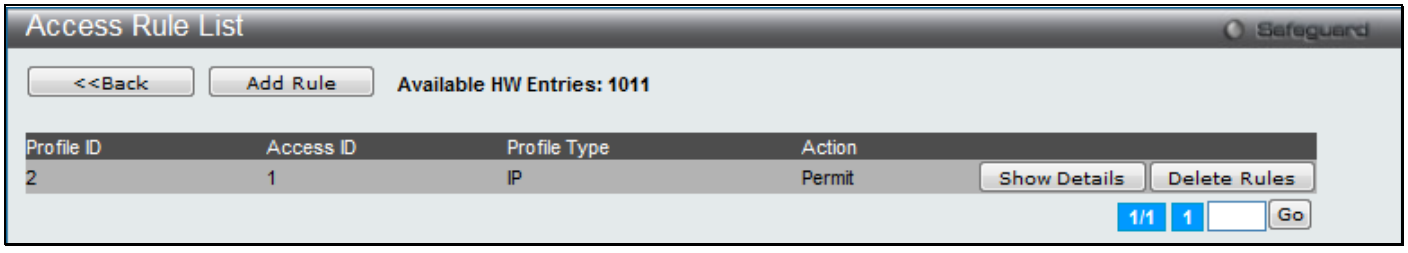


Figure 8-10 Access Rule List window (IPv4 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

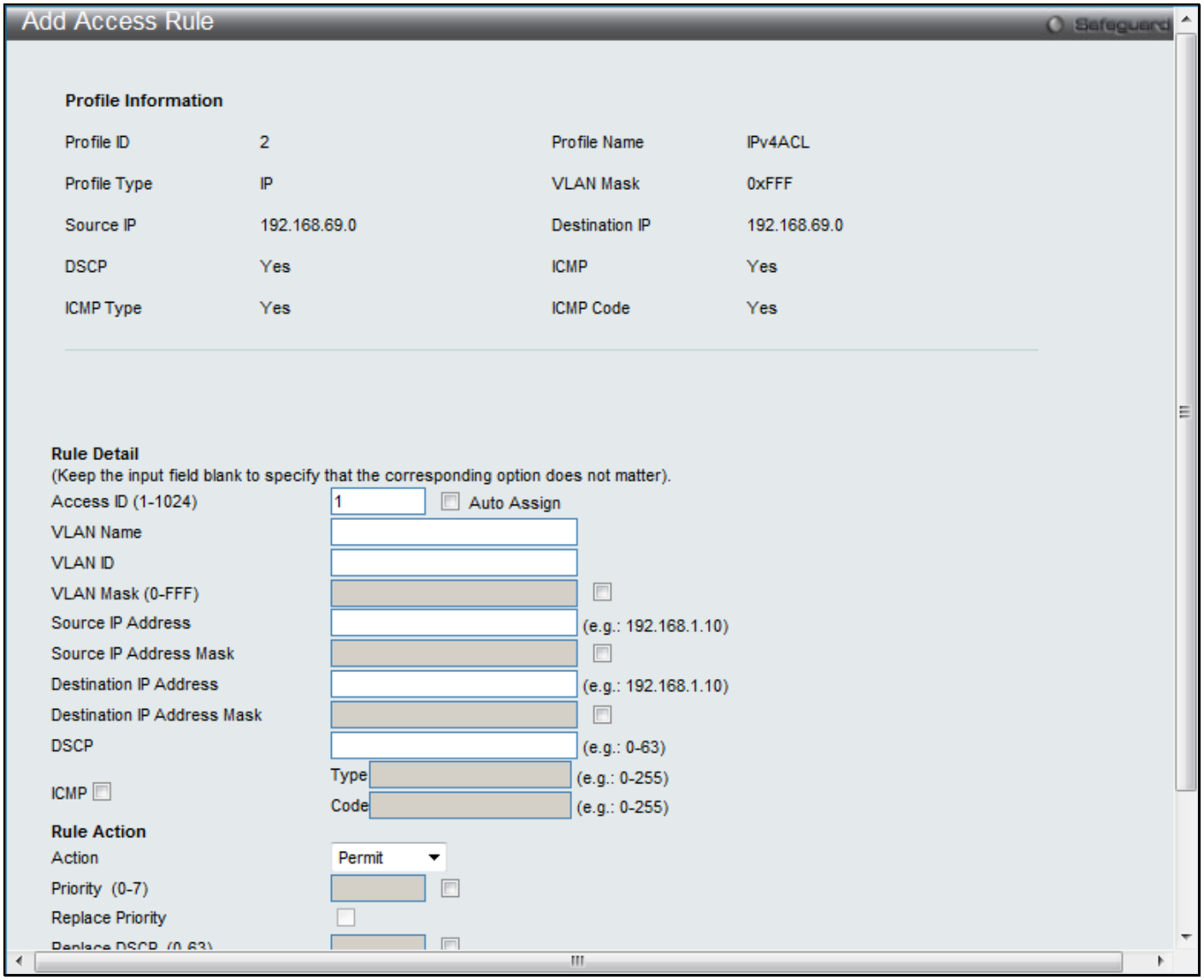


Figure 8-11 Add Access Rule window (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-1024)	Enter the access ID for this rule here. This ID must be between 1 and 1024. *Auto Assign* – Select this option to instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	Enter the VLAN name used here.
VLAN ID	Enter the VLAN ID used here.
VLAN Mask	Select and enter the VLAN mask value used here.
Source IP Address	Enter the source IP address used here.
Source IP Address Mask	Select and enter the source IP address mask used here.

Destination IP Address	Enter the destination IP address used here.
Destination IP Address Mask	Select and enter the destination IP address mask used here.
DSCP	Enter the DSCP value used here.
ICMP	Select this option to specify that the rule will be applied to ICMP traffic. *Type* – Enter the ICMP packet type value used here. *Code* – Enter the ICMP code value used here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	Enter the list of ports, used for this configuration, here.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

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

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

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

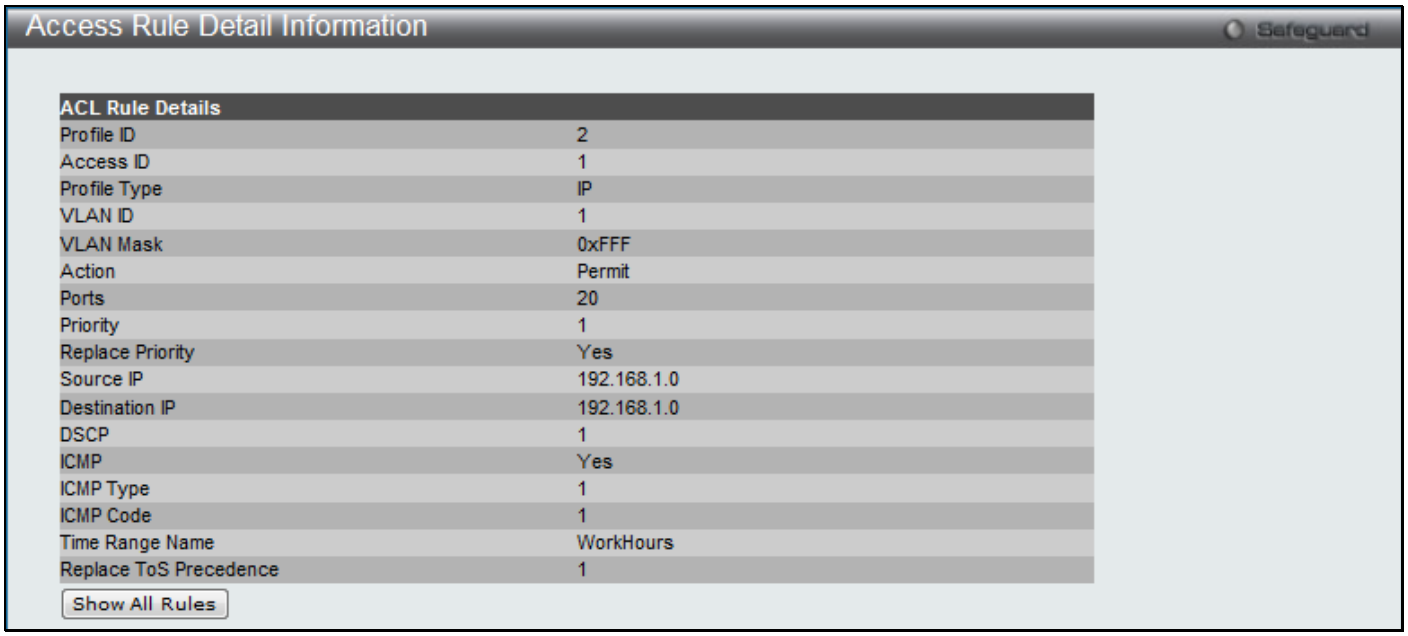


Figure 8-12 Access Rule Detail Information window (IPv4 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 ACL Profile

The window shown below is the **Add ACL Profile** window for IPv6. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

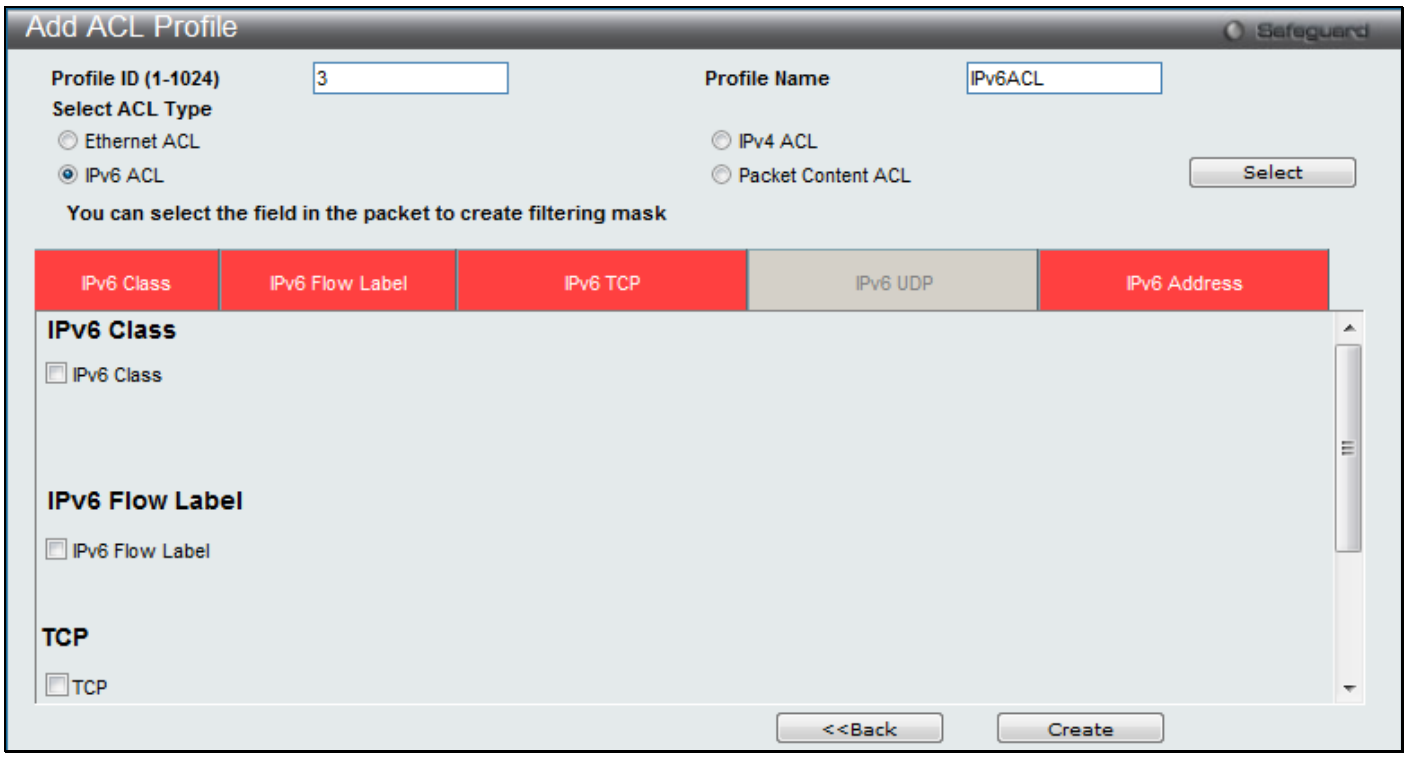


Figure 8-13 Add ACL Profile window (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-1024)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *1024*.

Select ACL Type	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
IPv6 Class	Ticking this check box will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports. *Destination Port Mask* – Specify the range of the TCP destination port range.
IPv6 UDP	*Source Port Mask* – Specify the range of the TCP source port range. *Destination Port Mask* – Specify the range of the TCP destination port mask.
IPv6 Source Address	The user may specify an IP address mask for the source IPv6 address by ticking the corresponding check box and entering the IP address mask.
IPv6 Destination Address	The user may specify an IP address mask for the destination IPv6 address by ticking the corresponding check box and entering the IP address mask.

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

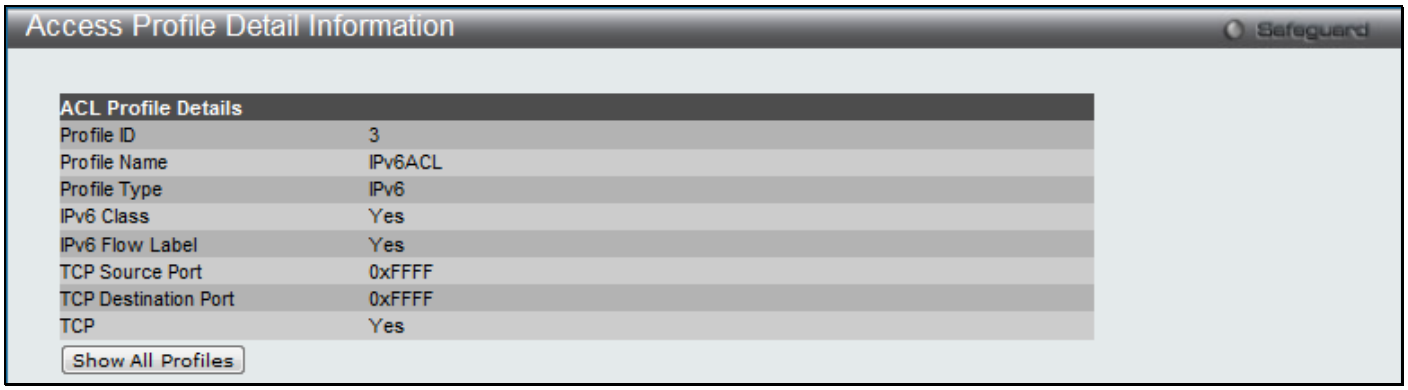


Figure 8-14 Access Profile Detail Information window (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

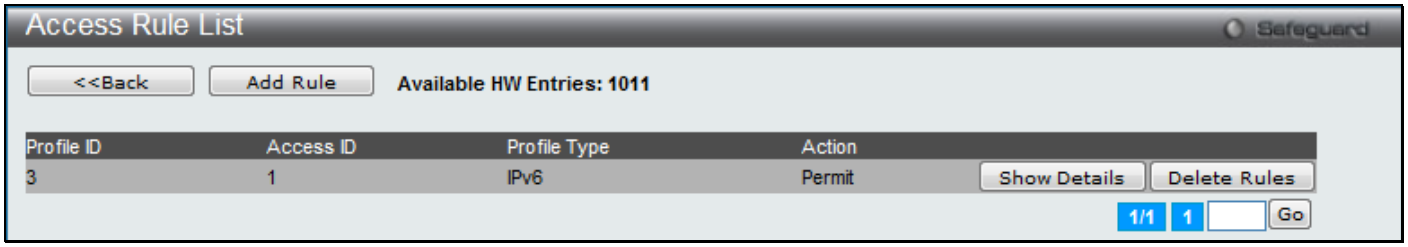


Figure 8-15 Access Rule List window (IPv6 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

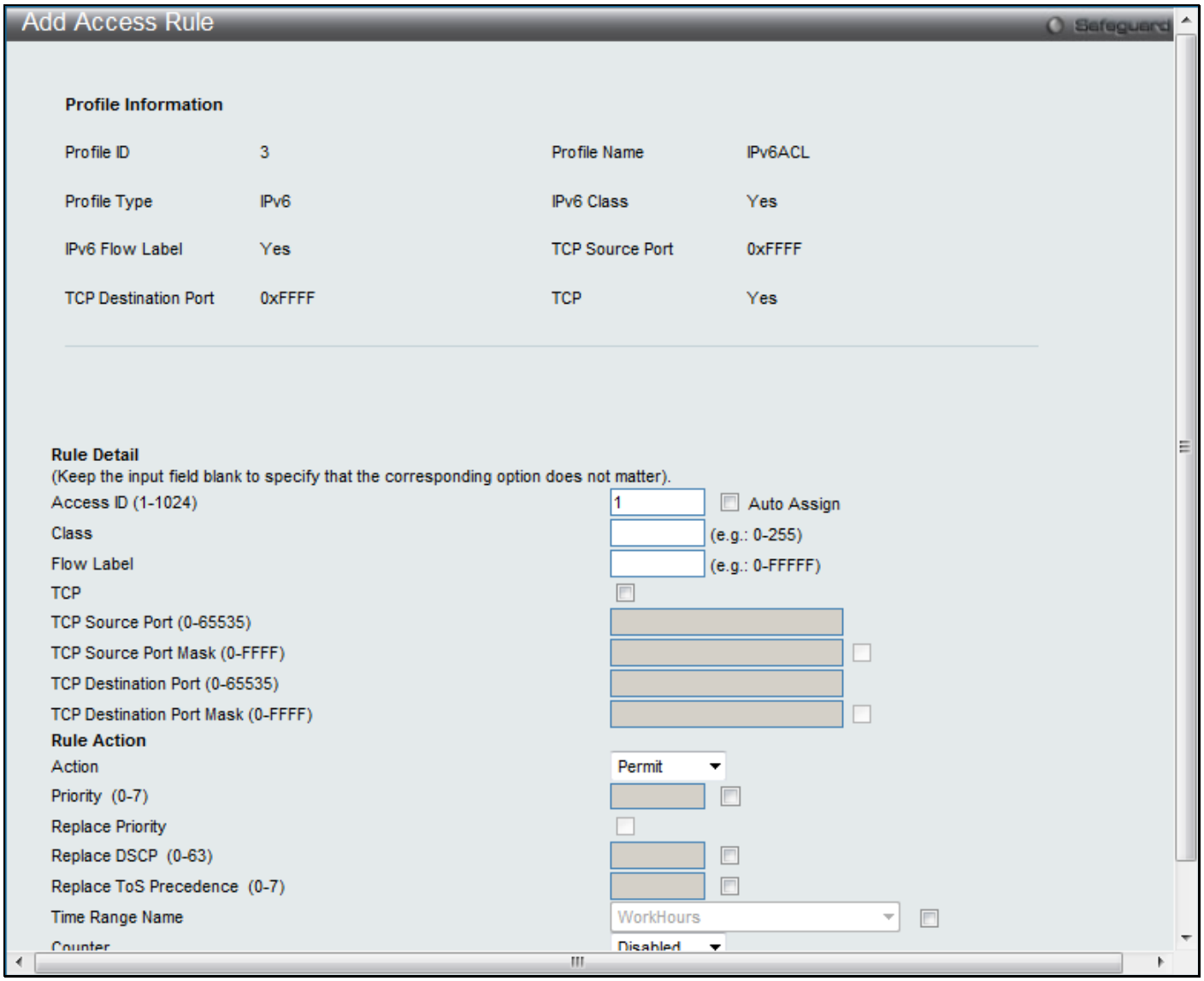


Figure 8-16 Add Access Rule window (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-1024)	Enter the access ID for this rule here. This ID must be between 1 and 1024. *Auto Assign* – Select this option to instruct the Switch to automatically assign an Access ID for the rule being created.
Class	Enter the IPv6 class mask value used here.
Flow Label	Enter the IPv6 flow label mask value used here.
TCP	Select this option to specify that the rule will be applied to TCP traffic.
TCP Source Port	Enter the TCP source port value used here.
TCP Source Port Mask	Enter the TCP source port mask value used here.
TCP Destination Port	Enter the TCP destination port value used here.
TCP Destination Port Mask	Enter the TCP destination port mask value used here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.

	Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	Enter the list of ports, used for this configuration, here.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

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

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

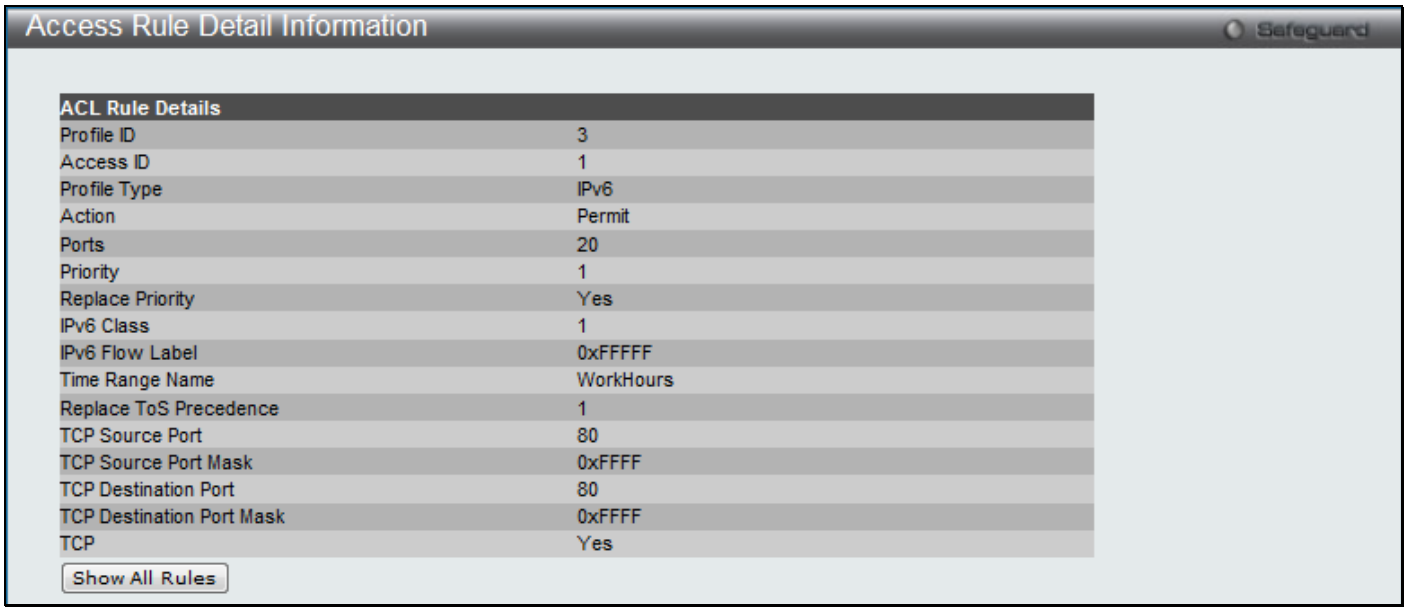


Figure 8-17 Access Rule Detail Information window (IPv6 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding a Packet Content ACL Profile

The window shown below is the **Add ACL Profile** window for Packet Content: To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

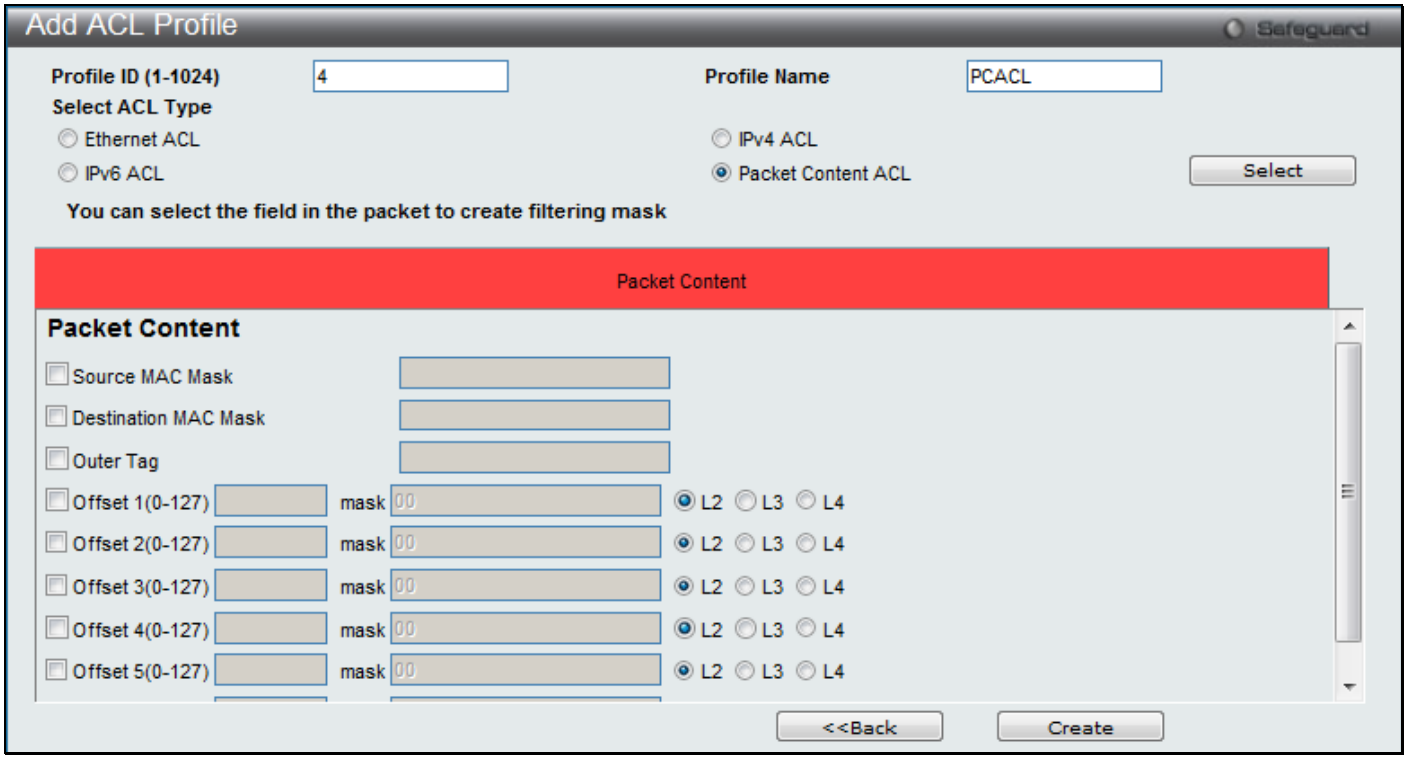


Figure 8-18 Add ACL Profile window (Packet Content ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-1024)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *1024.*
Select ACL Type	Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
Packet Content	*Source MAC* - Specifies the source MAC mask. *Destination MAC* - Specifies the destination MAC mask. *Outer Tag* - Specifies the outer VLAN tag of the packet to mask. This constitutes only the 12-bit VID fields. *Offset1, Offset2, Offset3, Offset4, Offset5, Offset6* - Defines the UDF fields that the device filters. Each UDF field consists of 1-byte of data, which is n bytes away from the offset reference (where n is the offset value). The offset ranges are from 0 to 127. The offset reference can be one of the following: *L2* – The offset starts counting from the byte after the end of the VLAN tags (start of ether type). *L3* – The offset starts counting right after the ether type field. The packet must have a valid L2 header and a recognizable ether type in order to be recognized. *L4* – The offset starts counting right after the end of the IP header. The packet must have a valid IP header in order to be recognized.

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

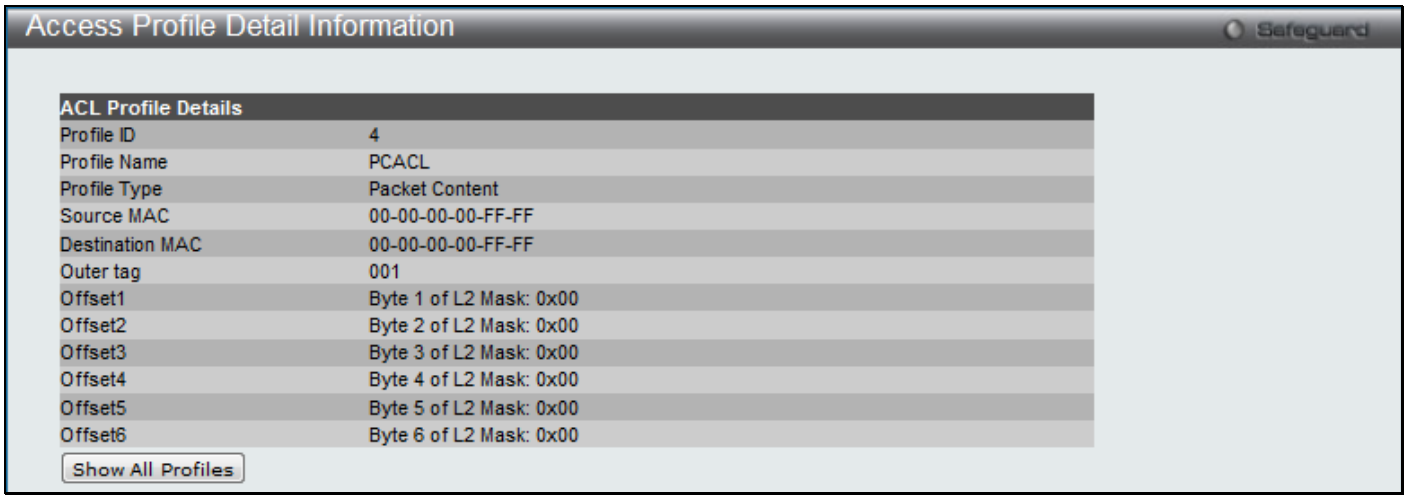


Figure 8-19 Access Profile Detail Information window (Packet Content ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (i.e. an ARP spoofing attack). For a more detailed explanation on how ARP protocol works and how to employ D-Link's unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix E at the end of this manual.

After clicking the **Add/View Rules** button, the following page will appear:

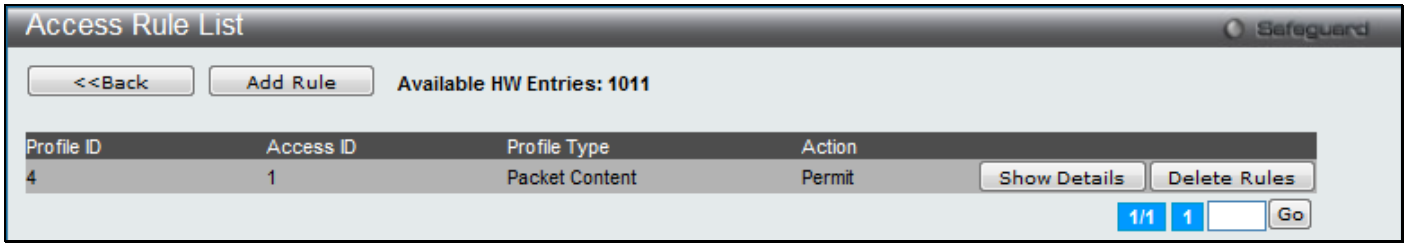


Figure 8-20 Access Rule List window (Packet Content ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

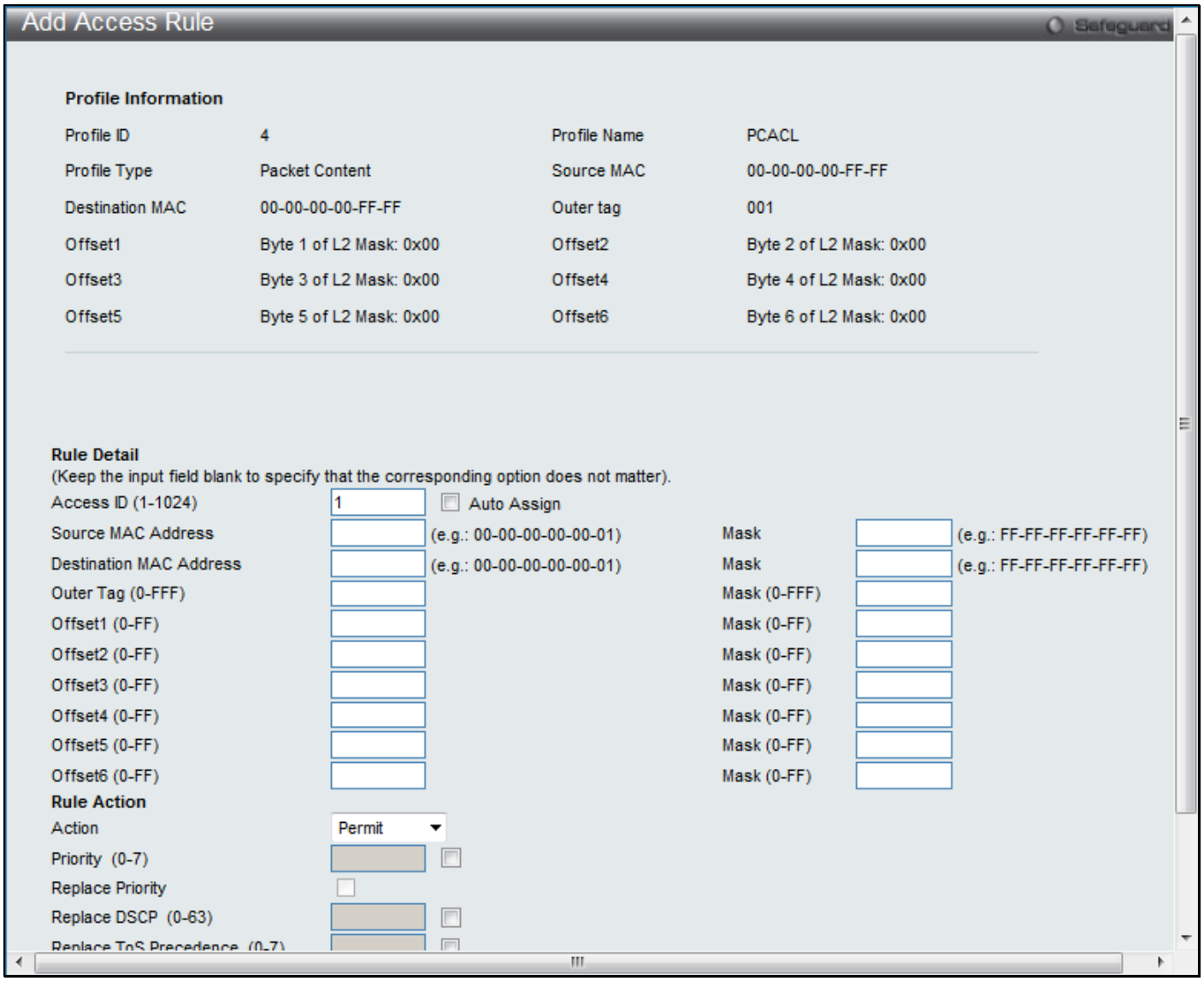


Figure 8-21 Add Access Rule window (Packet Content ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-1024)	Enter the access ID for this rule here. This ID must be between 1 and 1024. *Auto Assign* – Select this option to instruct the Switch to automatically assign an Access ID for the rule being created.
Source MAC Address	Enter the source MAC address used here. *Mask* – Enter the source MAC address mask used here.
Destination MAC Address	Enter the destination MAC address used here. *Mask* – Enter the destination MAC address mask used here.
Outer Tag	Enter the outer VLAN tag of the packet to mask. This constitutes only the 12-bit VID fields. *Mask* – Enter the outer tag mask value used here.
Offset1-6	Enter the data to match for each UDF data field defined in the profile here. *Mask* – Enter the offset mask value used here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a

	target port must be set.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	Enter the list of ports, used for this configuration, here.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

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

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

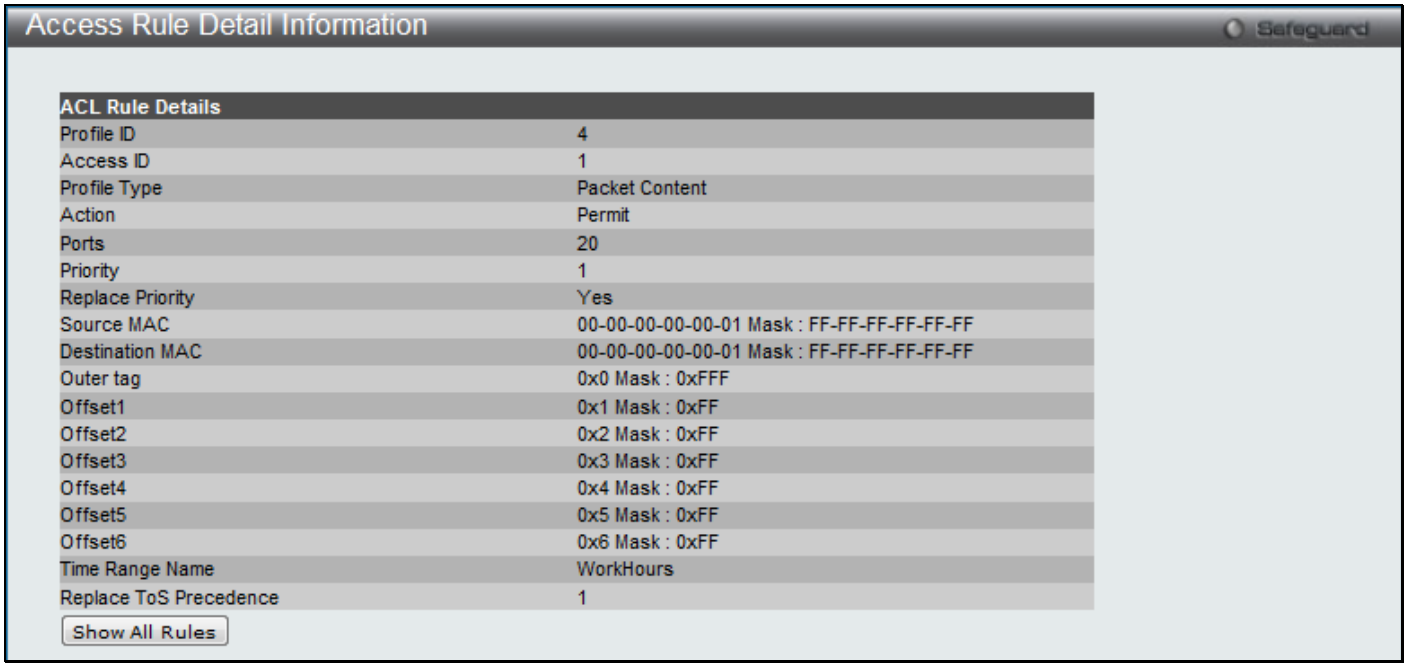


Figure 8-22 Access Rule Detail Information window (Packet Content ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

CPU Access Profile List

Due to a chipset limitation and needed extra switch security, the Switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user's implementation. As an added feature for the CPU Filtering, the Switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

NOTE: CPU Interface Filtering is used to control traffic access to the switch directly such as protocols transition or management access. A CPU interface filtering rule won't impact normal L2/3 traffic forwarding. However, a improper CPU interface filtering rule may cause the network to become unstable.

Creating an access profile for the CPU is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.

Users may globally enable or disable the CPU Interface Filtering State mechanism by using the radio buttons to change the running state. Choose Enabled to enable CPU packets to be scrutinized by the Switch and Disabled to disallow this scrutiny.

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

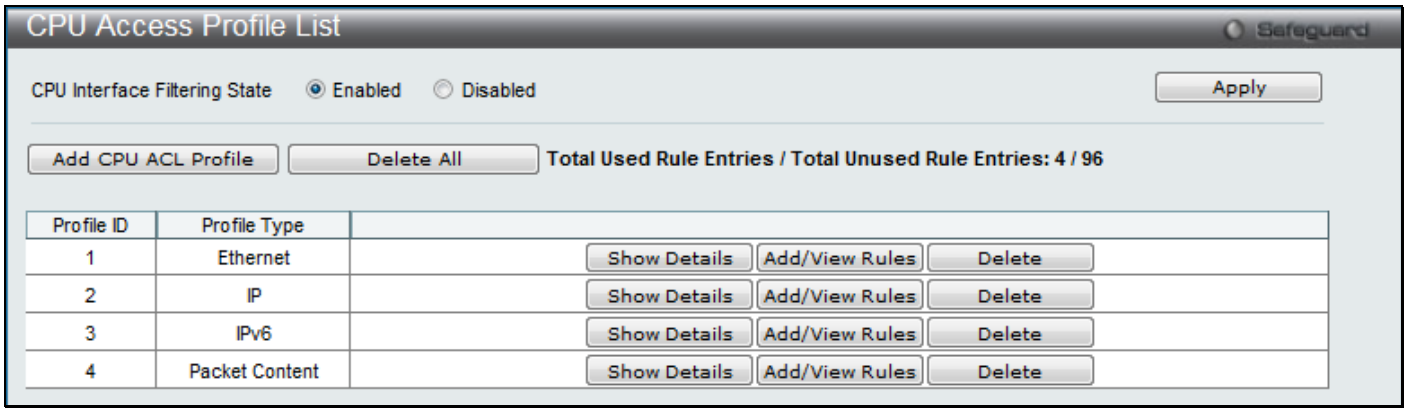


Figure 8-23 CPU Access Profile List window

The fields that can be configured are described below:

Parameter	Description
CPU Interface Filtering State	Here the user can enable or disable the CPU interface filtering state.

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

Click the **Add CPU ACL Profile** button to add an entry to the **CPU ACL Profile List**.
Click the **Delete All** button to remove all access profiles from this table.
Click the **Show Details** button to display the information of the specific profile ID entry.
Click the **Add/View Rules** button to view or add CPU ACL rules within the specified profile ID.
Click the **Delete** button to remove the specific entry.

There are four **Add CPU ACL Profile** windows;

- one for Ethernet (or MAC address-based) profile configuration,
- one for IPv6 address-based profile configuration,
- one for IPv4 address-based profile configuration, and
- one for packet content profile configuration.

Adding a CPU Ethernet ACL Profile

The window shown below is the **Add CPU ACL Profile** window for Ethernet. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:

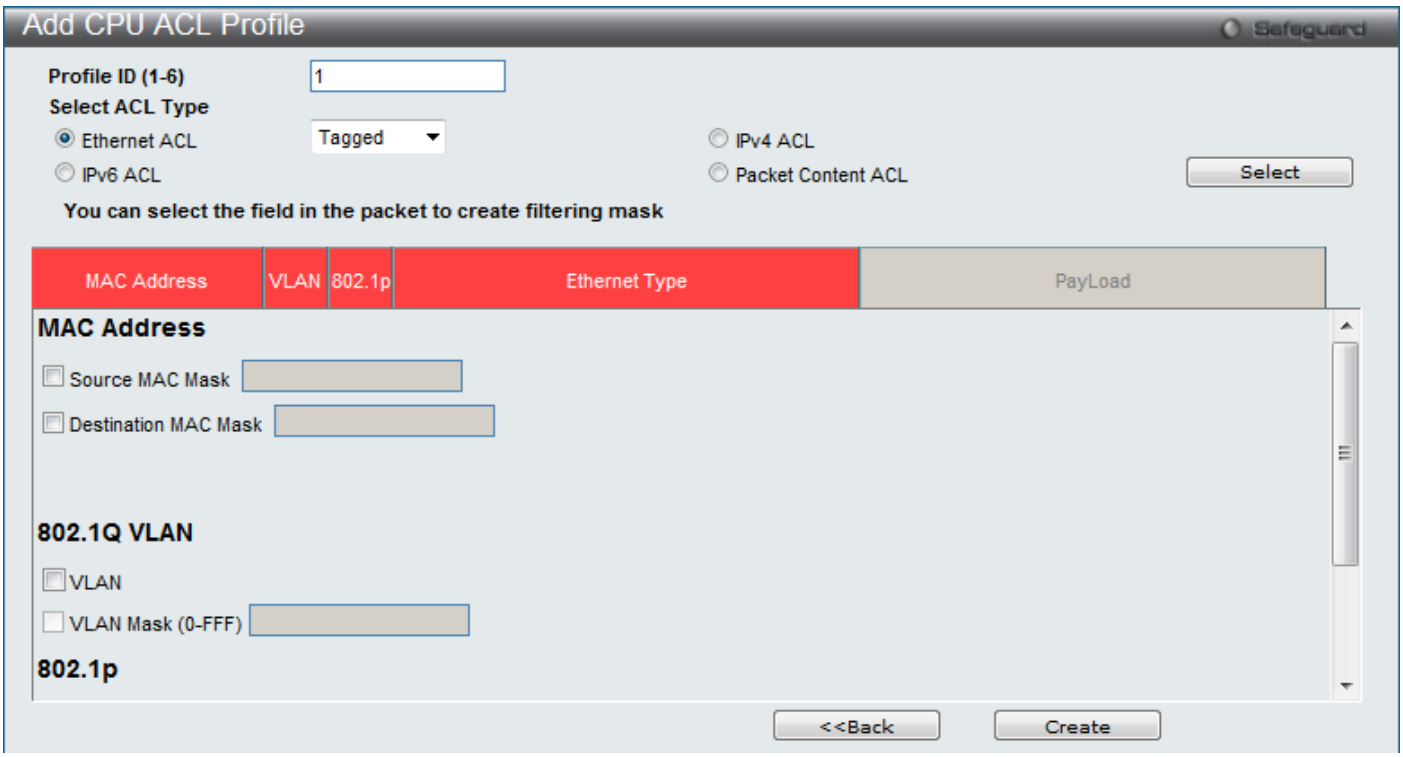


Figure 8-24 Add CPU ACL Profile window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the window according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select an CPU ACL type. Click the **Create** button to create a profile.

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

After clicking the **Show Details** button, the following page will appear:

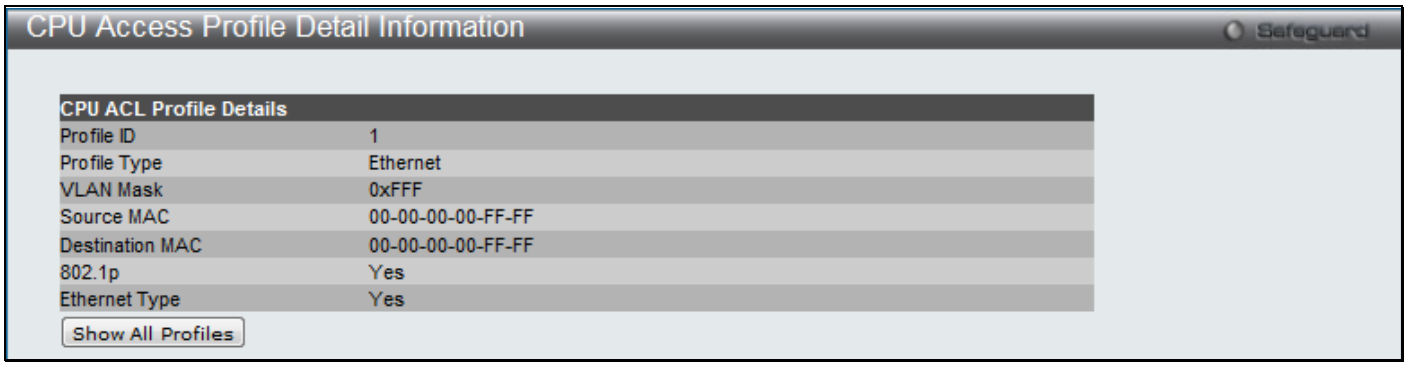


Figure 8-25 CPU Access Profile Detail Information window (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

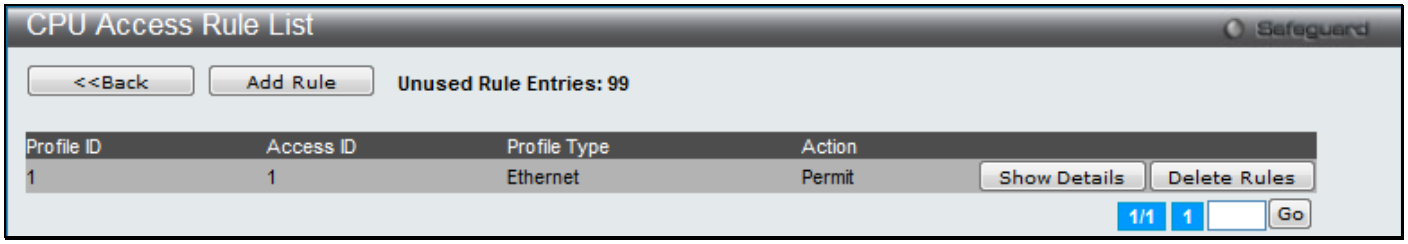


Figure 8-26 CPU Access Rule List window (Ethernet ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

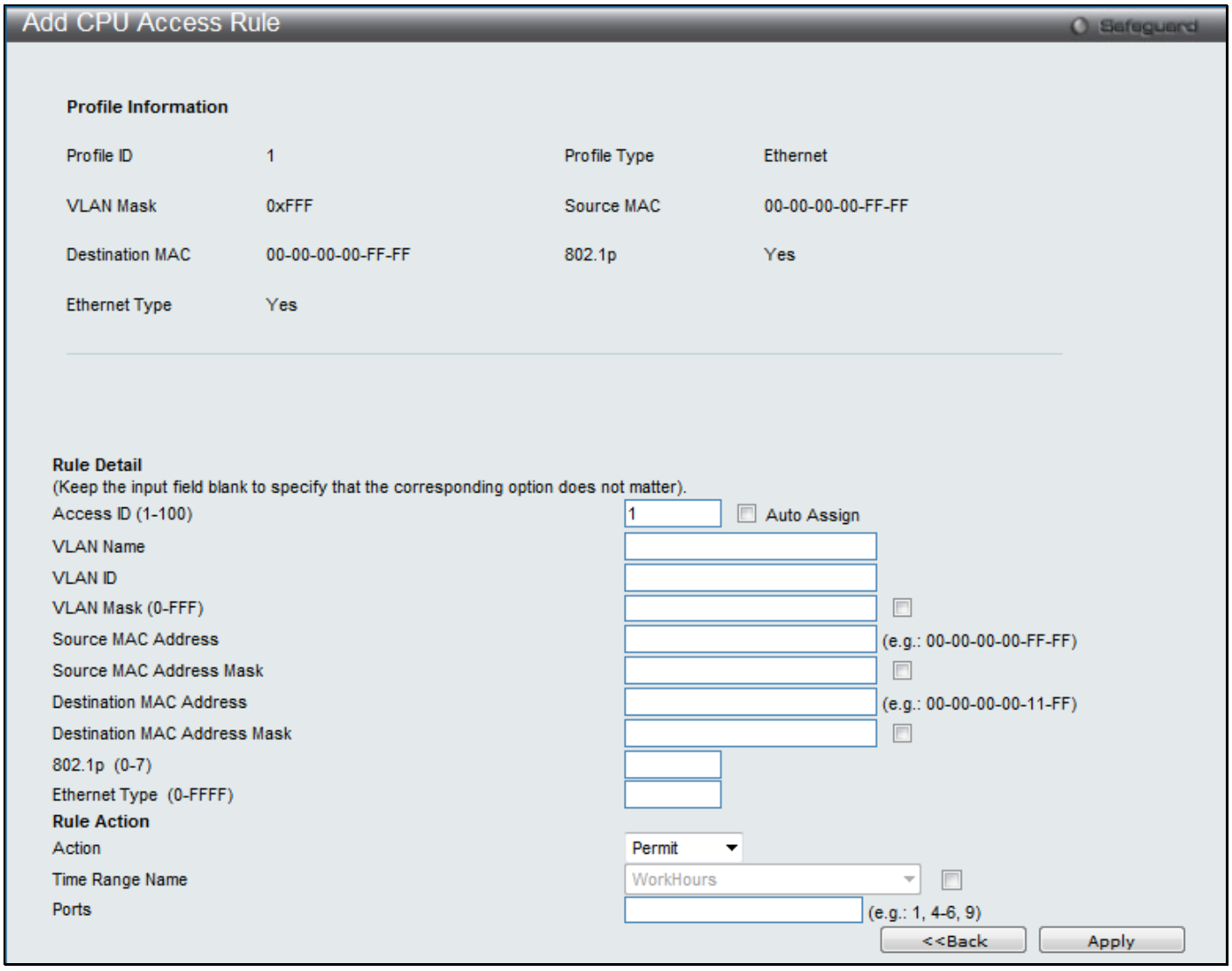


Figure 8-27 Add CPU Access Rule window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
VLAN Name	Enter the VLAN name used here.
VLAN ID	Enter the VLAN ID used here.
VLAN Mask	Select and enter the VLAN mask value used here.
Source MAC Address	Enter the source MAC address used here.
Source MAC Address Mask	Select and enter the source MAC address mask used here.
Destination MAC Address	Enter the destination MAC address used here.
Destination MAC Address Mask	Select and enter the destination MAC address mask used here.
802.1p	Enter the 802.1p priority tag value used here. This value must be between 0 and 7.
Ethernet Type	Enter the Ethernet type value used here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).

	Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Ethernet Type (0-FFFF)	Enter the appropriate Ethernet Type information.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter the list of ports, used for this configuration, here.

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

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

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:

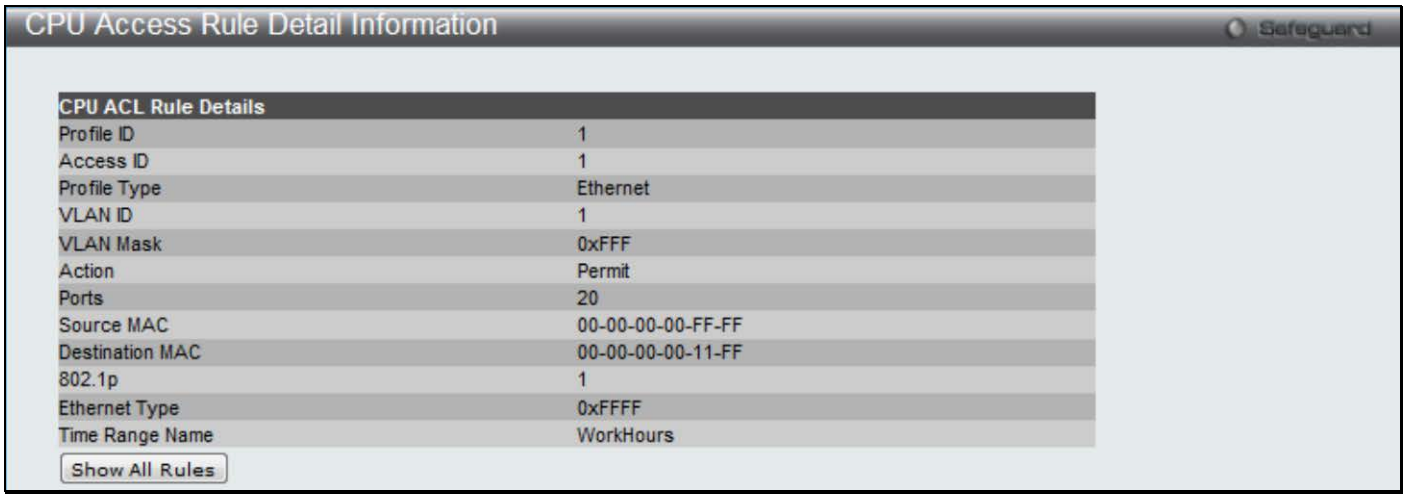


Figure 8-28 CPU Access Rule Detail Information window (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

Adding a CPU IPv4 ACL Profile

The window shown below is the **Add CPU ACL Profile** window for IP (IPv4). To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:

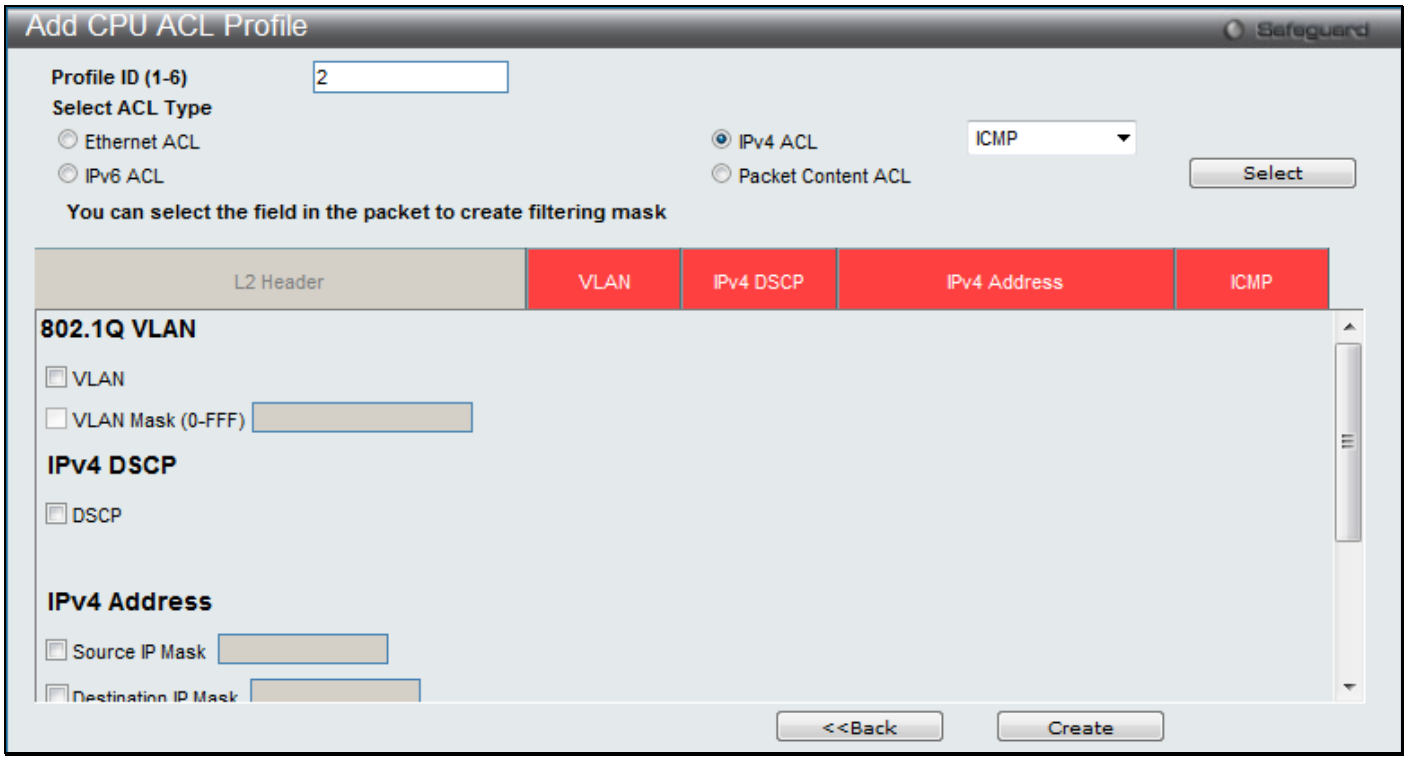


Figure 8-29 Add CPU ACL Profile window (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify *Code* to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value.

	Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires a source port mask and/or a destination port mask is to be specified. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff). *Protocol ID Mask* – Specify that the rule applies to the IP Protocol ID Traffic. *User Define* – Specify the L4 part mask.

Click the **Select** button to select an CPU ACL type. Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

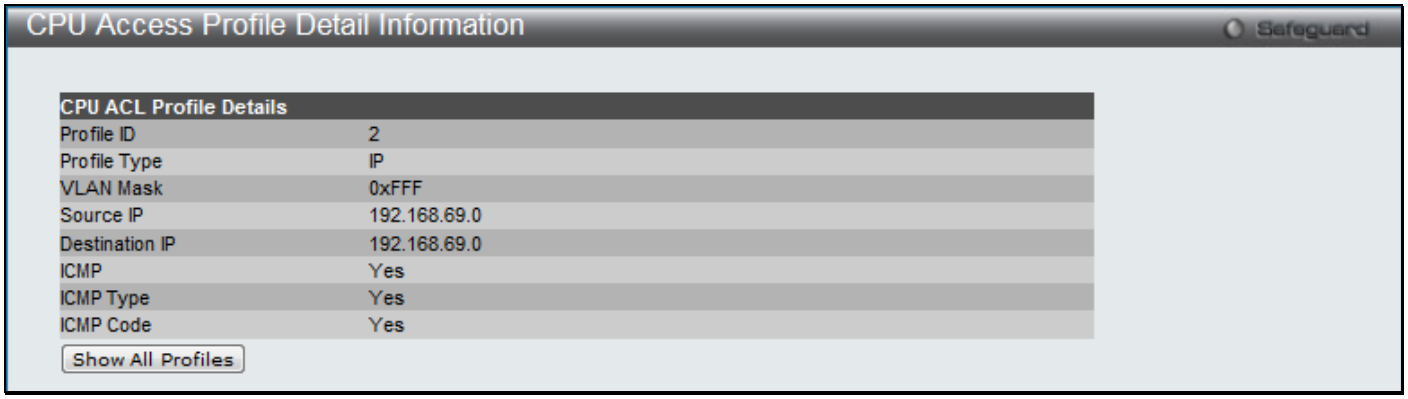


Figure 8-30 CPU Access Profile Detail Information window (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

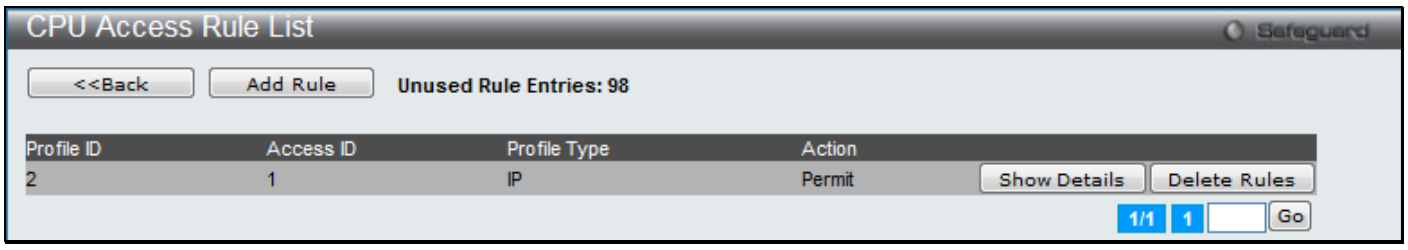


Figure 8-31 CPU Access Rule List window (Ethernet ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

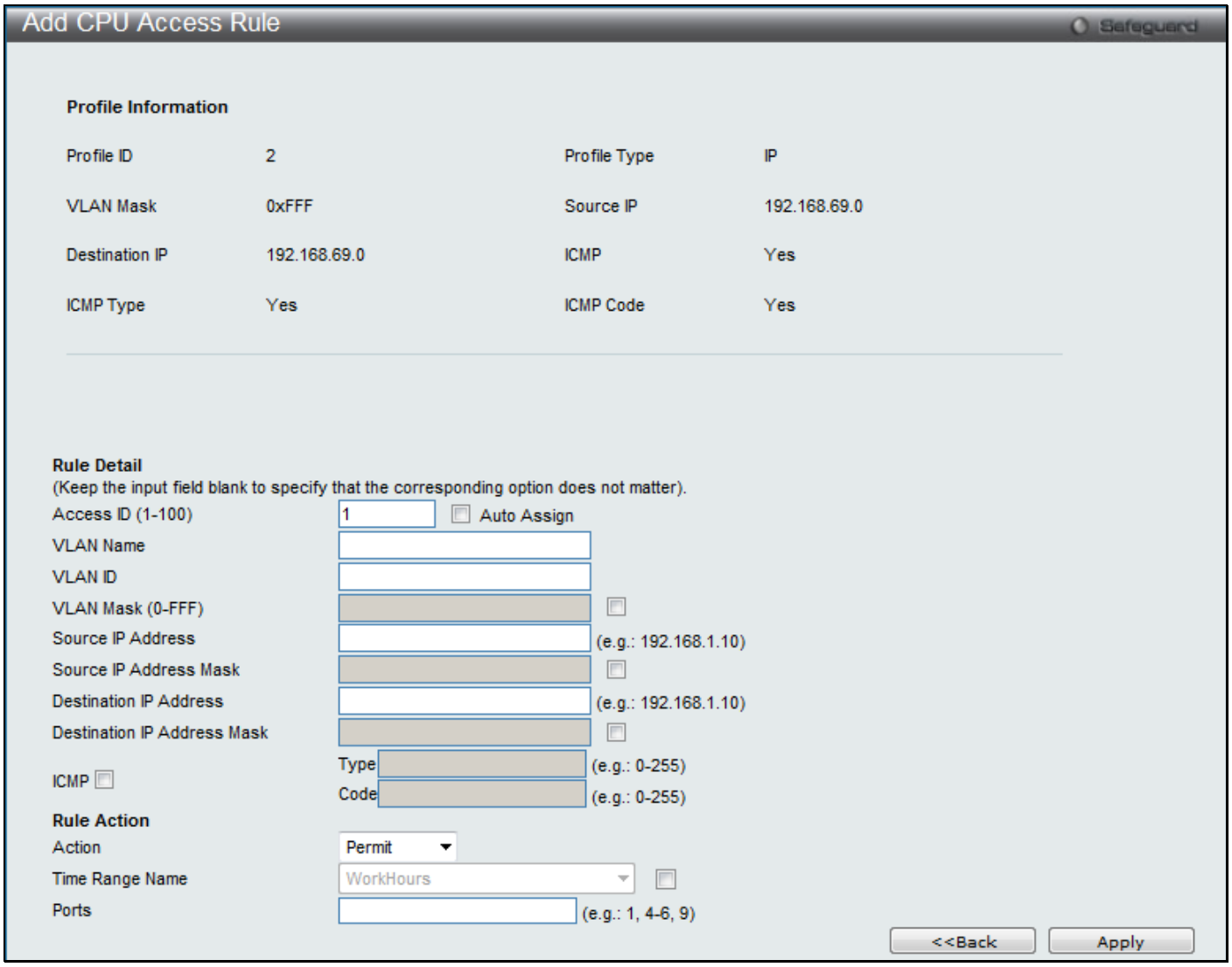


Figure 8-32 Add CPU Access Rule window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
VLAN Name	Enter the VLAN name used here.
VLAN ID	Enter the VLAN ID used here.
VLAN Mask	Select and enter the VLAN mask value used here.
Source IP Address	Enter the source IP address used here.
Source IP Address Mask	Select and enter the source IP address mask used here.
Destination IP Address	Enter the destination IP address used here.
Destination IP Address Mask	Select and enter the destination IP address mask used here.
DSCP	Enter the DSCP value used here.

ICMP	Select this option to specify that the rule will be applied to ICMP traffic. *Type* – Enter the ICMP packet type value used here. *Code* – Enter the ICMP code value used here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter the list of ports, used for this configuration, here.

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

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

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:

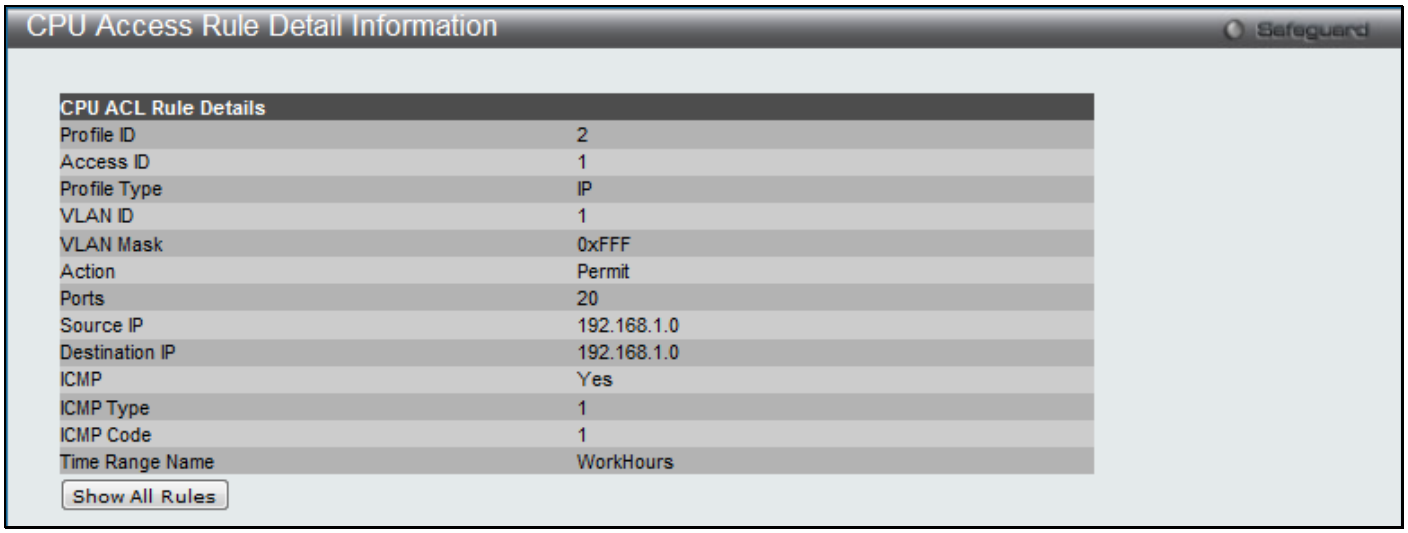


Figure 8-33 CPU Access Rule Detail Information window (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

Adding a CPU IPv6 ACL Profile

The window shown below is the **Add CPU ACL Profile** window for IPv6. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:

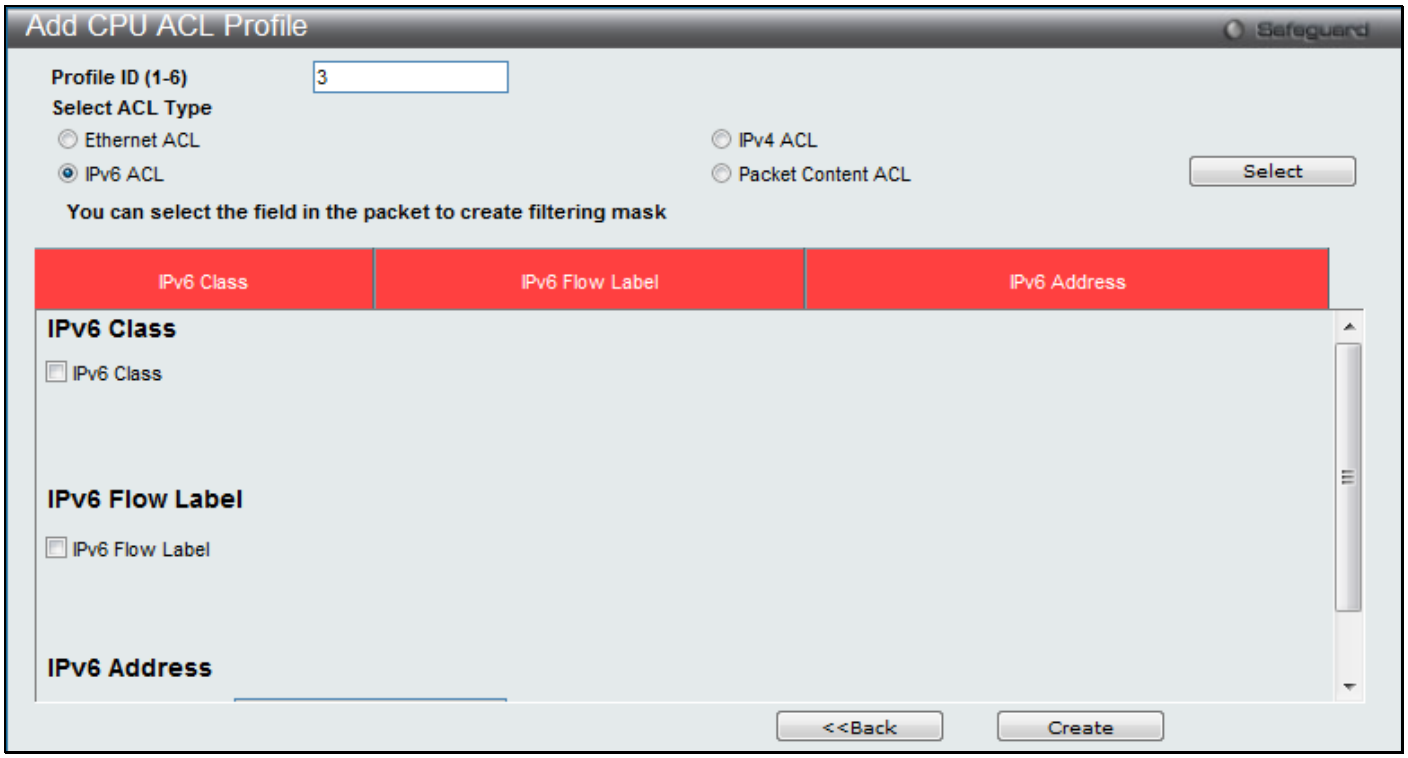


Figure 8-34 Add CPU ACL Profile window (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
IPv6 Class	Checking this field will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Checking this field will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports. *Destination Port Mask* – Specify the range of the TCP destination port range.
IPv6 UDP	*Source Port Mask* – Specify the range of the TCP source port range. *Destination Port Mask* – Specify the range of the TCP destination port mask.
IPv6 Source Address	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
IPv6 Destination Address	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.

Click the **Select** button to select an CPU ACL type. Click the **Create** button to create a profile.

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

After clicking the **Show Details** button, the following page will appear:

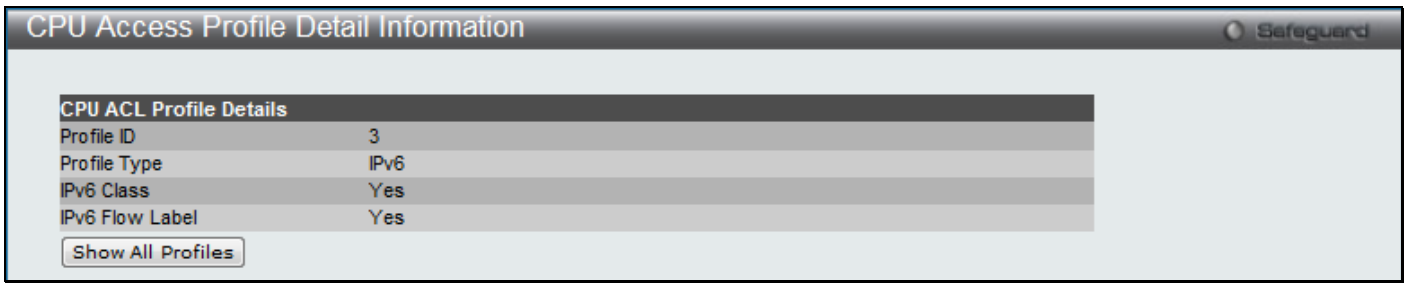


Figure 8-35 CPU Access Profile Detail Information window (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

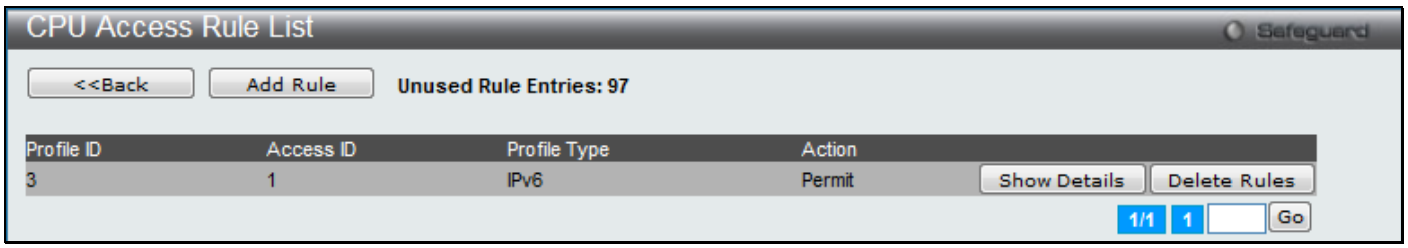


Figure 8-36 CPU Access Rule List window (IPv6 ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

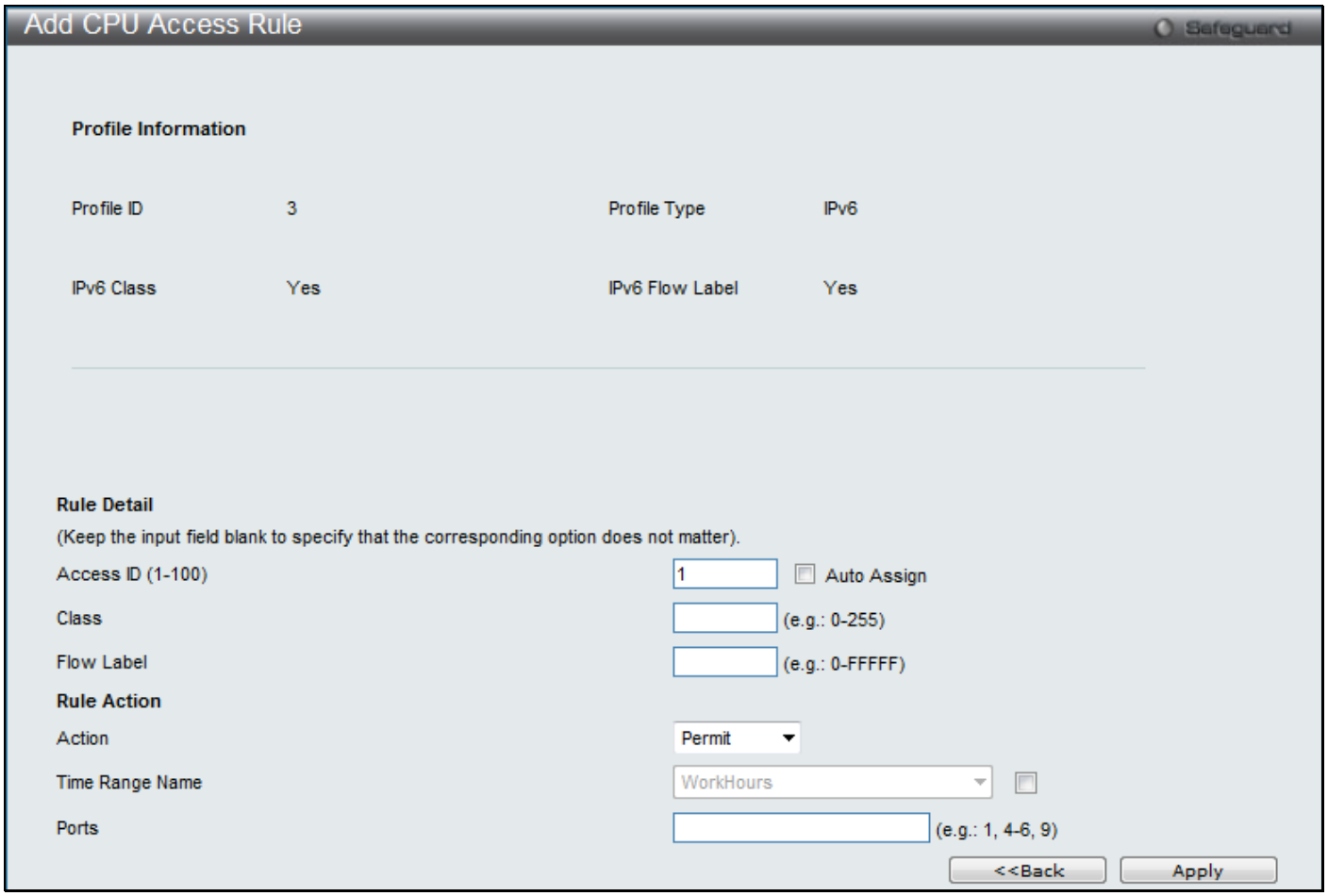


Figure 8-37 Add CPU Access Rule window (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Class	Enter the IPv6 class mask value used here.
Flow Label	Enter the IPv6 flow label mask value used here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter the list of ports, used for this configuration, here.

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

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

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:

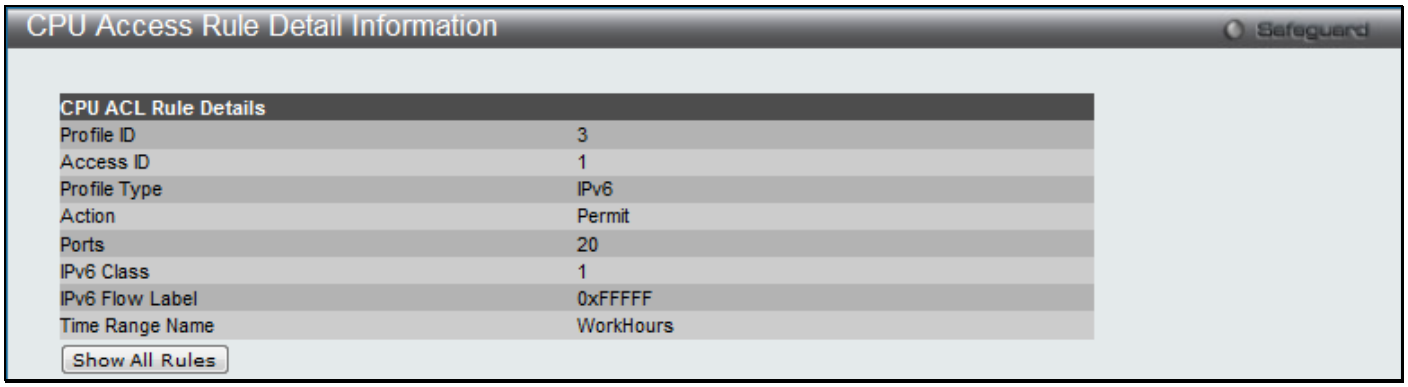


Figure 8-38 CPU Access Rule Detail Information window (IPv6 ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

Adding a CPU Packet Content ACL Profile

The window shown below is the **Add CPU ACL Profile** window for Packet Content. To use specific filtering masks in this ACL profile, click on the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:

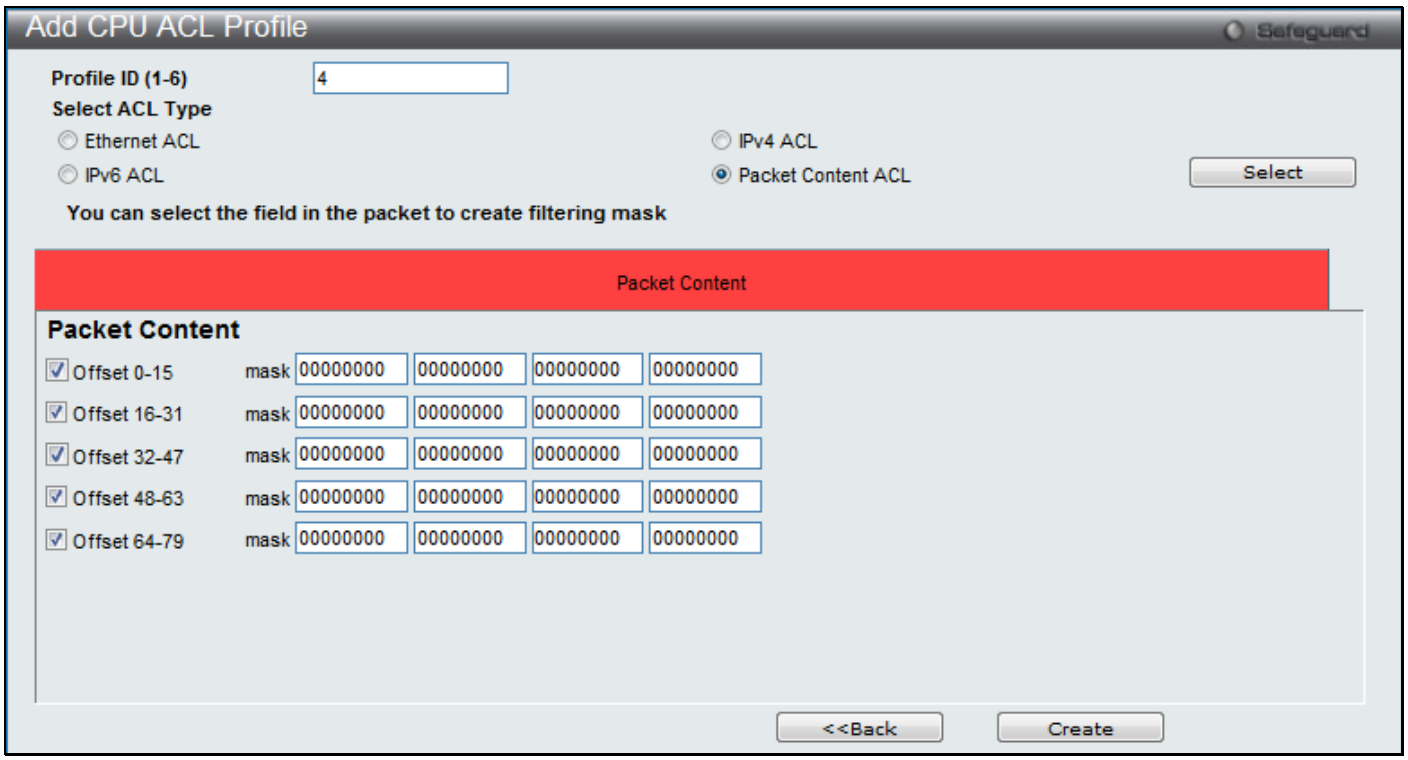


Figure 8-39 Add CPU ACL Profile window (Packet Content ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to*6.*
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header.

	Select Packet Content Mask to specify a mask to hide the content of the packet header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: *0-15* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. *16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. *32-47* – Enter a value in hex form to mask the packet from byte 32 to byte 47. *48-63* – Enter a value in hex form to mask the packet from byte 48 to byte 63. *64-79* – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click the **Select** button to select an CPU ACL type. Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

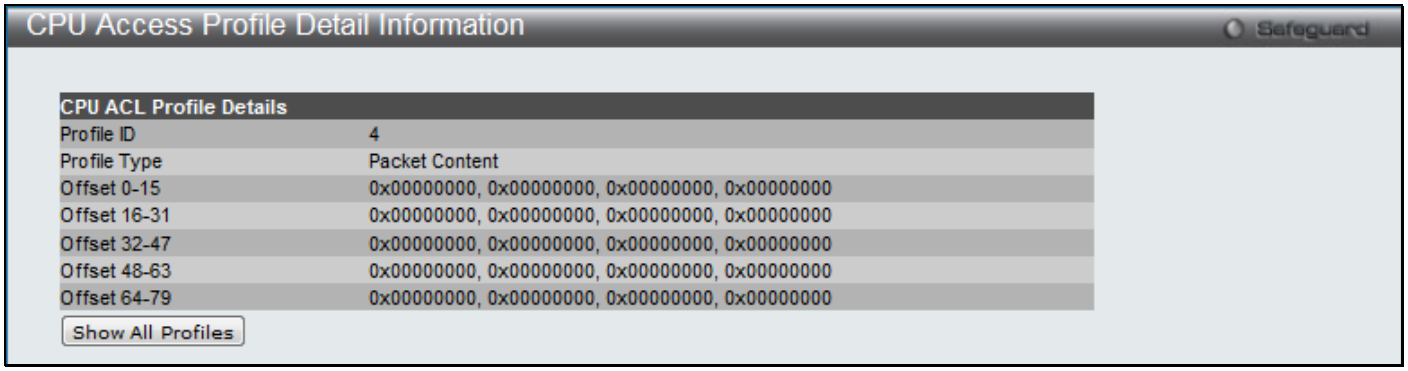


Figure 8-40 CPU Access Profile Detail Information window (Packet Content ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

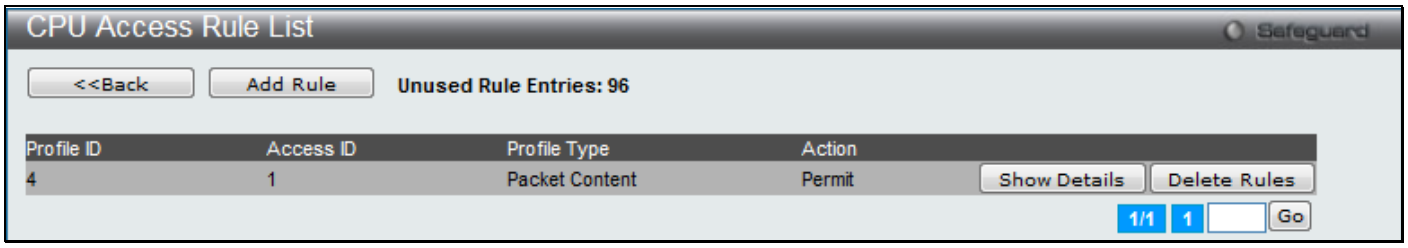


Figure 8-41 CPU Access Rule List window (Packet Content ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

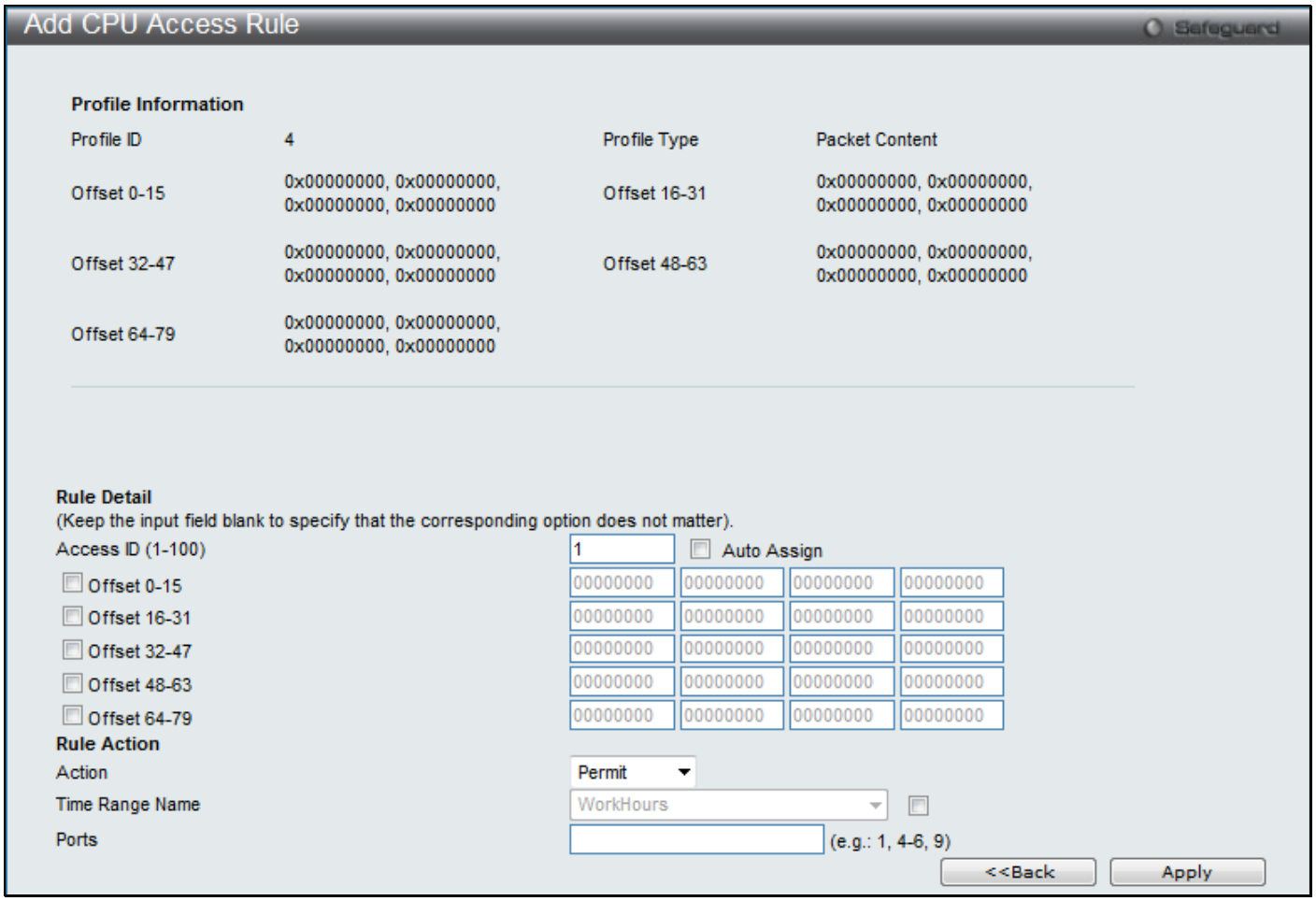


Figure 8-42 Add CPU Access Rule window (Packet Content ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: Offset 0-15 - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. Offset 16-31 - Enter a value in hex form to mask the packet from byte 16 to byte *31.* Offset 32-47 - Enter a value in hex form to mask the packet from byte 32 to byte 47. Offset 48-63 - Enter a value in hex form to mask the packet from byte 48 to byte 63. Offset 64-79 - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter the list of ports, used for this configuration, here.

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

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

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:

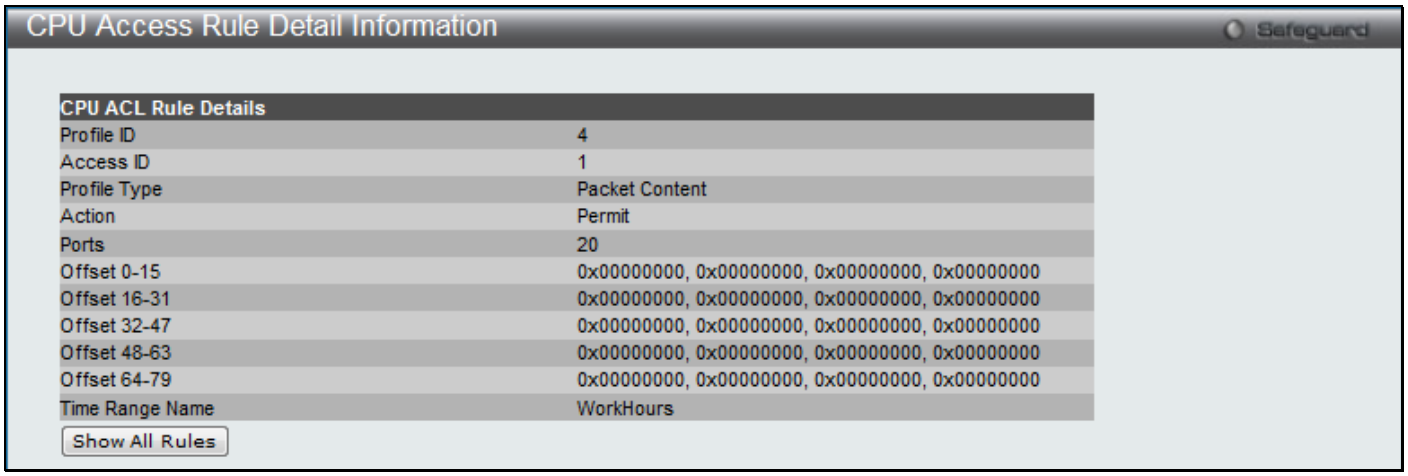


Figure 8-43 CPU Access Rule Detail Information window (Packet Content ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

ACL Finder

The ACL rule finder helps you to identify any rules that have been assigned to a specific port and edit existing rules quickly.

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

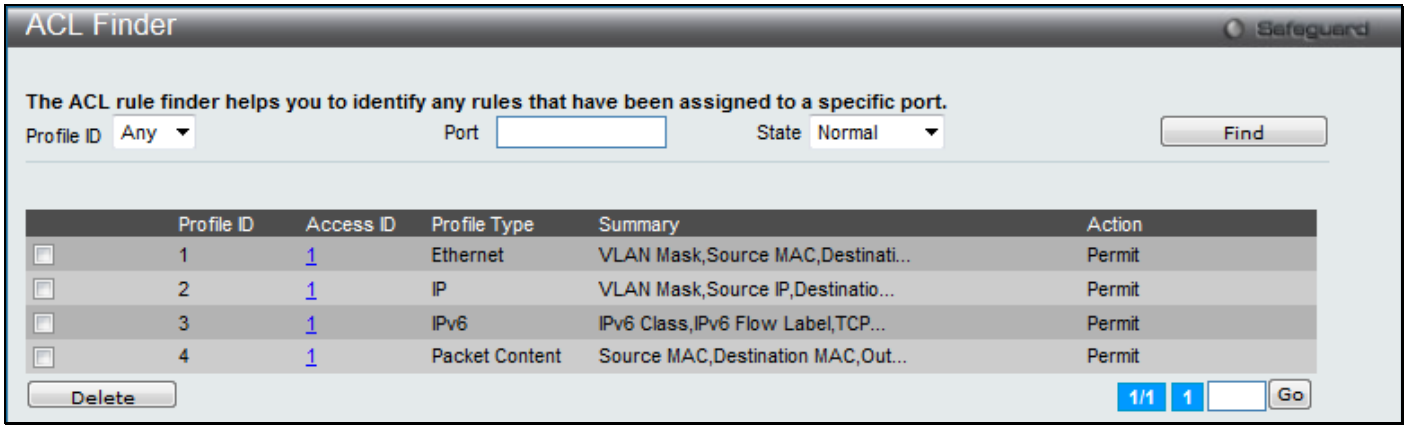


Figure 8-44 ACL Finder window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can select the Profile ID for the ACL rule finder to identify the rule.
Port	Here the user can enter the port number for the ACL rule finder to identify the rule.
State	Here the user can select the state. If the state is set to **Normal** then it will allows the user to find normal ACL rules. If the state is set to **CPU** then it allows the user to find CPU ACL rules. If the state is set to Egress then it will allow the user to find Egress ACL rules.

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

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

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

ACL Flow Meter

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

trTCM – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow's surpassing of two rates, the CIR and the PIR.

CIR – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn't exceed the CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

PIR – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.

PBS – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.

srTCM – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

EBS – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.

DSCP – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.

The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.

Green – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.

Yellow – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either Permit or Drop exceeded packets. Users may also choose to change the DSCP field of the packets.

Red – When an IP flow is in the red mode, its configurable parameters can be set in the Exceed field. Users may choose to either Permit or Drop exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the Counter check box. If the counter is enabled, the counter setting in the access profile will be disabled. Users may only enable two counters for one flow meter at any given time.

To view this window, click **ACL** > **ACL Flow Meter**, as shown below.

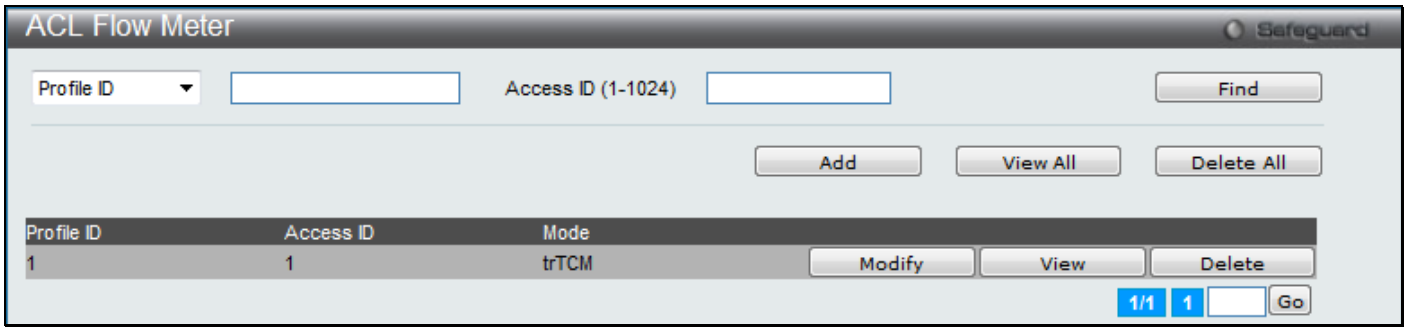


Figure 8-45 ACL Flow Meter window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID	Here the user can enter the Access ID for the flow meter.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Add** button to add a new entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Delete All** button to remove all the entries listed.
Click the **Modify** button to re-configure the specific entry.
Click the **View** button to display the information of the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the **Add** or the **Modify** button, the following page will appear:

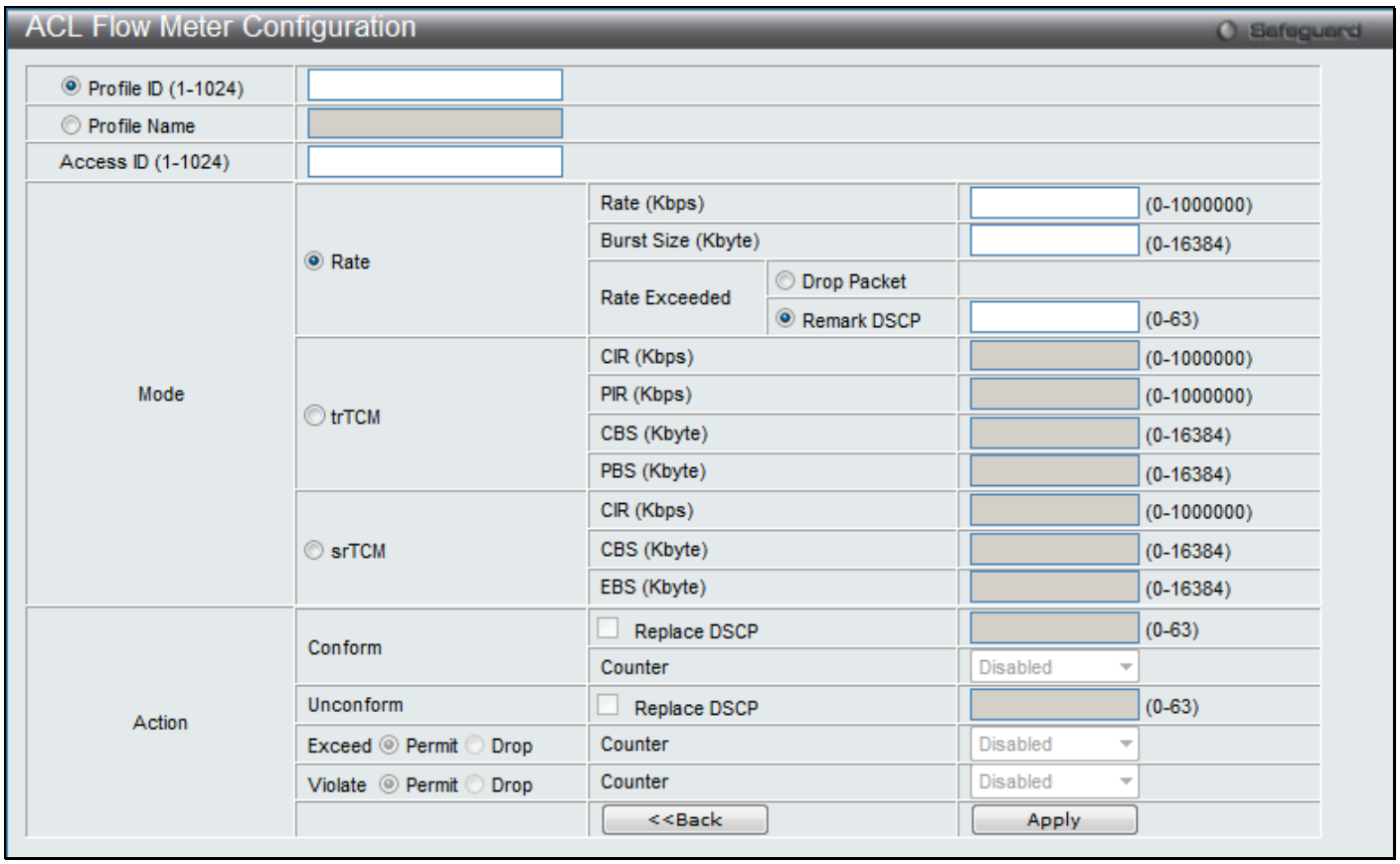


Figure 8-46 ACL Flow Meter Configuration window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-1024)	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID (1-1024)	Here the user can enter the Access ID for the flow meter.
Mode	**Rate** – Specify the rate for single rate two color mode. *Rate* – Specify the committed bandwidth in Kbps for the flow. *Burst Size* – Specify the burst size for the single rate two color mode. The unit is in kilobyte. *Rate Exceeded* – Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following:

	Drop Packet – Drop the packet immediately. *Remark DSCP* – Mark the packet with a specified DSCP. The packet is set to drop for packets with a high precedence. **trTCM** – Specify the "two-rate three-color mode." *CIR* – Specify the Committed information Rate. The unit is Kbps. CIR should always be equal or less than PIR. *PIR* – Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR. *CBS* – Specify the Committed Burst Size. The unit is in kilobyte. *PBS* – Specify the Peak Burst Size. The unit is in kilobyte. **srTCM** – Specify the "single-rate three-color mode". *CIR* – Specify the Committed Information Rate. The unit is in Kbps. *CBS* – Specify the Committed Burst Size. The unit is in kilobyte. *EBS* – Specify the Excess Burst Size. The unit is in kilobyte.
Action	**Conform** – This field denotes the green packet flow. Green packet flows may have their *DSCP* field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter. *Replace DSCP* – Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow. **Un-conform** – This changes the DSCP of an un-conforming (yellow or red) packet. *Replace DSCP* – Packets that are in the yellow and red flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace. **Exceed** – This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow. **Violate** – This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

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

After clicking the **View** button, the following page will appear:

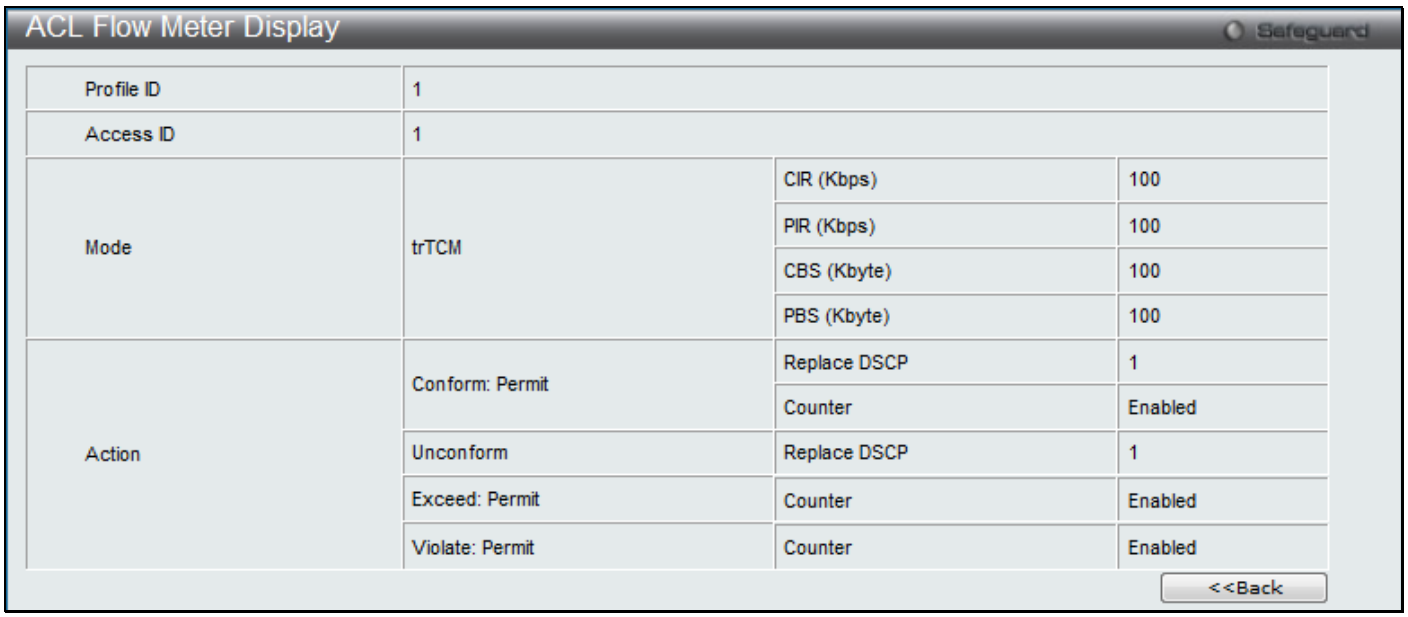


Figure 8-47 ACL Flow Meter Display window

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

Egress Access Profile List

Egress ACL performs per-flow processing of packets when they egress from the Switch ports. The Switch supports three Profile Types, Ethernet ACL, IPv4 ACL, and IPv6 ACL.

To view this window, click **ACL > Egress Access Profile List** as shown below:

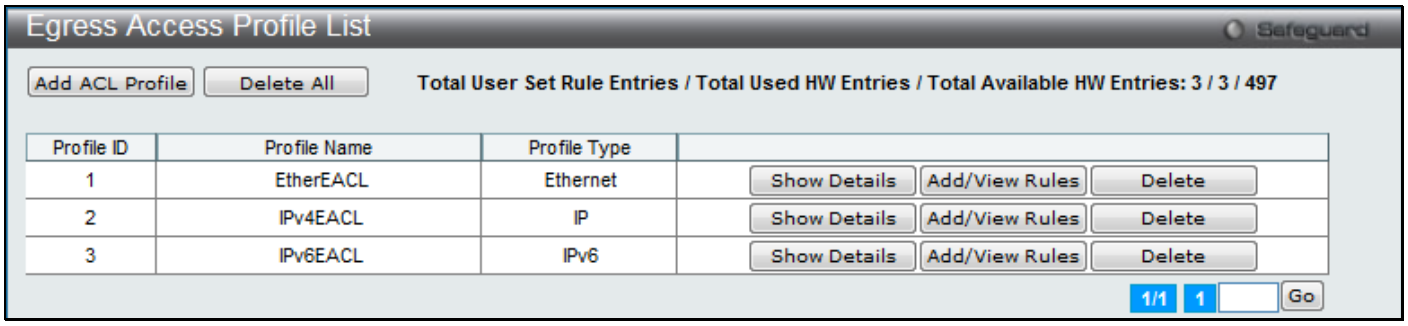


Figure 8-48 Egress Access Profile List window

Adding an Ethernet ACL Profile

The window shown below is the Add Egress ACL Profile window for Ethernet. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

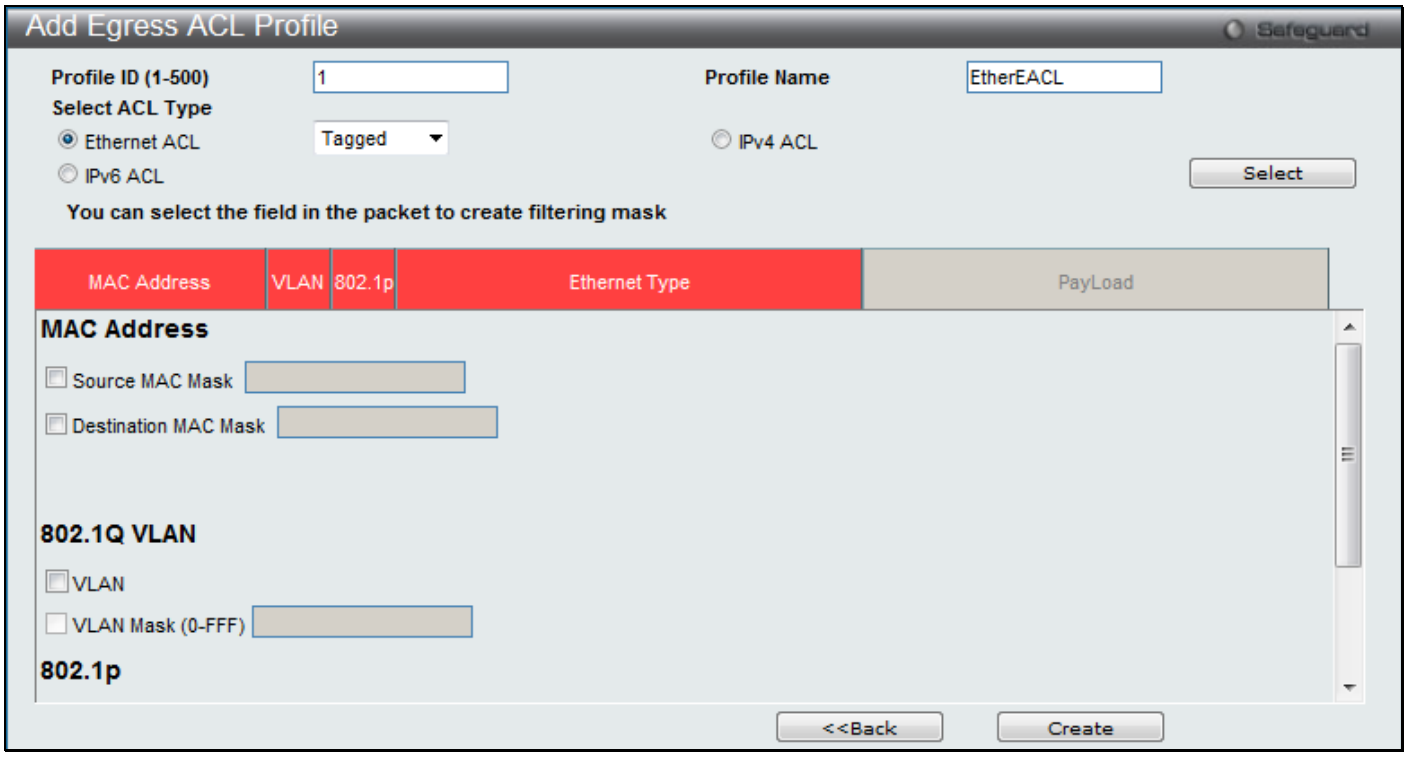


Figure 8-49 Add Egress ACL Profile window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-500)	Enter a unique identifier number for this profile set. This value can be set from *1* to *500.*
Profile Name	Enter a profile name for the profile created.

Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select an ACL type.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Create** button to create a profile.

After clicking the **Show Details** button, the following page will appear:

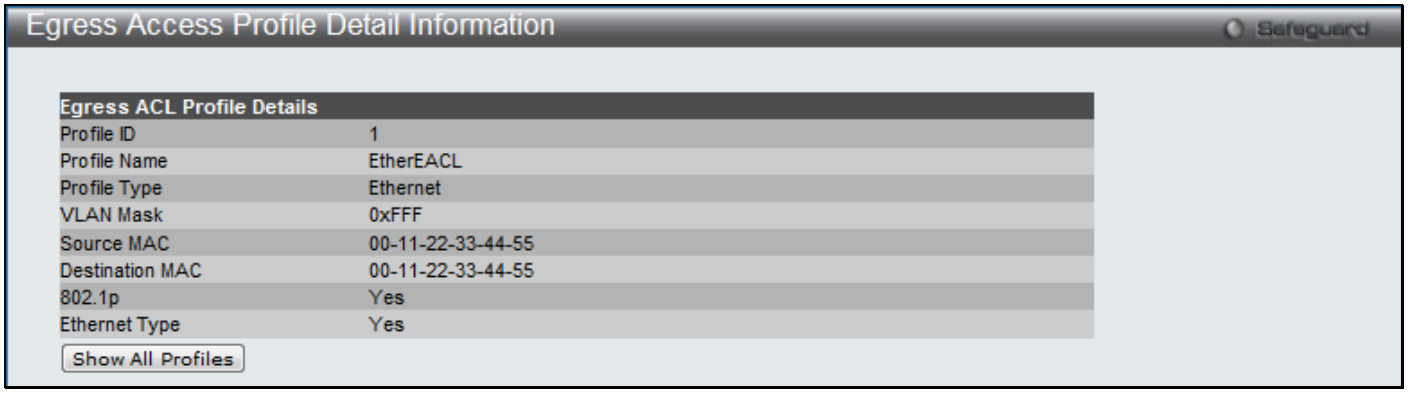


Figure 8-50 Egress Access Profile Detail Information window (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **Egress Access Profile List** window.

After clicking the **Add/View Rules** button, the following page will appear:

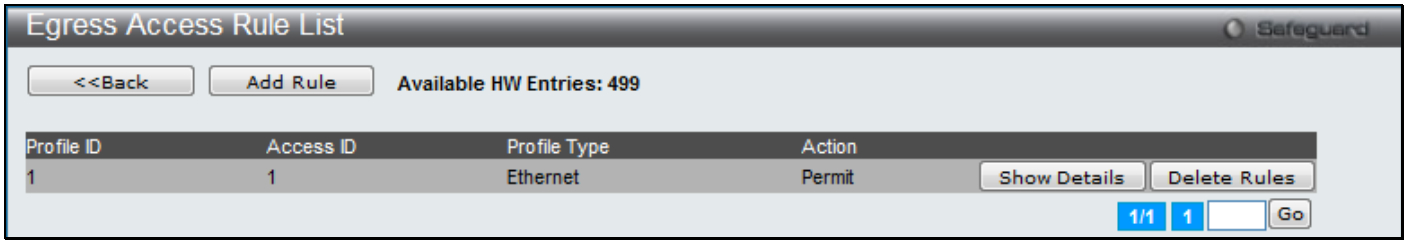


Figure 8-51 Egress Access Rule List window (Ethernet ACL)

Click the **<<Back** button to return to the previous page.
Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

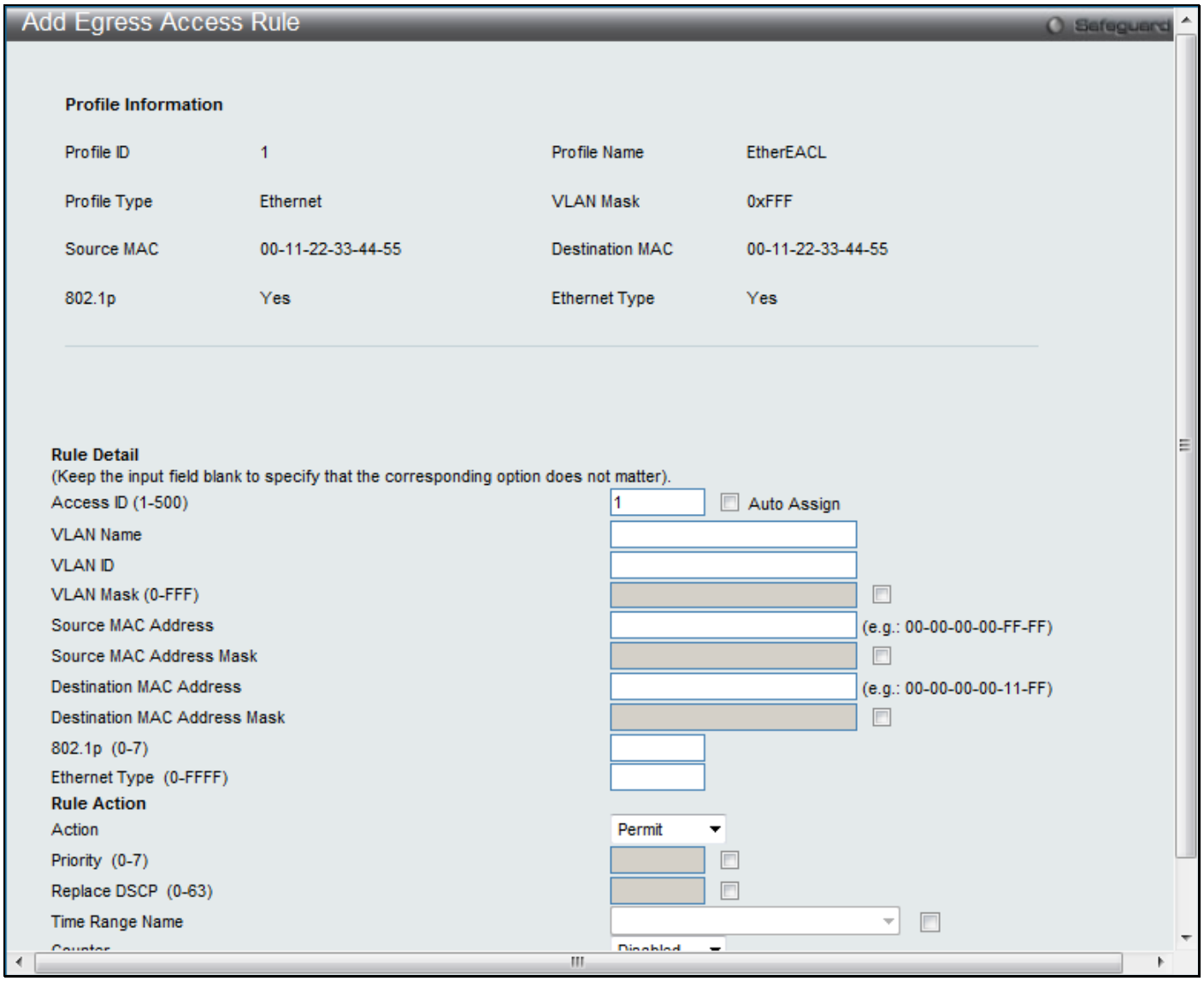


Figure 8-52 Add Egress Access Rule window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-500)	Type in a unique identifier number for this access. This value can be set from 1 to 500. **Auto Assign** – Tick the check box will instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	Enter the VLAN name used here.
VLAN ID	Enter the VLAN ID used here.
VLAN Mask	Select and enter the VLAN mask value used here.
Source MAC Address	Enter the source MAC address used here.
Source MAC Address Mask	Select and enter the source MAC address mask used here.
Destination MAC Address	Enter the destination MAC address used here.
Destination MAC Address Mask	Select and enter the destination MAC address mask used here.
802.1p	Enter the 802.1p priority tag value used here. This value must be between 0 and 7.
Ethernet Type	Enter the Ethernet type value used here.

Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Port	Specify a port number to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access 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.

After clicking the **Show Details** button in the **Egress Access Rule List**, the following page will appear:

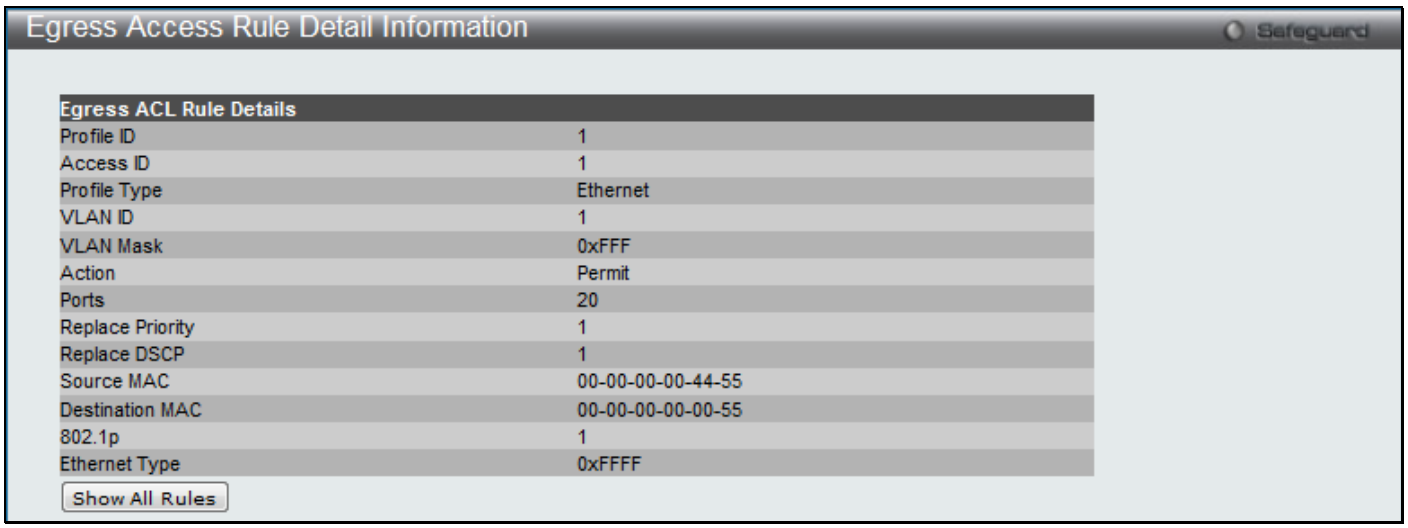


Figure 8-53 Egress Access Rule Detail Information window (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv4 Egress ACL Profile

The window shown below is the Add Egress ACL Profile window for IPv4. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

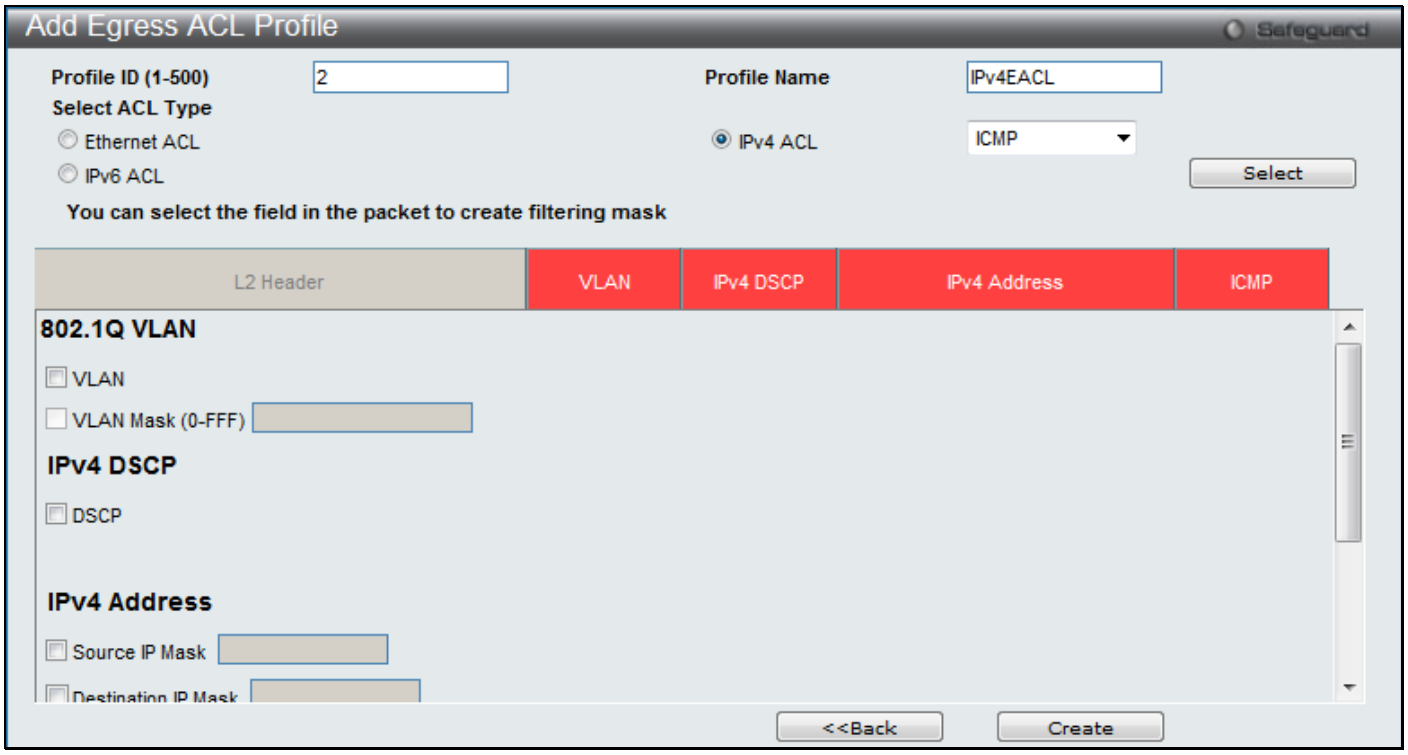


Figure 8-54 Add Egress ACL Profile window (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-500)	Enter a unique identifier number for this profile set. This value can be set from 1 to 500.
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask	Enter an IP address mask for the source IP address.
IPv4 Destination IP Mask	Enter an IP address mask for the destination IP address.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.

	Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. *flag bit* - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff. *Protocol ID Mask* - Specify that the rule applies to the IP protocol ID traffic. *User Define* - Specify the Layer 4 part mask

Click the **Select** button to select an ACL type.

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

Click the **Create** button to create a profile.

After clicking the **Show Details** button, the following page will appear:

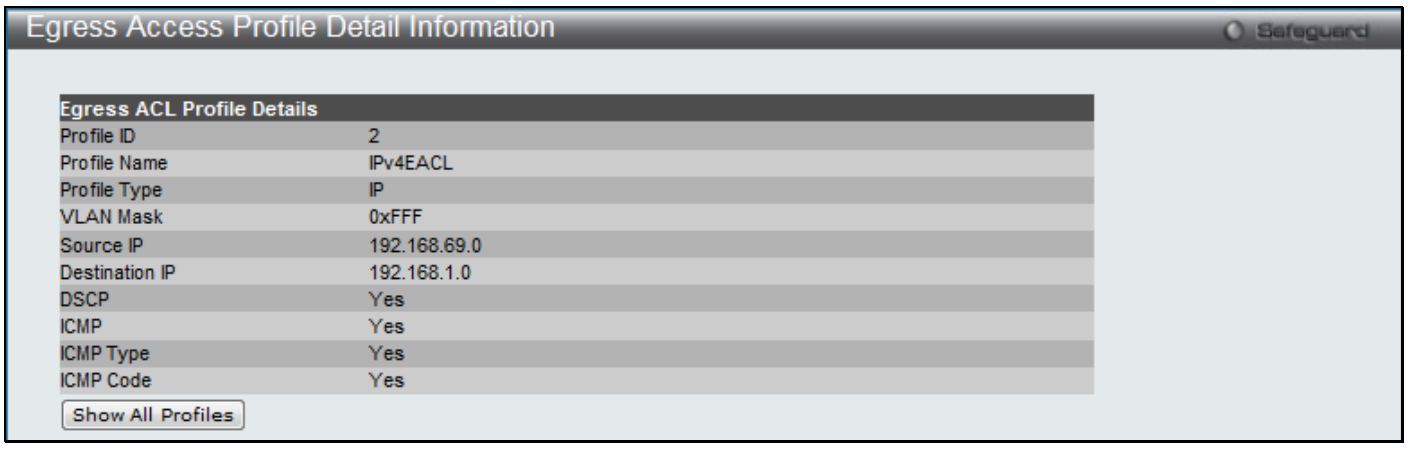


Figure 8-55 Egress Access Profile Detail Information window (IPv4 ACL)

Click the **Show All Profiles** button to navigate back to the **Egress Access Profile List** window.

After clicking the **Add/View Rules** button, the following page will appear:

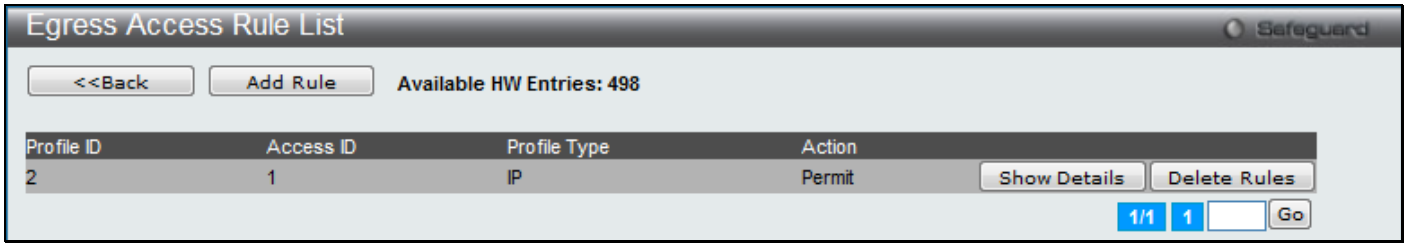


Figure 8-56 Egress Access Rule List window (IPv4 ACL)

Click the **<<Back** button to return to the previous page.
Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

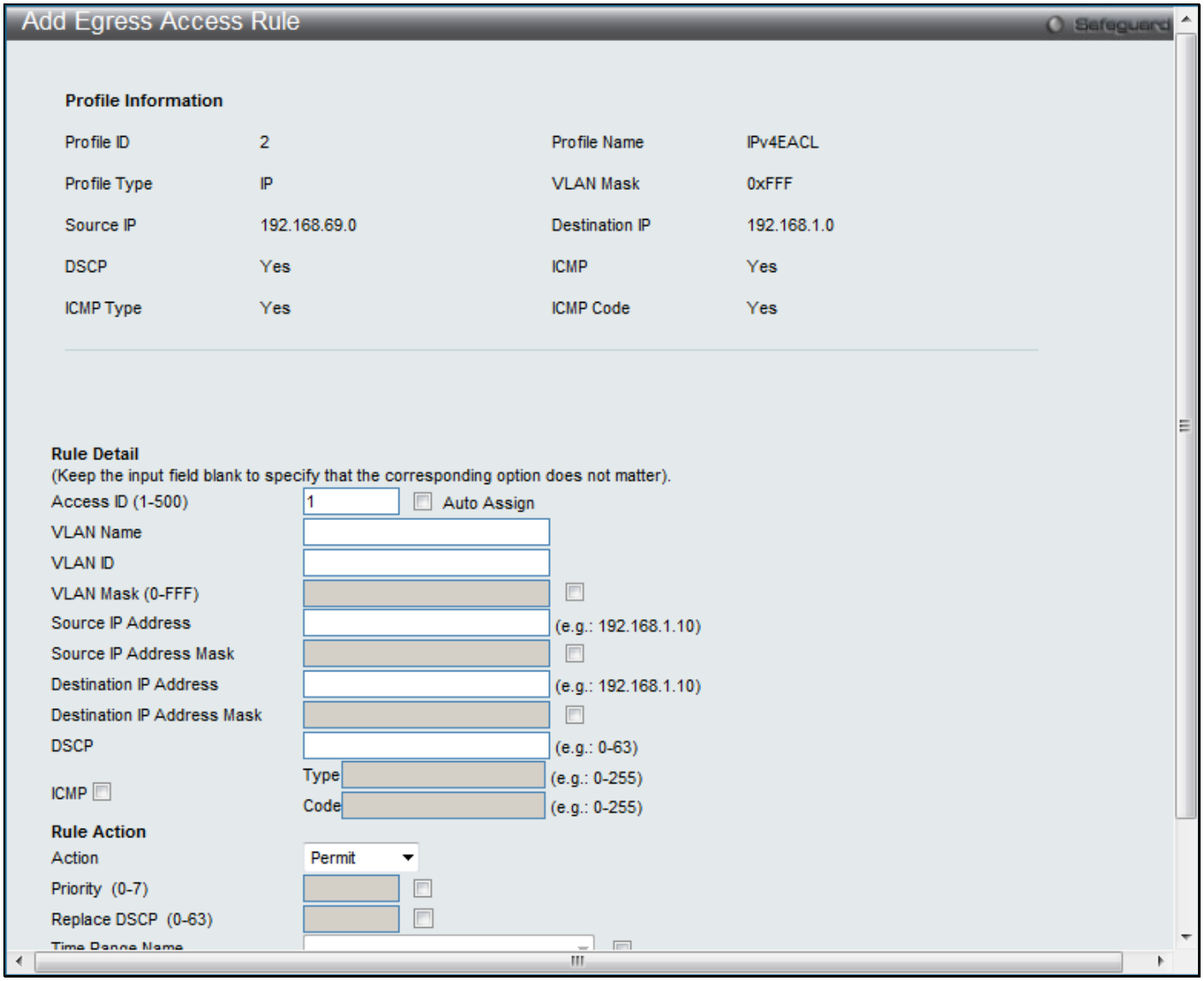


Figure 8-57 Add Egress Access Rule (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-500)	Type in a unique identifier number for this access. This value can be set from 1 to 500. **Auto Assign** – Tick the check box will instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	Enter the VLAN name used here.
VLAN ID	Enter the VLAN ID used here.
VLAN Mask	Select and enter the VLAN mask value used here.
Source IP Address	Enter the source IP address used here.
Source IP Address	Select and enter the source IP address mask used here.

Mask	
Destination IP Address	Enter the destination IP address used here.
Destination IP Address Mask	Select and enter the destination IP address mask used here.
DSCP	Enter the DSCP value used here.
ICMP	Select this option to specify that the rule will be applied to ICMP traffic. *Type* – Enter the ICMP packet type value used here. *Code* – Enter the ICMP code value used here.
Action	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	Specify a port number to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access 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.

After clicking the **Show Details** button in the **Egress Access Rule List**, the following page will appear:

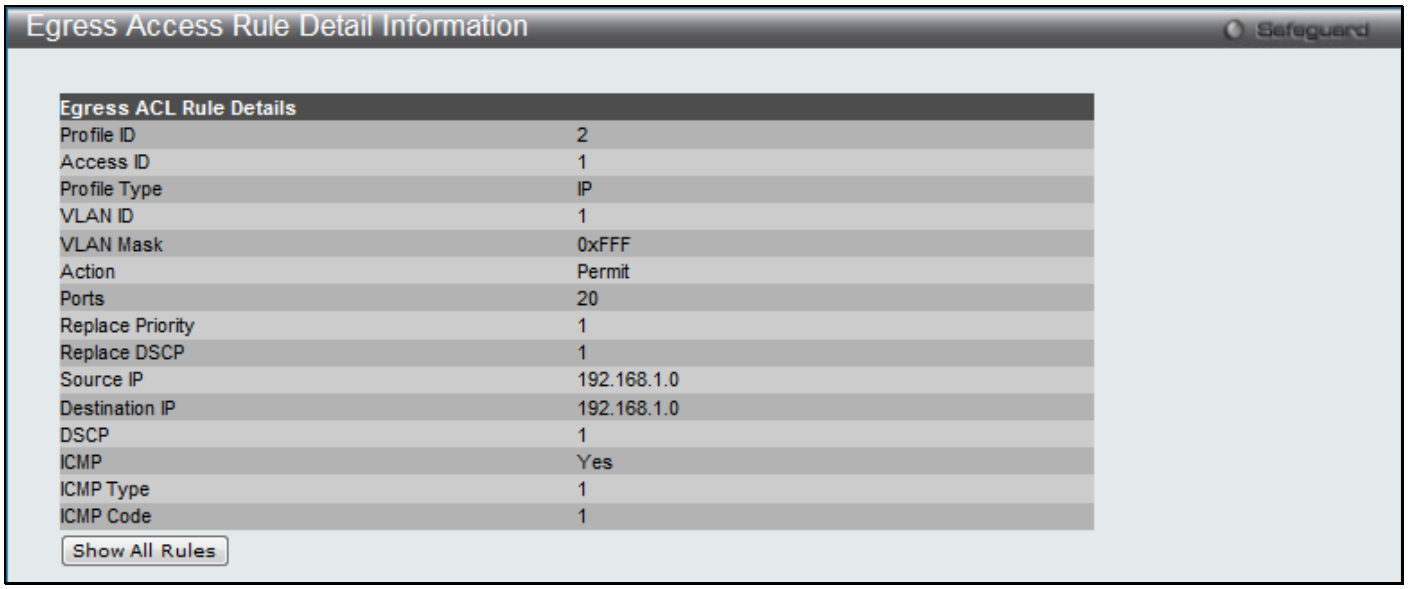


Figure 8-58 Egress Access Rule Detail Information (IPv4 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 Egress ACL Profile

The window shown below is the Add Egress ACL Profile window for IPv6. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

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

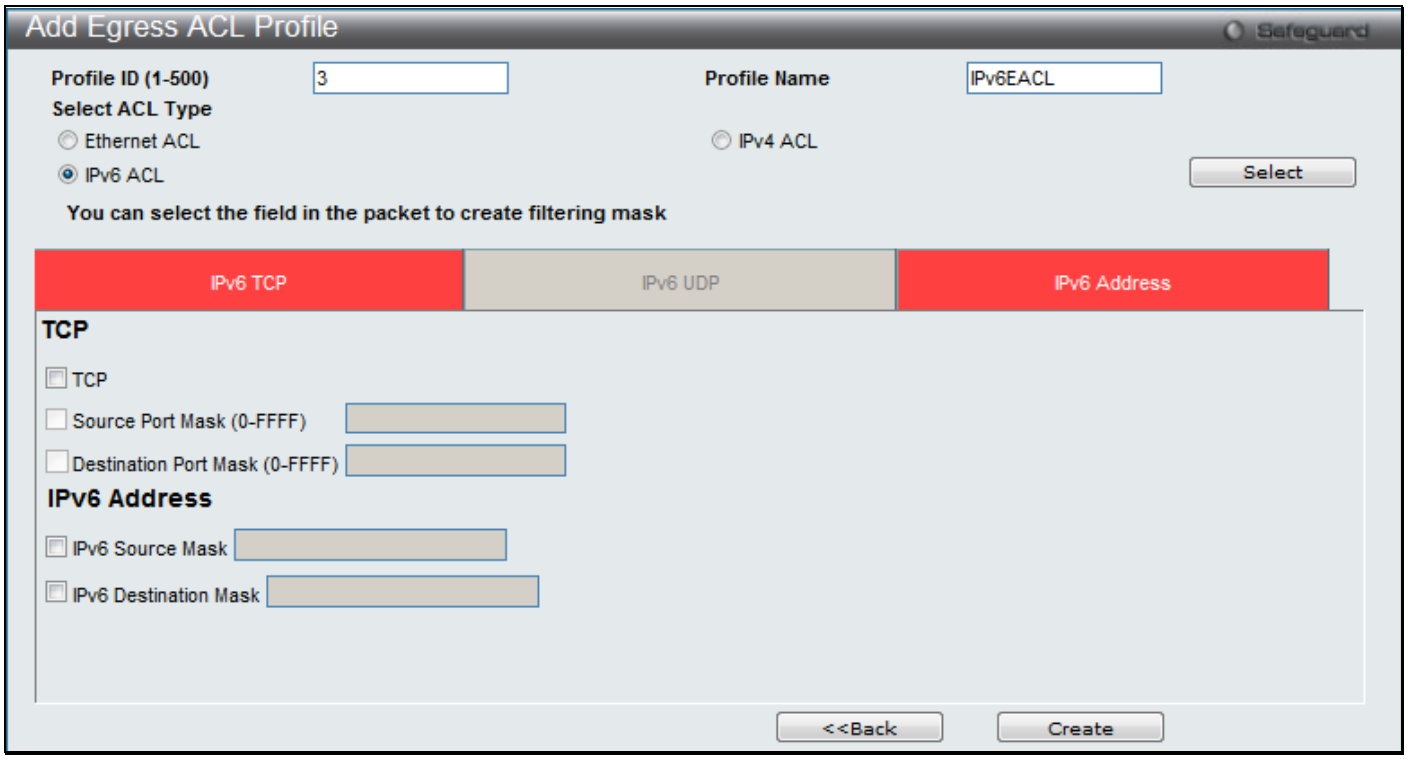


Figure 8-59 Add Egress ACL Profile window (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-500)	Enter a unique identifier number for this profile set. This value can be set from 1 to 500.
Profile Name	Enter a profile name for the profile created.

Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports. *Destination Port Mask* – Specify the range of the TCP destination port range.
IPv6 UDP	*Source Port Mask* – Specify the range of the UDP source port range. *Destination Port Mask* – Specify the range of the UDP destination port mask.
IPv6 Source Mask	The user may specify an IPv6 address mask for the source IPv6 address by ticking the corresponding check box and entering the IPv6 address mask, e.g. FFFF:FFFF::FFFF.
IPv6 Destination Mask	The user may specify an IPv6 address mask for the destination IPv6 address by ticking the corresponding check box and entering the IPv6 address mask, e.g. FFFF:FFFF::FFFF.

Click the **Select** button to select an ACL type.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Create** button to create a profile.

After clicking the **Show Details** button, the following page will appear:

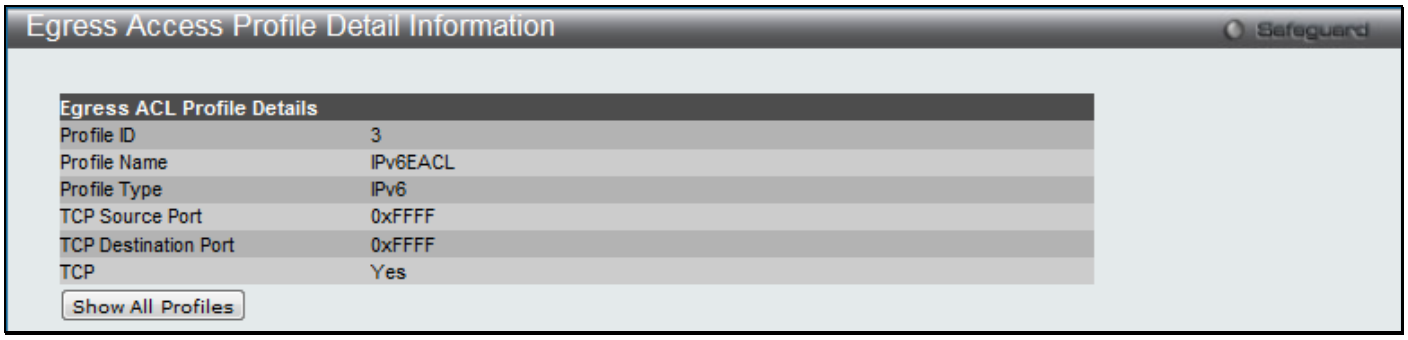


Figure 8-60 Egress Access Profile Detail Information window (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **Egress Access Profile List** window.

After clicking the **Add/View Rules** button, the following page will appear:

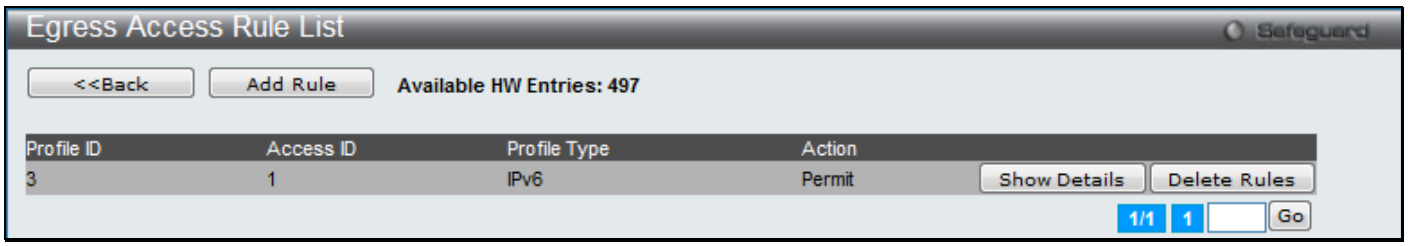


Figure 8-61 Egress Access Rule List window (IPv6 ACL)

Click the **<<Back** button to return to the previous page.
Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** 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 **Add Rule** button, the following page will appear:

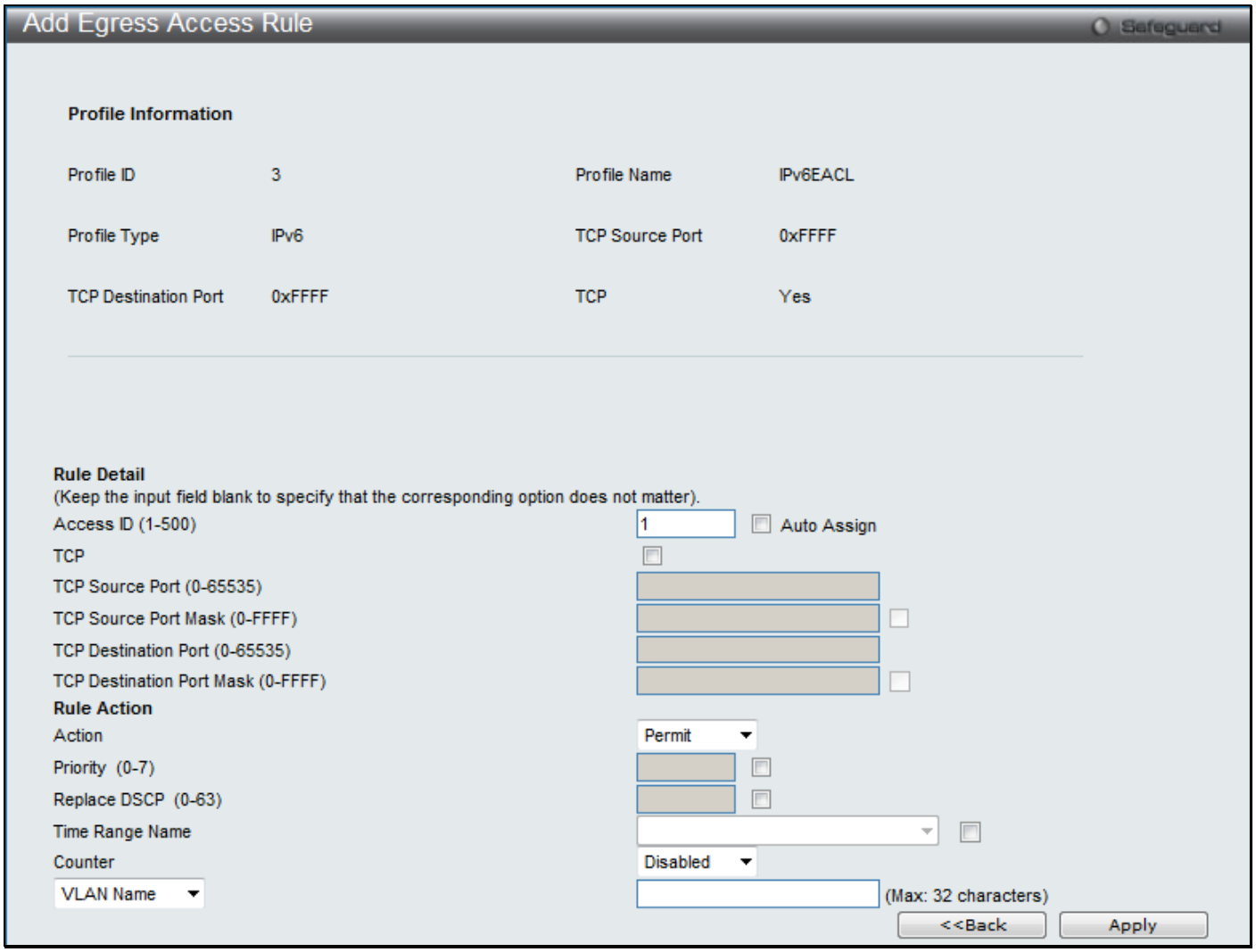


Figure 8-62 Add Egress Access Rule (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Access ID (1-500)	Type in a unique identifier number for this access. This value can be set from 1 to 500. **Auto Assign** – Tick the check box will instruct the Switch to automatically assign an Access ID for the rule being created.
TCP	Select this option to enable the TCP protocol.
TCP Source Port (0-65535)	Enter the value of the IPv6 layer 4 TCP source port here.
TCP Source Port Mask (0-FFFF)	Enter the IPv6 TCP source port mask here.
TCP Destination Port (0-65535)	Enter the value of the IPv6 layer 4 TCP destination port.
TCP Destination Port Mask (0-FFFF)	Enter the IPv6 TCP destination port mask here.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Priority (0-7)	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will

	have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	Specify a port number to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access 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.

After clicking the **Show Details** button in the **Egress Access Rule List**, the following page will appear:

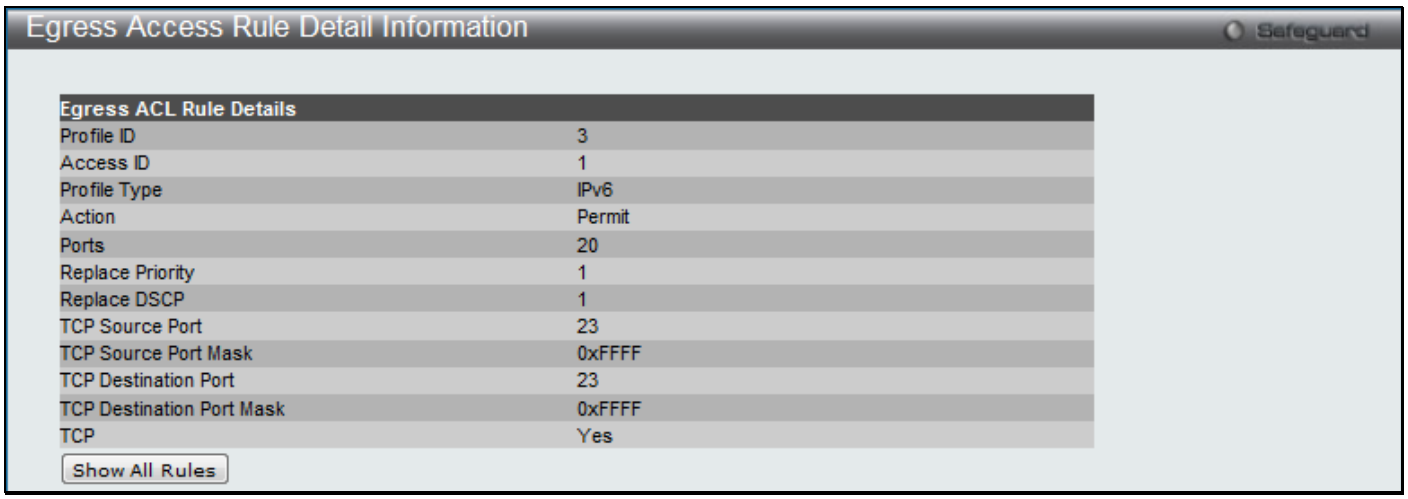


Figure 8-63 Egress Access Rule Detail Information (IPv6 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Egress ACL Flow Meter

This window is used to configure the packet flow-based metering based on an egress access profile and rule.

To view this window, click **ACL > Egress ACL Flow Meter** as shown below:

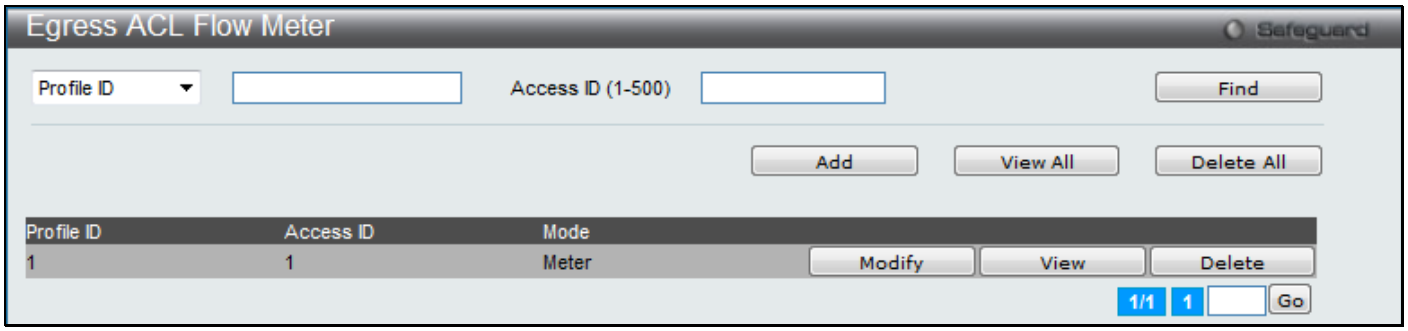


Figure 8-64 Egress ACL Flow Meter window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID (1-500)	Here the user can enter the Access ID for the flow meter.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Add** button to add a new entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Delete All** button to remove all the entries listed.
Click the **Modify** button to re-configure the specific entry.
Click the **View** button to display the information of the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the **Add** or **Modify** button, the following page will appear:

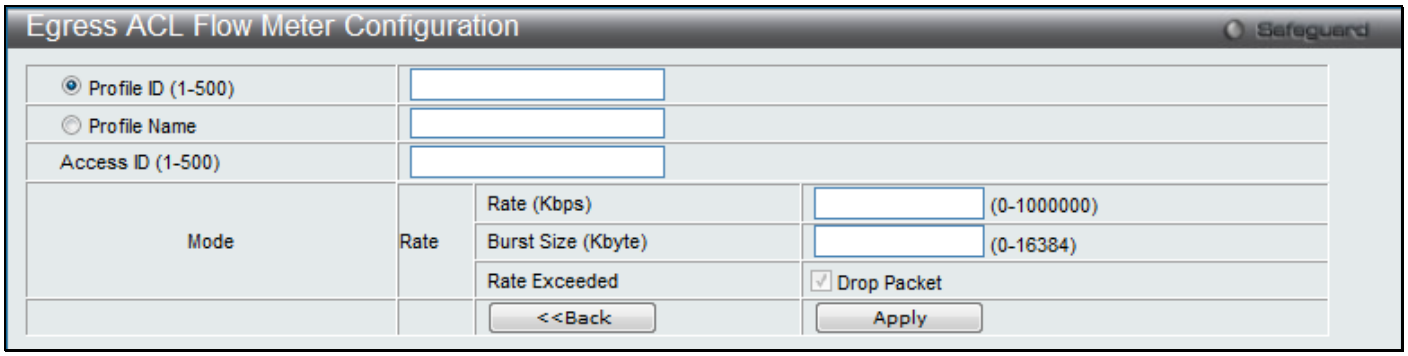


Figure 8-65 Egress ACL Flow Meter Configuration window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-500)	Enter the Profile ID for the flow meter.
Profile Name	Enter the Profile Name for the flow meter.
Access ID (1-500)	Enter the Access ID for the flow meter.
Mode	**Rate** – Specify the rate for single rate two color mode. *Rate* – Specify the committed bandwidth in Kbps for the flow. *Burst Size* – Specify the burst size for the single rate two color mode. The unit is in kilobyte. *Rate Exceeded* – Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as the following: *Drop Packet* – Drop the packet immediately.

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

After clicking the **View** button, the following page will appear:

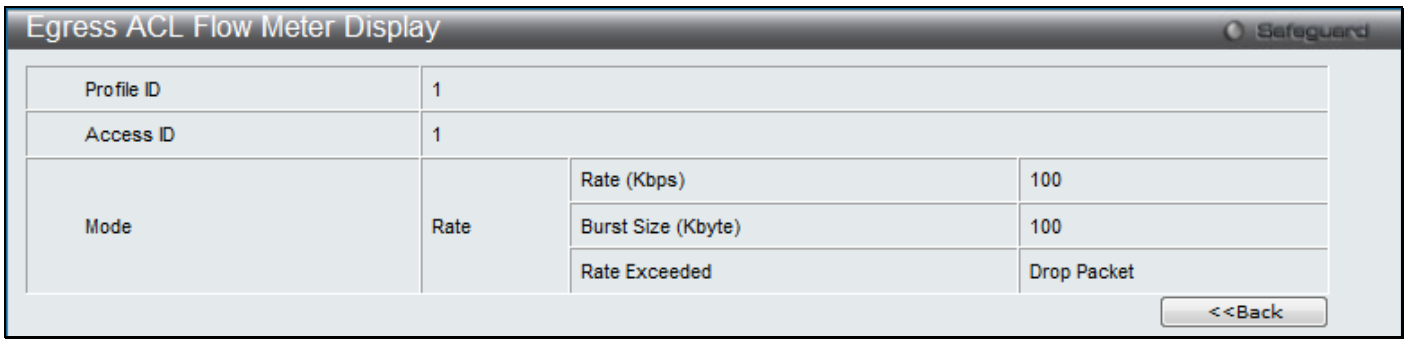


Figure 8-66 Egress ACL Flow meter Display window

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

Chapter 9 Security

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:

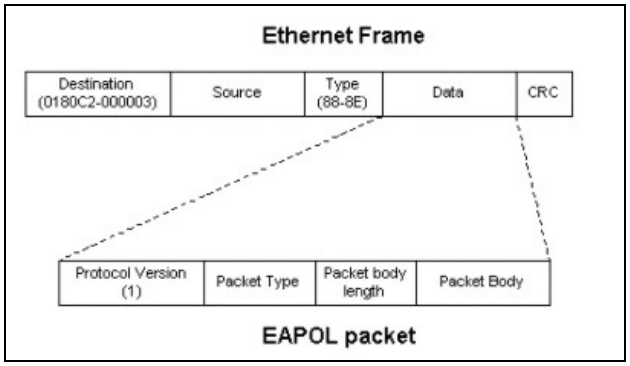


Figure 9-1 EAPOL Packet window

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.

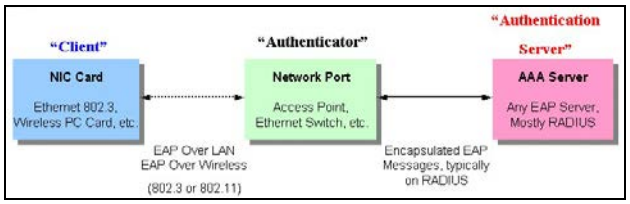


Figure 9-2 Authenticator window

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.

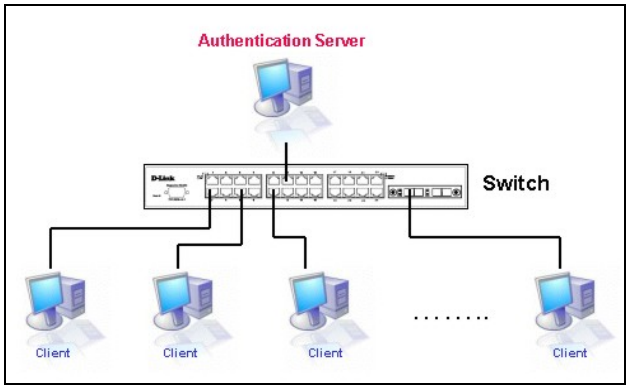


Figure 9-3 Authentication Server window

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.

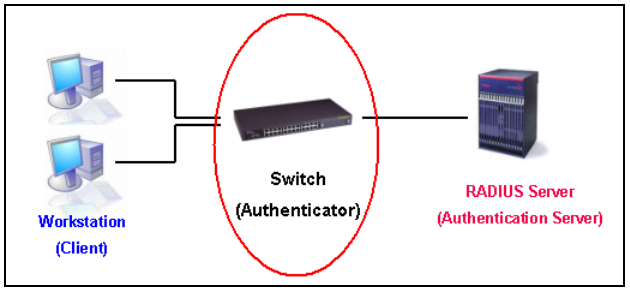


Figure 9-4 Authenticator window

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X State must be *Enabled*. (**Security / 802.1X /802.1X Settings**)
2. The 802.1X settings must be implemented by port (**Security** / **802.1X** / **802.1X Settings**)
3. A RADIUS server must be configured on the Switch. (**Security** / **802.1X** / **Authentic RADIUS Server**)

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.

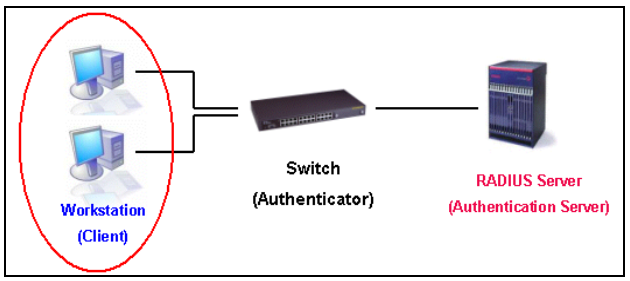


Figure 9-5 Client window

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 unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

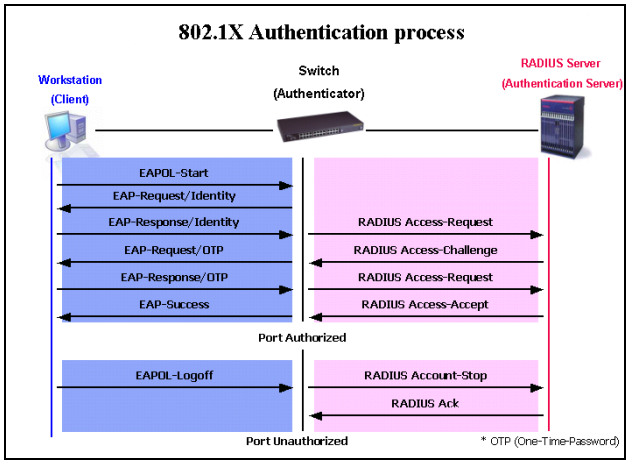


Figure 9-6 Authentication Process window

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1. 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.
2. Host-Based Access Control – Using this method, the Switch will automatically learn up to a maximum of 16 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.

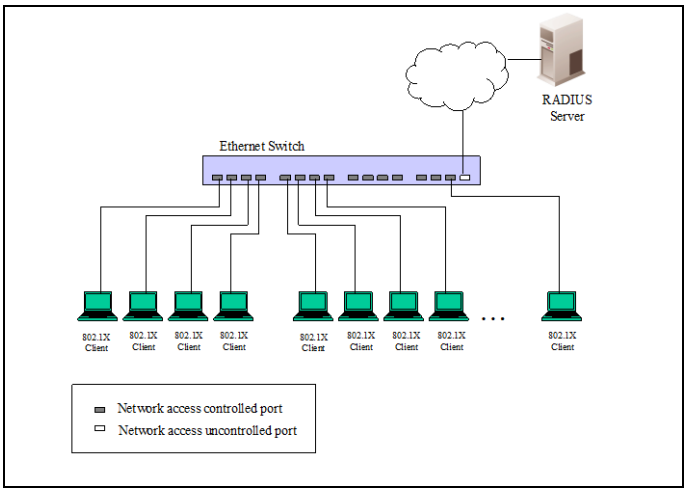


Figure 9-7 Port-Based Network Access Control window

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.

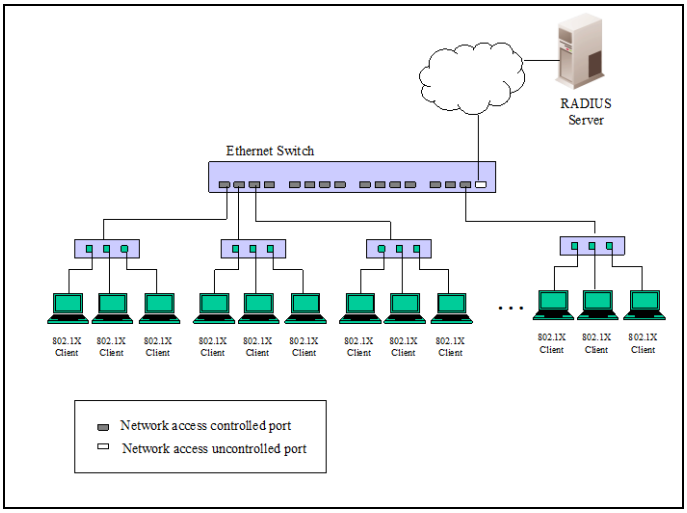


Figure 9-8 Host-Based Network Access Control window

802.1X Global Settings

Users can configure the 802.1X global parameter.

To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:

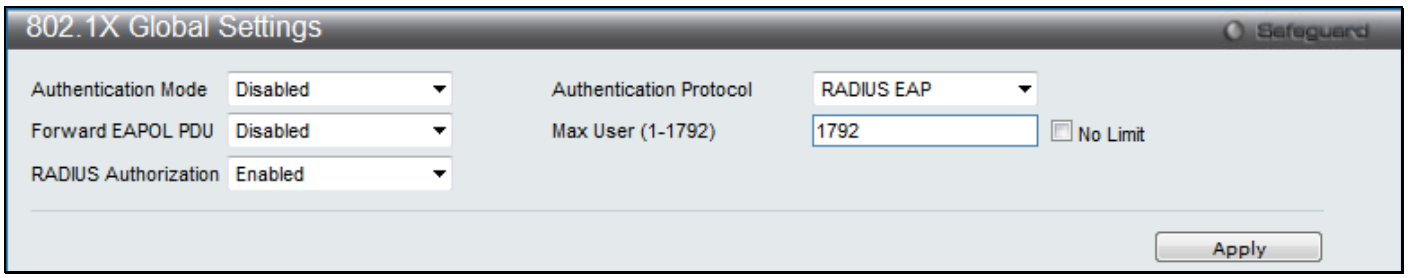


Figure 9-9 802.1X Global Settings window

The fields that can be configured are described below:

Parameter	Description
Authentication Mode	Choose the 802.1X authenticator mode, *Disabled*, *Port-based*, or *MAC-based*.
Authentication Protocol	Choose the authenticator protocol, *Local* or *RADIUS EAP*.
Forward EAPOL PDU	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max User (1-1792)	Specifies the maximum number of users. The limit on the maximum users is *1792* users.
RADIUS Authorization	This option is used to enable or disable acceptation of authorized configuration. When the authorization is enabled for 802.1X’s RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled.

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

802.1X Port Settings

Users can configure the 802.1X authenticator port settings.

To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:

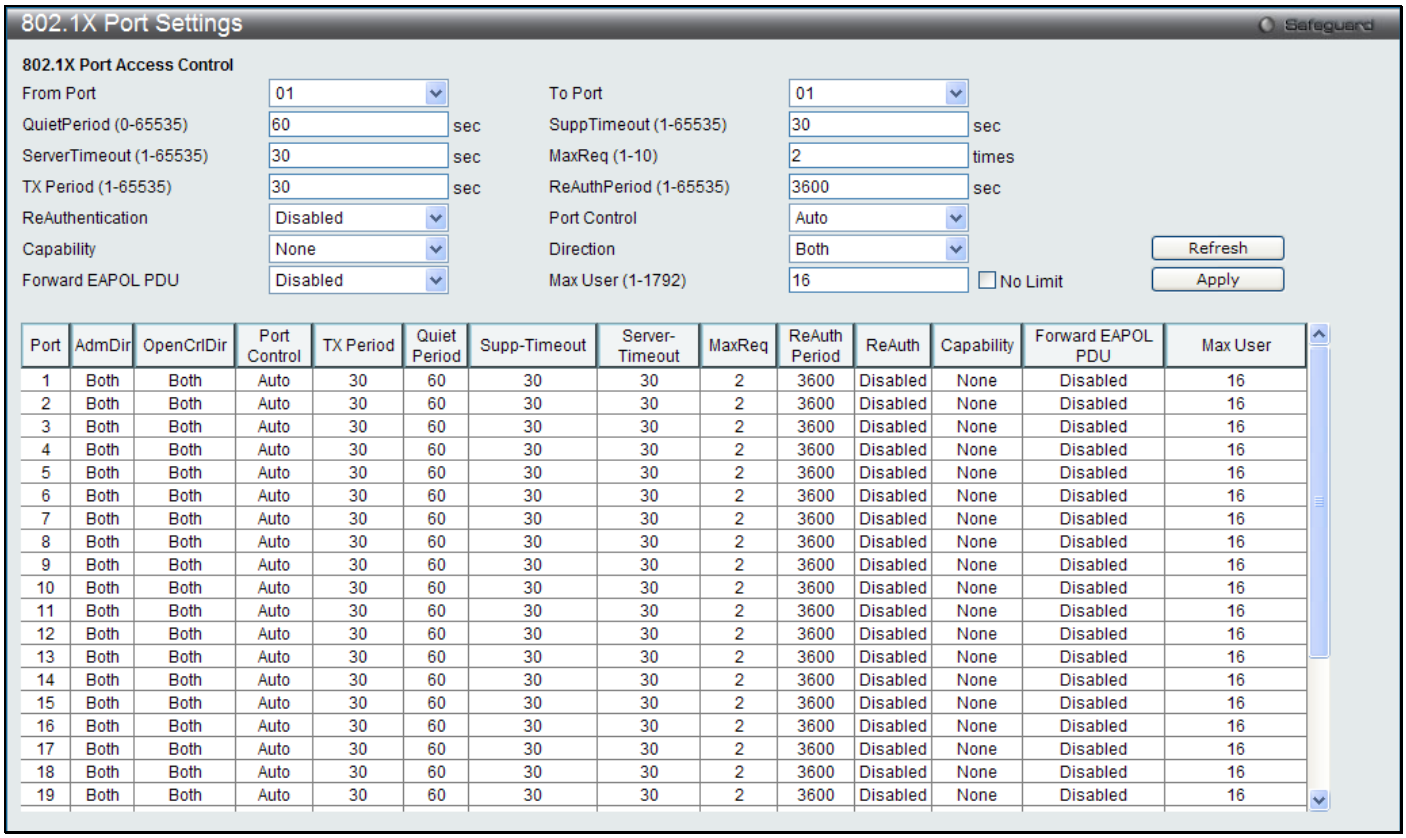


Figure 9-10 802.1X Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be configured.
QuietPeriod (0-65535)	This allows the user to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2*.
TxPeriod (1-65535)	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic re-authentication of the client. The default setting is *3600* seconds.
ReAuthentication	Determines whether regular re-authentication will take place on this port. The default setting is *Disabled*.
Port Control	This allows the user to control the port authorization state. Select *ForceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *ForceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication

	services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated, a user must pass the authentication process to gain access to the network. Select *None* disable 802.1X functions on the port.
Direction	Sets the administrative-controlled direction to *Both* or *In.* If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. If *In* is selected, the control is only exerted over incoming traffic through the port the user selected in the first field.
Forward EAPOL PDU	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max User (1-1792)	Specifies the maximum number of users. The maximum user limit is 1792 users. By default, the maximum value is selected. Tick the **No Limit** check box to have unlimited users.

Click the **Refresh** button to refresh the display table so that new entries will appear.
Click the **Apply** button to accept the changes made.

802.1X User Settings

Users can set different 802.1X users in switch's local database.

To view the following window, click **Security > 802.1X > 802.1X User Settings**, as shown below:

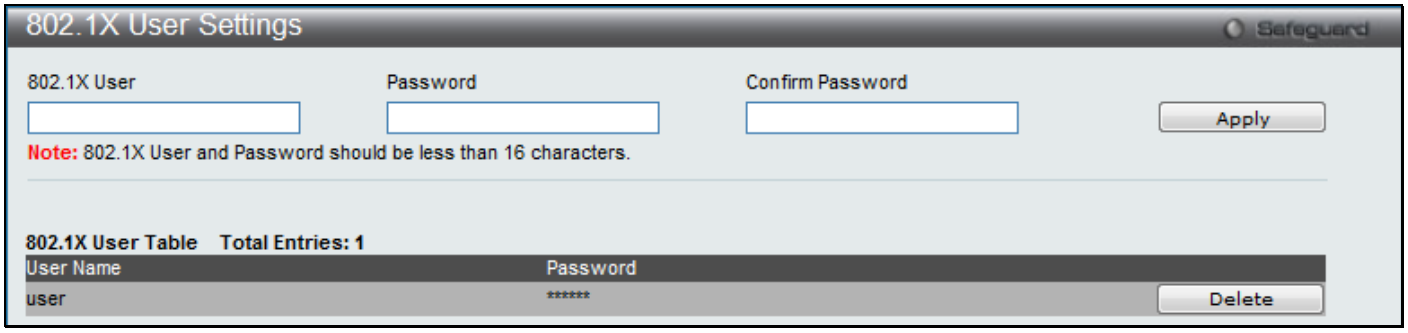


Figure 9-11 802.1X User Settings window

The fields that can be configured are described below:

Parameter	Description
802.1X User	The user can enter an 802.1X user's username in here.
Password	The user can enter an 802.1X user's password in here.
Confirm Password	The user can re-enter an 802.1X user's password in here.

Click the **Apply** button to accept the changes made.
Click the **Delete** button to remove the specific entry.

NOTE: The **802.1X User** and **Password** values should be less than 16 characters.

Guest VLAN Settings

On 802.1X security-enabled networks, there is a need for non- 802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or older operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN.

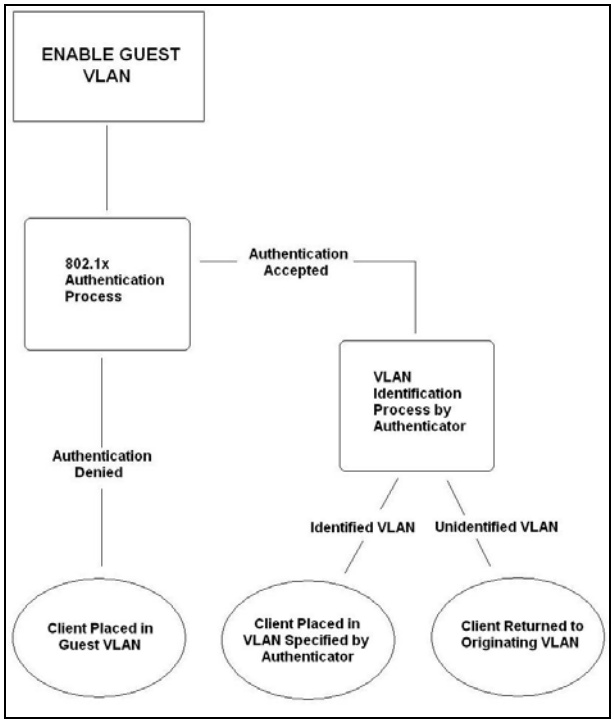


Figure 9-12 Guest VLAN window

If authenticated and the authenticator possess the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.

Remember, to set an 802.1X guest VLAN, the user must first configure a normal VLAN, which can be enabled here for guest VLAN status. Only one VLAN may be assigned as the 802.1X guest VLAN.

To view the following window, click **Security > 802.1X > Guest VLAN Settings**, as shown below:

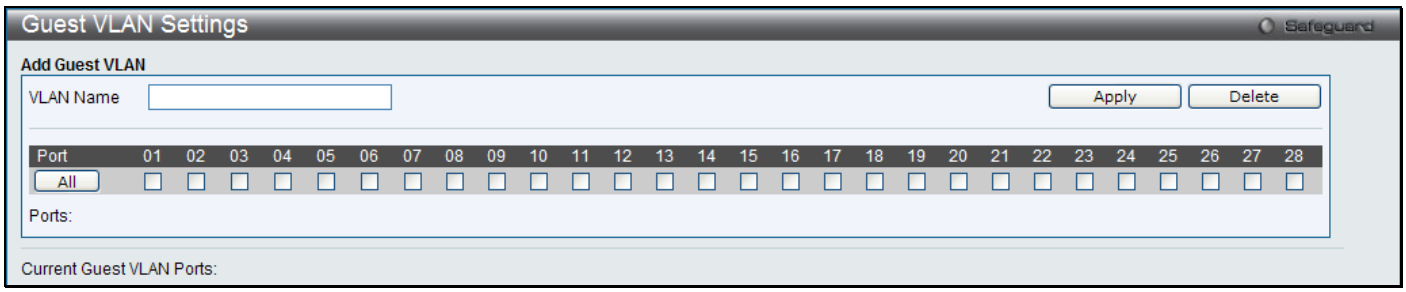


Figure 9-13 Guest VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as an 802.1X guest VLAN.
Port	Set the ports to be enabled for the 802.1X guest VLAN. Click the **All** button to select all the ports.

Click the **Apply** button to accept the changes made.
Click the **Delete** button to remove the specific entry based on the information entered.

Authenticator State

This window is used to display the authenticator state.

To view this window, click **Security > 802.1X > Authenticator State** as shown below:

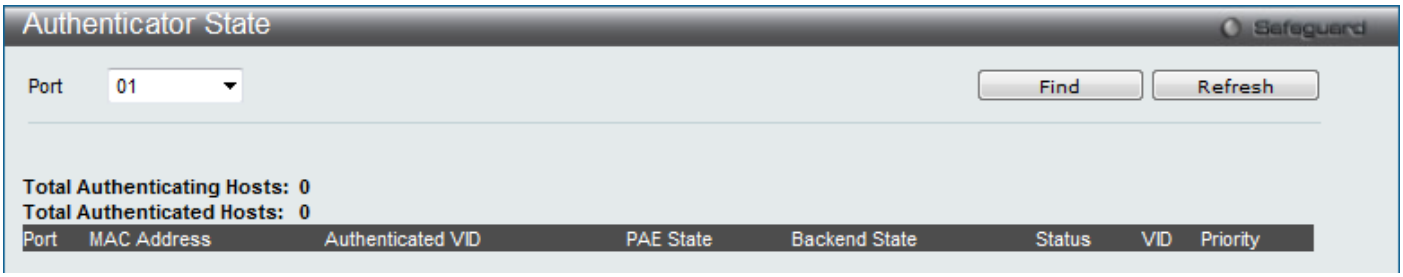


Figure 9-14 Authenticator State window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port to display.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Refresh** button to refresh the display table so that new entries will appear.

NOTE: The user must first globally enable **Authentication Mode** in the **Error! Reference source not found.** window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Authenticator Statistics

This window is used to display the authenticator statistics information.

To view this window, click **Security > 802.1X > Authenticator Statistics** as shown below:

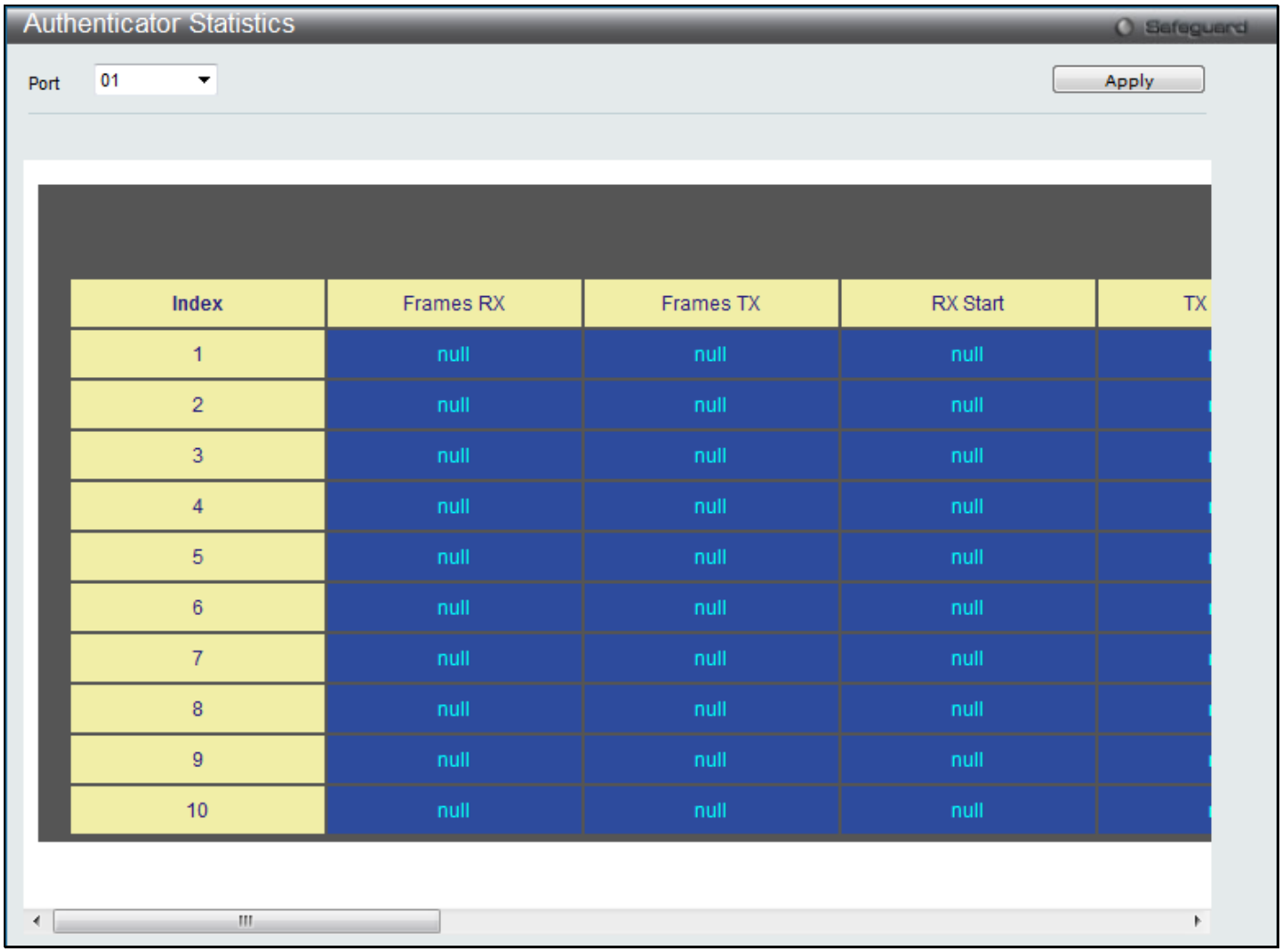


Figure 9-15 Authenticator Statistics – Port-based window

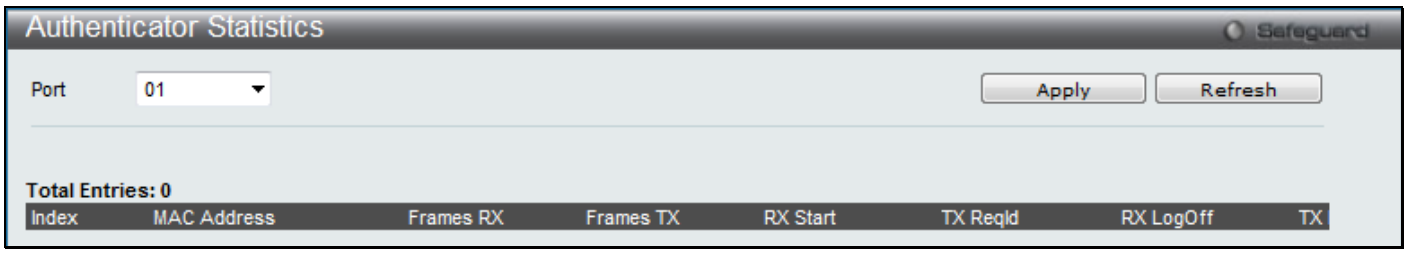


Figure 9-16 Authenticator Statistics - MAC-based window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port to display.

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

NOTE: The user must first globally enable **Authentication Mode** in the **Error! Reference source not found.** window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Authenticator Session Statistics

This window is used to display the authenticator session statistics information.

To view this window, click **Security > 802.1X > Authenticator Session Statistics** as shown below:

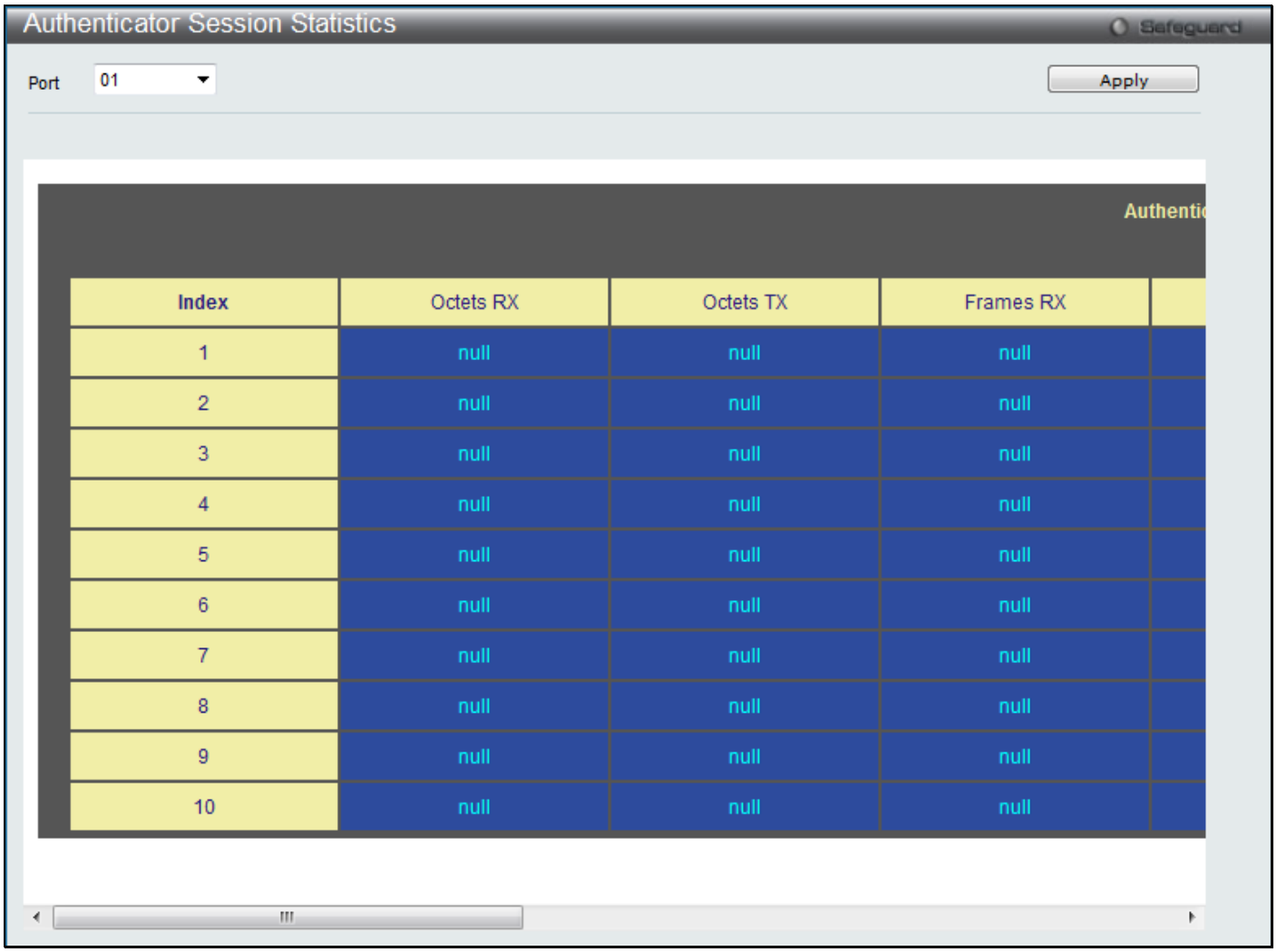


Figure 9-17 Authenticator Session Statistics - Port-based window

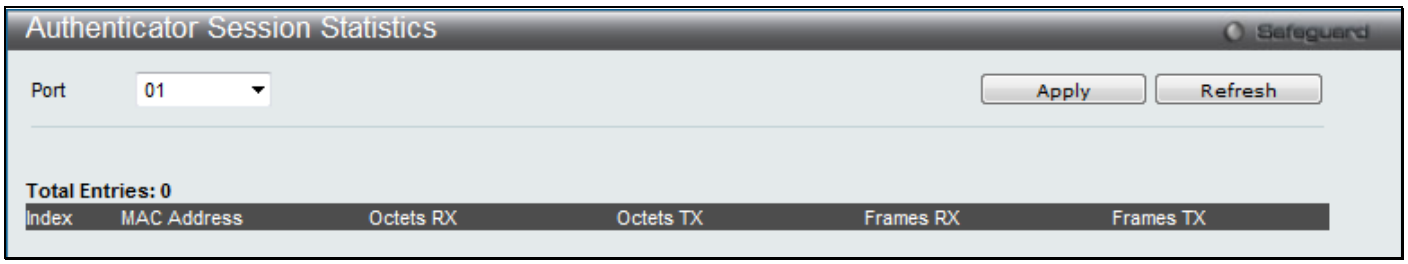


Figure 9-18 Authenticator Session Statistics - MAC-based window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port to display.

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

NOTE: The user must first globally enable **Authentication Mode** in the **Error! Reference source not found.** window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Authenticator Diagnostics

This window is used to display the authenticator diagnostics information.

To view this window, click **Security > 802.1X > Authenticator Diagnostics** as shown below:

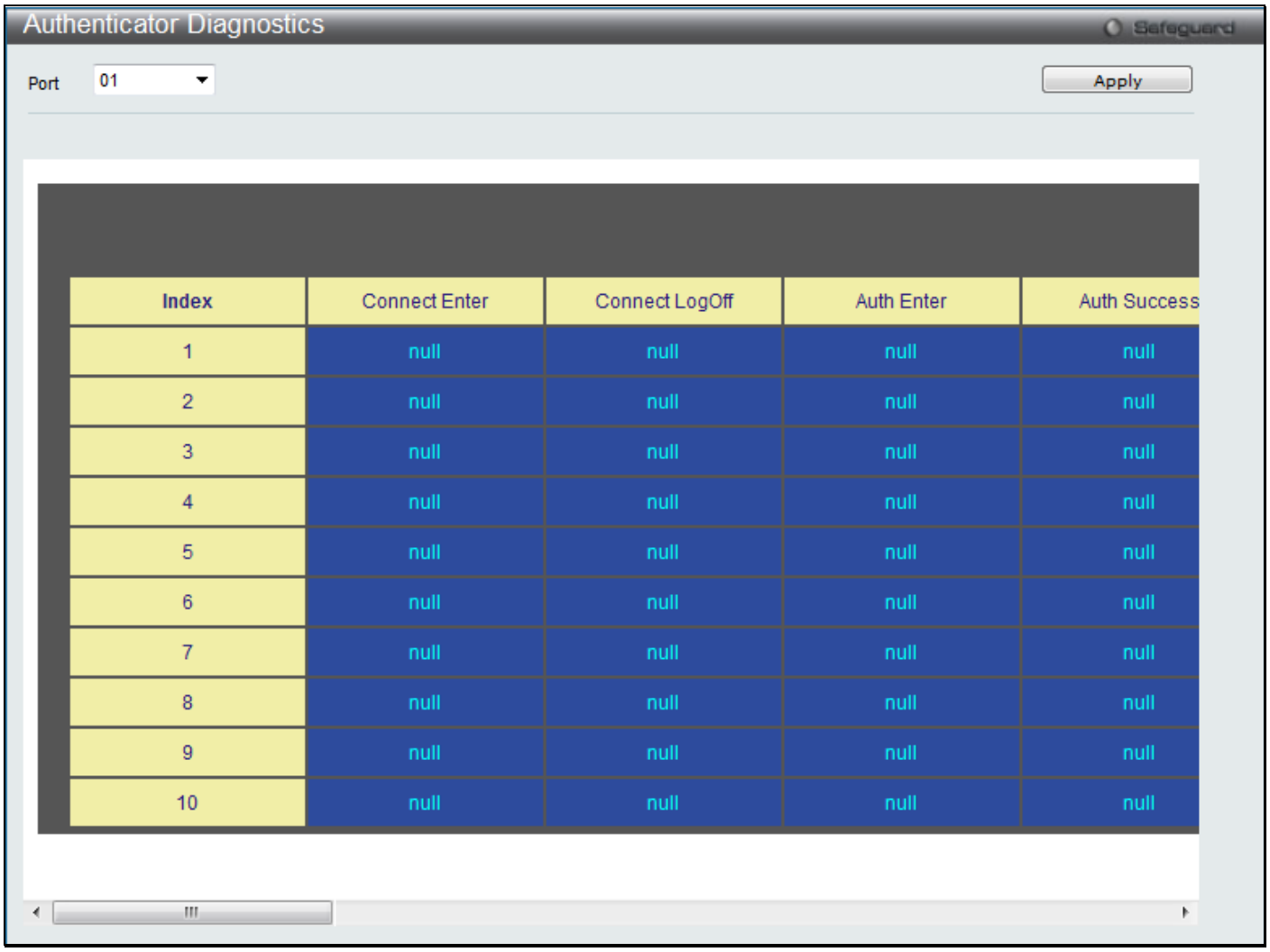


Figure 9-19 Authenticator Diagnostics - Port-based window

Figure 9-20 Authenticator Diagnostics - MAC-based window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select a port to display.

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

NOTE: The user must first globally enable **Authentication Mode** in the **Error! Reference source not found.** window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Initialize Port(s)

This window is used to initialize the 802.1X authentication state machine of ports and displays the current initialized ports.

To view this window, click **Security > 802.1X > Initialize Port(s)** as shown below:

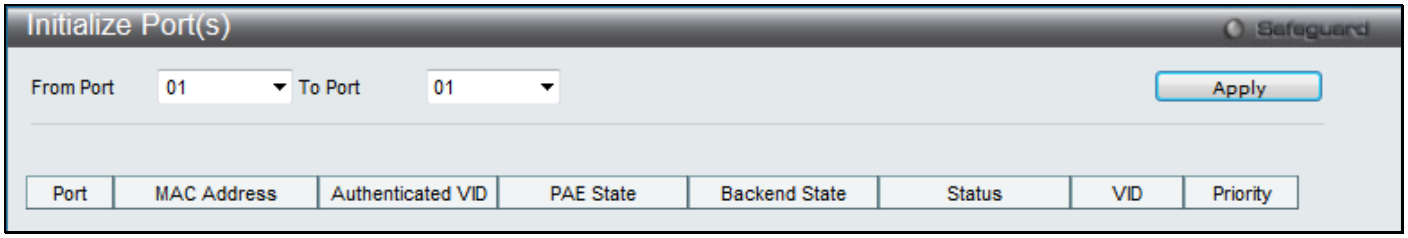


Figure 9-21 Initialize Port(s) - Port-based window

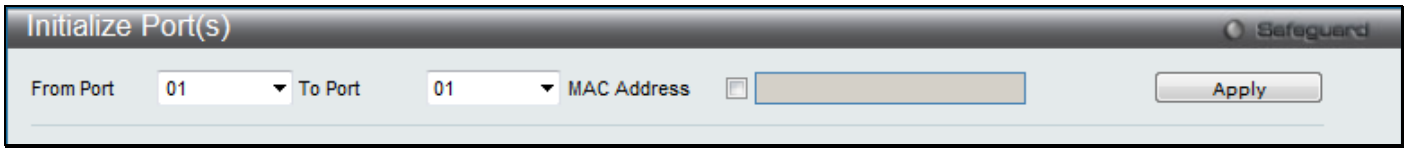


Figure 9-22 Initialize Port(s) - MAC-based window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to select a range of ports to initialize.
MAC Address	Select and enter the appropriate MAC address used here. This option is only available when the **Authentication Mode** has been set to **MAC-based** in the **802.1X Global Settings** window.

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

NOTE: The user must first globally enable **Authentication Mode** in the **Error! Reference source not found.** window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Reauthenticate Port(s)

This window is used to re-authenticate the device connected with the ports and display the current status of the re-authenticated port-based port(s).

This window appears when the **Authentication State** is enabled in **802.1X Global Settings** window.

To view this window, click **Security > 802.1X > Reauthenticate Port(s)** as shown below:

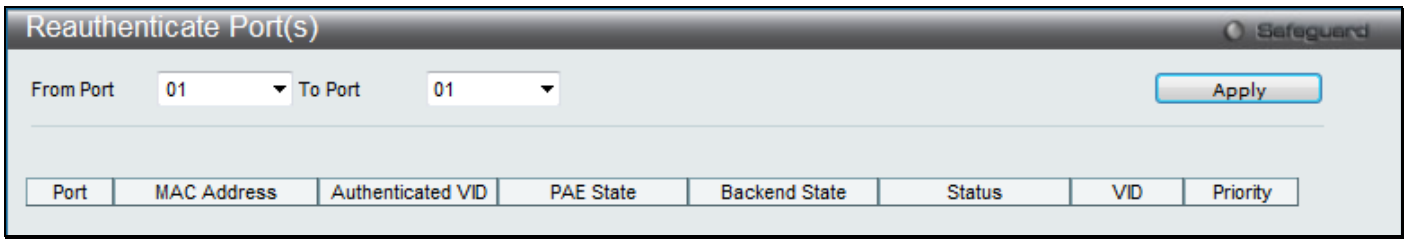


Figure 9-23 Reauthenticate Port(s) - Port-based window

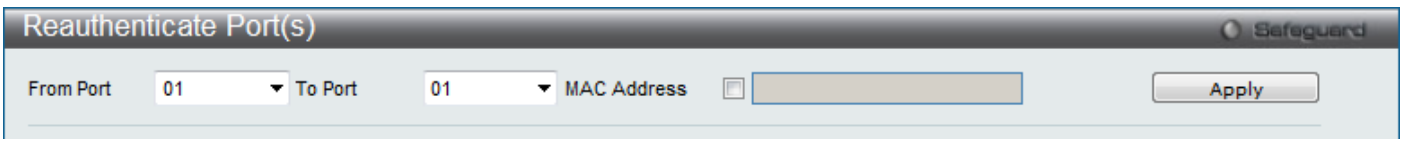


Figure 9-24 Reauthenticate Port(s) - MAC-based window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to select a range of ports to re-authenticate.
MAC Address	Select and enter the appropriate MAC address used here. This option is only available when the **Authentication Mode** has been set to **MAC-based** in the **802.1X Global Settings** window.

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

RADIUS

Authentication RADIUS Server Settings

The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

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

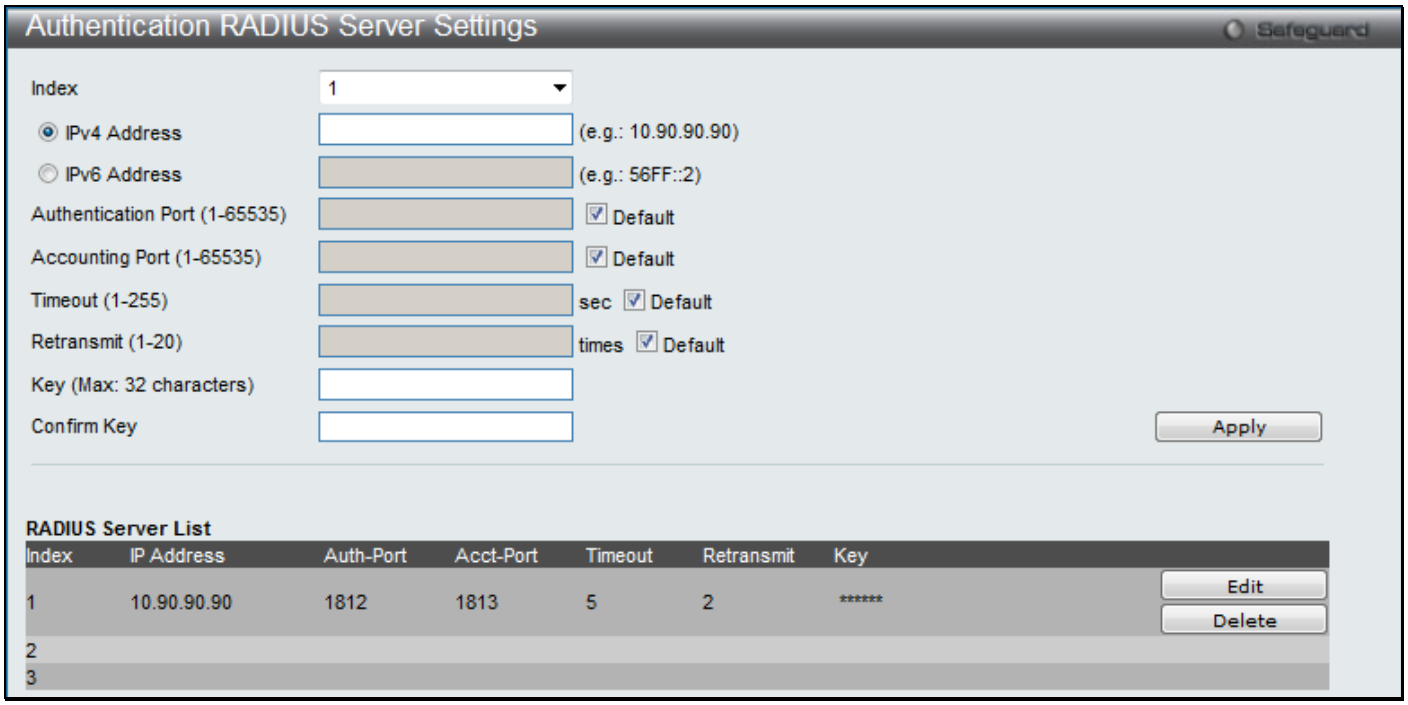


Figure 9-25 Authentication RADIUS Server Settings window

The fields that can be configured are described below:

Parameter	Description
Index	Choose the desired RADIUS server to configure: 1, 2 or 3 and select the IPv4 Address or IPv6 Address.
IPv4 Address	Set the RADIUS server IPv4 address.
IPv6 Address	Set the RADIUS server IPv6 address.
Authentication Port (1-65535)	Set the RADIUS authentication server(s) UDP port which is used to transmit RADIUS data between the Switch and the RADIUS server.
Accounting Port (1-65535)	Set the RADIUS account server(s) UDP port which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server.
Timeout (1-255)	Set the RADIUS server age-out, in seconds.
Retransmit (1-20)	Set the RADIUS server retransmit time, in times.

Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the key the same as that of the RADIUS server.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the specified entry.
Click the **Delete** button to remove the specified entry.

RADIUS Accounting Settings

Users can configure the state of the specified RADIUS accounting service.

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

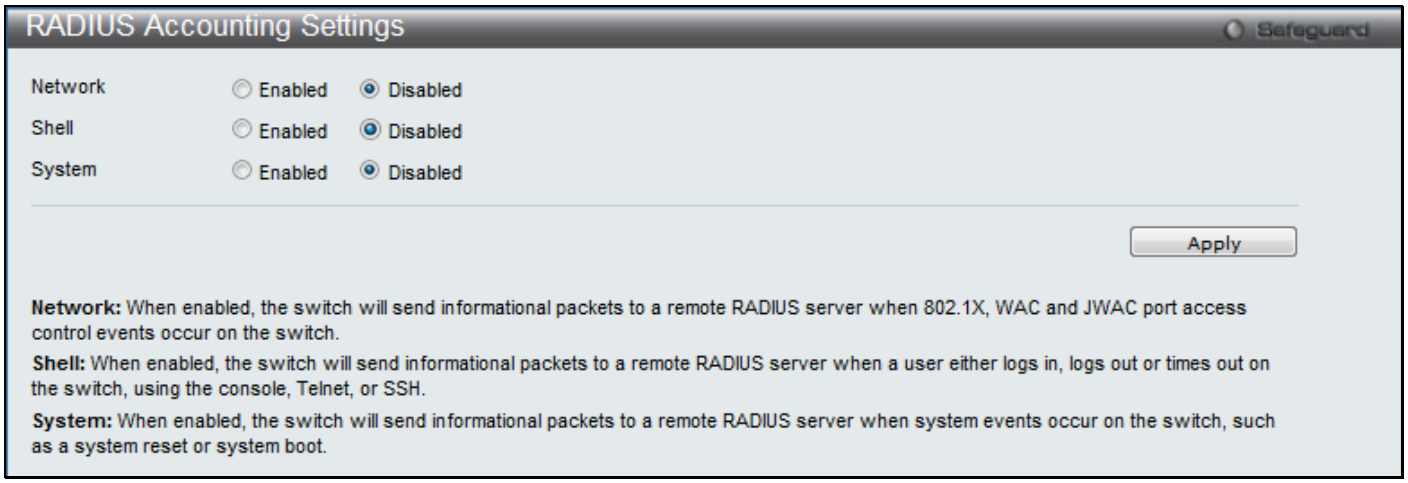


Figure 9-26 RADIUS Accounting Settings window

The fields that can be configured are described below:

Parameter	Description
Network	When enabled, the Switch will send informational packets to a remote RADIUS server when 802.1X, WAC and JWAC port access control events occur on the Switch.
Shell	When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet, or SSH.
System	When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot.

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

RADIUS Authentication

Users can display information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

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

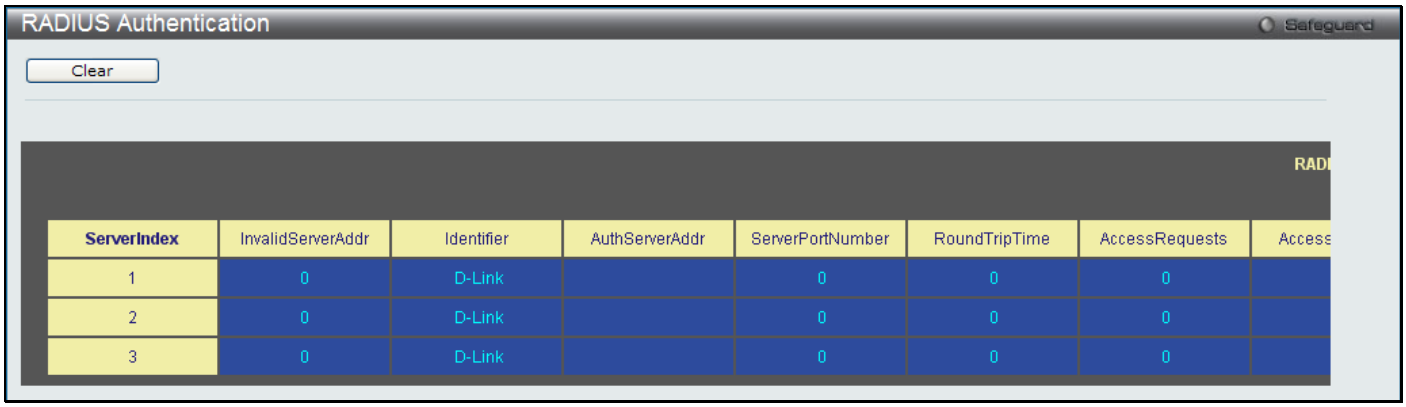


Figure 9-27 RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The fields that can be displayed are described below:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
InvalidServerAddresses	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client.
AuthServerAddress	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as

	a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Click the **Clear** button to clear the current statistics shown.

RADIUS Account Client

Users can display managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view the following window, click **Security > RADIUS > RADIUS Account Client**, as shown below:

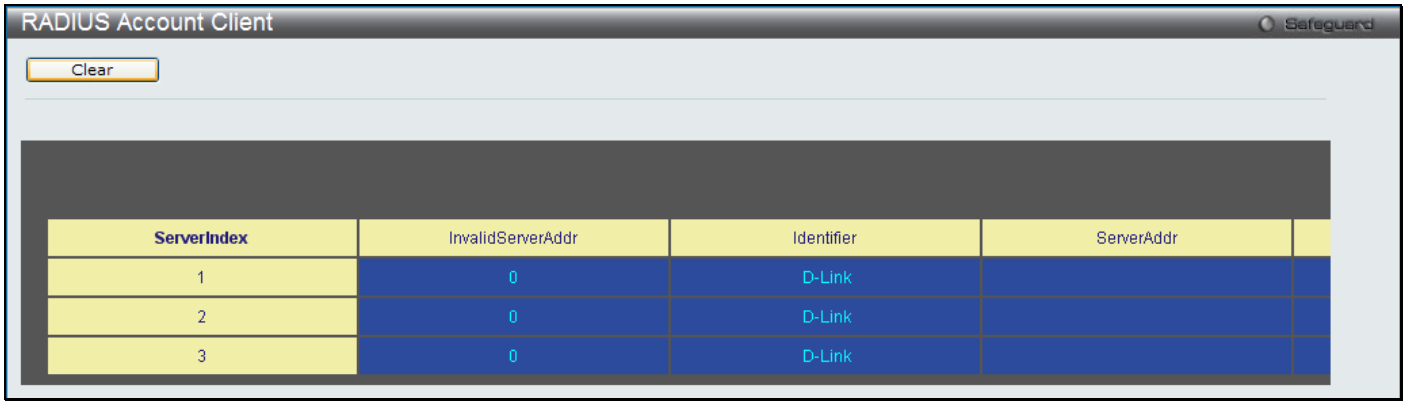


Figure 9-28 RADIUS Account Client window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

The fields that can be displayed are described below:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS accounting client.
ServerAddr	The (conceptual) table listing the RADIUS accounting servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and

	unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Click the **Clear** button to clear the current statistics shown.

IP-MAC-Port Binding (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 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. For the xStack® DES-3810-28 series of switches, active and inactive entries use the same database. The maximum number of entries is 511. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

IMPB Global Settings

Users can enable or disable the Trap/Log State and DHCP Snoop state on the Switch. The Trap/Log field will enable and disable the sending of trap/log messages for IP-MAC-port binding. When enabled, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.

To view the following window, click **Security > IP-MAC-Port Binding (IMPB) > IMPB Global Settings**, as shown below:

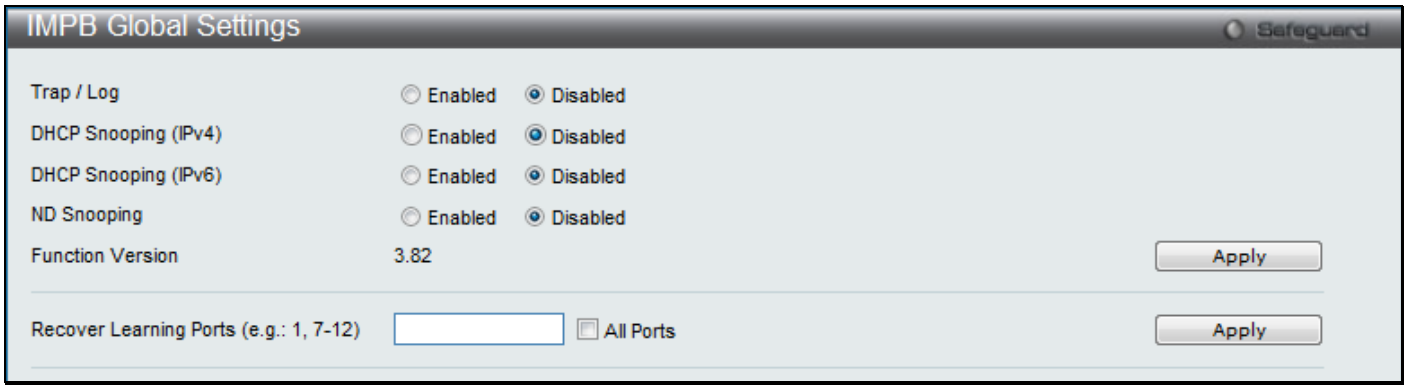


Figure 9-29 IMPB Global Settings window

The fields that can be configured are described below:

Parameter	Description
Trap / Log	Click the radio buttons to enable or disable the sending of trap/log messages for IP-MAC-port binding. When *Enabled*, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP/IP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch. The default is *Disabled*.
DHCP Snooping (IPv4)	Click the radio buttons to enable or disable DHCP snooping (IPv4) for IP-MAC-port binding. The default is *Disabled*.
DHCP Snooping (IPv6)	Click the radio buttons to enable or disable DHCP snooping (IPv6) for IP-MAC-port binding. The default is *Disabled*.
ND Snooping	Click the radio buttons to enable or disable enable ND snooping on the Switch. The default is *Disabled*.
Recover Learning Ports	Enter the port numbers used to recover the learning port state. Tick the **All** check box to apply to all ports.

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

IMPB Port Settings

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with the State, Allow Zero IP and Forward DHCP Packet field, and configure the port's Max Entry.

To view the following window, click **Security > IP-MAC-Port Binding (IMPB) > IMPB Port Settings**, as shown below:

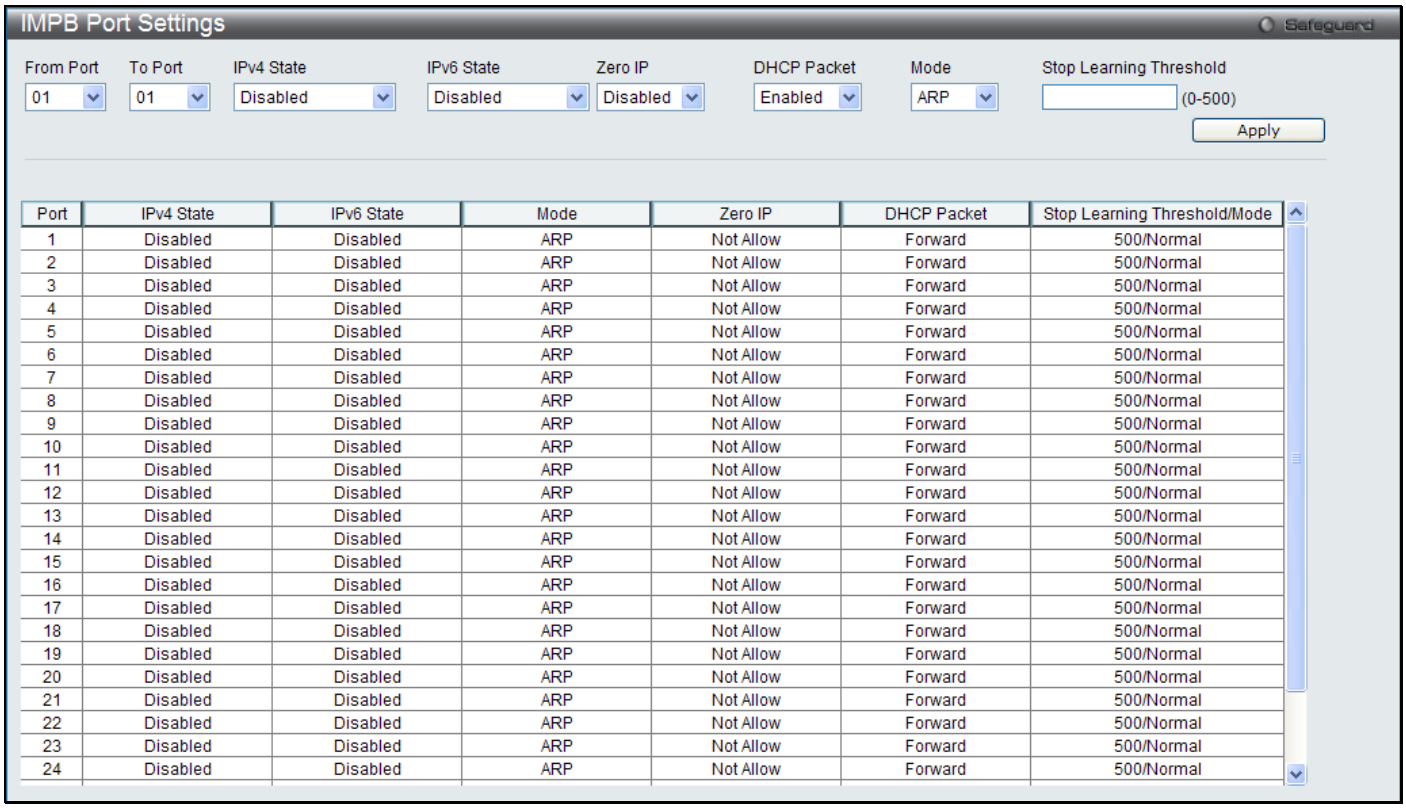


Figure 9-30 IMPB Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports for IP-MAC-port binding.
IPv4 State	Use the pull-down menu to enable or disable these ports for IPv4 binding.
IPv6 State	Use the pull-down menu to enable or disable these ports for IPv6 binding.

	Enabled (Strict) - This mode provides a stricter method of control. If the user selects this mode, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the S/W learns the entries for the ports. The port will check ARP packets and IP packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic state. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is strict if not specified. The ports with strict mode will capture unicast DHCP packets through the ACL module. If configuring IP-MAC-port binding in strict mode when IP-MAC-port binding DHCP snooping is enabled, it will create an ACL profile and the rules according to the ports. If there is not enough profile or rule space for an ACL profile or rule table, it will return a warning message and will not create an ACL profile and rules to capture unicast DHCP packets. *Enabled (Loose)* - This mode provides a looser way of control. If the user selects loose mode, ARP packets and IP broadcast packets will be sent to the CPU. The packets will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP broadcast packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic state. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.
Zero IP	Use the pull-down menu to enable or disable this feature. Allow zero IP configures the state which allows ARP packets with 0.0.0.0 source IP to bypass.
DHCP Packet	By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded in strict mode. This setting is effective when DHCP snooping is enabled, in the case when a DHCP packet which has been trapped by the CPU needs to be forwarded by the software. This setting controls the forwarding behavior in this situation.
Mode	Toggle between *ARP* and *ACL*. When configuring the port mode to ACL, the Switch will create an ACL access entry corresponding to the entries of this port. If the port changes to ARP, all the ACL access entries will be deleted automatically. The default mode is *ARP*.
Stop Learning Threshold	Here is displayed the number of blocked entries on the port. The default value is *500*.

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

IMPB Entry Settings

This table is used to create static IP-MAC-binding port entries and view all IMPB entries on the Switch.

To view the following window, click **Security > IP-MAC-Port Binding (IMPB) > IMPB Entry Settings**, as shown below:

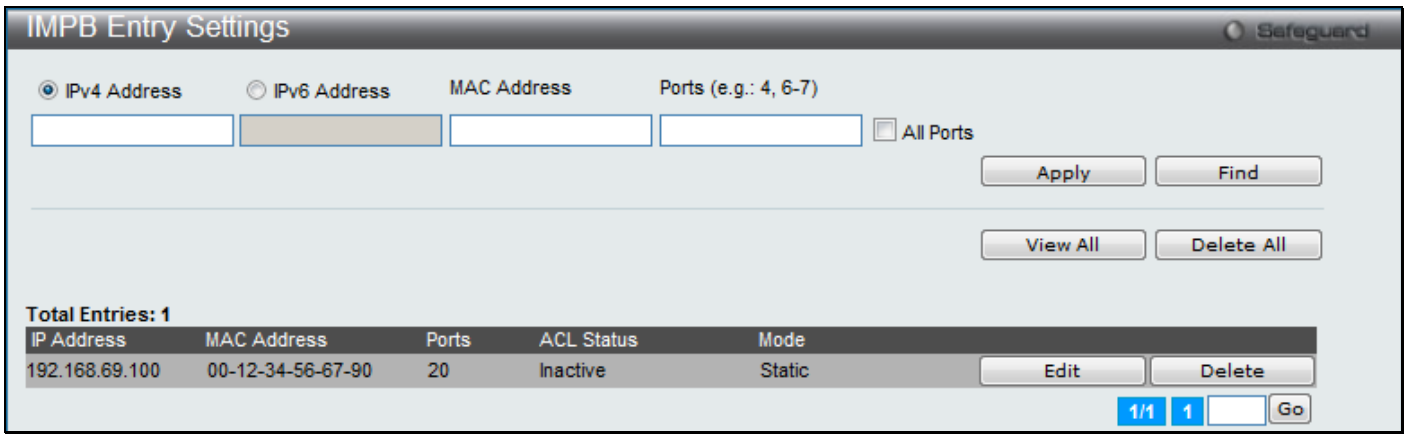


Figure 9-31 IMPB Entry Settings window

The fields that can be configured are described below:

Parameter	Description
IPv4 Address	Enter the IPv4 address to bind to the MAC address set below.
IPv6 Address	Enter the IPv6 address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Ports	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click the **All Ports** check box to configure this entry for all ports on the Switch.

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 **View All** button to display all the existing entries.
Click the **Delete All** button to remove all the entries listed.
Click the **Edit** button to re-configure the specified 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.

MAC Block List

This table is used to view unauthorized devices that have been blocked by IP-MAC binding restrictions.

To view the following window, click **Security > IP-MAC-Port Binding (IMPB) > MAC Block List**, as shown below:

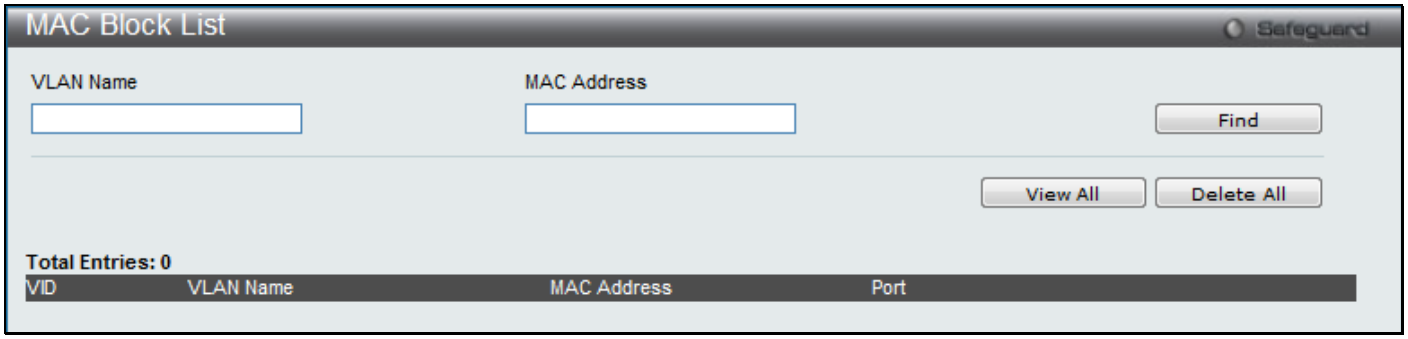


Figure 9-32 MAC Block List window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter a VLAN Name.
MAC Address	Enter a MAC address.

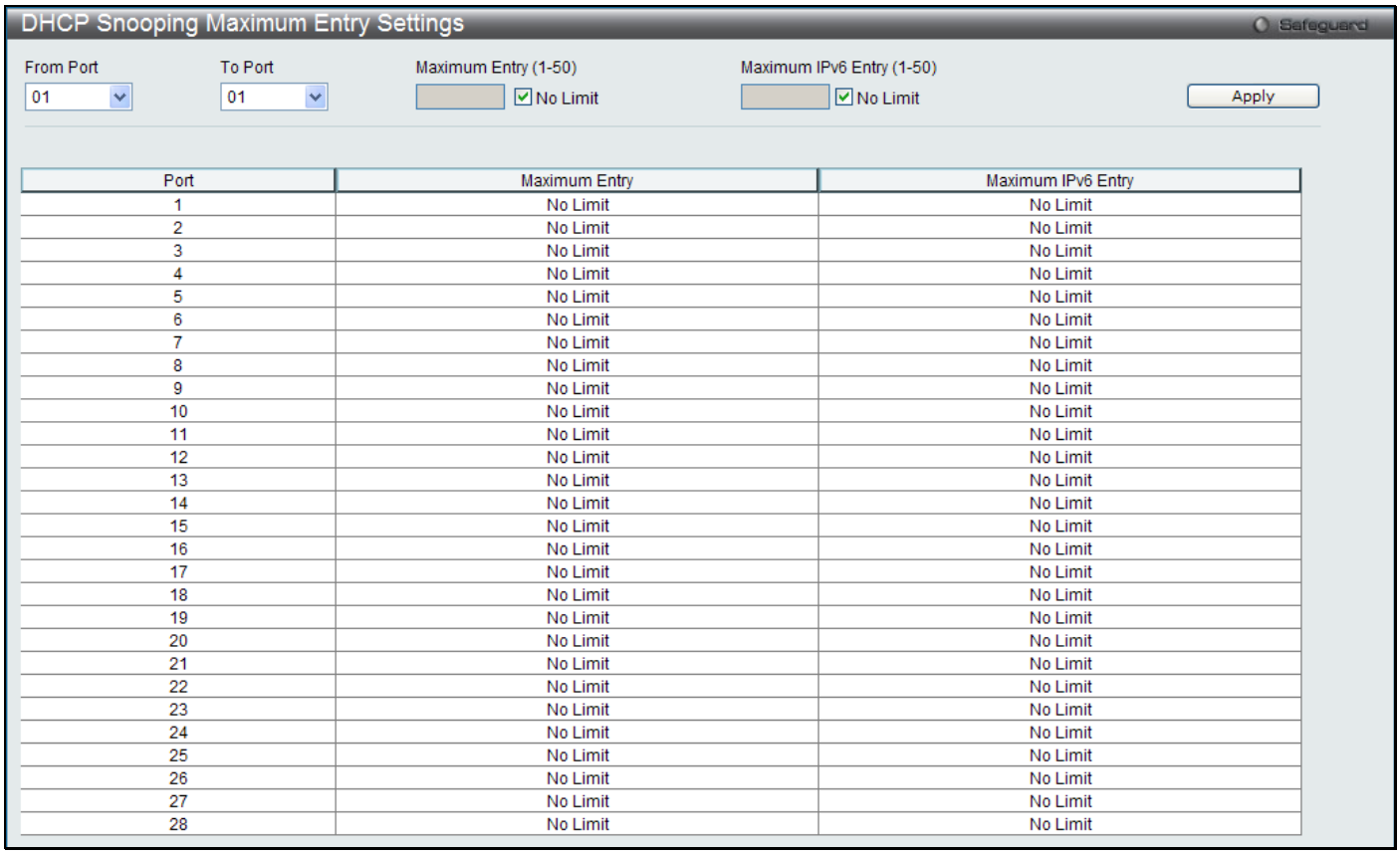
Click the **Find** button to find an unauthorized device that has been blocked by the IP-MAC binding restrictions
Click the **View All** button to display all the existing entries.
Click the **Delete All** button to remove all the entries listed.

DHCP Snooping

DHCP Snooping Maximum Entry Settings

Users can configure the maximum DHCP snooping entry for ports on this page.

To view the following window, click **Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Maximum Entry Settings**, as shown below:



Port	Maximum Entry	Maximum IPv6 Entry
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit
22	No Limit	No Limit
23	No Limit	No Limit
24	No Limit	No Limit
25	No Limit	No Limit
26	No Limit	No Limit
27	No Limit	No Limit
28	No Limit	No Limit

Figure 9-33 DHCP Snooping Max Entry Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of ports to use.
Maximum Entry (1-50)	Enter the maximum entry value. Tick the **No Limit** check box to have unlimited maximum number of the learned entries.
Maximum IPv6 Entry (1-50)	Enter the maximum entry value for IPv6 DHCP Snooping. Tick the **No Limit** check box to have unlimited maximum number of the learned entries.

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

DHCP Snooping Entry

This table is used to view dynamic entries on specific ports. To view particular port settings, enter the port number and click **Find**. To view all entries click **View All**, and to delete an entry, click **Clear**.

To view the following window, click **Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Entry**, as shown below:

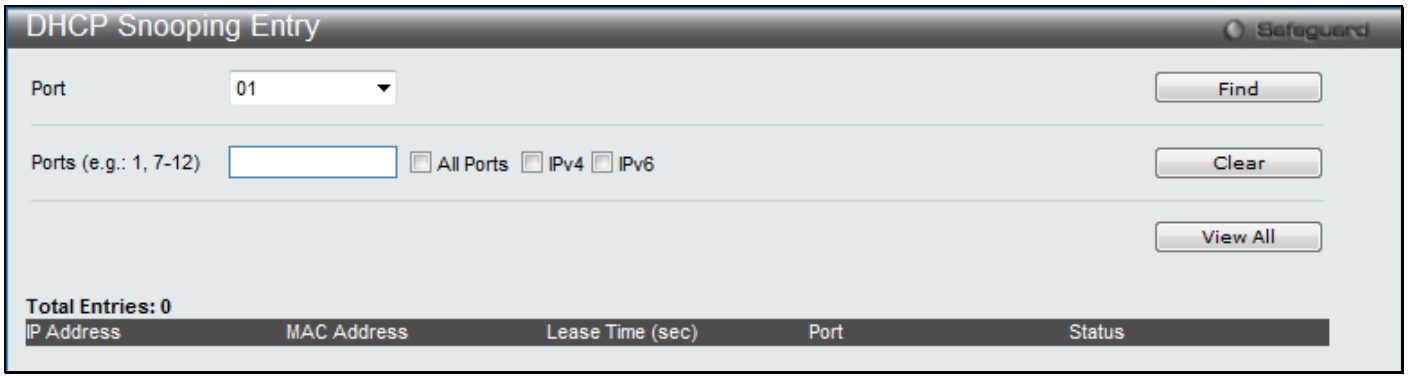


Figure 9-34 DHCP Snooping Entry window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select the desired port.
Ports	Specify the ports for DHCP snooping entries. Tick the **All Ports** check box to select all entries for all ports. Tick the **IPv4** check box to select IPv4 DHCP snooping learned entries. Tick the **IPv6** check box to select IPv6 DHCP snooping learned entries..

Click the **Find** button to locate a specific entry based on the port number selected.

Click the **Clear** button to clear all the information entered in the fields.

Click the **View All** button to display all the existing entries.

ND Snooping

ND Snooping Maximum Entry Settings

Users can configure the maximum ND Snooping entry for ports on this page.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > ND Snooping > ND Snooping Maximum Entry Settings** as shown below:

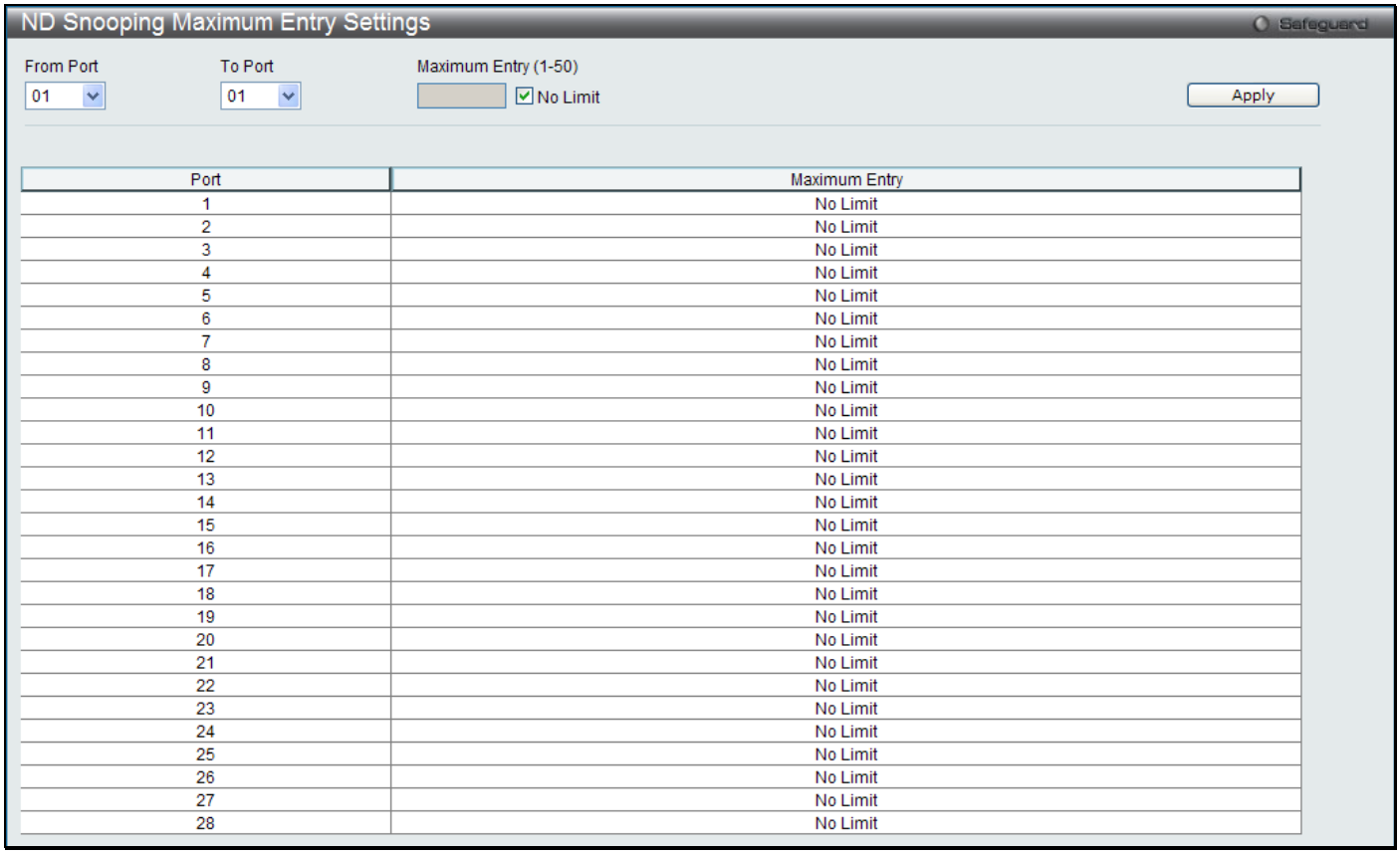


Figure 9-35 ND Snooping Maximum Entry Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to select a range of ports that require a restriction on the maximum number of entries that can be learned with ND snooping.
Maximum Entry (1-50)	Enter the maximum entry value. Tick the **No Limit** check box to have unlimited maximum number of the learned entries.

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

ND Snooping Entry

This window is used to view dynamic entries on specific ports.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > ND Snooping > ND Snooping Entry** as shown below:

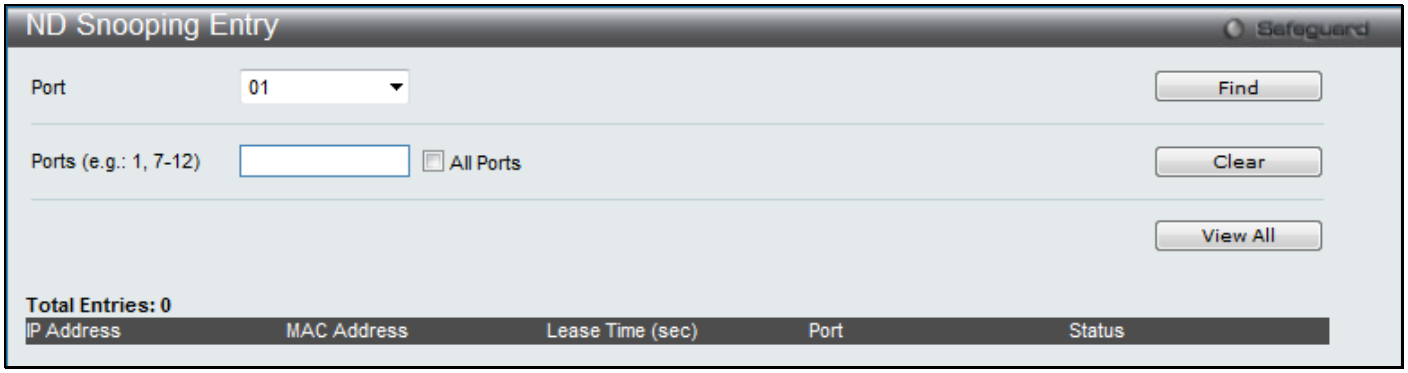


Figure 9-36 ND Snooping Entry window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select the desired port.
Ports	Specify the ports for ND snooping entries. Tick the **All Ports** check box to select all entries for all ports.

Click the **Find** button to locate a specific entry based on the port number selected.

Click the **Clear** button to clear all the information entered in the fields.

Click the **View All** button to display all the existing entries.

MAC-based Access Control (MAC)

MAC-based access control is a method to authenticate and authorize access using either a port or host. For port-based MAC, the method decides port access rights, while for host-based MAC, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In MAC-based access control, MAC user information in a local database or a RADIUS server database is searched for authentication. Following the authentication result, users achieve different levels of authorization.

Notes about MAC-based access control

There are certain limitations and regulations regarding MAC-based access control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.
2. If a port is granted clearance for a MAC address in a VLAN that is not a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the Switch.
3. Ports that have been enabled for Link Aggregation, Port Security, or GVRP authentication cannot be enabled for MAC-based Authentication.

MAC-based Access Control Settings

This window is used to set the parameters for the MAC-based access control function on the Switch. The user can set the running state, method of authentication, RADIUS password, view the Guest VLAN configuration to be associated with the MAC-based access control function of the Switch, and configure ports to be enabled or disabled for the MAC-

based access control feature of the Switch. Please remember, ports enabled for certain other features, listed previously, and cannot be enabled for MAC-based access control.

To view the following window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings**, as shown below:

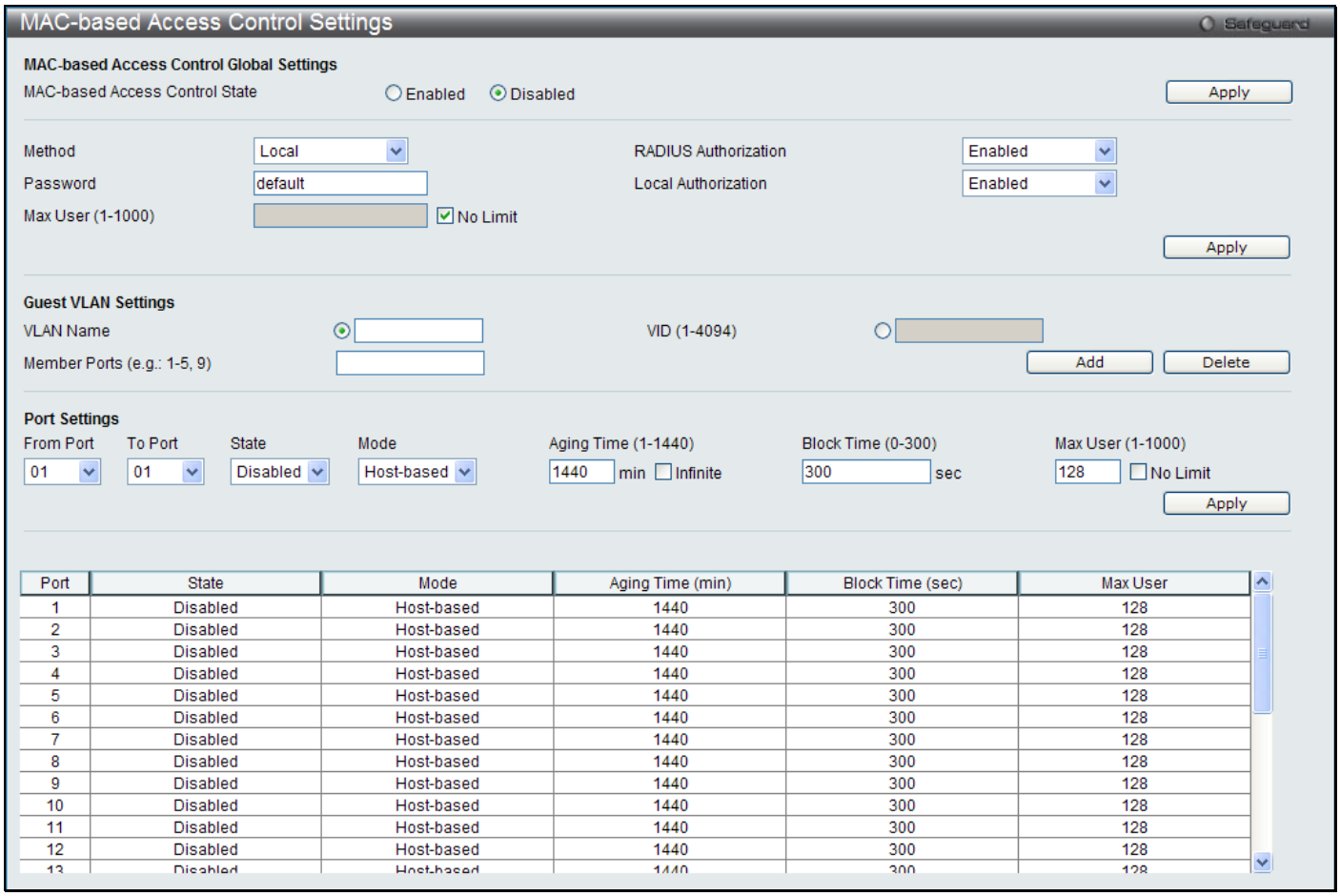


Figure 9-37 MAC-based Access Control Settings window

The fields that can be configured are described below:

Parameter	Description
MAC-based access control State	Toggle to globally enable or disable the MAC-based access control function on the Switch.
Method	Use this drop-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based access control. This MAC address list can be configured in the MAC-based access control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based access control. Remember, the MAC list must be previously set on the RADIUS server.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
RADIUS Authorization	Here the user can enable or disable the use of RADIUS Authorization.
Local Authorization	Here the user can enable or disable the use of Local Authorization.
Max User (1-1000)	Here the user can specify the maximum amount of users of the switch.
VLAN Name	Enter the name of the previously configured Guest VLAN being used for this function.

VID (1-4094)	Click the button and enter a Guest VLAN ID.
Member Ports	Enter the list of ports that have been configured for the Guest VLAN.
From Port / To Port	Select a range of ports to be configured for MAC-based access control.
State	Use this drop-down menu to enable or disable MAC-based access control on the port or range of ports selected in the Port Settings section of this window.
Mode	Toggle between *Port Based* and *Host Based*.
Aging Time (1-1440)	Enter a value between *1* and *1440* minutes. The default is *1440*.
Block Time (0-300)	Enter a value between *1* and *300* seconds. The default is *300*.
Max User (1-1000)	Here the user can enter the maximum user used for this configuration. When **No Limit** is selected, there will be no user limit applied to this rule.

Click the **Apply** button to accept the changes made for each individual section.
Click the **Delete** button to remove the specific entry based on the information entered.

MAC-based Access Control Local Settings

Users can set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this window, it will be placed in the VLAN associated with it here. The Switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

To view the following window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings**, as shown below:

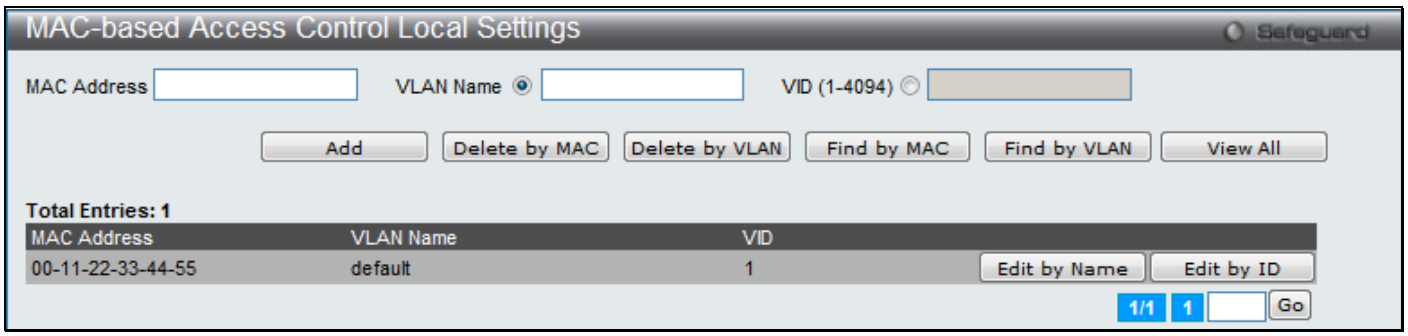


Figure 9-38 MAC-based Access Control Local Settings window

The fields that can be configured are described below:

Parameter	Description
MAC address	The user can enter the MAC address that will be added to the local authentication list here.
VLAN Name	The user can enter the VLAN name of the corresponding MAC address here.
VID (1-4094)	The user can enter the VLAN ID of the corresponding MAC address here.

Click the **Add** button to add a new entry based on the information entered.
Click the **Delete by MAC** button to remove the specific entry based on the MAC address entered.
Click the **Delete by VLAN** button to remove the specific entry based on the VLAN name or ID entered.
Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.
Click the **Find by VLAN** button to locate a specific entry based on the VLAN name or ID entered.
Click the **View All** button to display all the existing entries.

To change the selected MAC address' VLAN Name, the user can click the **Edit by Name** button.

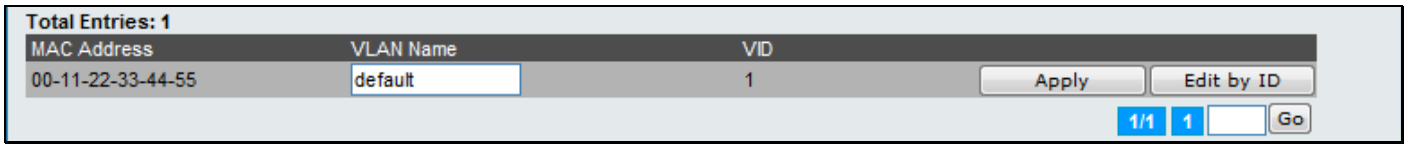


Figure 9-39 Edit by VLAN Name window

To change the selected MAC address' VID value, the user can click the **Edit by ID** button.

Figure 9-40 Edit by VID window

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.

MAC-based Access Control Authentication State

Users can display MAC-based access control Authentication State information.

To view the following window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State**, as shown below:

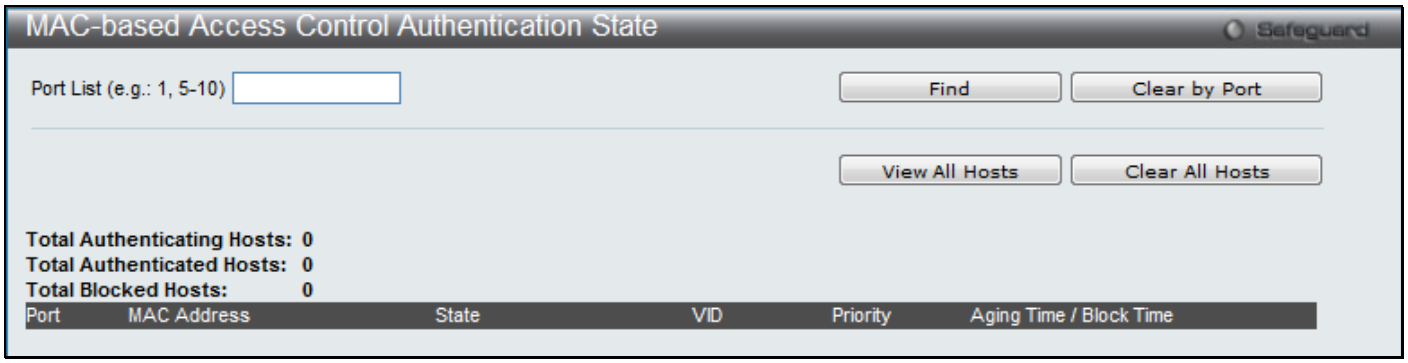


Figure 9-41 MAC-based Access Control Authentication State window

To display MAC-based access control Authentication State information, enter a port number in the space provided and then click the **Find** button.

Click the **Clear by Port** button to clear all the information linked to the port number entered.

Click the **View All Hosts** button to display all the existing hosts.

Click the **Clear All hosts** button to clear out all the existing hosts.

Web-based Access Control (WAC)

Web-based Authentication Login 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 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 packets and this port is un-authenticated, 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:

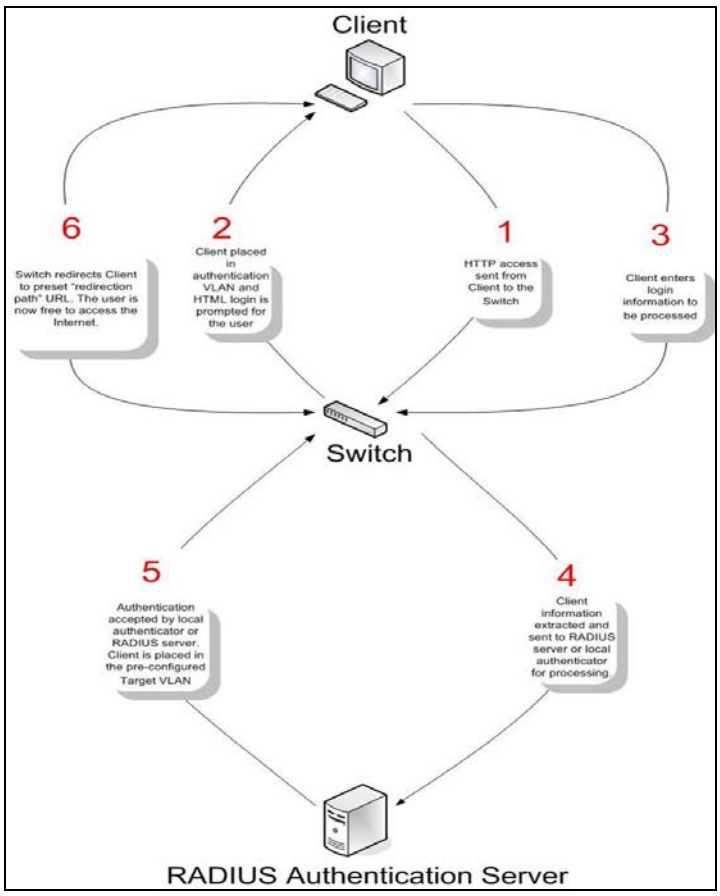


Figure 9-42 Web Authentication Process window

Conditions and Limitations

1. If the client is utilizing DHCP to attain an IP address, the authentication VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.
2. 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.

3. 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.

WAC Global Settings

Users can configure the Switch for the Web-based access control function.

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

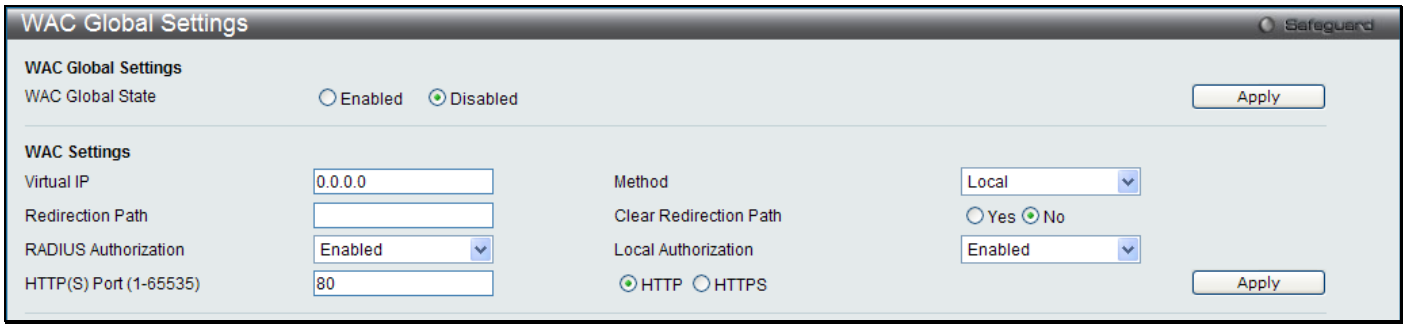


Figure 9-43 WAC Global Settings window

The fields that can be configured are described below:

Parameter	Description
WAC Global State	Use this selection menu to either enable or disable the Web Authentication on the Switch.
Virtual IP	Enter a virtual IP address. This address is only used by WAC and is not known by any other modules of the Switch.
Method	Use this drop-down menu to choose the authenticator for Web-based Access Control. The user may choose: *Local* – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch configured using the **WAC User Settings** window (**Security** > **Web-based Access Control** > **WAC User Settings**) seen below. *RADIUS* – Choose this parameter to use a remote RADIUS server as the authenticating method for users trying to access the network via the switch. This RADIUS server must have already been pre-assigned by the administrator using the **Authentication RADIUS Server Settings** window (**Security** > **RADIUS** > **Authentication RADIUS Server Settings**).
Redirection Path	Enter the URL of the website that authenticated users placed in the VLAN are directed to once authenticated.
Clear Redirection Path	The user can enable or disable this option to clear the redirection path.
RADIUS Authorization	The user can enable or disable this option to enable RADIUS Authorization or not.
Local Authorization	The user can enable or disable this option to enable Local Authorization or not.
HTTP(S) Port (1-65535)	Enter a HTTP port number. Port *80* is the default. *HTTP* – Specifies that the TCP port will run the WAC HTTP protocol. The default value is 80. HTTP port cannot run at TCP port 443. *HTTPS* – Specifies that the TCP port will run the WAC HTTPS protocol. The default value is 443. HTTPS cannot run at TCP port 80.

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

NOTE: A successful authentication should direct the client to the stated web page. If the client does not reach this web page, yet does not receive a Fail! Message, the client will already be authenticated and therefore should refresh the current browser window or attempt to open a different web page.

WAC User Settings

Users can view and set local database user accounts for Web authentication.

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

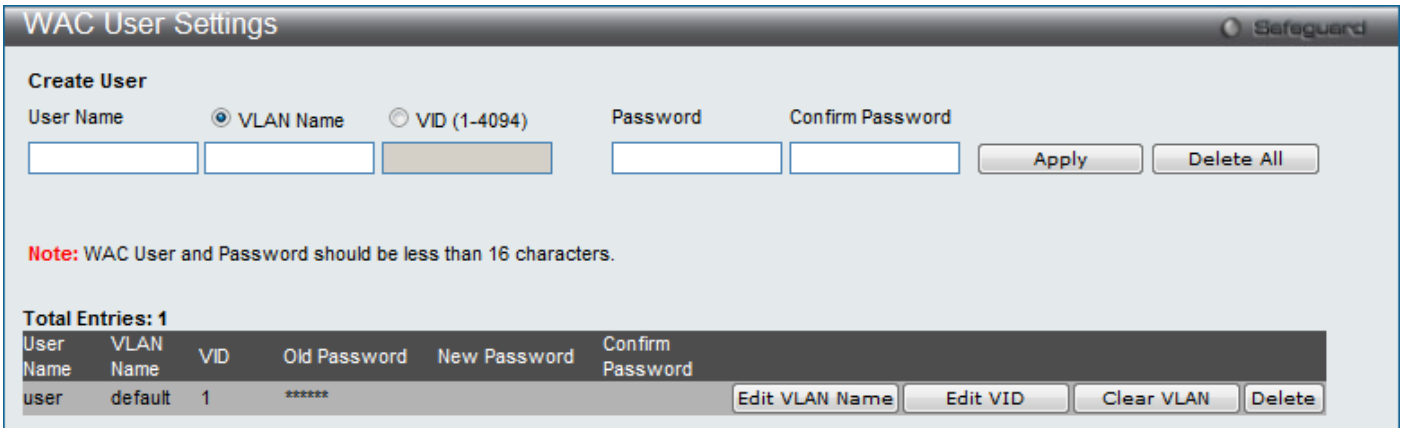


Figure 9-44 WAC User Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user name of up to 15 alphanumeric characters of the guest wishing to access the Web through this process. This field is for administrators who have selected *Local* as their Web-based authenticator.
VLAN Name	Click the button and enter a VLAN Name in this field.
VID (1-4094)	Click the button and enter a VID in this field.
Password	Enter the password the administrator has chosen for the selected user. This field is case-sensitive and must be a complete alphanumeric string. This field is for administrators who have selected *Local* as their Web-based authenticator.
Confirm Password	Retype the password entered in the previous field.

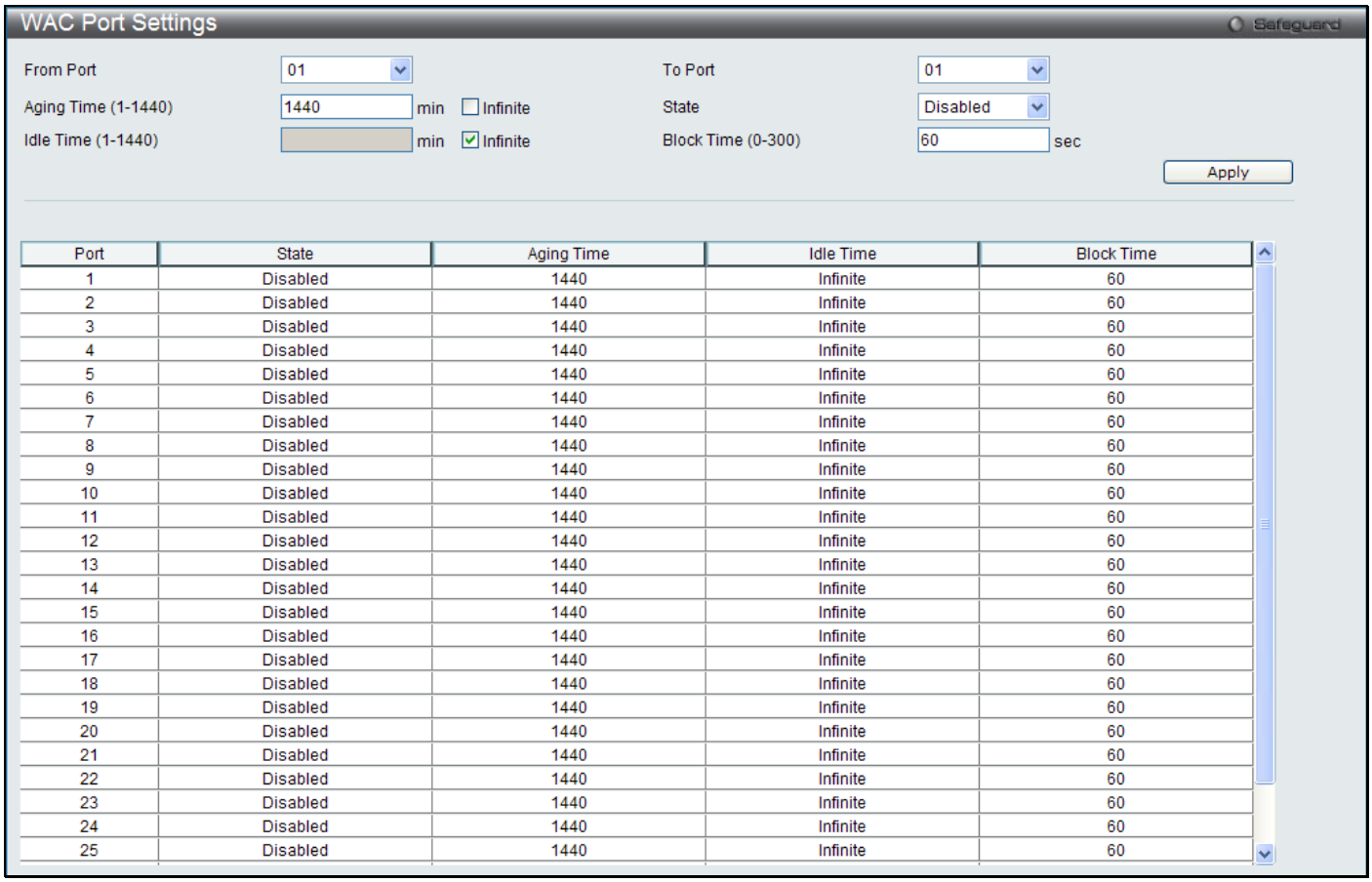
Click the **Apply** button to accept the changes made.
Click the **Delete All** button to remove all the entries listed.
Click the **Edit VLAN Name** button to re-configure the specific entry's VLAN Name.
Click the **Edit VID** button to re-configure the specific entry's VLAN ID.
Click the **Clear VLAN** button to remove the VLAN information from the specific entry.
Click the **Delete** button to remove the specific entry.

NOTE: WAC Usernames and Passwords should be less than 16 characters.

WAC Port Settings

Users can view and set port configurations for Web authentication.

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



Port	State	Aging Time	Idle Time	Block Time
1	Disabled	1440	Infinite	60
2	Disabled	1440	Infinite	60
3	Disabled	1440	Infinite	60
4	Disabled	1440	Infinite	60
5	Disabled	1440	Infinite	60
6	Disabled	1440	Infinite	60
7	Disabled	1440	Infinite	60
8	Disabled	1440	Infinite	60
9	Disabled	1440	Infinite	60
10	Disabled	1440	Infinite	60
11	Disabled	1440	Infinite	60
12	Disabled	1440	Infinite	60
13	Disabled	1440	Infinite	60
14	Disabled	1440	Infinite	60
15	Disabled	1440	Infinite	60
16	Disabled	1440	Infinite	60
17	Disabled	1440	Infinite	60
18	Disabled	1440	Infinite	60
19	Disabled	1440	Infinite	60
20	Disabled	1440	Infinite	60
21	Disabled	1440	Infinite	60
22	Disabled	1440	Infinite	60
23	Disabled	1440	Infinite	60
24	Disabled	1440	Infinite	60
25	Disabled	1440	Infinite	60

Figure 9-45 WAC Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be enabled as WAC ports.
Aging Time (1-1440)	This parameter specifies the time period during which an authenticated host will remain in the authenticated state. Enter a value between *0* and *1440* minutes. A value of *0* indicates the authenticated host will never age out on the port. The default value is *1440* minutes (24 hours).
State	Use this drop-down menu to enable the configured ports as WAC ports.
Idle Time (1-1440)	If there is no traffic during the Idle Time parameter, the host will be moved back to the unauthenticated state. Enter a value between *0* and *1440* minutes. A value of *0* indicates the Idle state of the authenticated host on the port will never be checked. The default value is *infinite*.
Block Time (0-300)	This parameter is the period of time a host will be blocked if it fails to pass authentication. Enter a value between *0* and *300* seconds. The default value is *60* seconds.

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

WAC Authentication State

Users can view and delete the hosts for Web authentication.

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

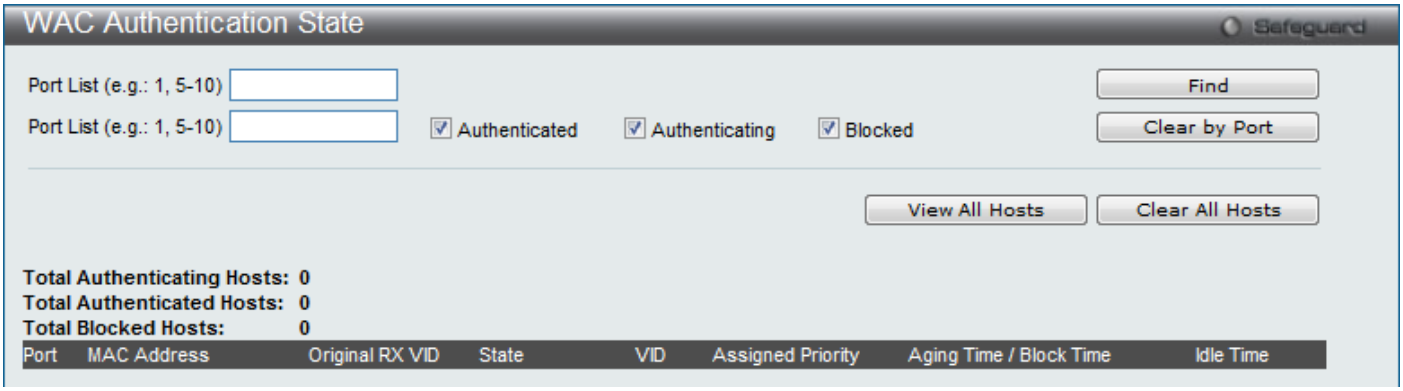


Figure 9-46 WAC Authentication State window

The fields that can be configured are described below:

Parameter	Description
Port List	Use the drop-down menus to select the desired range of ports and tick the appropriate check box(s), Authenticated, Authenticating, and Blocked.
Authenticated	Tick this check box to clear all authenticated users for a port.
Authenticating	Tick this check box to clear all authenticating users for a port.
Blocked	Tick this check box to clear all blocked users for a port.

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

Click the **Clear by Port** button to remove entry based on the port list entered.

Click the **View All Hosts** button to display all the existing entries.

Click the **Clear All Hosts** button to remove all the entries listed.

Japanese Web-based Access Control (JWAC)

JWAC Global Settings

Users can enable and configure Japanese Web-based Access Control on the Switch. JWAC and Web Authentication are mutually exclusive functions. That is, they cannot be enabled at the same time. To use the JWAC feature, computer users need to pass through two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the Switch. For the second stage, the authentication is similar to Web Authentication, except that there is no port VLAN membership change by JWAC after a host passes authentication. JWAC and WAC can share the same RADIUS server.

To view the following window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Global Settings**, as shown below:

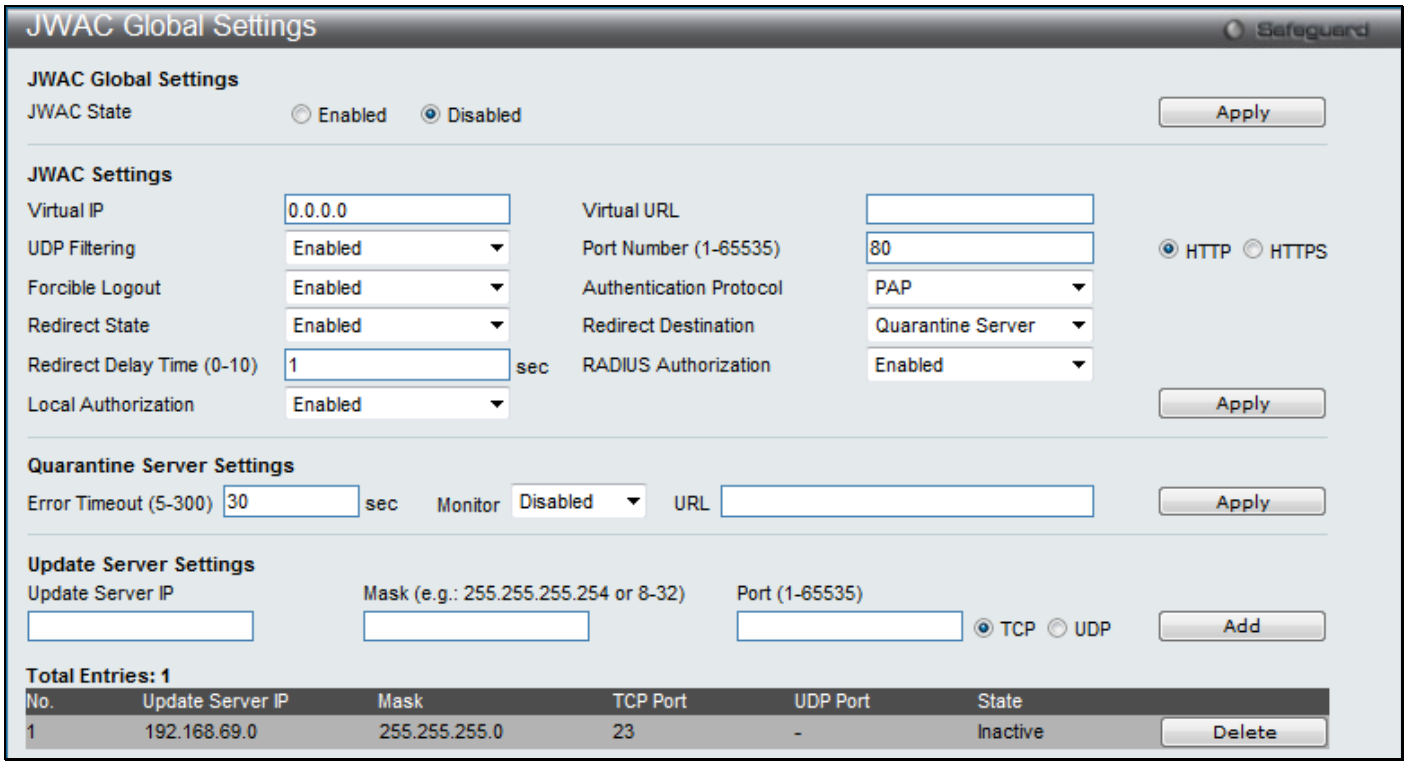


Figure 9-47 JWAC Global Settings window

The fields that can be configured are described below:

Parameter	Description
JWAC State	Use this selection menu to either enable or disable JWAC on the Switch.
Virtual IP	This parameter specifies the JWAC Virtual IP address that is used to accept authentication requests from an unauthenticated host. The Virtual IP address of JWAC is used to accept authentication requests from an unauthenticated host. Only requests sent to this IP will get a correct response. **NOTE:** This IP does not respond to ARP requests or ICMP packets.
Virtual URL	Here the user can enter the Virtual URL used.
UDP Filtering	This parameter enables or disables JWAC UDP Filtering. When UDP Filtering is *Enabled*, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped.
Port Number (1-65535)	This parameter specifies the TCP port that the JWAC Switch listens to and uses to finish the authenticating process.
Forcible Logout	This parameter enables or disables JWAC Forcible Logout. When Forcible Logout is *Enabled*, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will move back to the unauthenticated state.
Authentication Protocol	This parameter specifies the RADIUS protocol used by JWAC to complete a RADIUS authentication. The options include *Local*, *EAP MD5*, *PAP*, *CHAP*, *MS CHAP*, and *MS CHAPv2*.
Redirect State	This parameter enables or disables JWAC Redirect. When the redirect quarantine server is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When the redirect JWAC login page is enabled, the unauthenticated host will be redirected to the JWAC login page in the Switch to finish authentication. When redirect is disabled, only access to the quarantine server and the JWAC login page from the unauthenticated host are allowed, all other web access will be denied. **NOTE:** When enabling redirect to the quarantine server, a quarantine server must be configured first.
Redirect Destination	This parameter specifies the destination before an unauthenticated host is redirected to

	either the *Quarantine Server* or the *JWAC Login Page*.
Redirect Delay Time (0-10)	This parameter specifies the Delay Time before an unauthenticated host is redirected to the Quarantine Server or JWAC Login Page. Enter a value between *0* and *10* seconds. A value of *0* indicates no delay in the redirect.
RADIUS Authorization	The user can enable or disable this option to enable RADIUS Authorization or not.
Local Authorization	The user can enable or disable this option to enable Local Authorization or not.
Error Timeout (5-300)	This parameter is used to set the Quarantine Server Error Timeout. When the Quarantine Server Monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from the Quarantine Server during the configured Error Timeout, the Switch then regards it as not working properly. Enter a value between *5* and *300* seconds.
Monitor	This parameter enables or disables the JWAC Quarantine Server Monitor. When *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 access attempts to the JWAC Login Page forcibly if the Redirect is enabled and the Redirect Destination is configured to be a Quarantine Server.
URL	This parameter specifies the JWAC Quarantine Server URL. If the Redirect is enabled and the Redirect Destination is the Quarantine Server, when an unauthenticated host sends the HTTP request packets to a random Web server, the Switch will handle this HTTP packet and send back a message to the host to allow it access to the Quarantine Server with the configured URL. When a computer is connected to the specified URL, the quarantine server will request the computer user to input the user name and password to complete the authentication process.
Update Server IP	This parameter specifies the Update Server IP address.
Mask	This parameter specifies the Server IP net mask.
Port (1-65535)	Here the user can enter the port number used by the Update Server.

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

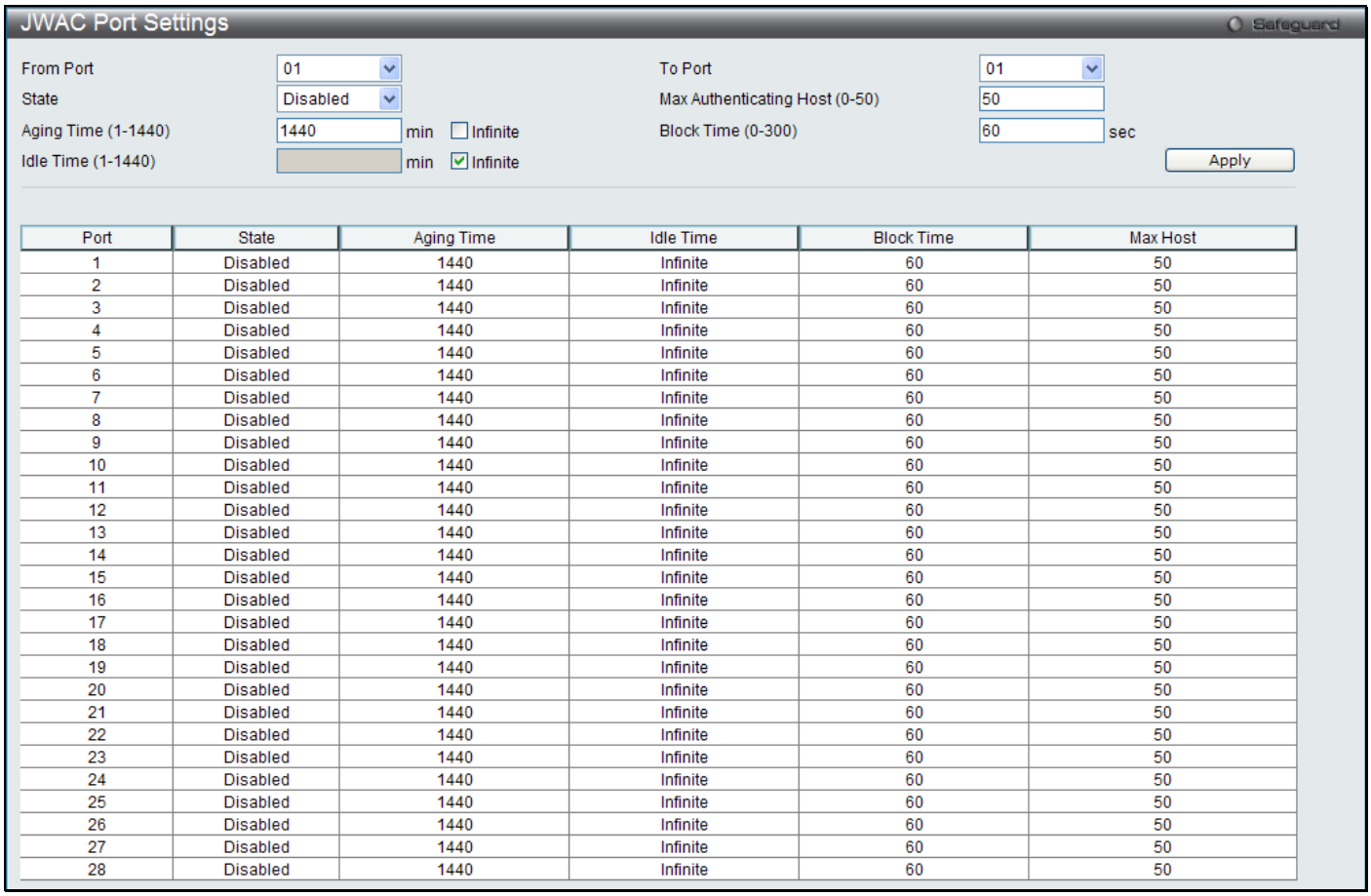
Click the **Add** button to add a new entry.

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

JWAC Port Settings

Users can configure JWAC port settings for the Switch.

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



Port	State	Aging Time	Idle Time	Block Time	Max Host
1	Disabled	1440	Infinite	60	50
2	Disabled	1440	Infinite	60	50
3	Disabled	1440	Infinite	60	50
4	Disabled	1440	Infinite	60	50
5	Disabled	1440	Infinite	60	50
6	Disabled	1440	Infinite	60	50
7	Disabled	1440	Infinite	60	50
8	Disabled	1440	Infinite	60	50
9	Disabled	1440	Infinite	60	50
10	Disabled	1440	Infinite	60	50
11	Disabled	1440	Infinite	60	50
12	Disabled	1440	Infinite	60	50
13	Disabled	1440	Infinite	60	50
14	Disabled	1440	Infinite	60	50
15	Disabled	1440	Infinite	60	50
16	Disabled	1440	Infinite	60	50
17	Disabled	1440	Infinite	60	50
18	Disabled	1440	Infinite	60	50
19	Disabled	1440	Infinite	60	50
20	Disabled	1440	Infinite	60	50
21	Disabled	1440	Infinite	60	50
22	Disabled	1440	Infinite	60	50
23	Disabled	1440	Infinite	60	50
24	Disabled	1440	Infinite	60	50
25	Disabled	1440	Infinite	60	50
26	Disabled	1440	Infinite	60	50
27	Disabled	1440	Infinite	60	50
28	Disabled	1440	Infinite	60	50

Figure 9-48 JWAC Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports to be enabled as JWAC ports.
State	Use this drop-down menu to enable the configured ports as JWAC ports.
Max Authenticating Host (0-50)	This parameter specifies the maximum number of host process authentication attempts allowed on each port at the same time. The default value is *50*. Enter a value between 0 and 50 attempts.
Aging Time (1-1440)	Specify the time period during which an authenticated host will remain in the authenticated state. Enter a value between *1*and *1440* minutes. Tick the **Infinite** check box to indicate the authenticated host will never age out on the port. The default value is *1440* minutes (24 hours).
Block Time (0-300)	This parameter is the period of time a host will be blocked if it fails to pass authentication. Enter a value between *0* and *300* seconds. The default value is *60.*
Idle Time (1-1440)	If there is no traffic during the Idle Time parameter, the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. Tick the **Infinite** check box to indicate the Idle state of the authenticated host on the port will never be checked. The default value is *infinite*.

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

JWAC User Settings

On this page the user can configure a JWAC user of the switch's local database.

To view the following window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC User Settings**, as shown below:

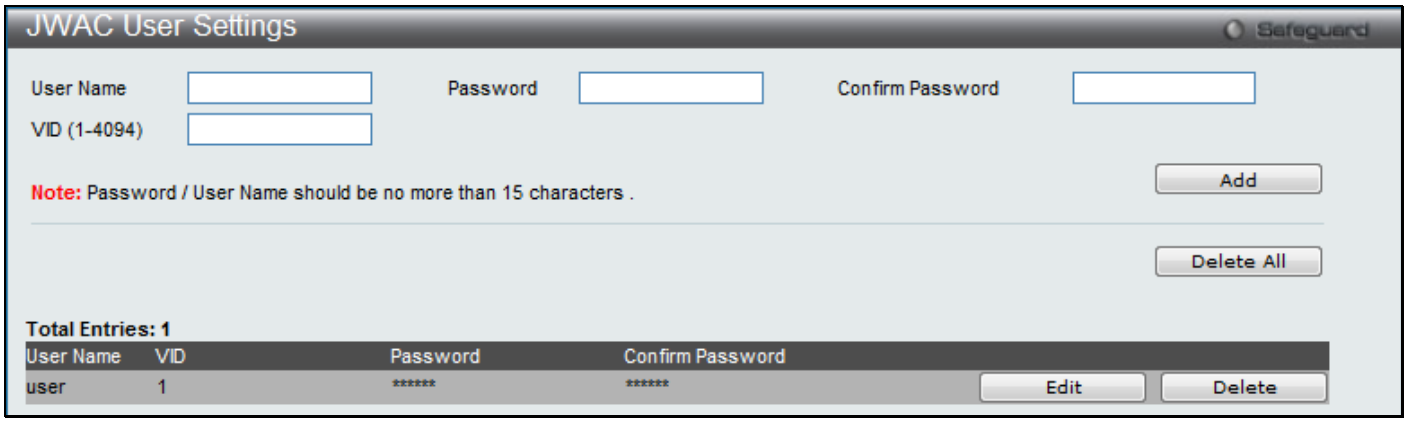


Figure 9-49 JWAC User Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter a username of up to 15 alphanumeric characters.
Password	Enter the password the administrator has chosen for the selected user. This field is case-sensitive and must be a complete alphanumeric string.
Confirm Password	Retype the password entered in the previous field.
VID (1-4094)	Enter a VLAN ID number between *1* and *4094*.

Click the **Add** button to add a new entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

NOTE: The **Username** and **Password** values should be less than 16 characters.

JWAC Authentication State

Users can display Japanese Web-based Access Control Host Table information.

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

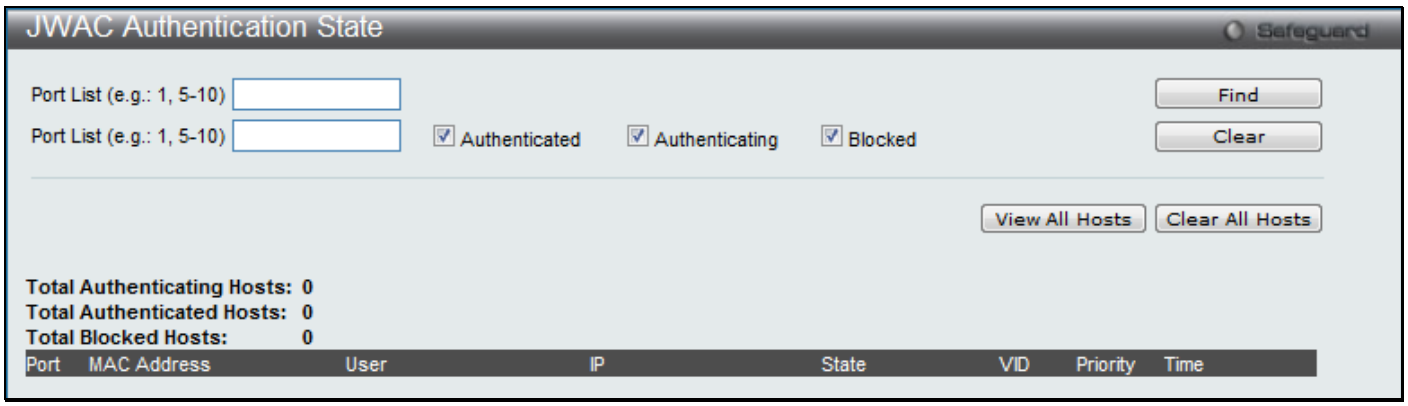


Figure 9-50 JWAC Authentication State window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter a port or range of ports.
Authenticated	Tick this check box to only clear authenticated client hosts.
Authenticating	Tick this check box to only clear client hosts in the authenticating process.
Blocked	Tick this check box to only clear client hosts being temporarily blocked because of the failure of authentication.

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

Click the **Clear** button to remove entry based on the port list entered.

Click the **View All Hosts** button to display all the existing entries.

Click the **Clear All Hosts** button to remove all the entries listed.

JWAC Customize Page Language

Users can configure JWAC page and language settings for the Switch. The current firmware supports either English or Japanese.

To view the following window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language**, as shown below:

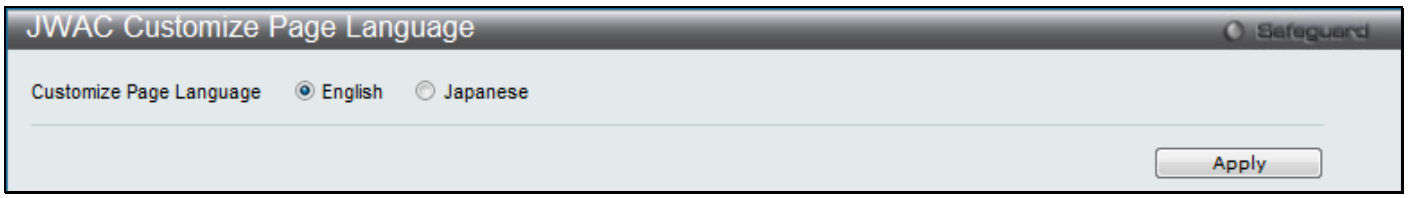


Figure 9-51 JWAC Customize Page Language window

To set the language used on the JWAC page, click the radio button for either English or Japanese.

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

JWAC Customize Page

Users can configure JWAC page settings for the Switch.

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

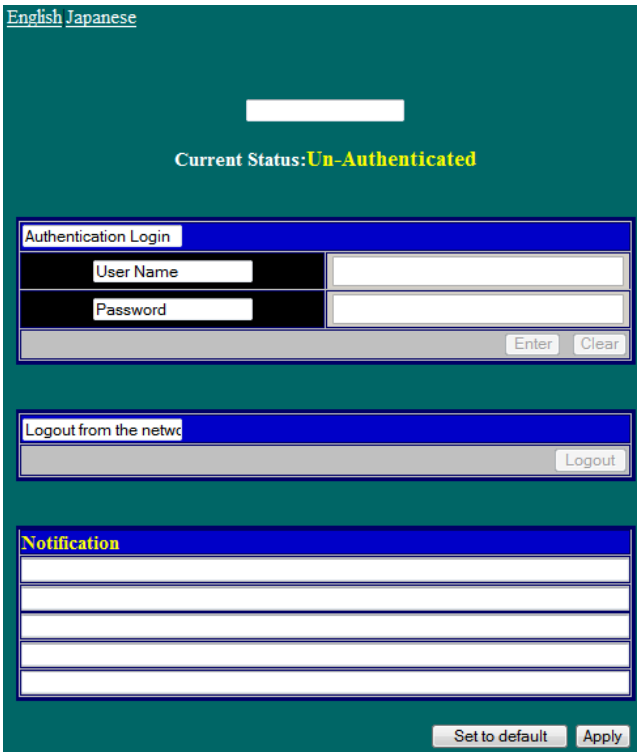


Figure 9-52 JWAC Login window

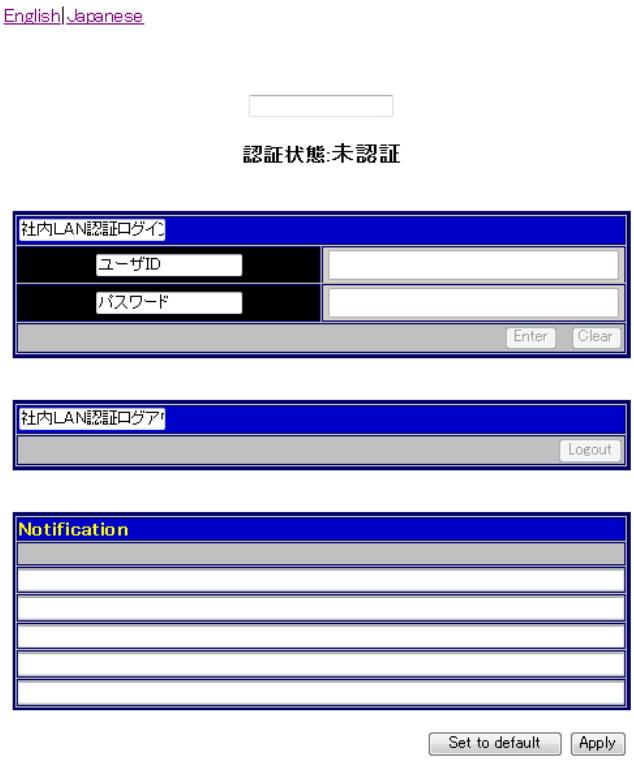


Figure 9-53 JWAC Login window

Complete the JWAC authentication information on this window to set the JWAC page settings. Enter a name for the Authentication in the first field and then click the **Apply** button. Next, enter a User Name and a Password and then click the **Enter** button.

Compound Authentication

Compound Authentication

Modern networks employ many authentication methods. The Compound Authentication methods supported by this Switch include 802.1X, MAC-based access control (MAC), Web-based Access Control (WAC), Japan Web-based Access Control (JWAC), and IP-MAC-Port Binding (IMPB). The Compound Authentication feature allows clients running different authentication methods to connect to the network using the same switch port.

The Compound Authentication feature can be implemented using one of the following modes:

Any (MAC, 802.1X or WAC) Mode

In the diagram below the Switch port has been configured to allow clients to authenticate using 802.1X, MAC, or WAC. When a client tries to connect to the network, the Switch will try to authenticate the client using one of these methods and if the client passes they will be granted access to the network.

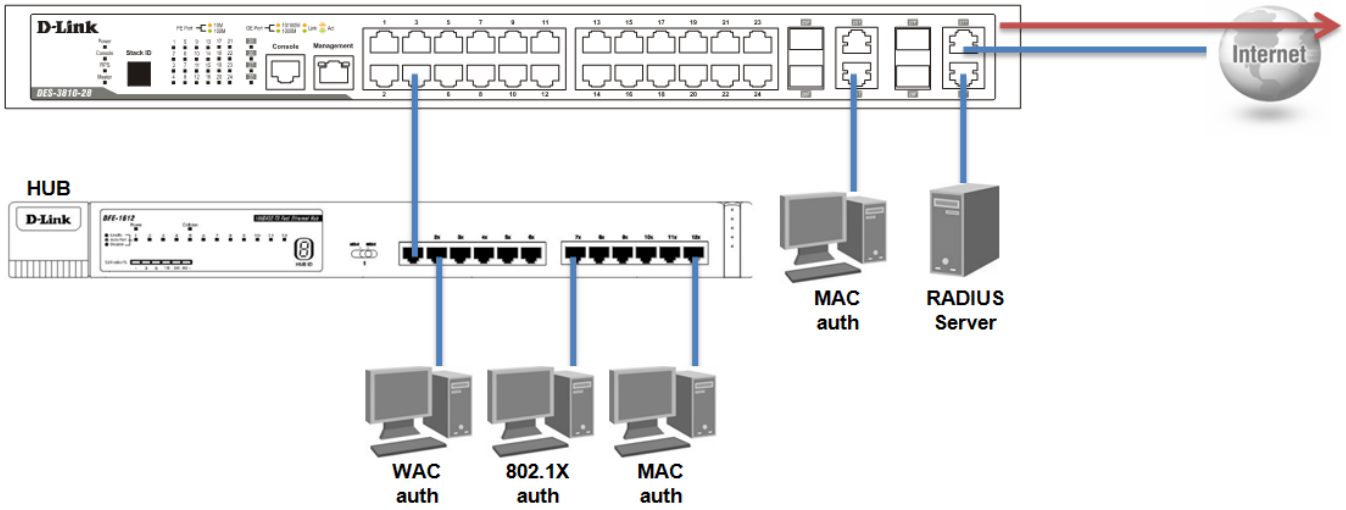


Figure 9-54 Any (MAC, 802.1X or WAC) Mode window

Any (MAC, 802.1X or JWAC) Mode

In the diagram below the Switch port has been configured to allow clients to authenticate using 802.1X, MAC, or JWAC. When a client tries to connect to the network, the Switch will try to authenticate the client using one of these methods and if the client passes they will be granted access to the network.

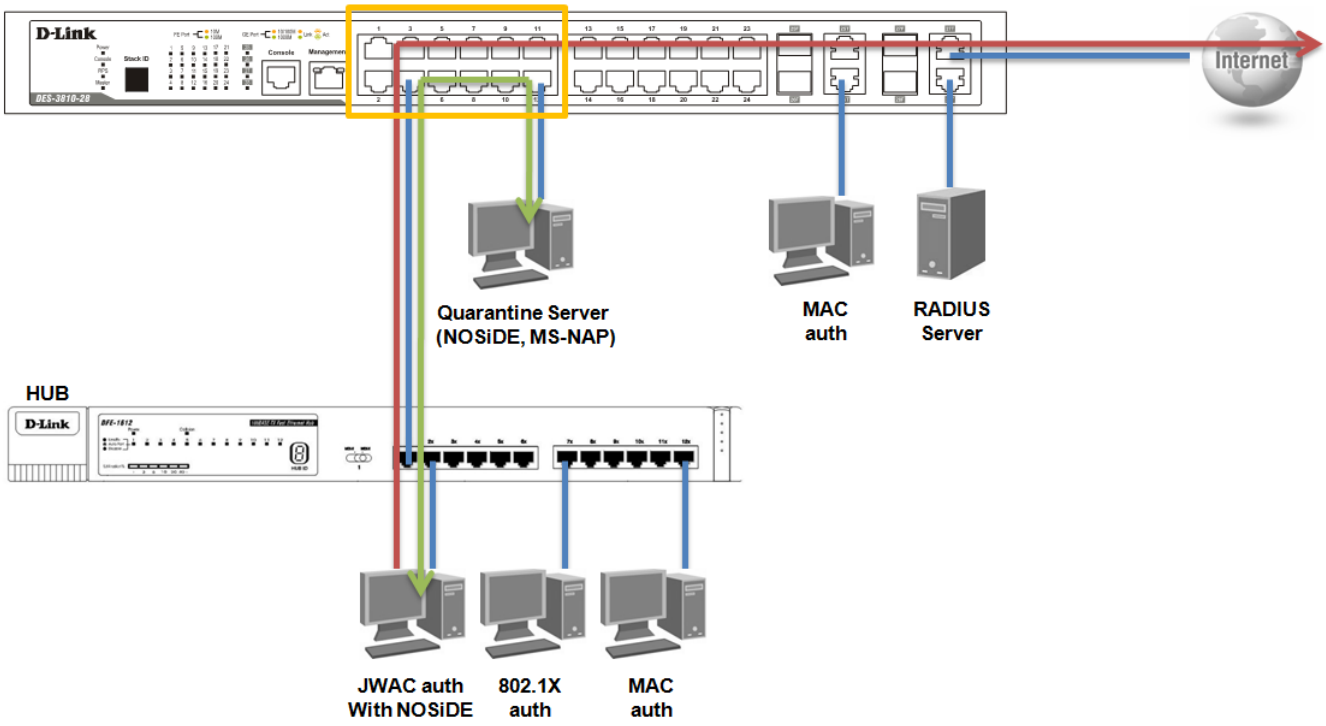


Figure 9-55 Any (MAC, 802.1X or JWAC) Mode window

802.1X & IMPB Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table after trying one of the supported authentication methods. The IMPB Table is used to create a 'white list' that checks if the IP streams being sent by authorized hosts have been granted or not. In the above diagram the Switch port has been configured to allow clients to authenticate using 802.1X. If the client is in the IMPB table and tries to connect to the network using this authentication method and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

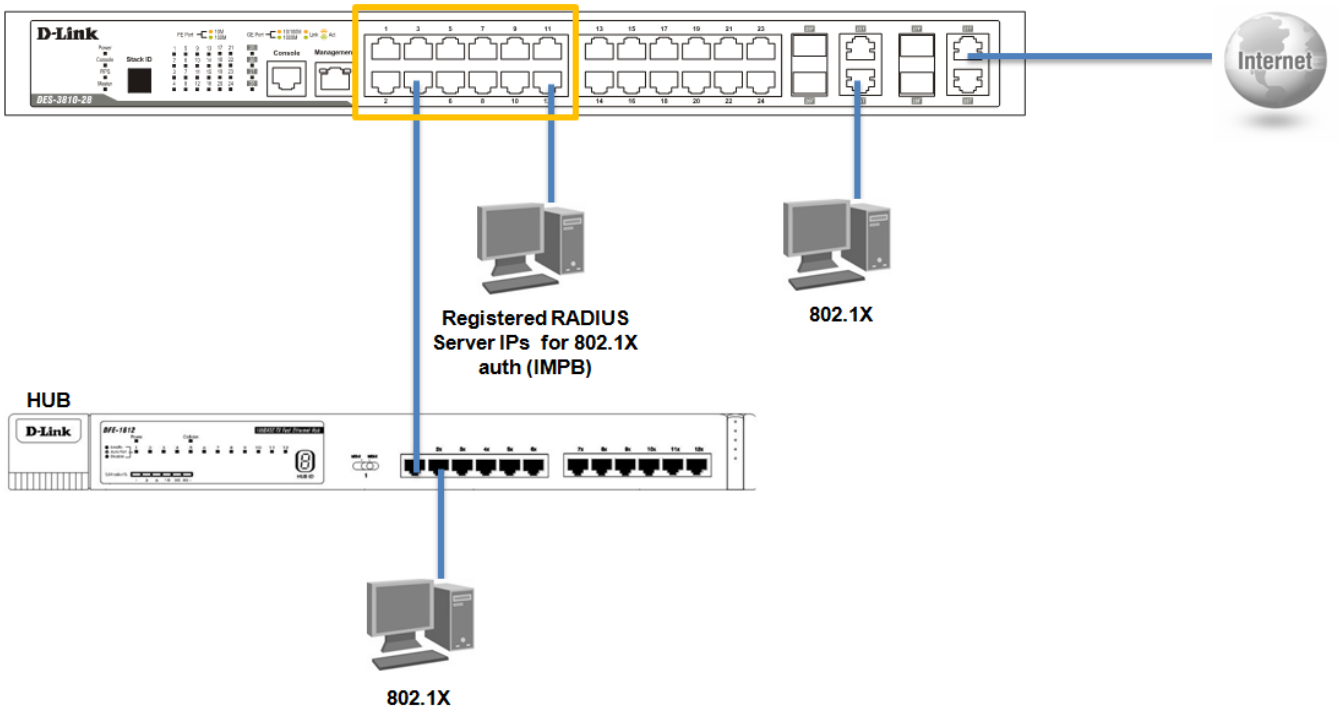


Figure 9-56 802.1X & IMPB Mode window

IMPB & WAC/JWAC Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table after trying one of the supported authentication methods. The IMPB Table is used to create a 'white-list' that checks if the IP streams being sent by authorized hosts have been granted or not. In the above diagram, the Switch port has been configured to allow clients to authenticate using either WAC or JWAC. If the client is in the IMPB table and tries to connect to the network using either of these supported authentication methods and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

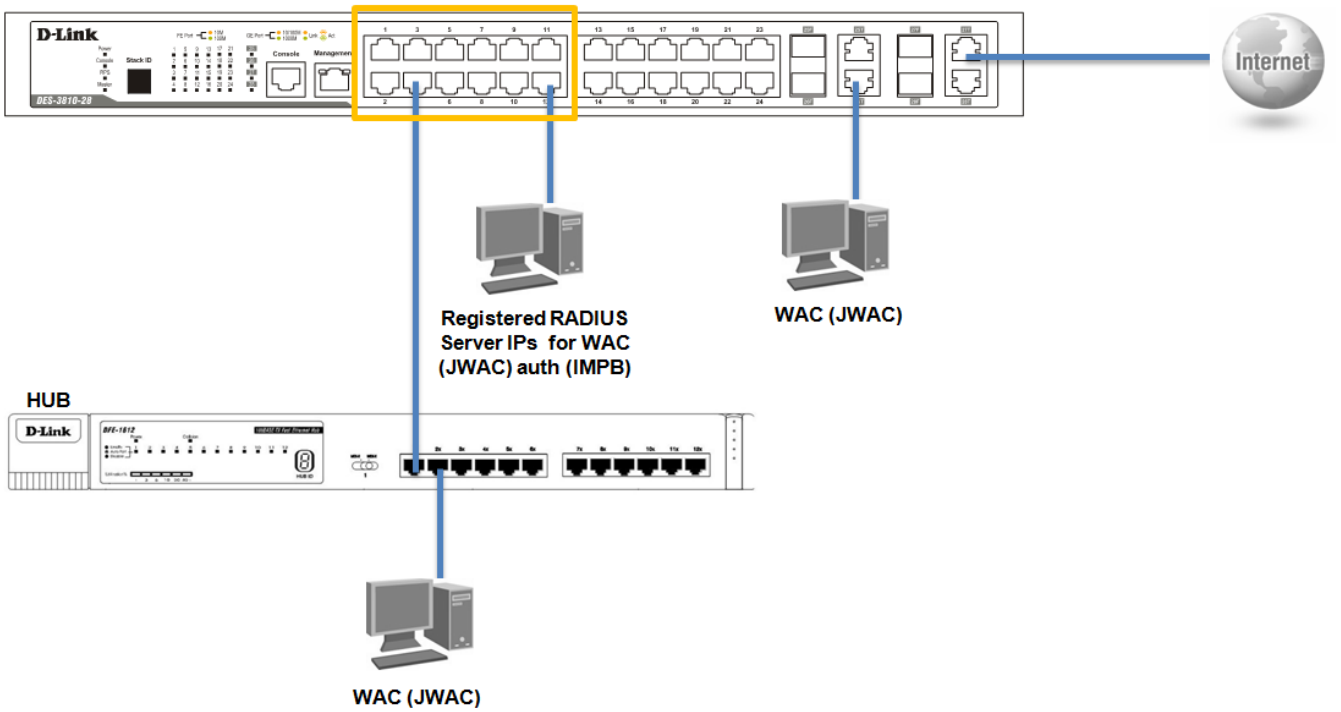


Figure 9-57 IMPB & WAC/JWAC Mode window

MAC & IMPB Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table after trying one of the supported authentication methods. The IMPB Table is used to create a 'white list' that checks if the IP streams

being sent by authorized hosts have been granted or not. In the above diagram the Switch port has been configured to allow clients to authenticate using MAC. If the client is in the IMPB table and tries to connect to the network using this authentication method and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

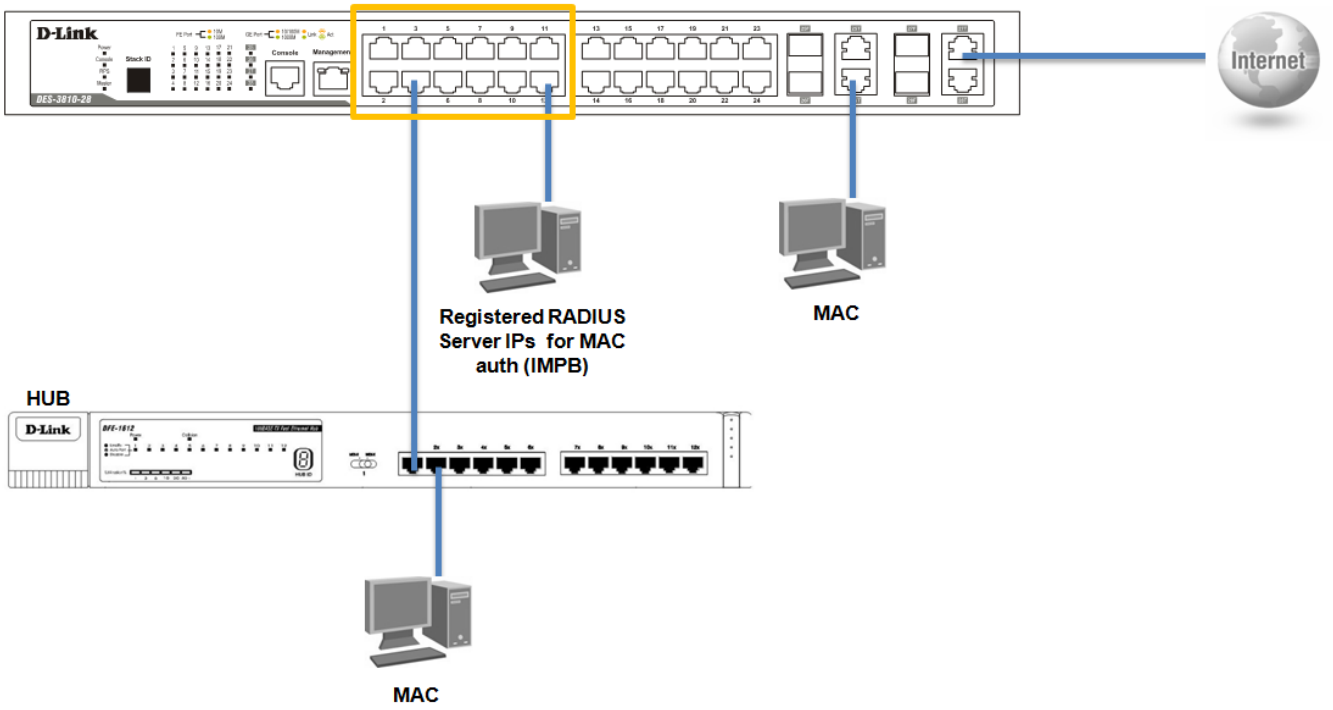


Figure 9-58 MAC & IMPB Mode window

The **Compound Authentication** folder contains two windows: **Compound Authentication Settings**, **Compound Authentication Guest VLAN Settings**.

Compound Authentication Settings

Users can configure Authorization Network State Settings and compound authentication methods for a port or ports on the Switch.

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

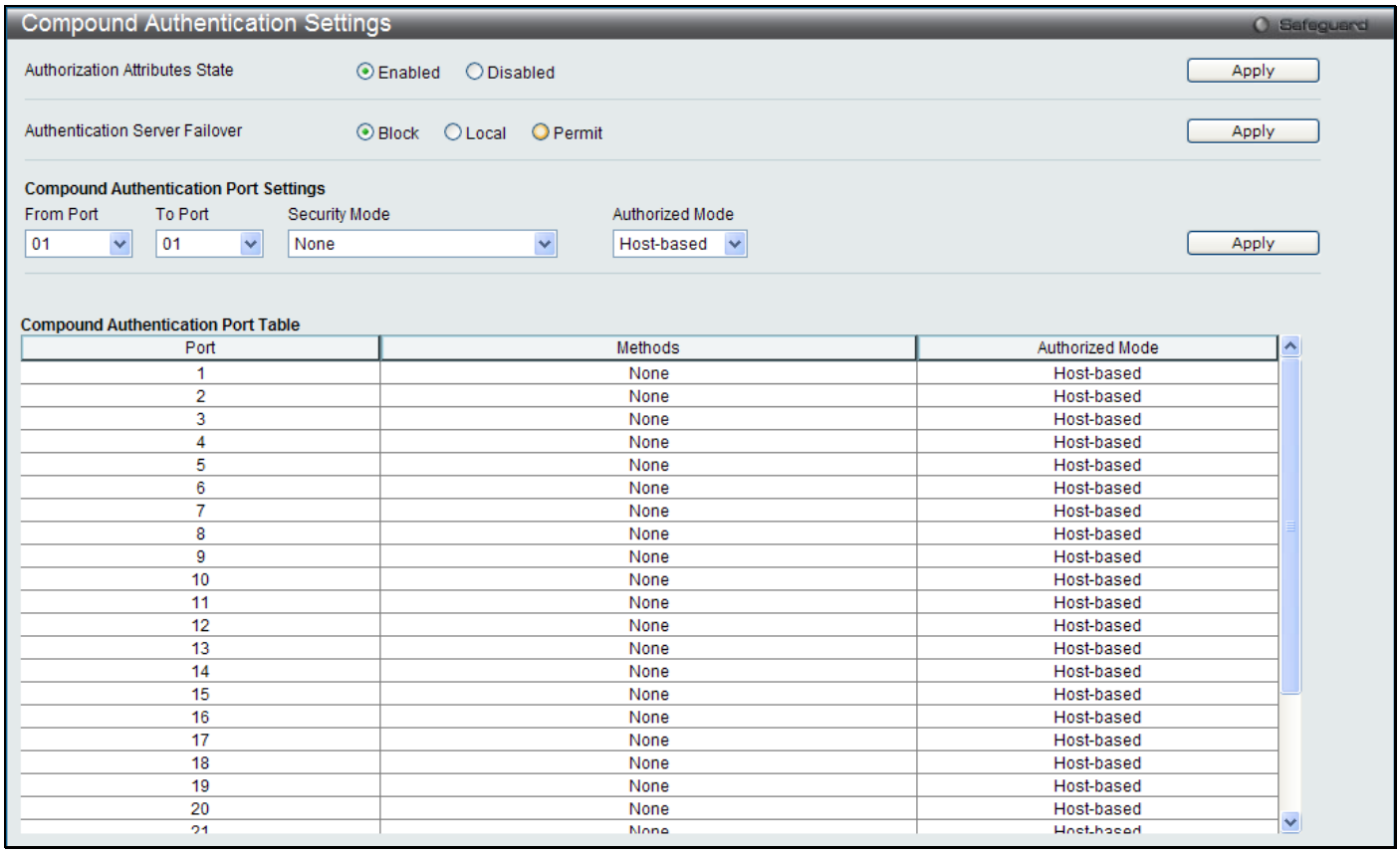


Figure 9-59 Compound Authentication Settings window

The fields that can be configured are described below:

Parameter	Description
Authorization Attributes State	Here the user can enable of disable the Authorization Network State.
Authentication Server Failover	Here the user can configure the authentication server failover function. **Local**. The switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated, otherwise, it authenticated. **Permit**. The client is always regarded as authenticated. If guest VLAN is enabled, clients will stay on the guest VLAN, otherwise, they will stay on the original VLAN. **Block** (default setting). The client is always regarded as un-authenticated.
From Port / To Port	Select a range of ports to be enabled as compound authentication ports.
Security Mode	The compound authentication method options include: None, Any (MAC, 802.1X or WAC/JWAC), 802.1X+IMPB, IMPB+JWAC, IMPB+WAC, and MAC+IMPB. None means all compound authentication methods are disabled. *Any (MAC, 802., WAC or JWAC)* - If any of the authentication methods pass, then access will be granted. In this mode, MAC, 802.1X and WAC/JWAC) can be enabled on a port at the same time. In Any (MAC, 802.1X or WAC/JWAC mode, whether an individual security module is active on a port depends on its system state. As system states of WAC and JWAC are mutually exclusive, only one of them will active on a port at the same time. *802.1X+IMPB* - 802.1X will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. *IMPB+JWAC* - JWAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. *IMPB+WAC* - WAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. *MAC+IMPB* - MAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed.

Authorized Mode	Toggle between *Host Based* and *Port Based*. When *Port Based* is selected, if one of the attached hosts passes the authentication, all hosts on the same port will be granted access to the network. If the user fails the authorization, this port will keep trying the next authentication method. When *Host Based* is selected, users are authenticated individually.

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

Compound Authentication Guest VLAN Settings

Users can assign ports to or remove ports from a guest VLAN.

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

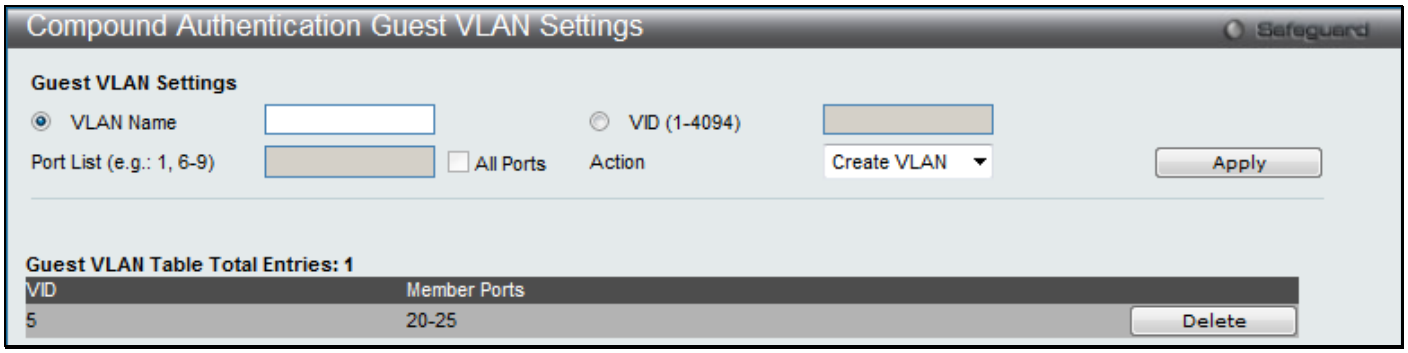


Figure 9-60 Compound Authentication Guest VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the button and assign a VLAN as a Guest VLAN. The VLAN must be an existing static VLAN.
VID (1-4094)	Click the button and assign a VLAN ID for a Guest VLAN. The VLAN must be an existing static VLAN before this VID can be configured.
Port List	The list of ports to be configured. Alternatively, tick the All check box to set every port at once.
Action	Use the drop-down menu to choose the desired operation: *Create VLAN*, *Add Ports*, or *Delete Ports*.

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

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

Port Security

Port Security Settings

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port lock is enabled. The port can be locked by changing the Admin State pull-down menu to *Enabled* and clicking **Apply**.

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 Settings**, as shown below:

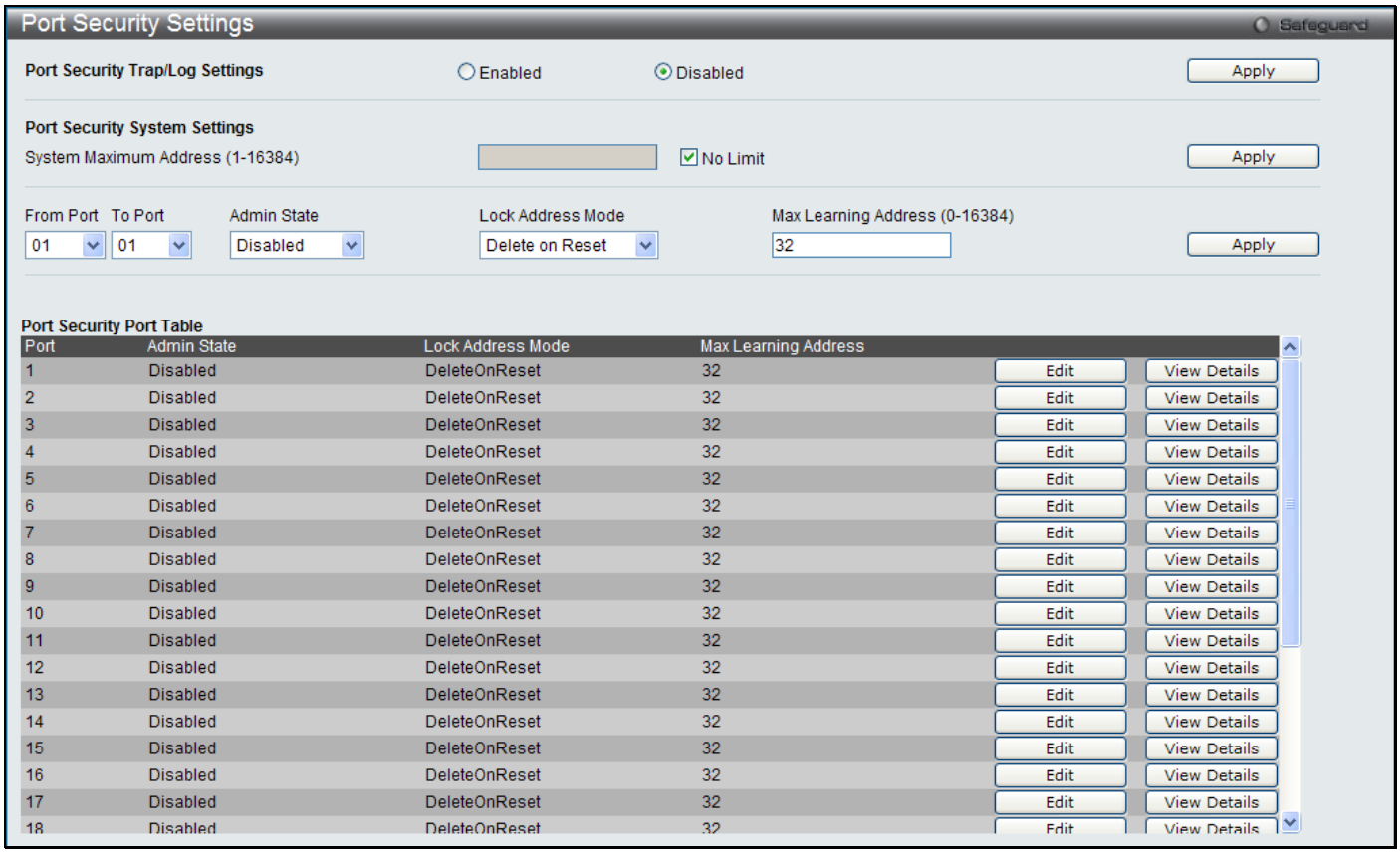


Figure 9-61 Port Security Settings window

The fields that can be configured are described below:

Parameter	Description
Port Security Trap/Log Settings	Use the radio button to enable or disable Port Security Traps and Log Settings on the Switch.
System Max Address (1-16384)	Here the user can enter the system maximum address.
From Port / To Port	Select a range of ports to be configured.
Admin State	This pull-down menu allows the user to enable or disable Port Security (locked MAC address table for the selected ports).
Lock Address Mode	This pull-down menu allows the option of how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: *Permanent* – The locked addresses will only age out after the Switch has been reset. *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset or rebooted.
Max Learning Address (0-16384)	Specifies the maximum value of port security entries that can be learned on this port.

Click the **Apply** button to accept the changes made for each individual section.
Click the **Edit** button to re-configure the specific entry.
Click the **View Detail** button to display the information of the specific entry.

After clicking the **View Detail** button, the following page will appear:

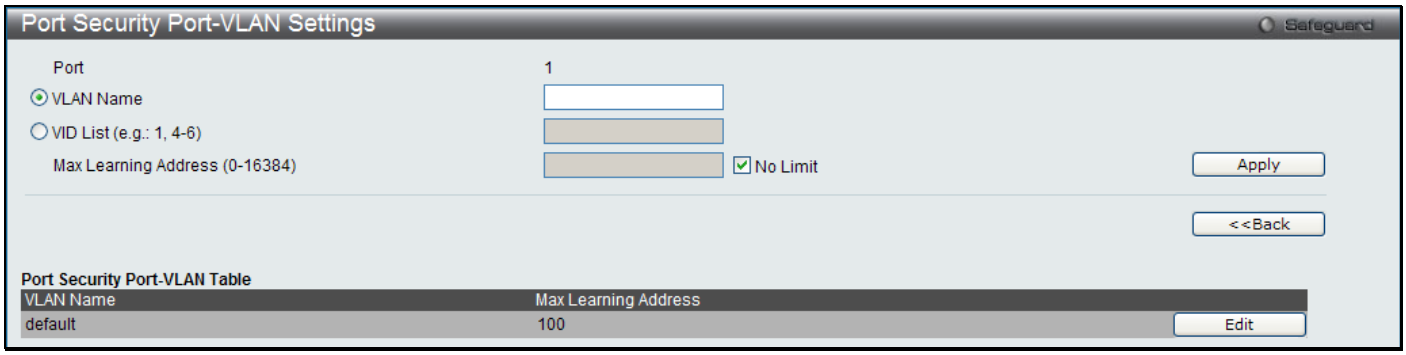


Figure 9-62 Port Security Port-VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Select and enter the VLAN name for this configuration here.
VID List	Select and enter the VLAN ID for this configuration here.
Max Learning Address (0-16384)	Enter the maximum value of port security entries that can be learned on this port. Selecting the option *No Limit* will assign a no limit value to this field.

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

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

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

Port Security VLAN Settings

Users can configure the maximum number of port-security entries that can be learned on a specific VLAN.

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

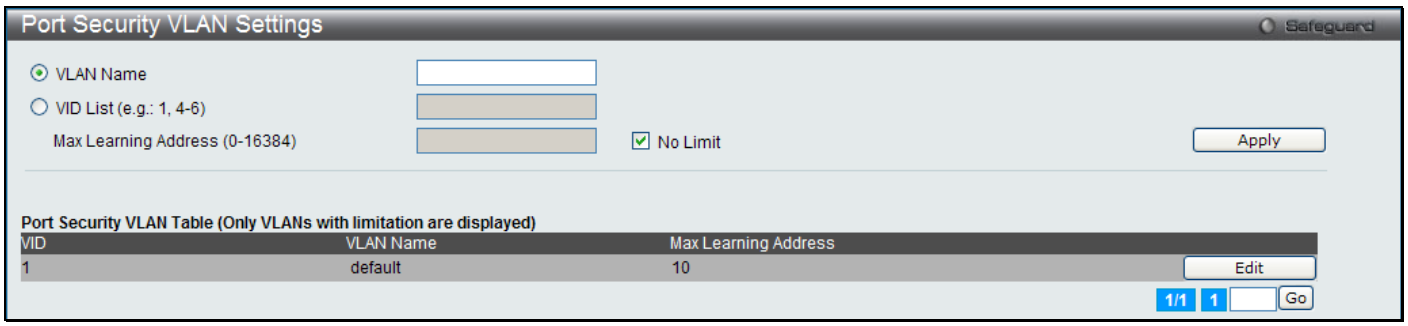


Figure 9-63 Port Security VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Here the user can enter the VLAN Name.
VID List	Specifies a list of the VLAN be VLAN ID.
Max Learning Address (0-16384)	Specifies the maximum number of port-security entries that can be learned by this VLAN. Selecting the option *No Limit* will assign a no limit value to this field.

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.

Port Security Entries

Users can remove an entry from the port security entries learned by the Switch and entered into the forwarding database.

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

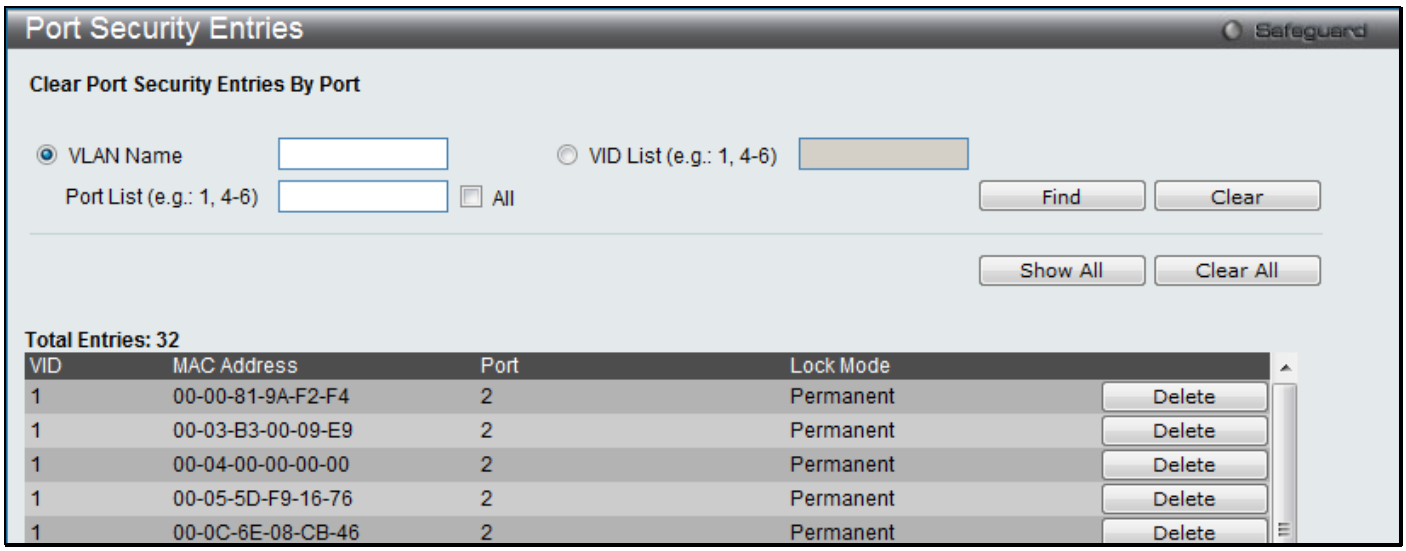


Figure 9-64 Port Security Entries window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
VID List	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
Port List	Enter the port number or list here to be used for the port security entry search. When **All** is selected, all the ports configured 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 entries based on the information entered.

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

Click the **Clear All** button to remove all the entries listed.

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

ARP Spoofing Prevention Settings

The user can configure the spoofing prevention entry to prevent spoofing of MAC for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry, but either its sender MAC field or source MAC field does not match the gateway MAC of the entry will be dropped by the system.

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

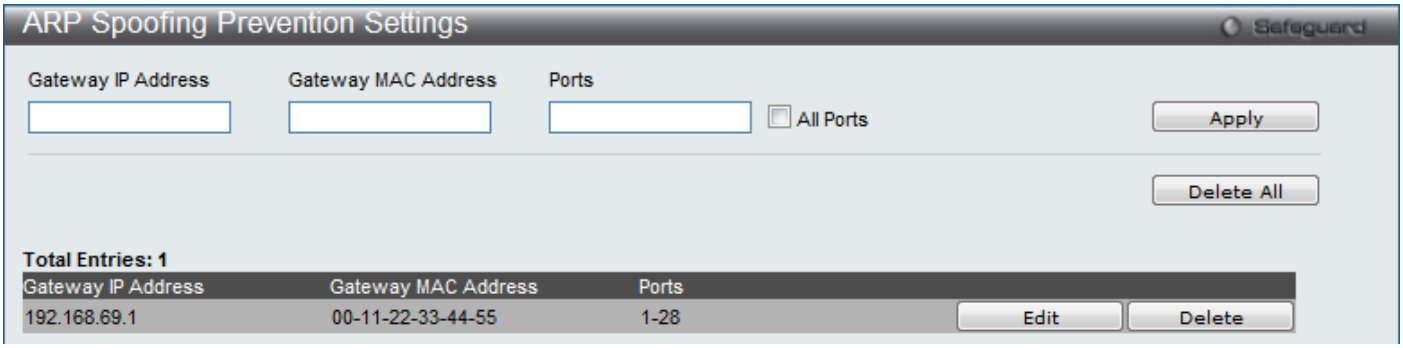


Figure 9-65 ARP Spoofing Prevention Settings window

The fields that can be configured are described below:

Parameter	Description
Gateway IP Address	Here the user can enter the gateway IP address to help prevent ARP Spoofing.
Gateway MAC Address	Here the user can enter the gateway MAC address to help prevent ARP Spoofing.
Ports	Here the user can enter the port numbers that this feature applies to. Alternatively, tick **All Ports** check box to apply this feature to all the ports of the switch.

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

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

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

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

BPDU Attack Protection

This page is used to configure the BPDP protection function for the ports on the switch. In generally, there are two states in BPDU 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. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU

To view the following window, click **Security > BPDU Attack Protection**, as shown below:

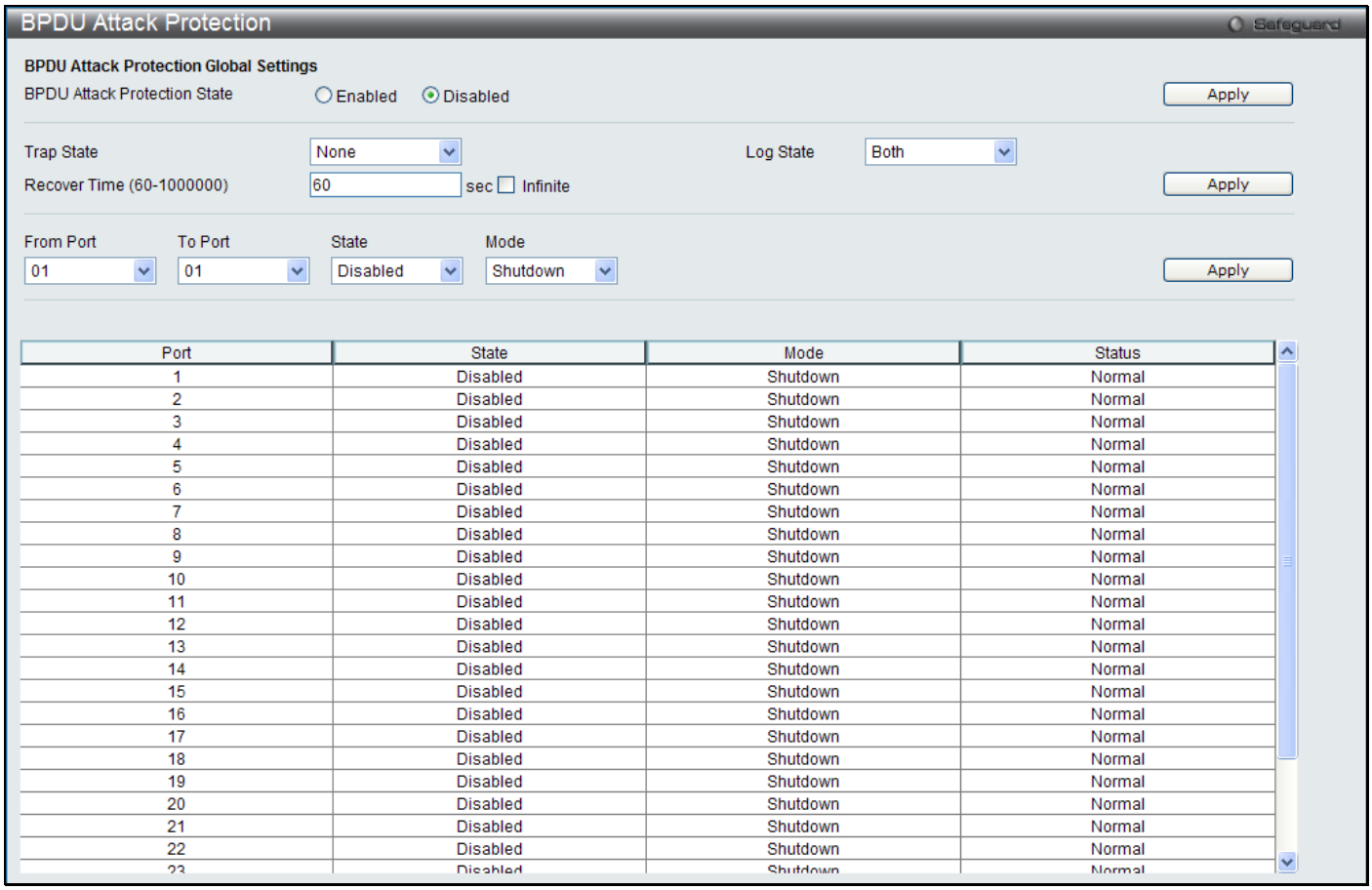


Figure 9-66 BPDU Attack Protection window

The fields that can be configured are described below:

Parameter	Description
BPDU Attack Protection State	Here the user can enable or disable the BPDU Attack Protection state.
Trap State	Here the user can specify when a trap will be sent. Options to choose from are **None, Attack Detected, Attack Cleared** or **Both**.
Log State	Here the user can specify when a log entry will be sent. Options to choose from are **None, Attack Detected, Attack Cleared** or **Both**.
Recover Time (60-1000000)	Specified the BPDU protection Auto-Recovery timer. The default value of the recovery timer is 60. Tick the **Infinite** check box so that the port will not be recovered automatically.
From Port / To Port	Here the user can select a range of ports to use for this configuration.
State	Here the user can enable or disable the protection mode for a specific port.
Mode	Specified the BPDU protection mode. The default mode is shutdown. *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 for each individual section.

Loopback Detection Settings

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the

network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to discarding state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the pull-down menu.

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

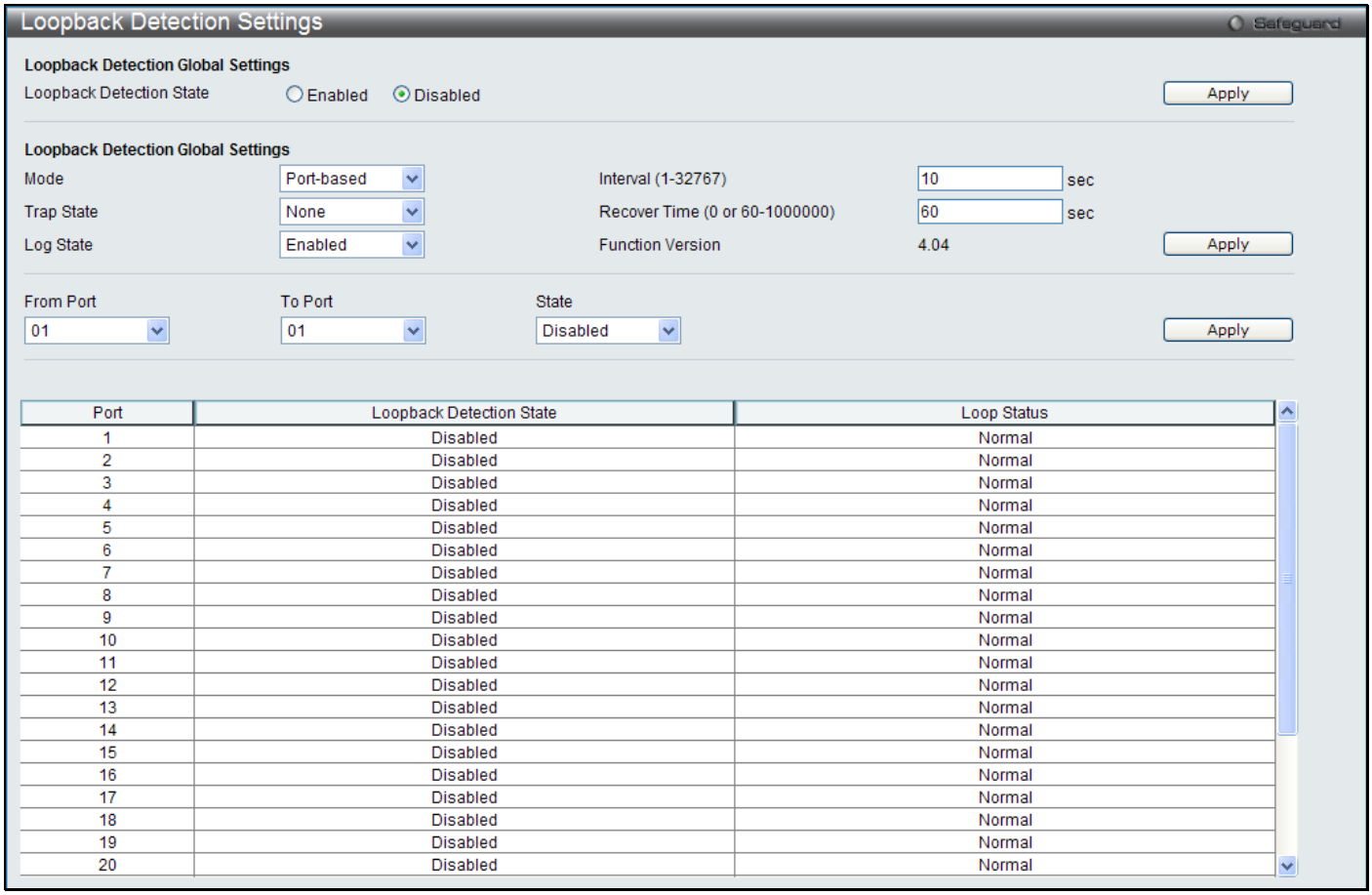


Figure 9-67 Loopback Detection Settings window

The fields that can be configured are described below:

Parameter	Description
Loopback Detection State	Use the radio button to enable or disable loopback detection. The default is Disabled.
Mode	Use the drop-down menu to toggle between *Port Based* and *VLAN Based*.
Trap State	Set the desired trap status: *None*, *Loop Detected*, *Loop Cleared*, or *Both*.
Log State	Specify the state of the log for loopback detection.
Interval (1-32767)	Set a Loopdetect Interval between *1* and *32767* seconds. The default is *10* seconds.
Recover Time (0 or 60-1000000)	Time allowed (in seconds) for recovery when a Loopback is detected. The Loopdetect Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loopdetect Recover Time. The default is *60* seconds.
From Port / To Port	Select a range of ports to be configured.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled*.

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

Traffic Segmentation Settings

Traffic segmentation is used to limit traffic flow from a single or group of ports, to a group of ports. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the master switch CPU.

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

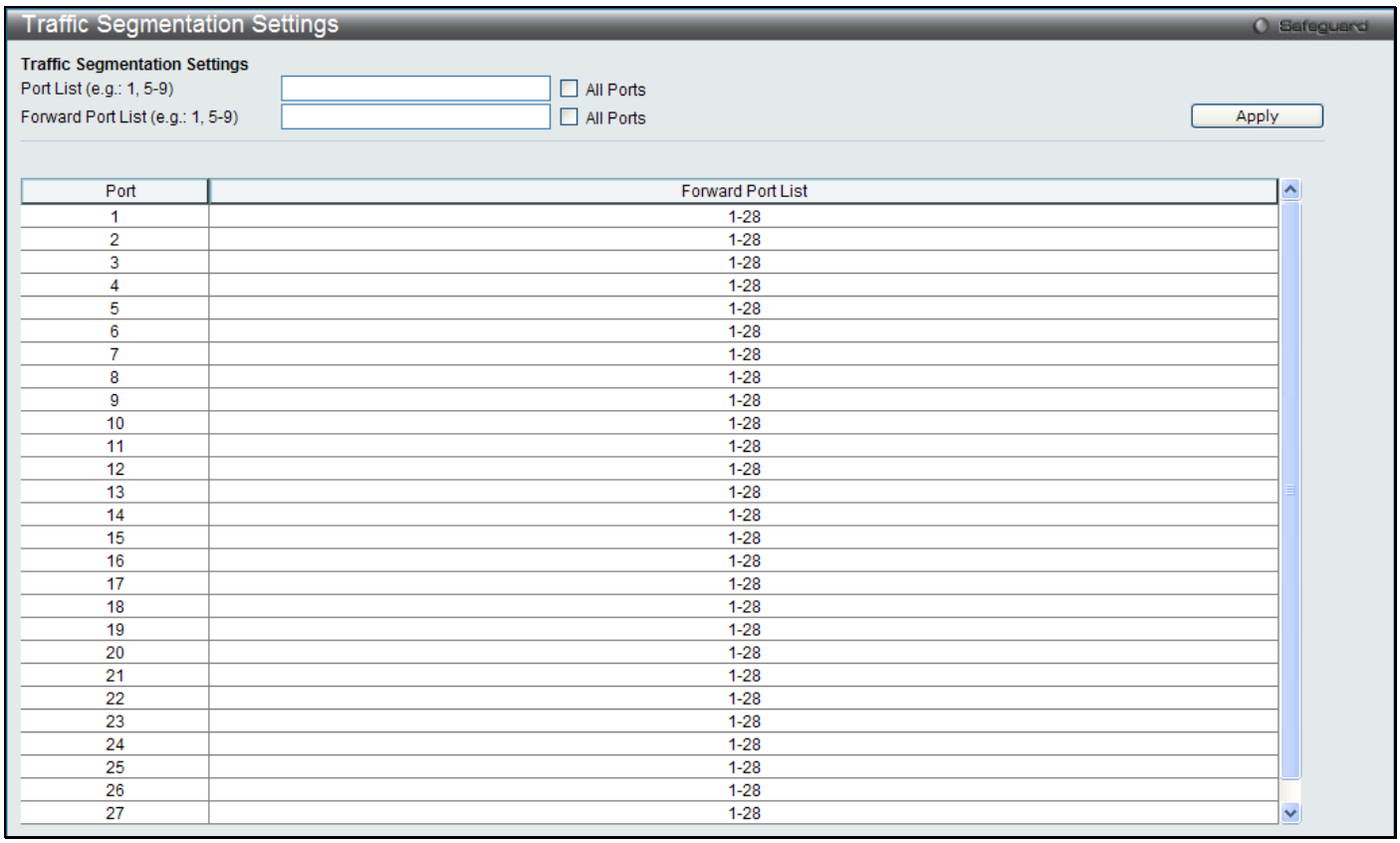


Figure 9-68 Traffic Segmentation Settings window

The fields that can be configured are described below:

Parameter	Description
Port List	Here the user can enter the ports to be included in the traffic segmentation setup. Select the **All Ports** button to select all the ports for the configuration.
Forward Port List	Here the user can enter the ports to be included in the traffic segmentation setup Select the **All Ports** button to select all the ports for the configuration.

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

NetBIOS Filtering Settings

NetBIOS is an application programming interface, providing a set of functions that applications use to communicate across networks. NetBEUI, the NetBIOS Enhanced User Interface, was created as a data-link-layer frame structure for NetBIOS. A simple mechanism to carry NetBIOS traffic, NetBEUI has been the protocol of choice for small MS-DOS- and Windows-based workgroups. NetBIOS no longer lives strictly inside of the NetBEUI protocol. Microsoft worked to create the international standards described in RFC 1001 and RFC 1002, NetBIOS over TCP/IP (NBT).

If the network administrator wants to block the network communication on more than two computers which use NETBUEI protocol, it can use NETBIOS filtering to filter these kinds of packets.

If the user enables the NETBIOS filter, the switch will create one access profile and three access rules automatically. If the user enables the extensive NETBIOS filter, the switch will create one more access profile and one more access rule.

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

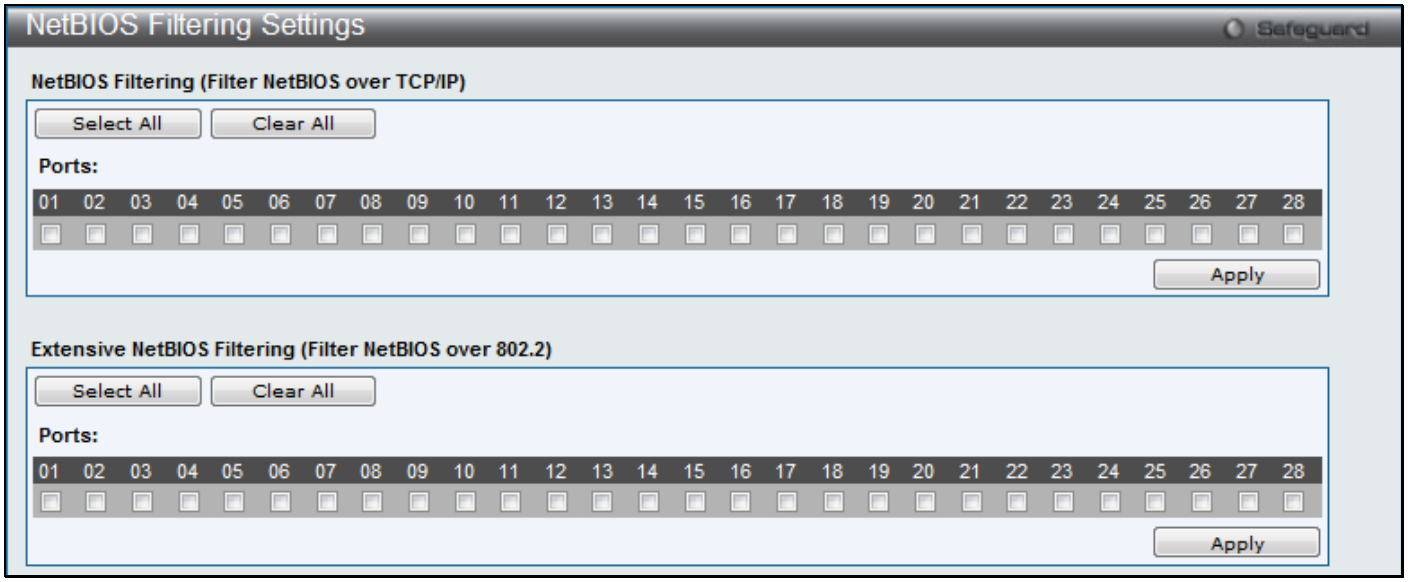


Figure 9-69 NetBIOS Filtering Settings window

The fields that can be configured are described below:

Parameter	Description
NetBIOS Filtering	Here the user can select the appropriate port to include in the NetBIOS filtering configuration.
Extensive NetBIOS Filtering	Here the user can select the appropriate port to include in the Extensive NetBIOS filtering configuration.

Click the **Select All** button to select all ports in each individual section.

Click the **Clear All** button to deselect all ports in each individual section.

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

DHCP Server Screening

This function allows the user 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 Port Settings

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers. When the DHCP server filter function is enabled, all DHCP server packets will be filtered from a specific port.

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

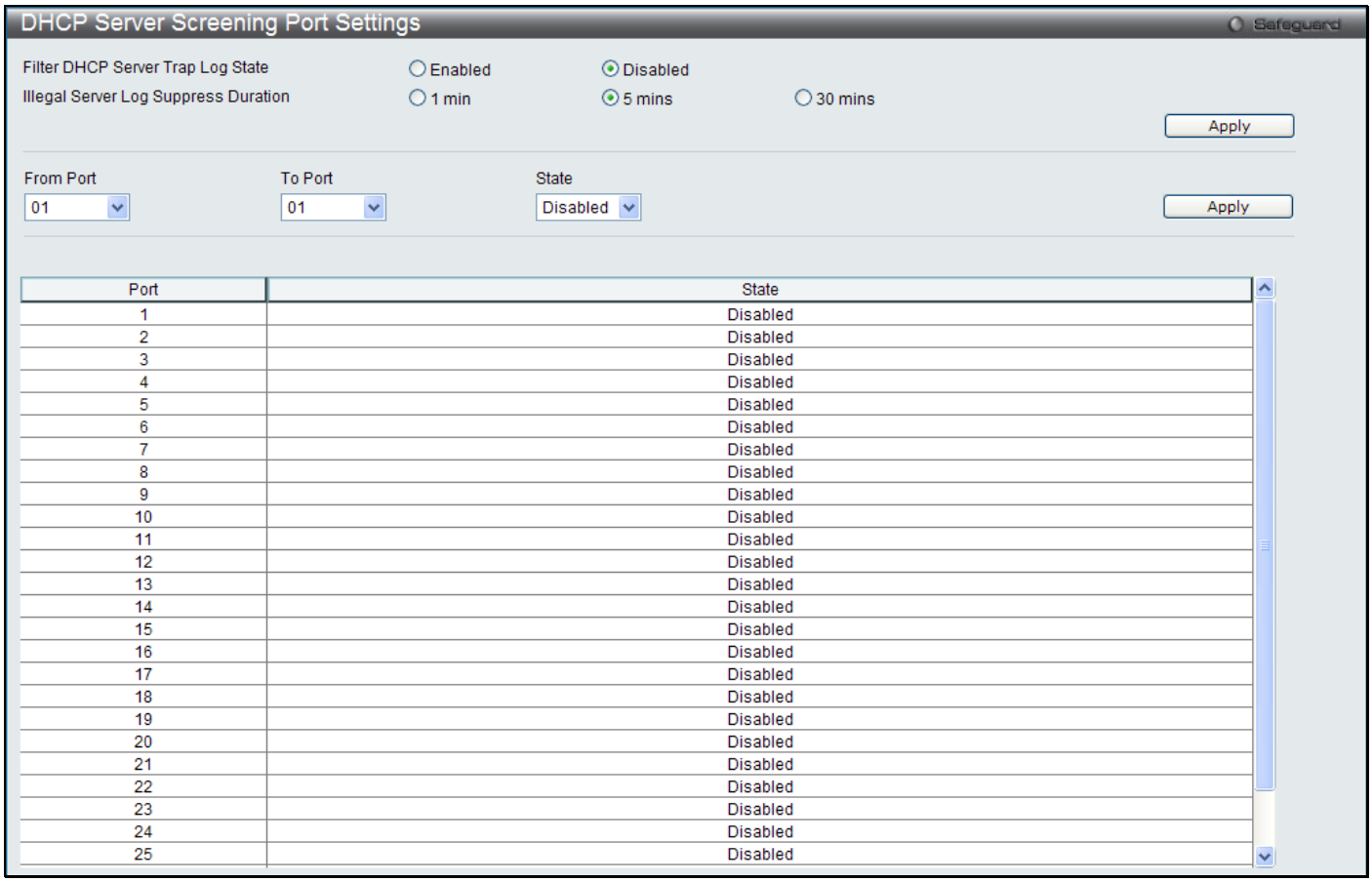


Figure 9-70 DHCP Server Screening Port Settings window

The fields that can be configured are described below:

Parameter	Description
Filter DHCP Server Trap Log State	Enable or disable this feature.
Illegal Server Log Suppress Duration	Choose an illegal server log suppress duration of 1 minute, 5 minutes, or 30 minutes.
From Port / To Port	A Select a range of ports to be configured.
State	Choose *Enabled* to enable the DHCP server screening or *Disabled* to disable it. The default is *Disabled*.

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

DHCP Offer Permit Entry Settings

Users can add or delete permit entries on this page.

To view the following window, click **Security > DHCP Server Screening > DHCP Offer Permit Entry Settings**, as shown below:

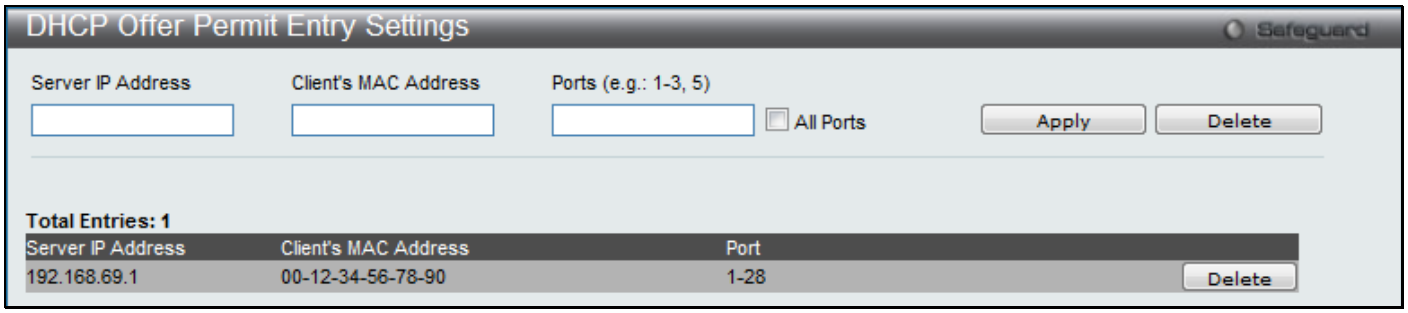


Figure 9-71 DHCP Offer Permit Entry Settings window

The fields that can be configured are described below:

Parameter	Description
Server IP Address	The IP address of the DHCP server to be permitted.
Client's MAC Address	The MAC address of the DHCP client.
Ports	The port numbers of the filter DHCP server. Select the **All Ports** option to include all the ports on this switch for this configuration.

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

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

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands allow users to secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- **TACACS** (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- **Extended TACACS (XTACACS)** - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- **TACACS+ (Terminal Access Controller Access Control System plus**) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server

Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Enable Admin

Users who have logged on to the Switch on the normal user level and wish to be promoted to the administrator level can use this window. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

To view the following window, click **Security > Access Authentication Control > Enable Admin**, as shown below:

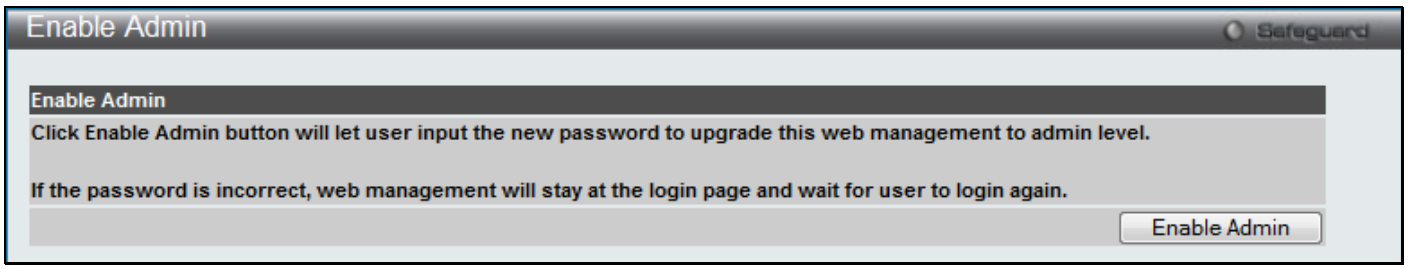


Figure 9-72 Enable Admin window

When this window appears, click the **Enable Admin** button revealing a window for the user to enter authentication (password, username), as seen below. A successful entry will promote the user to Administrator level privileges on the Switch.

Authentication Policy Settings

Users can enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

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

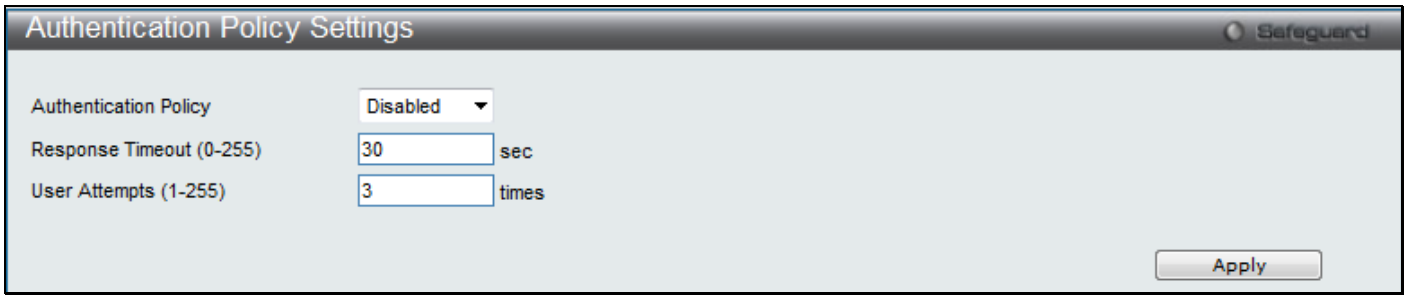


Figure 9-73 Authentication Policy Settings window

The fields that can be configured are described below:

Parameter	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

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

Application Authentication Settings

Users can configure Switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (Enable Admin**)** utilizing a previously configured method list.

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

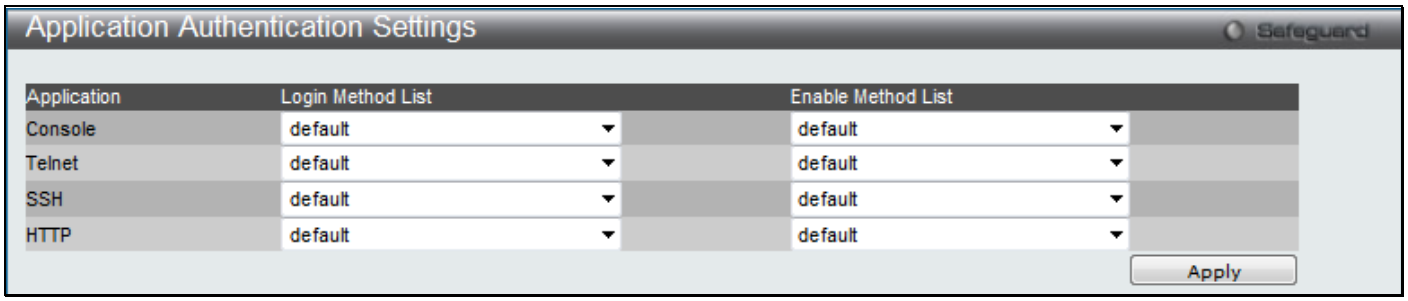


Figure 9-74 Application Authentication Settings window

The fields that can be configured are described below:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH, and the Web (HTTP) application.
Login Method List	Using the drop-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Login Method Lists Settings window for more information.
Enable Method List	Using the droop-down menu, configure an application to promote user level to admin-level

	users utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Enable Method Lists** window, in this section, for more information

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

Authentication Server Group Settings

Users can set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

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

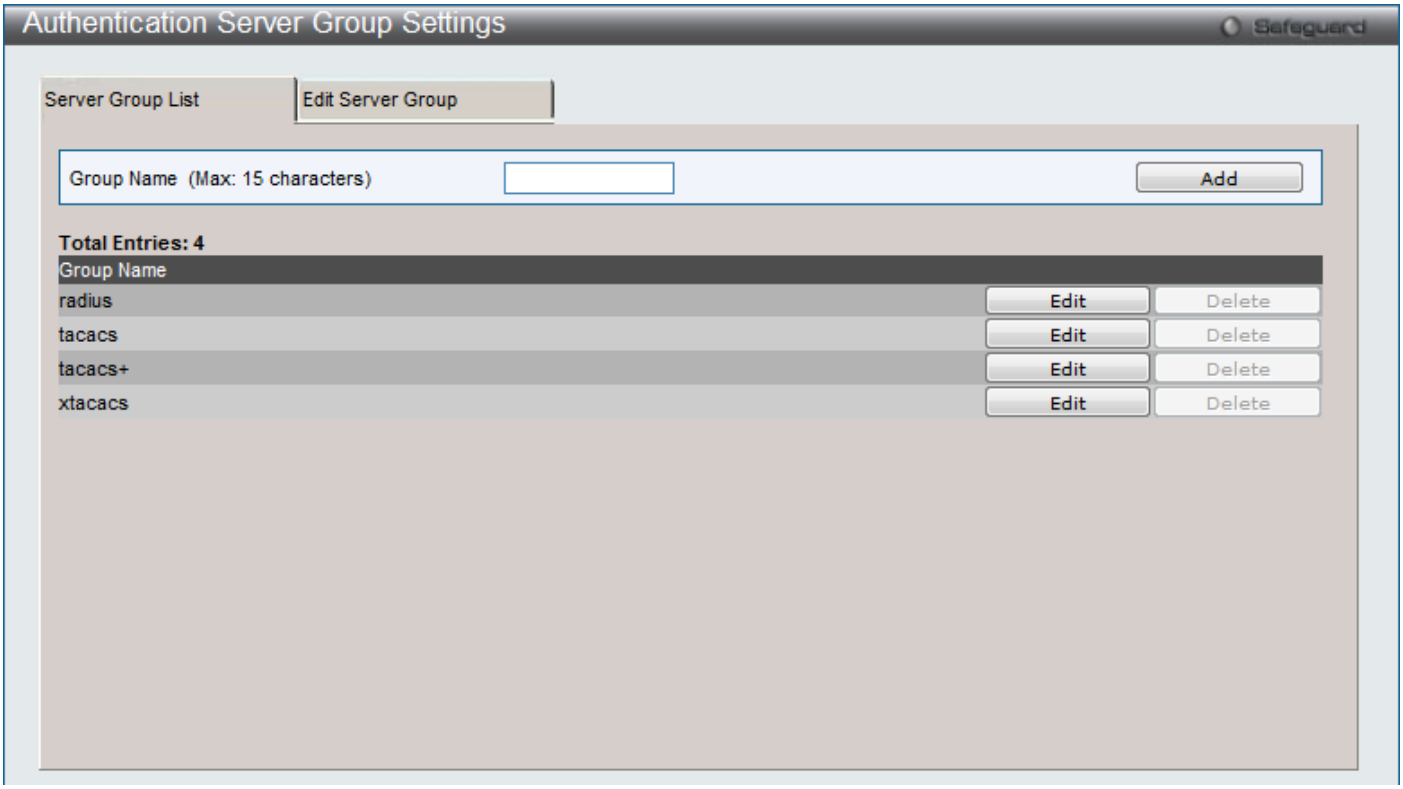


Figure 9-75 Authentication Server Group Settings window

This window displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To add a new Server Group, enter a name in the **Group Name** field and then click the **Add** button. To modify a particular group, click the **Edit** button (or the **Edit Server Group** tab), which will then display the following **Edit Server Group** tab:

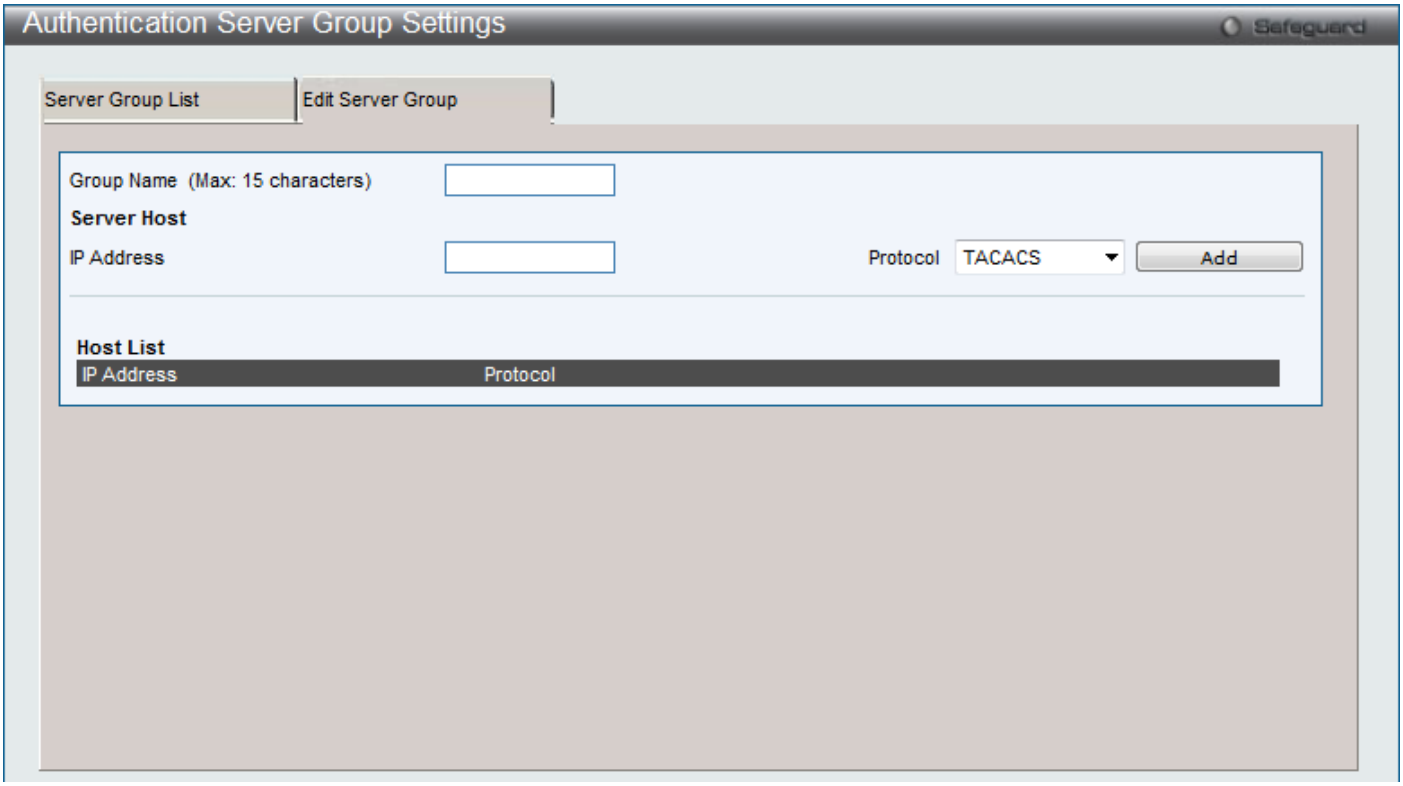


Figure 9-76 Authentication Server Group Settings –Edit Server Group window

To add an Authentication Server Host to the list, enter its name in the **Group Name** field, IP address in the **IP Address** field, use the drop-down menu to choose the **Protocol** associated with the IP address of the Authentication Server Host, and then click **Add** to add this Authentication Server Host to the group. The entry should appear in the Host List at the bottom of this tab.

NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE: The three built-in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

Authentication Server Settings

User-defined Authentication Server Hosts for the TACACS / XTACACS / TACACS+ / RADIUS security protocols can be set on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS / XTACACS / TACACS+ / RADIUS server host on a remote host. The TACACS / XTACACS / TACACS+ / RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS / XTACACS / TACACS+ / RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

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

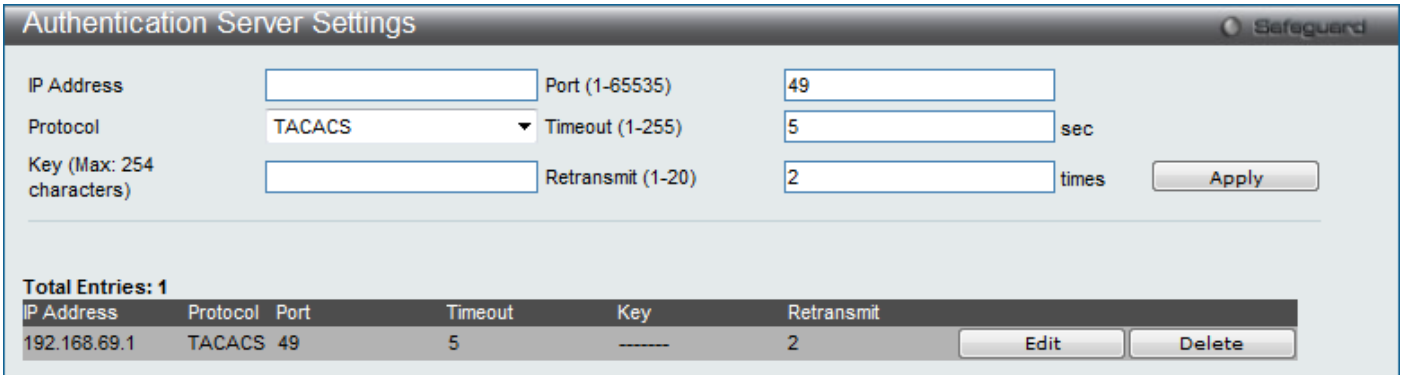


Figure 9-77 Authentication Server Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	The IP address of the remote server host to add.
Protocol	The protocol used by the server host. The user may choose one of the following: *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Retransmit (1-20)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.

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

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

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

NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other.

Login Method Lists Settings

User-defined or default Login Method List of authentication techniques can be configured for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS - XTACACS- local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependent on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a "User" privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator.

To view the following window, click **Security > Access Authentication Control > Login Method Lists Settings**, as shown below:

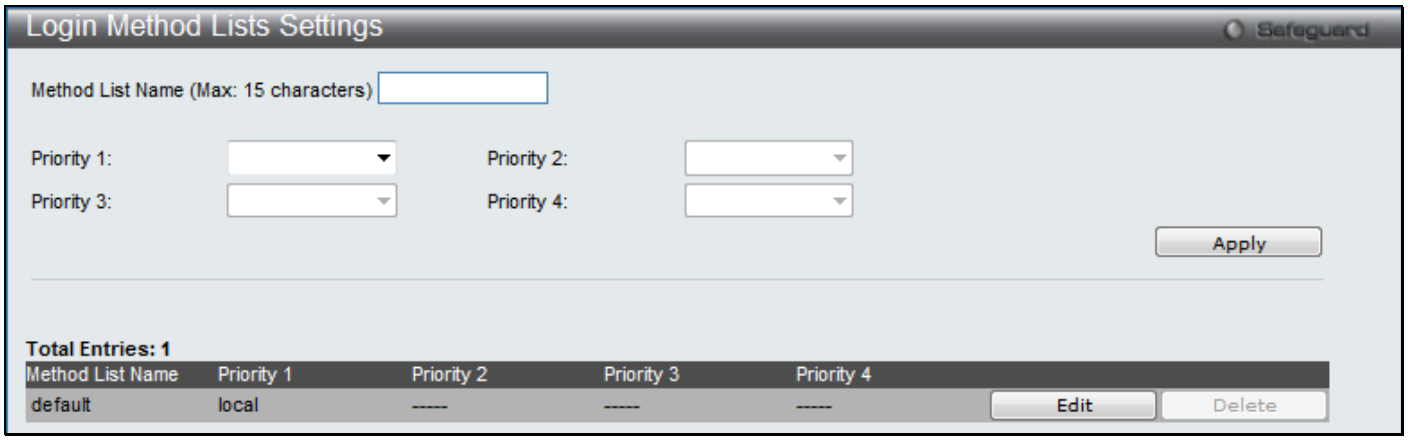


Figure 9-78 Login Method Lists Settings window

The fields that can be configured are described below:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. *none* - Adding this parameter will require no authentication needed to access 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 a Login Method List defined by the user.

Enable Method Lists Settings

Users can set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.

NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following window, click **Security > Access Authentication Control > Enable Method Lists Settings**, as shown below:

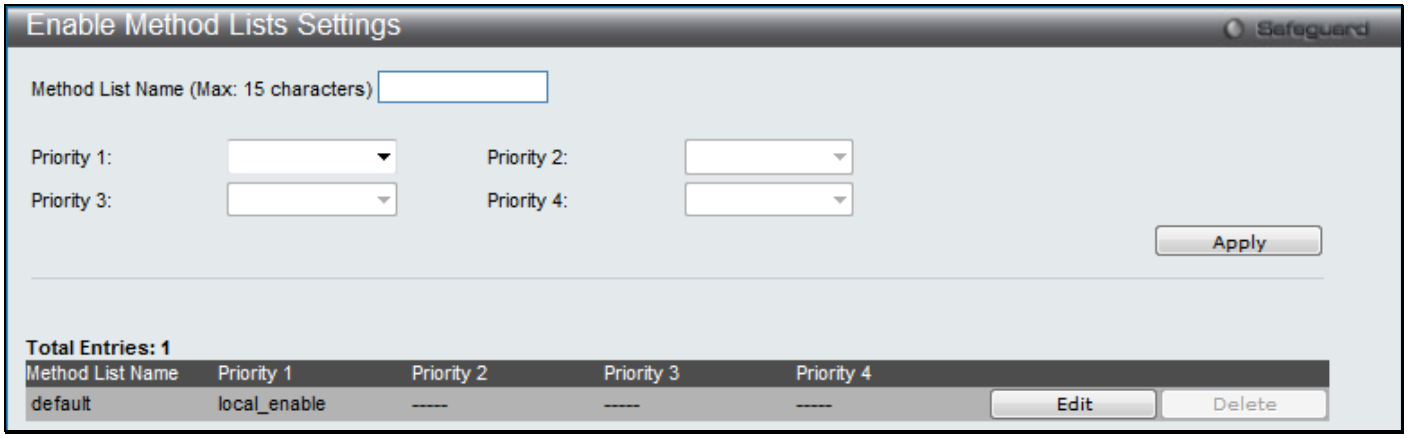


Figure 9-79 Enable Method Lists Settings window

The fields that can be configured are described below:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *local_enable* - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section entitled Local Enable Password. *none* - Adding this parameter will require no authentication needed to access the Switch. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

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.

Local Enable Password Settings

Users can configure the locally enabled password for Enable Admin. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security > Access Authentication Control > Local Enable Password Settings**, as shown below:

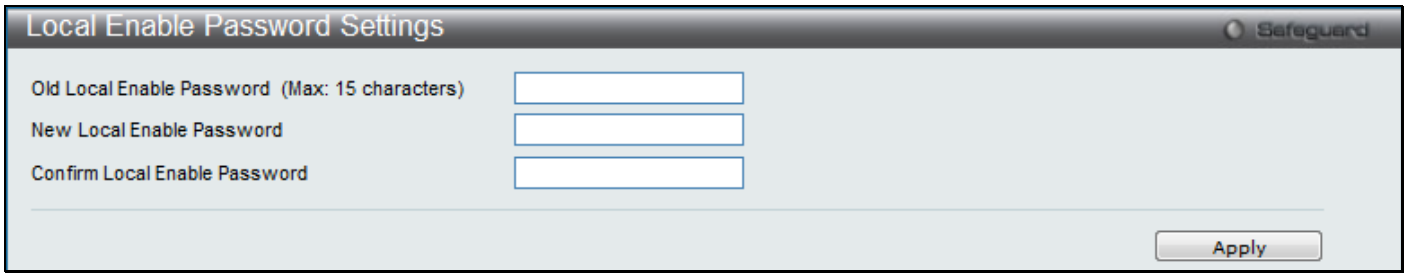


Figure 9-80 Local Enable Password Settings window

The fields that can be configured are described below:

Parameter	Description
Old Local Enable Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

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

SSL Settings

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

1. **Key Exchange:** The first part of the Cipher suite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

1. **Hash Algorithm**: This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

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

The **SSL Settings** window located on the next page will allow the user to enable SSL on the Switch and implement any one or combination of listed cipher suites on the Switch. A cipher suite is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible cipher suites for the SSL function, which are all enabled by default. To utilize a particular cipher suite, disable the unwanted cipher suites, leaving the desired one for authentication.

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. The Switch only supports certificate files with .der file extensions. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

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

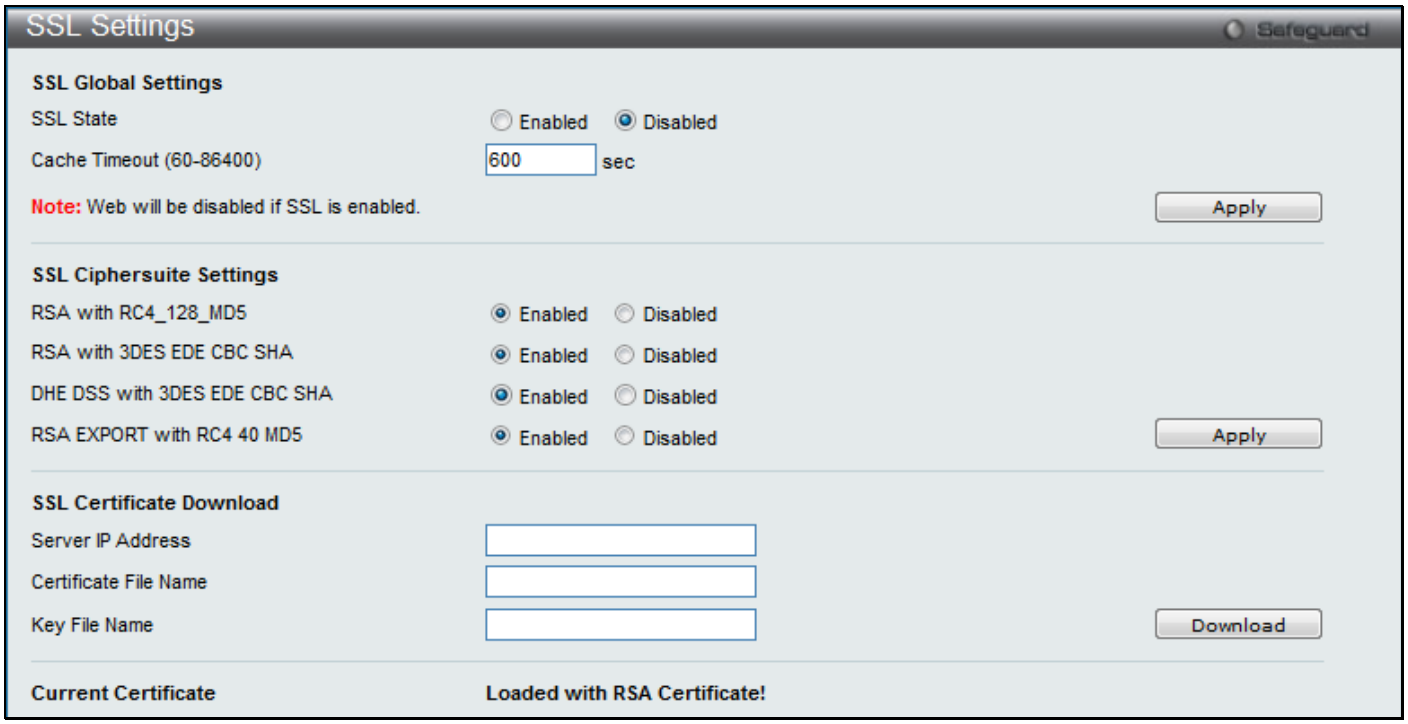


Figure 9-81 SSL Settings window

The fields that can be configured are described below:

Parameter	Description
SSL State	Use the radio buttons to enable or disable the SSL status on the Switch. The default is Disabled.
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.

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

To set up the **SSL cipher suite function** on the Switch, configure the parameters in the SSL Cipher suite Settings section described below:

Parameter	Description
RSA with	This cipher suite combines the RSA key exchange, stream cipher RC4 encryption with

RC4_128_MD5	128-bit keys and the MD5 Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA with 3DES EDE CBC SHA	This cipher suite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
DHS DSS with 3DES EDE CBC SHA	This cipher suite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA EXPORT with RC4 40 MD5	This cipher suite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.

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

To download SSL certificates, configure the parameters in the SSL Certificate Download section described below.

Parameter	Description
Server IP Address	Enter the IPv4 address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click the **Download** button to download the SSL certificate based on the information entered.

NOTE: Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface.

NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SSH

SSH is an abbreviation of Secure Shell, which 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:

1. 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.
2. 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.
3. 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 Authmode and Algorithm Settings** window.
4. 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 Settings

Users can configure and view settings for the SSH server.

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

Figure 9-82 SSH Settings window

The fields that can be configured are described below:

Parameter	Description
SSH Server State	Use the radio buttons to enable or disable SSH on the Switch. The default is Disabled.
Max. Session (1-8)	Enter a value between *1* and *8* to set the number of users that may simultaneously access the Switch. The default setting is *8*.
Connection Timeout (30-600)	Allows the user to set the connection timeout. The user may set a time between *120* and *600* seconds. The default setting is *120* seconds.
Authfail Attempts (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.
Rekey Timeout	This field is used to set the time period that the Switch will change the security shell encryptions by using the pull-down menu. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.
TCP Port Number (1-65535)	Here the user can enter the TCP Port Number used for SSH. The default value is *22*.

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

SSH Authentication Method and Algorithm Settings

Users can configure the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by ticking their corresponding check boxes. All algorithms are enabled by default.

To view the following window, click **Security > SSH > SSH Authentication Method and Algorithm Settings**, as shown below:

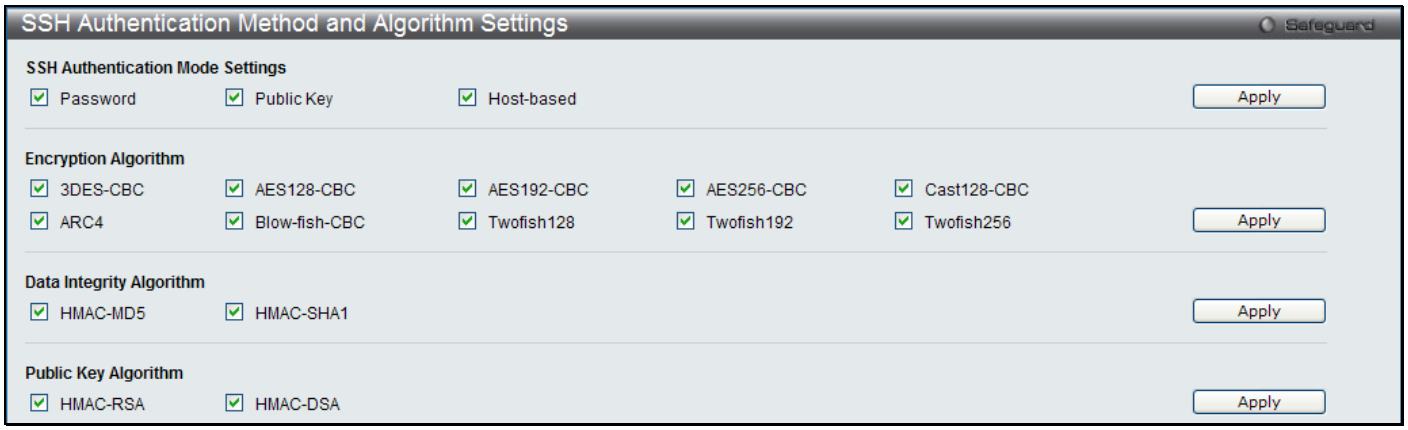


Figure 9-83 SSH Authentication Method and Algorithm Settings window

The fields that can be configured for **SSH Authentication Mode** are described below:

Parameter	Description
Password	This may be enabled or disabled to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This parameter is enabled by default.
Public Key	This may be enabled or disabled to choose if the administrator wishes to use a public key configuration set on a SSH server, for authentication. This parameter is enabled by default.
Host Based	This may be enabled or disabled to choose if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. This parameter is enabled by default.

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

The fields that can be configured for the **Encryption Algorithm** are described below:

Parameter	Description
3DES-CBC	Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
Cast128-CBC	Use the check box to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Use the check box to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish-CBC	Use the check box to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Use the check box to enable or disable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Use the check box to enable or disable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Use the check box to enable or disable the twofish256 encryption algorithm. The default is enabled.

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

The fields that can be configured for the **Data Integrity Algorithm** are described below:

Parameter	Description
HMAC-MD5	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.
HMAC-SHA1	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.

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

The fields that can be configured for the **Public Key Algorithm** are described below:

Parameter	Description
HMAC-RSA	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm (DSA) encryption. The default is enabled.

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

SSH User Authentication Lists

Users can configure parameters for users attempting to access the Switch through SSH. In the window above, the User Account “username” has been previously set using the **User Accounts** window in the **Configuration** folder. A User Account MUST be set in order to set the parameters for the SSH user.

To view the following window, click **Security > SSH > SSH User Authentication Lists**, as shown below:

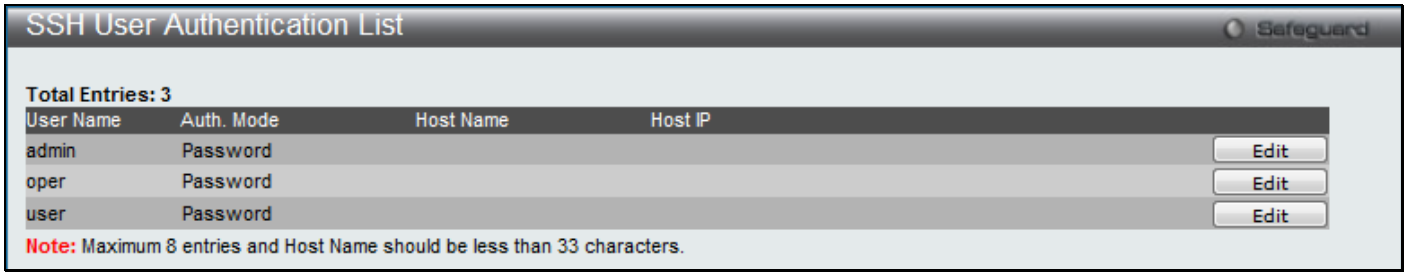


Figure 9-84 SSH User Authentication Lists window

The fields that can be configured are described below:

Parameter	Description
Auth. Mode	The administrator may choose one of the following to set the authorization for users attempting to access the Switch. *Host Based* – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *Password* – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation. *Public Key* – This parameter should be chosen if the administrator wishes to use the public key on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth.

	Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

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

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

NOTE: To set the SSH User Authentication Mode parameters on the Switch, a User Account must be previously configured.

Trusted Host Settings

Up to ten trusted host secure IP addresses or ranges may be configured and used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

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

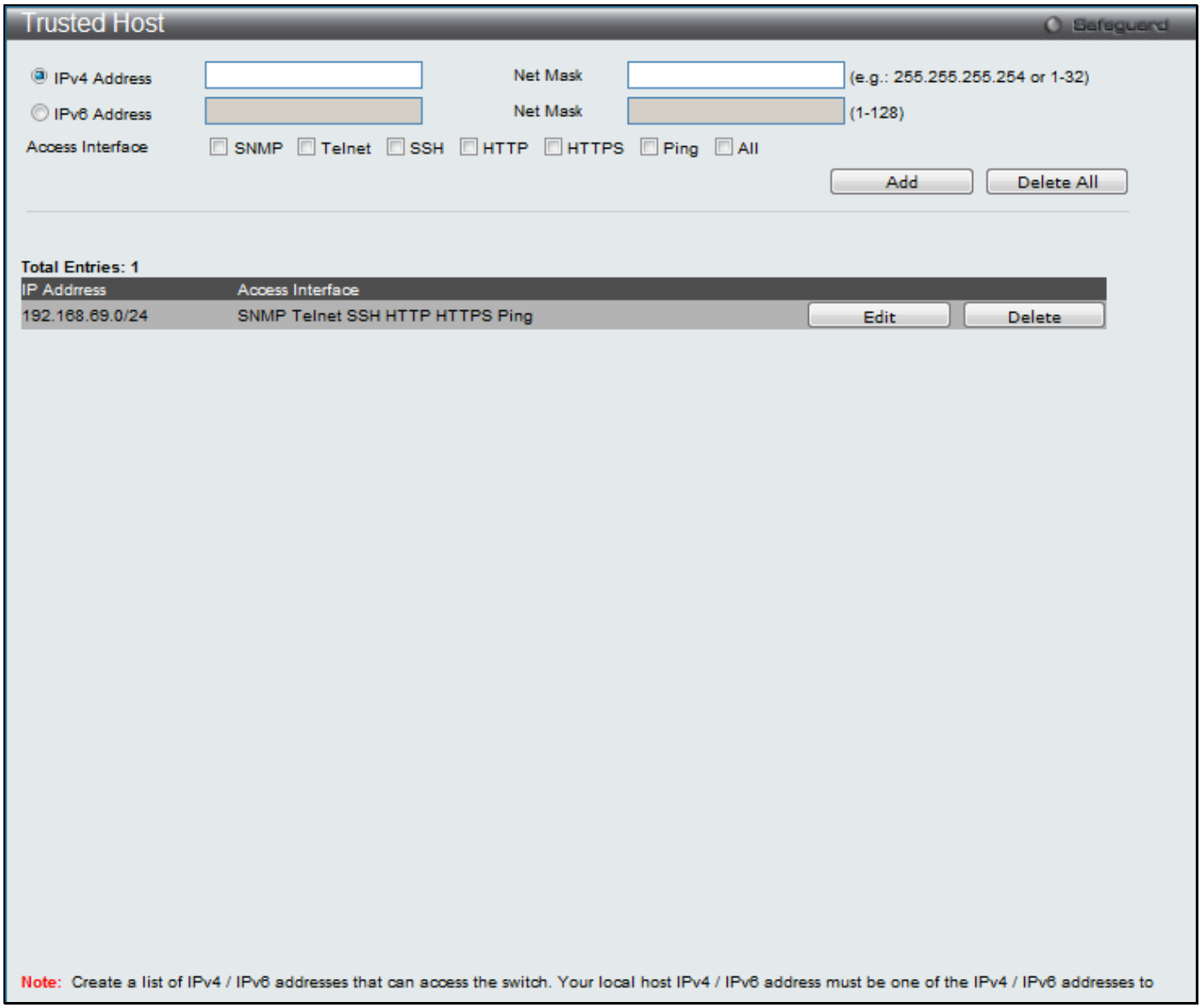


Figure 9-85 Trusted Host Settings window

The fields that can be configured are described below:

Parameter	Description
IPv4 Address	Here the user can enter an IPv4 address to add to the trusted host list.
Net Mask	Here the user can enter a IPv4 Net Mask address to add to the trusted host list.
IPv6 Address	Here the user can enter an IPv6 address to add to the trusted host list.
Net Mask	Here the user can enter a IPv6 Net Mask address to add to the trusted host list.
Access Interface	Here the user can select services that will be allowed to the trusted host.

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

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

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

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

Safeguard Engine Settings

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 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. The Safeguard Engine has two operating modes that can be configured by the user, *Strict* and *Fuzzy*. In *Strict* mode, when the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter the Exhausted mode. When in this mode, the Switch will drop all ARP and IP broadcast packets and packets from un-trusted IP addresses for a calculated time interval. Every five seconds, the Safeguard Engine will check to see if there are too many packets flooding the Switch. If the threshold has been crossed, the Switch will initially stop all ingress ARP and IP broadcast packets and packets from un-trusted IP addresses for five seconds. After another five-second checking interval arrives, the Switch will again check the ingress flow of packets. If the flooding has stopped, the Switch will again begin accepting all packets. Yet, if the checking shows that there continues to be too many packets flooding the Switch, it will stop accepting all ARP and IP broadcast packets and packets from un-trusted IP addresses for double the time of the previous stop period. This doubling of time for stopping these packets will continue until the maximum time has been reached, which is 320 seconds and every stop from this point until a return to normal ingress flow would be 320 seconds. For a better understanding, please examine the following example of the Safeguard Engine.

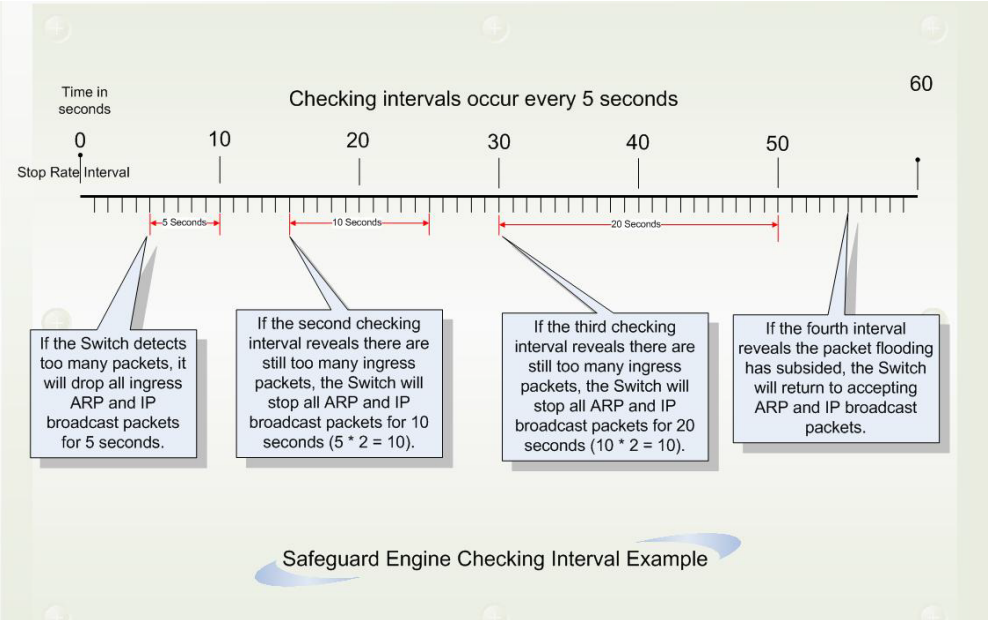


Figure 9-86 Safeguard Engine window

For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will discard ingress ARP and IP broadcast packets and packets from the illegal IP addresses. In the example above, the Switch doubled the time for dropping ARP and IP broadcast packets when consecutive flooding issues were detected

at 5-second intervals. (First stop = 5 seconds, second stop = 10 seconds, third stop = 20 seconds) Once the flooding is no longer detected, the wait period for dropping ARP and IP broadcast packets will return to 5 seconds and the process will resume.

In *Fuzzy* mode, once the Safeguard Engine has entered the Exhausted mode, the Safeguard Engine will decrease the packet flow by half. After returning to Normal mode, the packet flow will be increased by 25%. The switch will then return to its interval checking and dynamically adjust the packet flow to avoid overload of the Switch.

NOTICE: 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.

Users can enable the Safeguard Engine or configure advanced Safeguard Engine settings for the Switch.

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

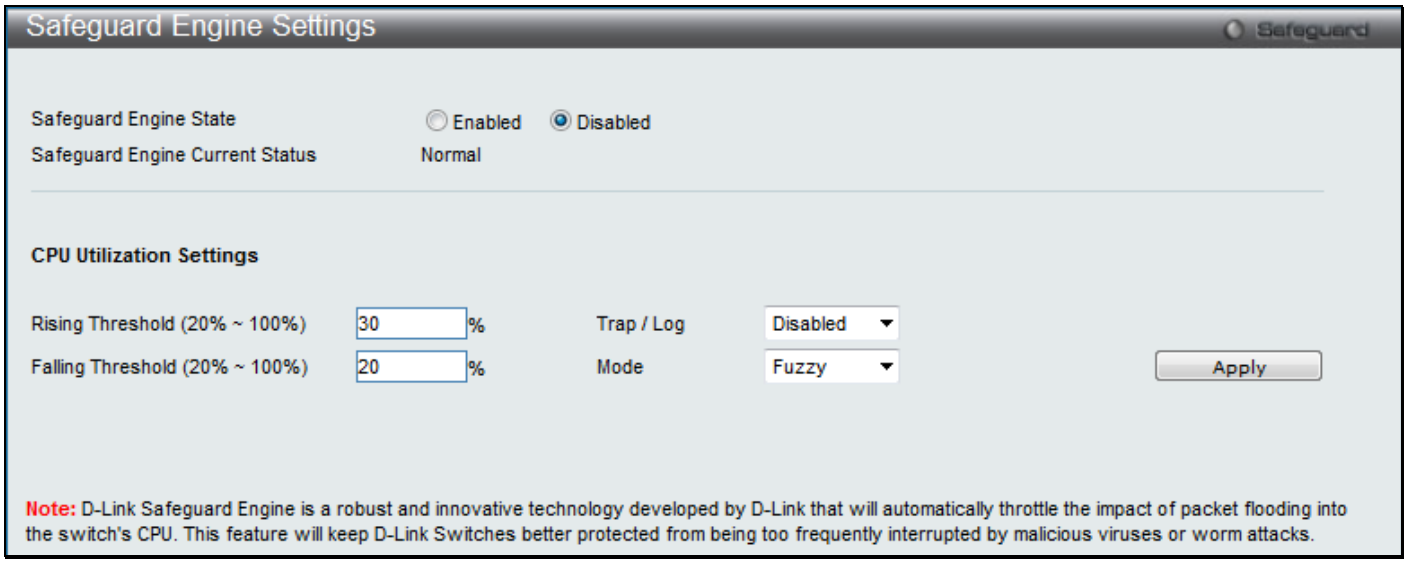


Figure 9-87 Safeguard Engine Settings window

The fields that can be configured are described below:

Parameter	Description
Safeguard Engine State	Use the radio button to globally enable or disable Safeguard Engine settings for the Switch.
Rising Threshold (20% - 100%)	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold (20% - 100%)	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.
Trap / Log	Use the pull-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select: *Fuzzy* – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. *Strict* – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided. The default setting is *Fuzzy* mode.

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

Chapter 10 Network Application

DHCP
DNS
PPPoE Circuit ID Insertion Settings
RCP Server Settings
SMTP Settings
SNTP
Flash File System Settings

DHCP

DHCP Relay

DHCP Relay Global Settings

Users can enable and configure DHCP Relay Global Settings. The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is equal to or greater than the hop count limit, the packet is dropped. The range is between *1* and *16* hops, with a default value of *4*. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a DHCP request packet. If the value in the seconds' field of the packet is less than the relay time threshold, the packet will be dropped. The range is between *0* and *65,535* seconds, with a default value of *0* seconds.

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

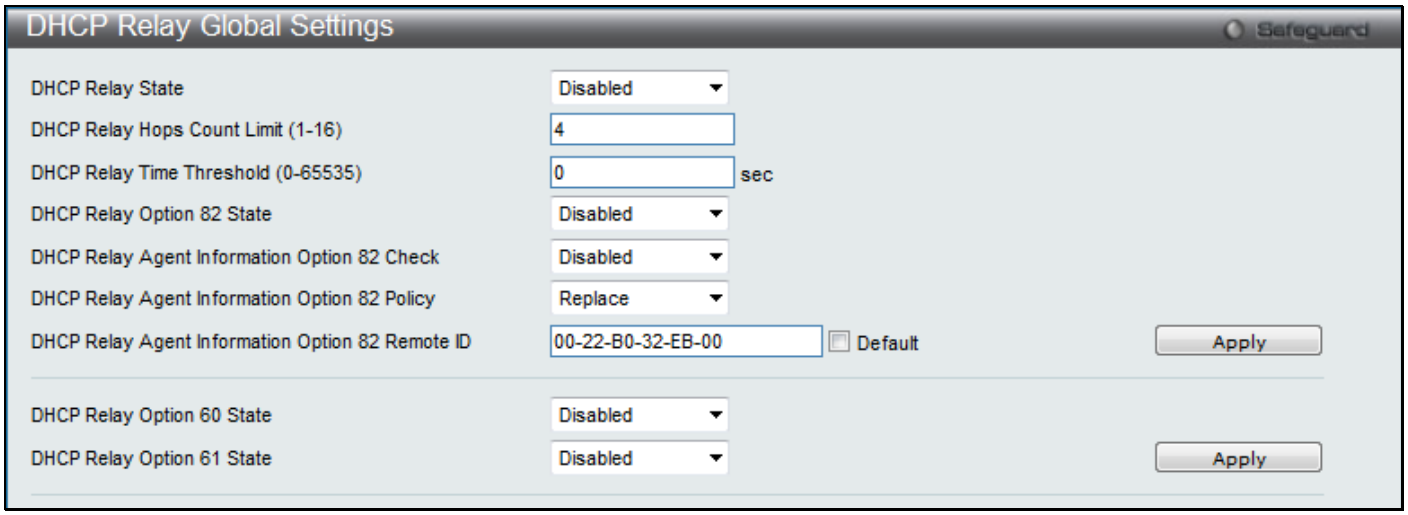


Figure 10-1 DHCP Relay Global Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Relay State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Relay service on the Switch. The default is *Disabled.*
DHCP Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP messages can be forwarded. The default hop count is *4*.
DHCP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the minimum time limit for routing a DHCP packet. If a value of *0* is entered, the Switch will not process the value in the seconds' field of the DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given DHCP packet.
DHCP Relay Option 82 State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Relay Agent Information Option 82 on the Switch.

	The default is *Disabled.* *Enabled* –When this field is toggled to *Enabled*, the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *Disabled*- When the field is toggled to *Disabled*, the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field. *Enabled* – When the field is toggled to *Enabled*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *Disabled* – When the field is toggled to *Disabled*, the relay agent will not check the validity of the packet's option 82 field.
DHCP Relay Agent Information Option 82 Policy	This field can be toggled between *Replace, Drop,* and *Keep* by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Relay Agent Information Option 82 Check is set to *Disabled*. The default is *Replace.* *Replace* – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
DHCP Relay Agent Information Option 82 Remote ID	Here the user can enter the DHCP Relay Agent Information Option 82 Remote ID.
DHCP Relay Option 60 State	Here the user can enable or disable the use of the DHCP Relay Option 60 State feature.
DHCP Relay Option 61 State	Here the user can enable or disable the use of the DHCP Relay Option 61 State feature.

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

NOTE: If the Switch receives a packet that contains the option 82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, users may configure a client with the option 82 field. In this situation, disable the information check feature so that the Switch does not drop the packet. Users may configure the action that the Switch takes when it receives a packet with existing option 82 information by configuring the DHCP Agent Information Option 82 Policy.

The Implementation of DHCP Relay Agent Information Option 82

The **DHCP Relay Option 82** command configures the DHCP relay agent information option 82 setting of the Switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:

NOTE: For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

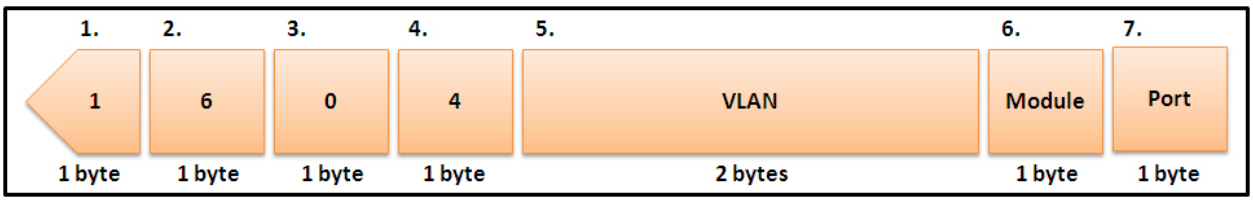


Figure 10-2 Circuit ID sub-option format

1. Sub-option type
2. Length
3. Circuit ID type
4. Length
5. VLAN: the incoming VLAN ID of DHCP client packet.
6. Module: For a standalone switch, the Module is always 0; for a stackable switch, the Module is the Unit ID.
7. Port: The incoming port number of the DHCP client packet, the port number starts from 1.

Remote ID sub-option format:

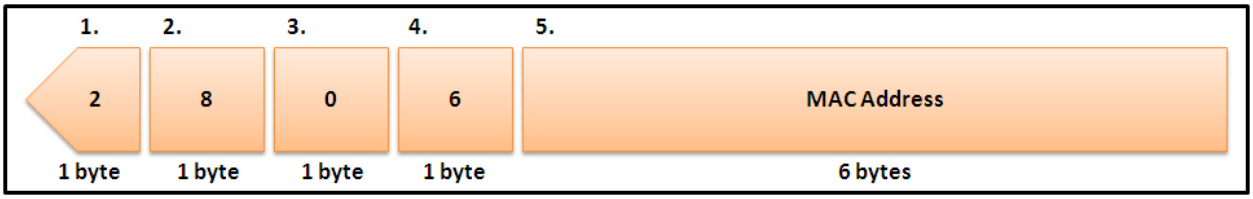


Figure 10-3 Remote ID sub-option format

1. Sub-option type
2. Length
3. Remote ID type
4. Length
5. MAC address: The Switch's system MAC address.

DHCP Relay Interface Settings

Users can set up a server, by IP address, for relaying DHCP information to the DHCP Server. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP client using this window. Properly configured settings will be displayed in the DHCP Relay Interface Table at the bottom of the window, once the user clicks the **Apply** button. The user may add up to four server IP addresses per IP interface on the Switch. Entries may be deleted by clicking the corresponding **Delete** button.

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

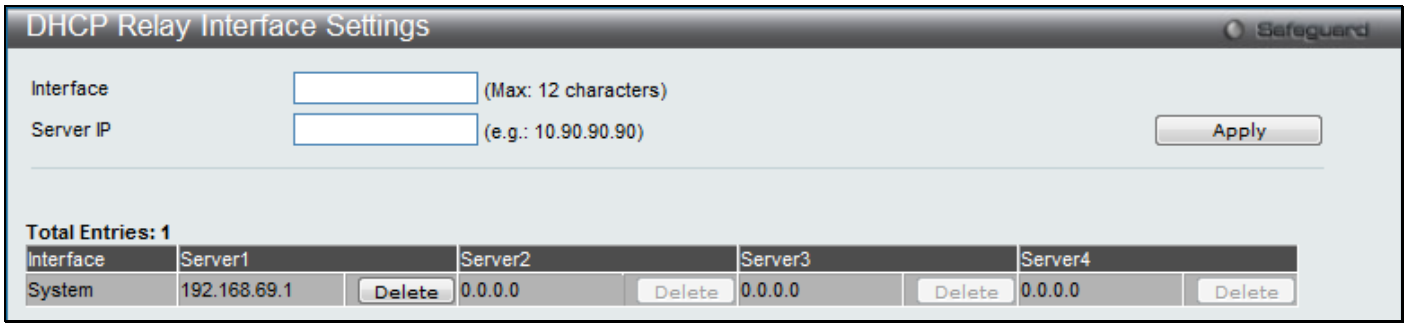


Figure 10-4 DHCP Relay Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface	The IP interface on the Switch that will be connected directly to the client.
Server IP	Enter the IP address of the DHCP server. Up to four server IPs can be configured per IP Interface.

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

DHCP Relay Option 60 Server Settings

On this page the user can configure the DHCP relay option 60 server parameters.

To view the following window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Server Settings**, as shown below:

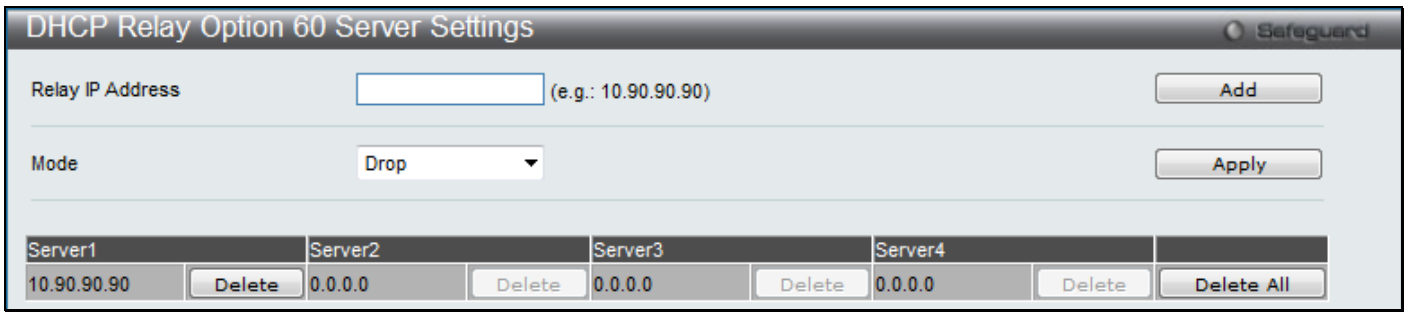


Figure 10-5 DHCP Relay Option 60 Server Settings window

The fields that can be configured are described below:

Parameter	Description
Relay IP Address	Here the user can enter the Relay IP Address.
Mode	Here the user can choose the DHCP Relay Option 60 Server mode.

Click the **Add** button to add a new entry based on the information entered.
Click the **Apply** button to accept the changes made.
Click the **Delete** button to remove the specific entry.
Click the **Delete All** button to remove all the entries listed.

NOTE: When there is no matching server found for the packet based on option 60, the relay servers will be determined by the default relay server setting.

DHCP Relay Option 60 Settings

This option decides whether the DHCP Relay will process the DHCP option 60 or not

To view the following window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings**, as shown below:

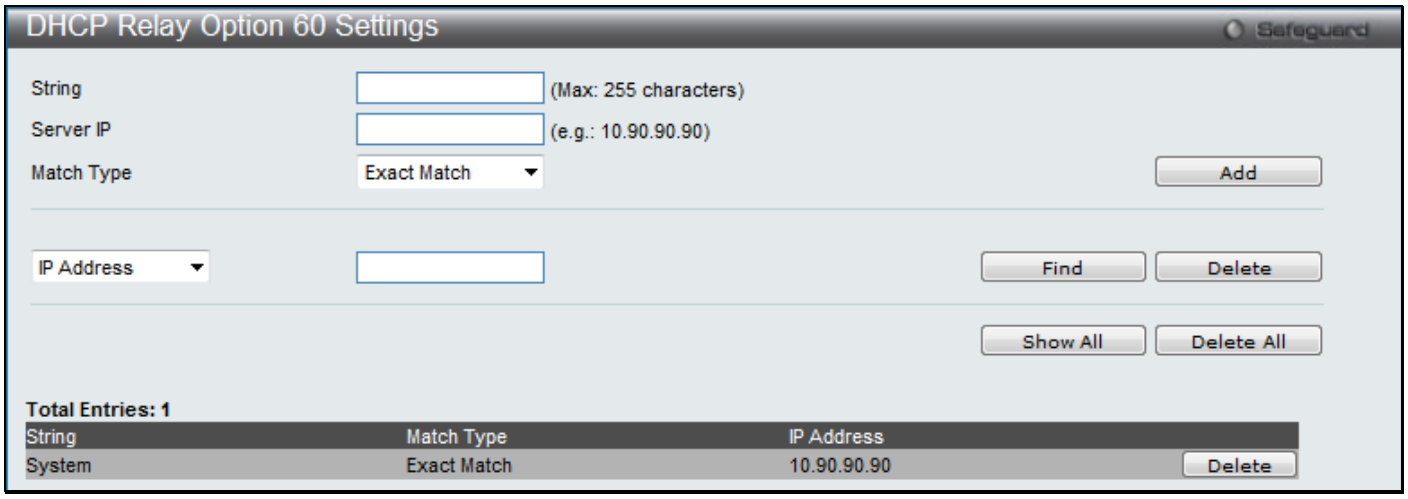


Figure 10-6 DHCP Relay Option 60 Settings window

The fields that can be configured are described below:

Parameter	Description
String	Here the user can enter the DHCP Relay Option 60 String value. Different strings can be specified for the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.
Server IP	Here the user can enter the DHCP Relay Option 60 Server IP address.
Match Type	Here the user can enter the DHCP Relay Option 60 Match Type value. *Exact Match* – The option 60 string in the packet must full match with the specified string. *Partial Match* – The option 60 string in the packet only need partial match with the specified string.
IP Address / String	Here the user can select *IP Address* or *String* from the drop-down menu. *IP Address* - Enter the DHCP Relay Option 60 IP address in the field next to the drop-down menu. *String* - Enter the DHCP Relay Option 60 String value in the field next to the drop-down menu.

Click the **Add** button to add a new entry based on the information entered.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Delete** button to remove the specific entry based on the information entered.
Click the **Show All** button to display all the existing entries.
Click the **Delete All** button to remove all the entries listed.
Click the **Delete** button to remove the specific entry.

DHCP Relay Option 61 Settings

On this page the user can configure, add and delete DHCP relay option 61 parameters.

To view the following window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Option 61 Settings**, as shown below:

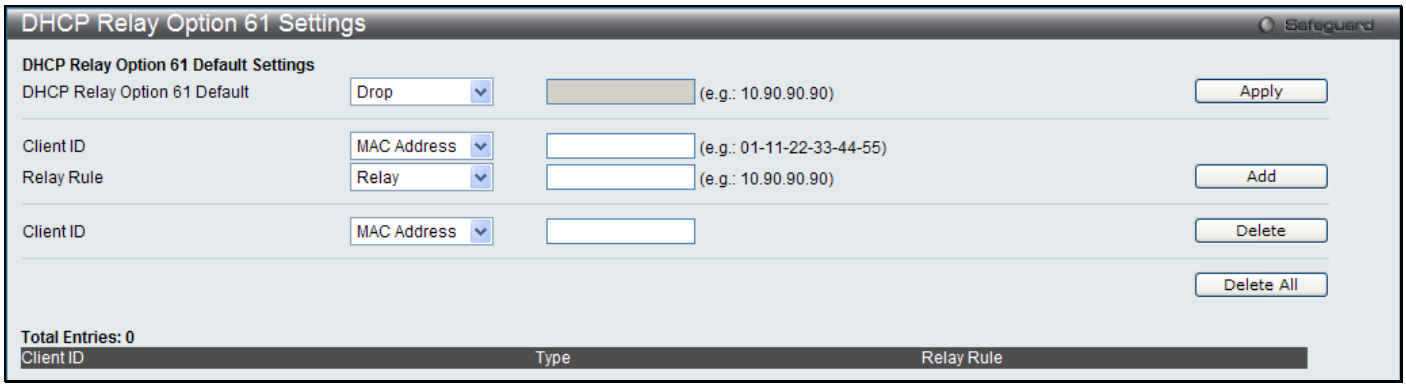


Figure 10-7 DHCP Relay Option 61 Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Relay Option 61 Default	Here the user can select the DHCP Relay Option 61 default action. *Drop* – Specify to drop the packet. *Relay* – Specify to relay the packet to an IP address. Enter the IP Address of the default relay server. When there is no matching server found for the packet based on option 61, the relay servers will be determined by this default relay server setting.
Client ID	*MAC Address* – The client's client-ID which is the hardware address of client. *String* – The client's client-ID, which is specified by administrator.
Relay Rule	*Drop* – Specify to drop the packet. *Relay* – Specify to relay the packet to an IP address.
Client ID	*MAC Address* – The client's client-ID which is the hardware address of client. *String* – The client's client-ID, which is specified by administrator.

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 specific entry based on the information entered.

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

DHCP Server

DHCP, or Dynamic Host Configuration Protocol, allows the switch to delegate 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 returns a response to the client, containing the previously mentioned IP information that the DHCP client then utilizes and sets on its local configurations.

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 allotted IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the pool 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 keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address.

DHCP Server Global Settings

On this page the user can configure the DHCP server global parameters.

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

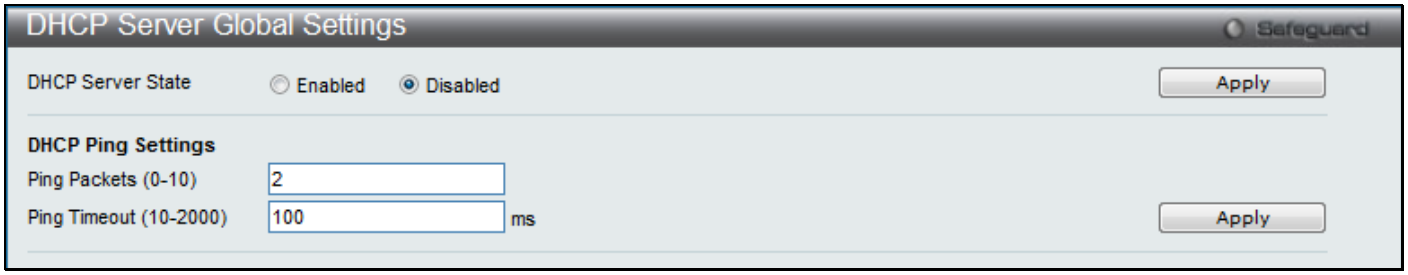


Figure 10-8 DHCP Server Global Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Server State	Here the user can enable or disable the DHCP Server State.
Ping Packets (0-10)	Here the user can choose the numbers of ping packet 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. 0 means there is no ping test. The default value is 2.
Ping Timeout (10-2000)	Here the user can choose the amount of time the DHCP server must waits before timing out a ping packet. The default value is 100.

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

DHCP Server Exclude Address Settings

The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. You must use this page to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.

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

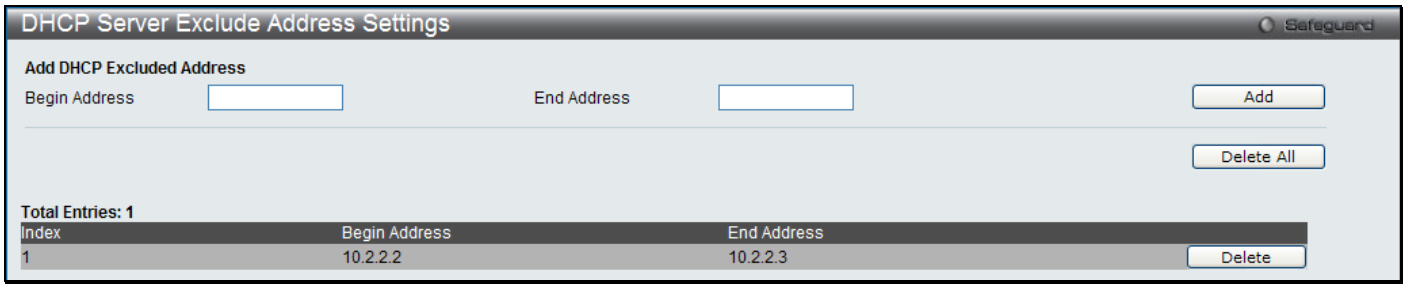


Figure 10-9 DHCP Server Exclude Address Settings window

The fields that can be configured are described below:

Parameter	Description
Begin Address	Here the user can enter the starting IP Address.
End Address	Here the user can enter the ending IP Address.

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

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

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

DHCP Server Pool Settings

On this page the user can add and delete the DHCP server pool.

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

Figure 10-10 DHCP Server Pool Settings window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Here the user can enter the DHCP Server Pool name.

Click the **Add** button to add a new entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.
Click the **Edit Class** to configure the DHCP pool class.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

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

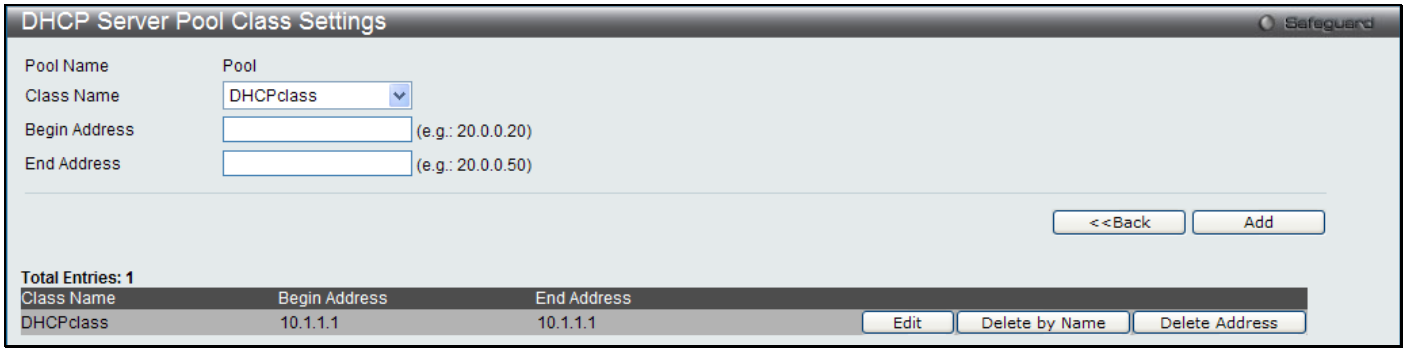


Figure 10-11 DHCP Server Pool Class Settings - Edit Class window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select a DHCP's class name. The DHCP's class name can be configured in DHCP Server Class Settings window.
Begin Address	Enter the beginning IP address of the range.
End Address	Enter the end IP address of the range.

Click the **<<Back** button to discard the changes made and return to the previous page.
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 by Name** button to remove the entries with the same class name.
Click the **Delete Address** button to remove the Begin Address and End Address of the specific entry.

After clicking the **Edit** button, the following page will appear:

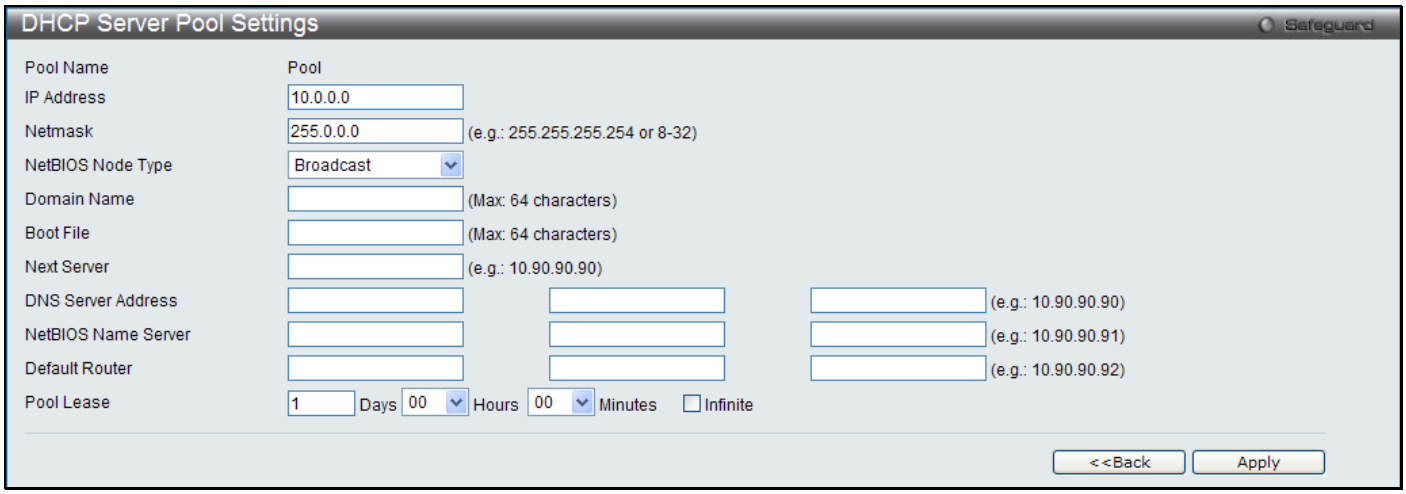


Figure 10-12 DHCP Server Pool Settings –Edit window

The fields that can be configured are described below:

Parameter	Description
IP Address	Here the user can enter the network address of the pool.
Netmask	Here the user can enter the Netmask for the network address.
NetBIOS Node Type	NetBIOS node type for a Microsoft DHCP client.
Domain Name	Domain name of client. The domain name configured here will be used as the default domain name by the client.
Boot File	File name of boot image. The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. If this option is input twice for the same pool, the second command will overwrite the first command. If the boot file is not specified, the boot file information will not be provided to the client.
Next Server	Here the user can enter the next server IP address.
DNS Server Address	IP address of DNS server. Specifies the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified in one command line.
NetBIOS Name Server	IP address of WINS server. Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. Up to three IP addresses can be specified in one command line.
Default Router	IP address of default router. Specifies the IP address of the default router for a DHCP client. Up to three IP addresses can be specified in one command line.
Pool Lease	By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid. Tick the **Infinite** check box to have unlimited lease. *Days* – Days of lease. *Hours* – Hours of lease. *Minutes* – Minutes of lease.

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

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

DHCP Server Class Settings

This window is used to configure DHCP server class settings

To view the following window, click **Network Application > DHCP > DHCP Server > DHCP Server Class Settings**, as shown below:

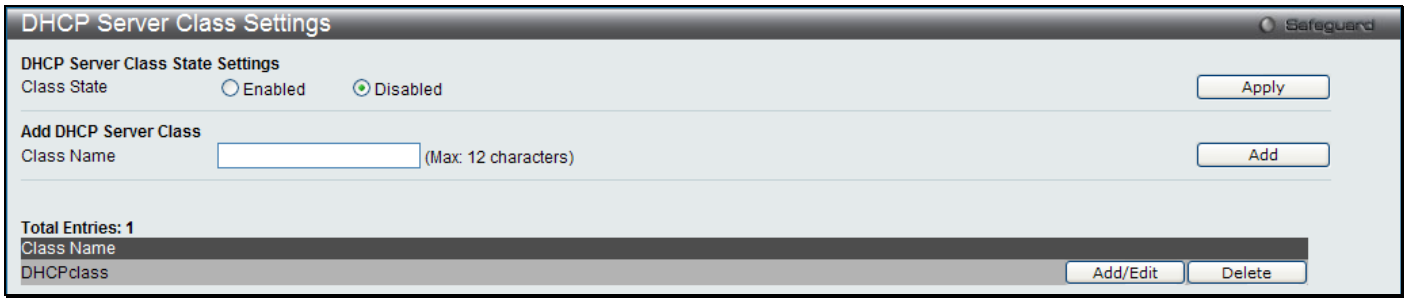


Figure 10-13 DHCP Server Class Settings window

The fields that can be configured are described below:

Parameter	Description
Class State	Click to enable or disable the DHCP server class state.
Class Name	Enter the DHCP server's class name.

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 **Add/Edit** button to configure the specific DHCP class options.
Click the **Delete** button to remove the specific entry.

After clicking the **Add/Edit** button, the following page will appear:

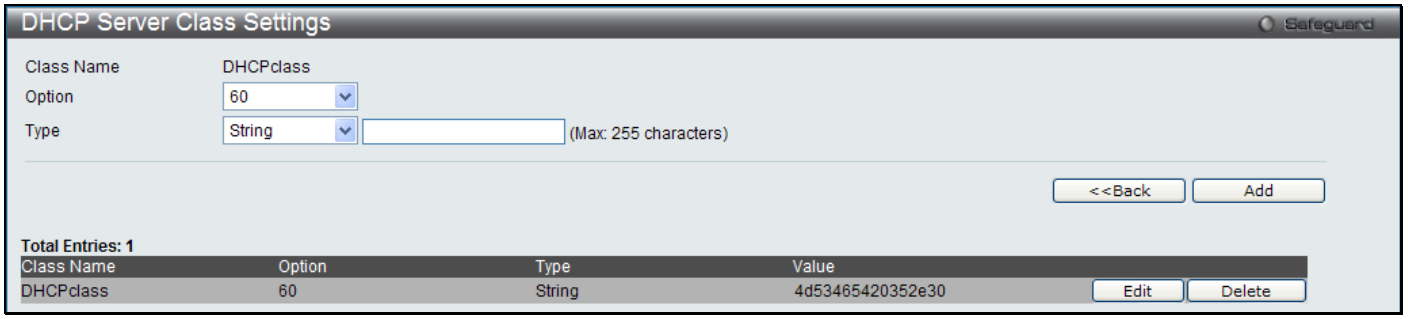


Figure 10-14 DHCP Server Class Settings - Add/Edit window

The fields that can be configured are described below:

Parameter	Description
Option	Use the drop-down menu to select DHCP class options.
Type	Use the drop-down menu to select the options type and enter the value of the type.

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

DHCP Server Manual Binding

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server. The dynamic binding entry will be created when an IP address is assigned to the client from the pool network's address.

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

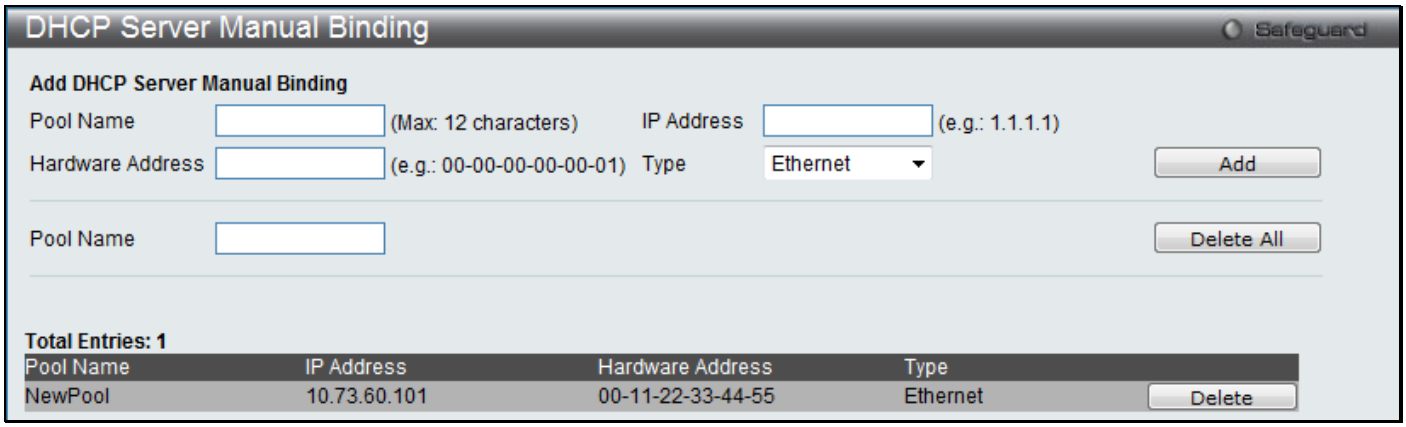


Figure 10-15 DHCP Server Manual Binding window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Here the user can enter the DHCP Server Pool name.
IP Address	IP address which will be assigned to specified client.
Hardware Address	Here the user can enter the hardware address.
Type	Either Ethernet or IEEE802 can be specified.

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

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

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

DHCP Server Dynamic Binding

On this page the user can delete the DHCP server dynamic binding table.

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

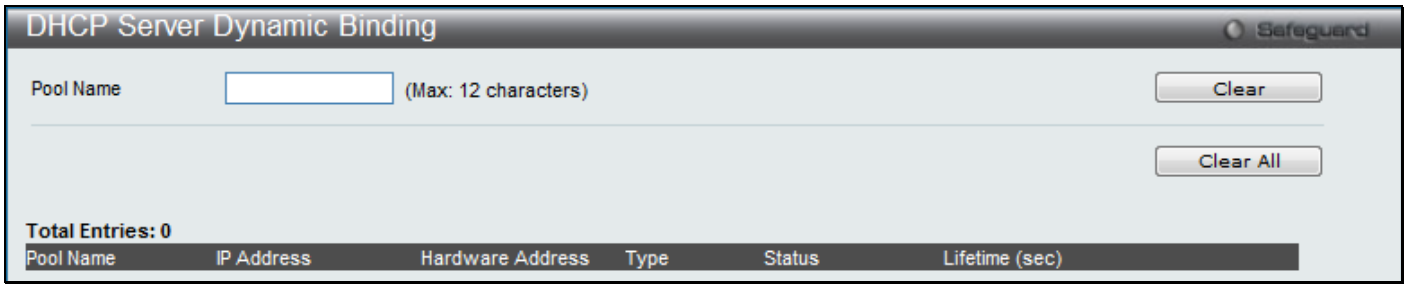


Figure 10-16 DHCP Server Dynamic Binding window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Here the user can enter the DHCP Server Pool name.

Click the **Clear** button to clear all the information entered in the fields.

Click the **Clear All** button to remove all the entries listed in the table.

DHCP Conflict IP

The DHCP server will use PING packet to determine whether an IP address is conflict with other host before binding this IP. The IP address which has been identified conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.

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

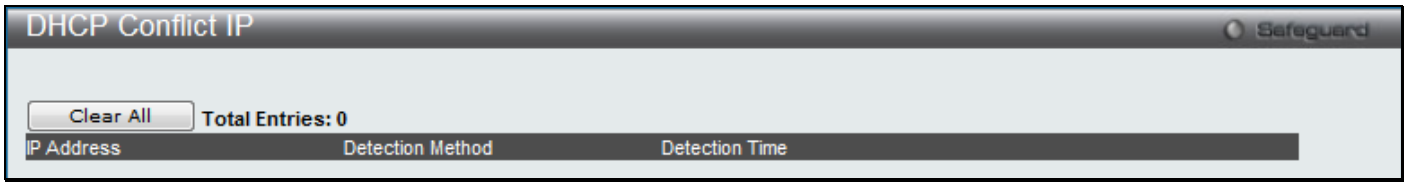


Figure 10-17 DHCP Conflict IP window

Click the **Clear All** button to remove all the entries listed in the table.

DHCP Local Relay Settings

The DHCP local relay settings allows the user to add option 82 into DHCP request packets when the DHCP local relay is enabled in the VLAN which received the DHCP request. If the DHCP local relay settings are not configured, the Switch will flood the packets to the VLAN. In order to add option 82 into the DHCP request packets, the DHCP local relay settings and the state of the Global VLAN need to be enabled.

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

Figure 10-18 DHCP Local Relay Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Local Relay Global State	Enable or disable the DHCP Local Relay Global State. The default is Disabled.
VLAN Name	This is the VLAN Name that identifies the VLAN the user wishes to apply the DHCP Local Relay operation.
State	Enable or disable the configure DHCP Local Relay for VLAN state.

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

DHCPv6 Relay

DHCPv6 Relay Global Settings

This window is used to configure the DHCPv6 relay function on the Switch.

To view this window, click **Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings** as shown below:

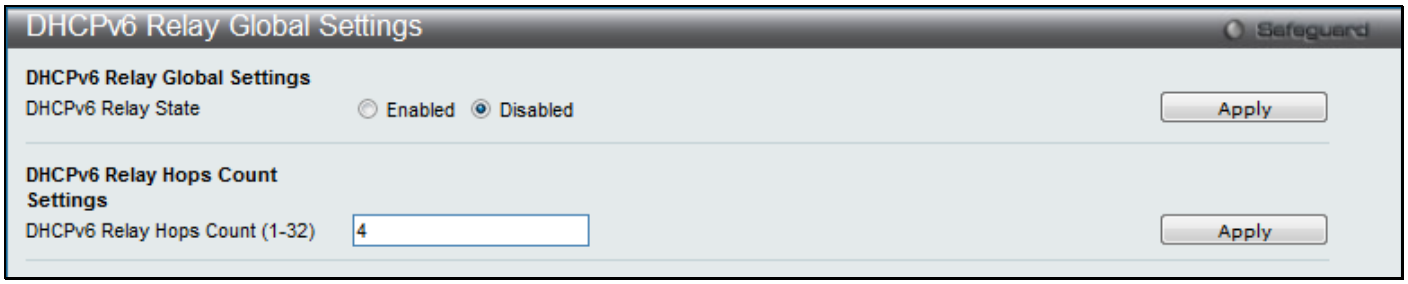


Figure 10-19 DHCPv6 Relay Global Settings window

The fields that can be configured are described below:

Parameter	Description
DHCPv6 Relay State	Click the radio buttons to enable or disable the DHCPv6 relay function.
DHCPv6 Relay Hops Count (1-32)	Enter the number of relay agents that have to be relayed in this message. The default value is *4*.

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

DHCPv6 Relay Settings

This window is used to configure the DHCPv6 relay state of one or all of the specified interfaces, and add or display a destination IPv6 address to or from the switch's DHCPv6 relay table.

To view this window, click **Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Settings** as shown below:

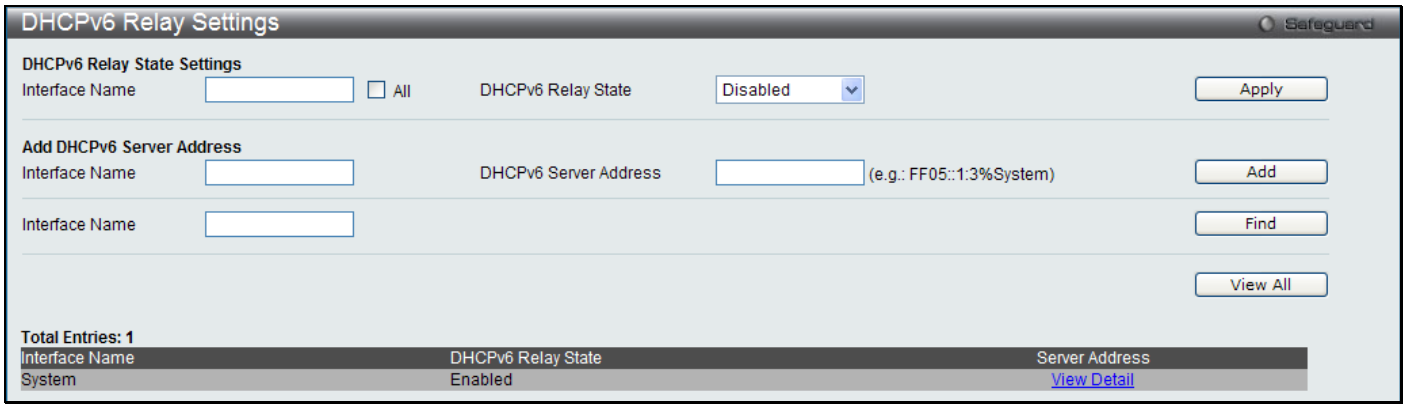


Figure 10-20 DHCPv6 Relay Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IPv6 interface. Tick the **All** check box to select all IPv6 interfaces.
DHCPv6 Relay State	Use the drop-down menu to enable or disable the DHCPv6 relay state of the interface.
DHCPv6 Server Address	Enter the DHCPv6 server IPv6 address.

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 **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the View Detail link to view more information regarding the specific entry.

After clicking the View Detail link, the following page will appear:

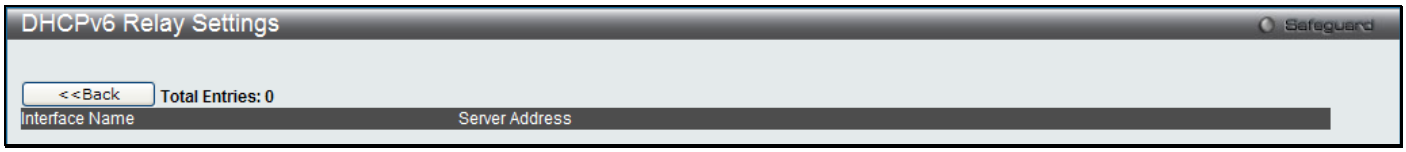


Figure 10-21 DHCPv6 Relay Settings - View Detail window

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

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 and 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 returns the address of the next DNS server the client should contact.

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 Relay

DNS Relay Global Settings

On this page the user can configure the DNS Relay global parameters.

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

Figure 10-22 DNS Relay Global Settings window

The fields that can be configured are described below:

Parameter	Description
DNS Relay State	Here the user can enable or disable the DNS relay state.
Primary Name Server	Here the user can enter the primary DNS server IP address.
Secondary Name Server	Here the user can enter the secondary DNS server IP address.
DNS Relay Cache State	Here the user can enable or disable the DNS relay cache state.
DNS Relay Static Table State	Here the user can enable or disable the DNS relay static table state.

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

DNS Relay Static Settings

Users can add or delete static entries into the switch's DNS resolution table.

To view the following window, click **Network Application > DNS > DNS Relay > DNS Relay Static Settings**, as shown below:

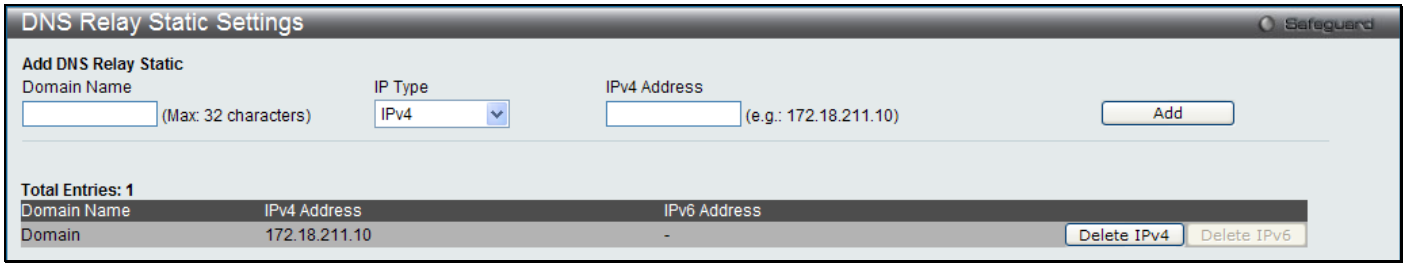


Figure 10-23 DNS Relay Static Settings window

The fields that can be configured are described below:

Parameter	Description
Domain Name	Here the user can enter the domain name.
IP Type	Use the drop-down menu to select using *IPv4* or *IPv6* address.
IPv4/IPv6 Address	Here the user can enter the IP address for the specified domain name.

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

Click the **Delete IPv4** button to remove the IPv4 address.

Click the **Delete IPv6** button to remove the IPv6 address.

PPPoE Circuit ID Insertion Settings

When the setting is enabled, the system will insert the circuit ID tag to the received PPPoE discover and request packet if the tag is absent, and remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The insert circuit ID will contain the following information: Client MAC address, Device ID and Port number.

By default, Switch IP address is used as the device ID to encode the circuit ID option.

To view the following window, click **Network Application > PPPoE Circuit ID Insertion Settings**, as shown below:

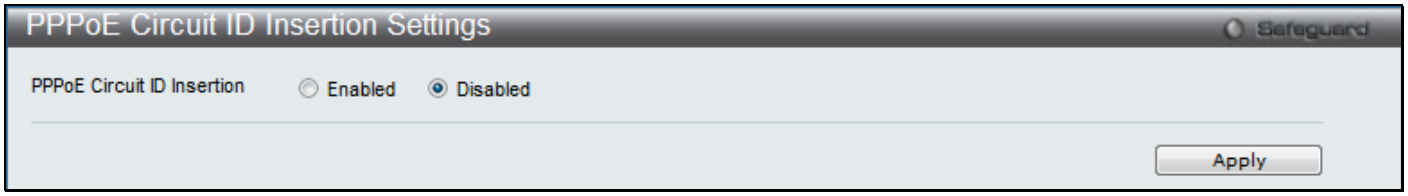


Figure 10-24 PPPoE Circuit ID Insertion Settings window

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

RCP Server Settings

This page is used to configure global RCP server information. This global RCP Server setting can be used when the Server or remote user name is not specified. Only **ONE** RCP server can be configured per system. If user does not specify the RCP Server in the CLI command, and global RCP Server was not configured, the Switch will ask user to input the Server IP address or remote user name while executing the RCP commands.

To view the following window, click **Network Application > RCP Server Settings**, as shown below:

Figure 10-25 RCP Server Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	The IP address of global RCP Server. By default, the server is unspecified.
User Name	The remote user name for logon into global RCP Server. By default, global server's remote user name is unspecified.

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.

SMTP Settings

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered in the window below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the

management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events, and enhancing security by recording questionable events occurring on the Switch.

Users can set up the SMTP server for the Switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

The Switch will send out e-mail to recipients when one or more of the following events occur:

- When a cold start occurs on the Switch.
- When a port enters a link down status.
- When a port enters a link up status.
- When SNMP authentication has been denied by the Switch.
- When a switch configuration entry has been saved to the NVRAM by the Switch.
- When an abnormality occurs on TFTP during a firmware download event. This includes in-process, invalid-file, violation, file-not-found, complete and time-out messages from the TFTP server.
- When a system reset occurs on the Switch.

Information within the e-mail from the SMTP server regarding switch events includes:

- The source device name and IP address.
- A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.
- The event that occurred on the Switch, prompting the e-mail message to be sent.
- When an event is processed by a user, such as save or firmware upgrade, the IP address, MAC address and User Name of the user completing the task will be sent along with the system message of the event occurred.
- When the same event occurs more than once, the second mail message and every repeating mail message following will have the system's error message placed in the subject line of the mail message.

The following details events occurring during the Delivery Process.

- Urgent mail will have high priority and be immediately dispatched to recipients while normal mail will be placed in a queue for future transmission.
- The maximum number of un-transmitted mail messages placed in the queue cannot exceed 30 messages. Any new messages will be discarded if the queue is full.
- If the initial message sent to a mail recipient is not delivered, it will be placed in the waiting queue until its place in the queue has been reached, and then another attempt to transmit the message is made.• The maximum attempts for delivering mail to recipients is three. Mail message delivery attempts will be tried every five minutes until the maximum number of attempts is reached. Once reached and the message has not been successfully delivered, the message will be dropped and not received by the mail recipient.
- If the Switch shuts down or reboots, mail messages in the waiting queue will be lost.

To view the following window, click **Network Application > SMTP Settings**, as shown below:

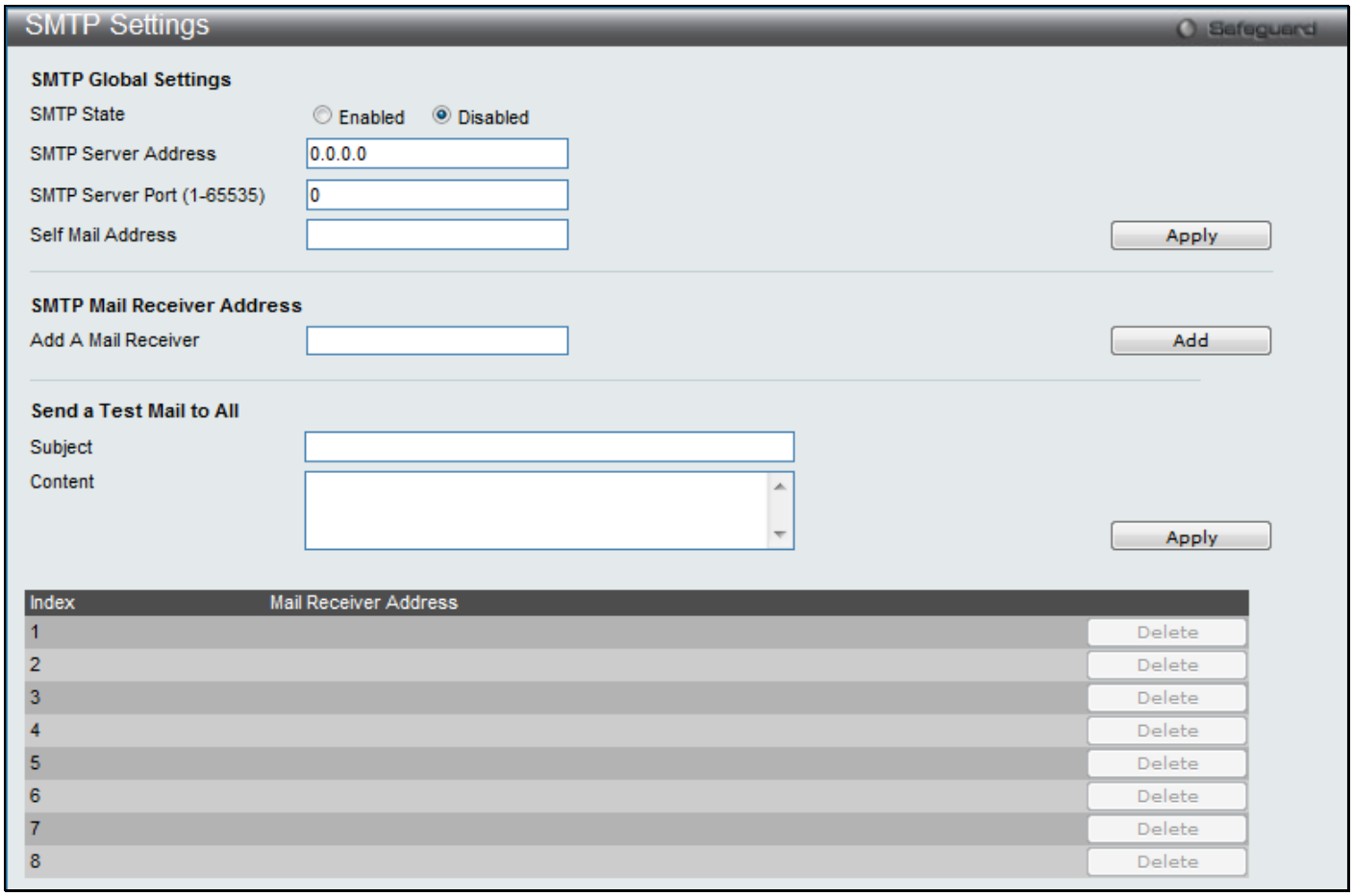


Figure 10-26 SMTP Settings window

The fields that can be configured are described below:

Parameter	Description
SMTP State	Use the radio button to enable or disable the SMTP service on this device.
SMTP Server Address	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port (1-65535)	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is *25*, yet a value between *1* and *65535* can be chosen.
Self Mail Address	Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self-mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters.
Add A Mail Receiver	Enter an e-mail address and click the **Add** button. Up to eight e-mail addresses can be added per Switch. To delete these addresses from the Switch, click the corresponding **Delete** button in the SMTP Mail Receiver Address table at the bottom of the window.
Subject	The subject of the test mail.
Content	The content of the test mail.

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

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

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

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.

SNTP Settings

Users can configure the time settings for the Switch.

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

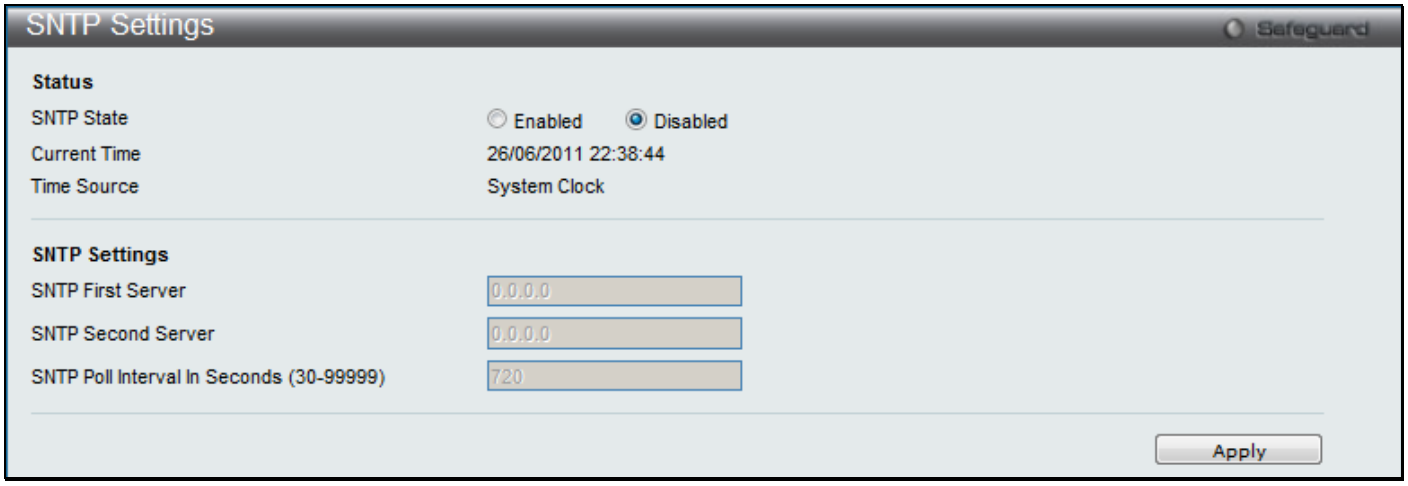


Figure 10-27 SNTP Settings window

The fields that can be configured or displayed are described below:

Parameter	Description
SNTP State	Use this radio button to enable or disable SNTP.
Current Time	Displays the Current Time.
Time Source	Displays the time source for the system.
SNTP First Server	The IP address of the primary server from which the SNTP information will be taken.
SNTP Second Server	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval In Seconds (30-99999)	The interval, in seconds, between requests for updated SNTP information.

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

Time Zone Settings

Users can configure time zones and Daylight Savings Time settings for SNTP.

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

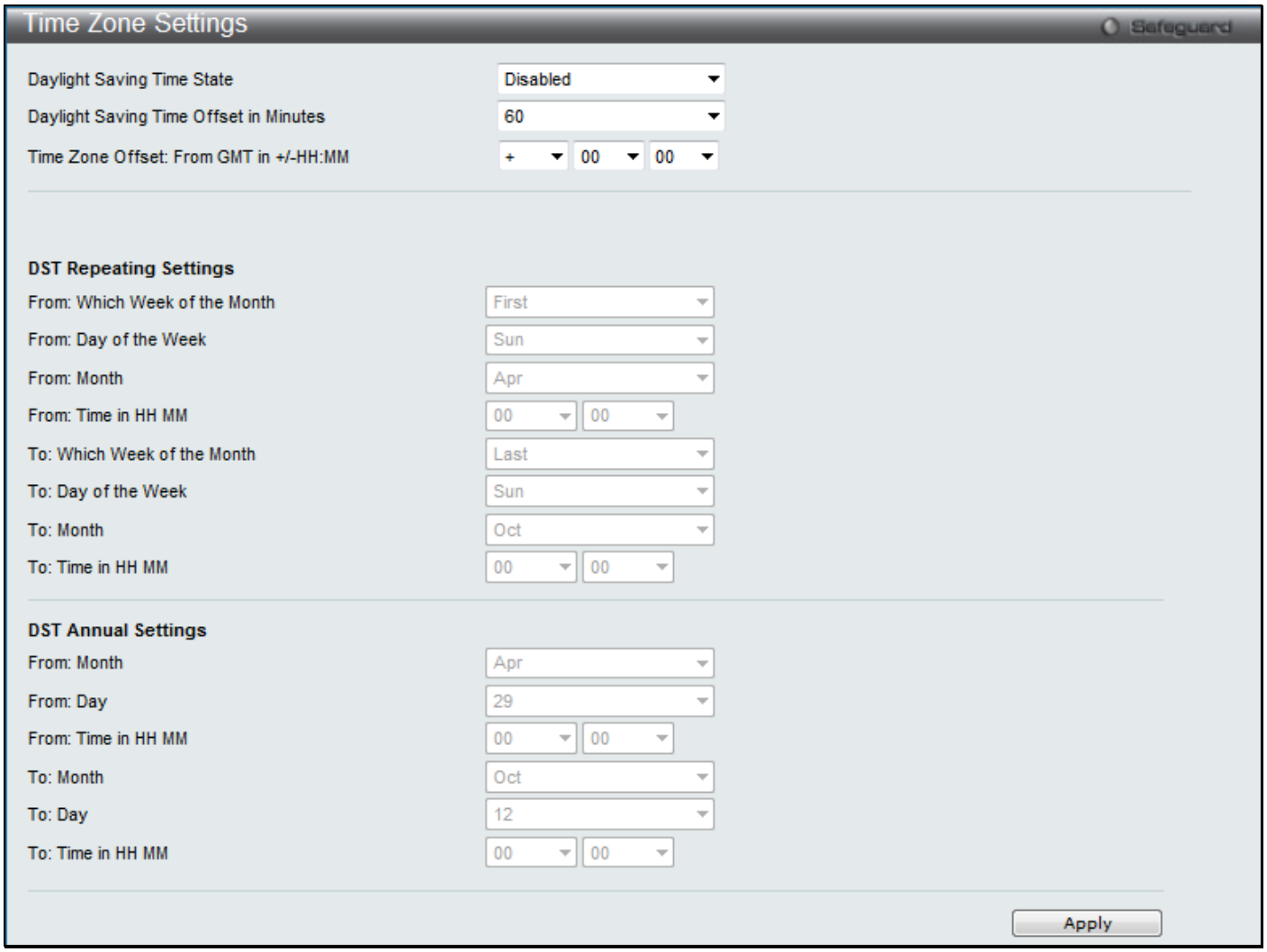


Figure 10-28 Time Zone Settings window

The fields that can be configured are described below:

Parameter	Description
Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset In Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset – *30*, *60*, *90*, or *120* minutes.
Time Zone Offset From GMT In +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT).

Parameter	Description
DST Repeating Settings	Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.
From: Which Week Of The Month	Enter the week of the month that DST will start.
From: Day Of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: Time In HH:MM	Enter the time of day that DST will start on.

To: Which Week Of The Month	Enter the week of the month the DST will end.
To: Day Of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: Time In HH:MM	Enter the time DST will end.

Parameter	Description
DST Annual Settings	Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the month DST will start on, each year.
From: Time In HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the month DST will end on, each year.
To: Time In HH:MM	Enter the time of day that DST will end on, each year.

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

Flash File System Settings

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 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.

In case the file system gets corrupted, Z-modem can be used to download the backup files directly to the system.

To view the following window, click **Network Application > Flash File System Settings**, as shown below:

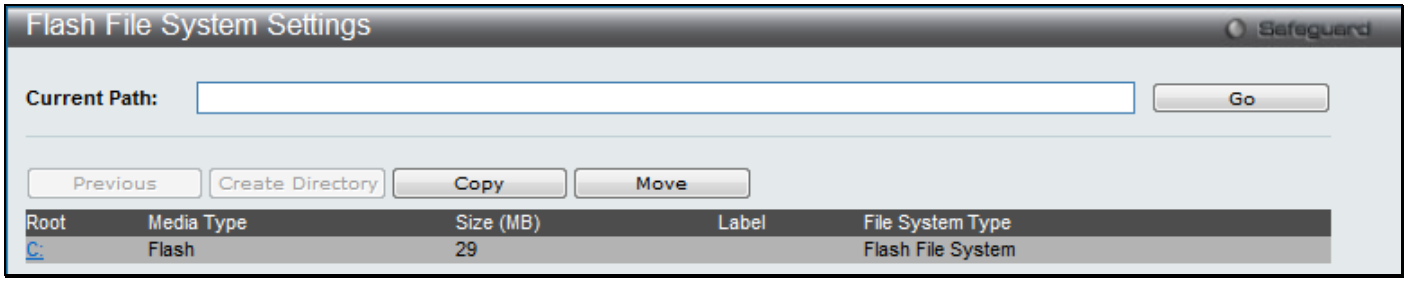


Figure 10-29 Flash File System Settings window

Enter the **Current Path** string and click the **Go** button to navigate to the path entered.
Click the C: link to navigate the C: drive

After clicking the C: link button, the following page will appear:

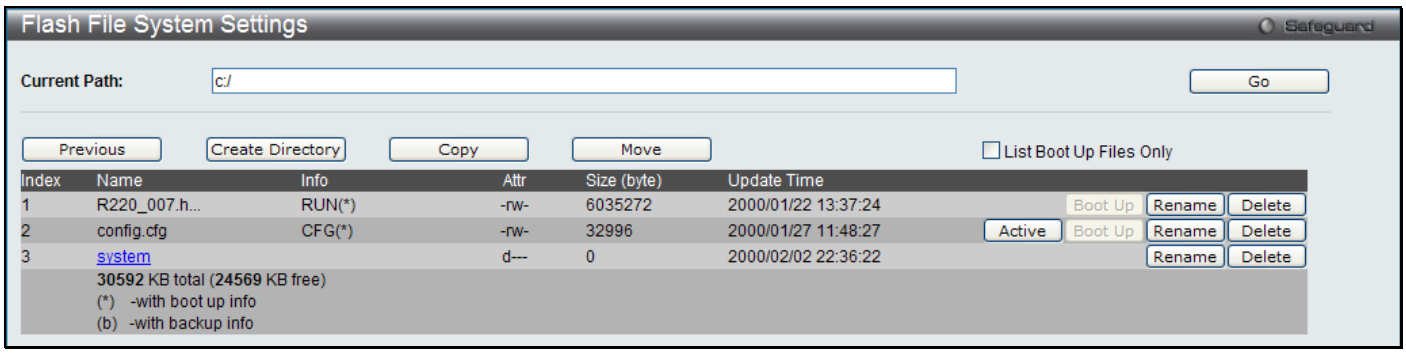


Figure 10-30 Flash File System Settings window

Click the **Previous** button to return to the previous page.
Click the **Create Directory** to create a new directory within the file system of the switch.
Click the **Copy** button to copy a specific file to the switch.
Click the **Move** button to move a specific file within the switch.
Tick the **List Boot Up Files Only** option to display only the boot up files.

Click the **Active** button to set a specific config file as the active runtime configuration.
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 page will appear:

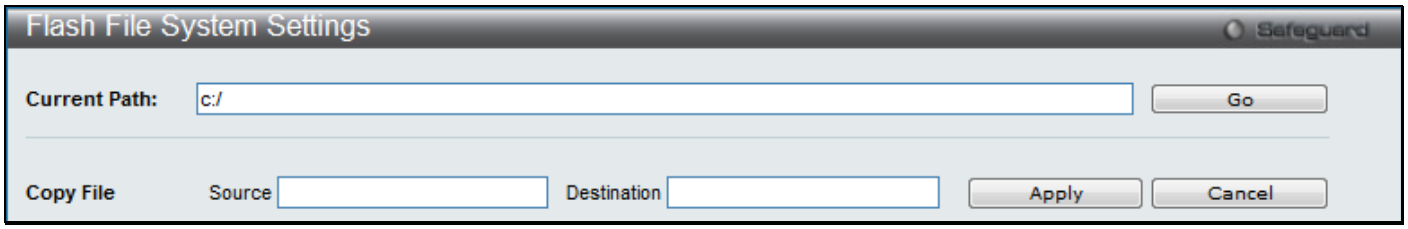


Figure 10-31 Flash File System Settings window

When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path.
Click the **Apply** button to initiate the copy.
Click the **Cancel** button the discard the process.

After clicking the **Move** button, the following page will appear:

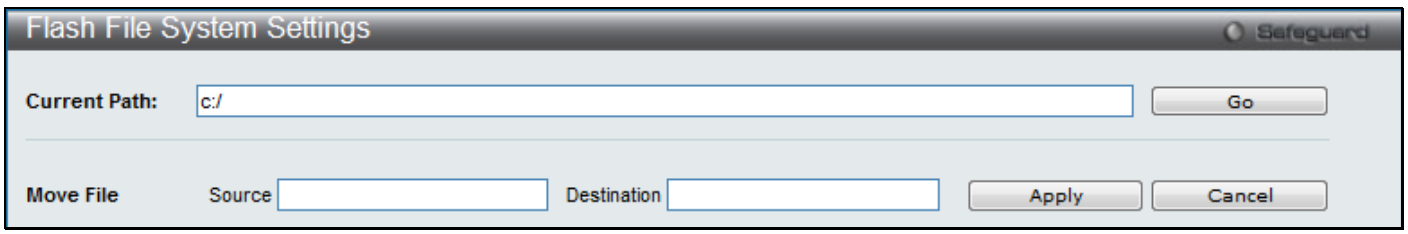


Figure 10-32 Flash File System Settings window

When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path.
Click the **Apply** button to initiate the copy. Click the **Cancel** button the discard the process.

Chapter 11 OAM

CFM
Ethernet OAM
DULD Settings
Cable Diagnostics

CFM

Connectivity Fault Management (CFM) or Ethernet Connectivity Fault Management is an end-to-end Ethernet layer OAM protocol. CFM is defined by IEEE 802.1ag and includes connectivity monitoring, fault notification and means of isolating faults on large Ethernet metropolitan-area networks (MANs) and WANs.

Ethernet has traditionally operated on isolated enterprise LANs. As Ethernet has been expanded to operate on the much larger scale carrier networks that encompass multiple administrative domains, the demands of the much larger and more complex networks required a new set of OAM capabilities. Since these larger scale networks have a very large user base, carry more diversified network applications and typically span a much larger geographical area than traditional enterprise Ethernet LANs where link uptime is crucial, a means of dealing with connectivity faults able to operate in Ethernet became necessary. Since none of the existing OAM protocols could adequately address this new circumstance, Ethernet Connectivity Fault Management has been developed in order to meet the new operational management needs created by the application of Ethernet technologies to MANs and WANs.

Ethernet CFM provides Ethernet network service providers with various benefits such as end-to-end service-level OAM and lower operating expenses, all operated on top of a familiar Ethernet platform.

CFM introduces some new terms and concepts to Ethernet, these are briefly described below.

Maintenance Domain

A maintenance domain is generic term referring to a management area created for the purpose of managing and administering a network. A maintenance domain is operated by a single entity or “owner” and defined by a boundary with a set of ports internal to this boundary.

An Ethernet CFM maintenance domain, referred to in this manual simply as an MD, exists in a hierarchical relationship to other MDs. Typically a large MAN or WAN can be partitioned into a hierarchy based on the size of domain that mirrors the structural relationship of customers, service providers and operators. The service providers have end-to-end service responsibility while operators provide service transport across sub-networks. The hierarchy is defined by a maintenance level value ranging from 0 to 7 where 7 is the highest level and 0 the lowest level. The larger the MD is, the higher its maintenance level will be. For example, if the customer domain is the largest MD, it should be assigned a maintenance level of 7, the operator MD being the smallest, receives a maintenance level of 0 with the service provider domain being in between these values. Maintenance levels are manually assigned by the network administrator. All levels of the MD hierarchy must operate together.

Nesting of MDs is allowed, however they cannot intersect since this violates the requirement that management of MDs be done by a single owner. If two or more domains are nested, the outer domain must be assigned a higher maintenance level than the nested domains.

CFM operations and message exchanges are conducted on a per-domain basis. This means for example, that CFM operating at level 3 does not allow discovery of the level 3 network by higher levels.

Maintenance Association

A maintenance association (MA) in CFM is a set of MEPs that have been configured with the same management domain level and maintenance association identifier (MAID).

Different MAs in an MD must have different MA Names. Different MAs in different MDs may have the same MA Name. The MEP list specified for a MA can be located in different devices. MEPs must be created on ports of these devices explicitly. A MEP will transmit CCM packets periodically across the MA. The receiving MEP will verify these received CCM packets from other MEPs against this MEP list for configuration integrity check.

Maintenance Point

A maintenance point in CFM is a point of demarcation on a port within a maintenance domain. Maintenance points filter CFM frames within the boundaries of an MD by dropping frames that do not belong to the correct maintenance level. There are two types of maintenance points, **Maintenance Endpoints** (MEPs) and **Maintenance Intermediate Points** (MIPs). MEPS and MIP are manually configured by a network administrator.

A MEP exists at the edge of a maintenance domain, defining the boundary of the MD. MEP functions include filtering CFM messages so that they are confined to the MD. A MEP can be configured to transmit Connectivity Check Messages (CCMs) and will transmit traceroute and loopback messages if configured to do so. A MEP can be Inward facing or Outward facing.

An Inward facing MEP source CFM frames toward the bridge relay function, not through the bridge port on which the MEP is configured. An Inward facing MEP drops all CFM frames at its level or lower that are received from the Inward side; and forwards all CFM frames at a higher level regardless of the origin of the frame, Inward or Outward. If the port on which the inward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can no longer transmit or receive CFM messages.

An Outward facing MEP source frames toward the bridge port and can only be configured on routed ports. An Outward facing port drops all CFM frames at it level or lower coming from the bridge relay function side. It processes all CFM frames at its level, and drops all CFM frames at a lower level, coming from the bridge port. An Outward facing port forwards all CFM frames at higher levels regardless of which direction the frames come in. If the port on which the outward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can still transmit and receive CFM messages through the bridge port.

A MIP is a maintenance point that is internal to an MD, not at the boundary. A MIP receives CFM frames from other MIPs and from MEPs. These frames are cataloged and forwarded using the bridge relay function and bridge port. All CFM frames at a lower level than the MIP are blocked and dropped regardless of the origin. All CFM frames at a higher level are forwarded regardless of the origin. If the port on which a MIP is configured is blocked by Spanning-Tree Protocol, the MIP cannot receive CFM messages or relay them toward the bridge relay function side. The MIP can, however, receive and respond to CFM messages from the bridge port.

CFM messages include Continuity Check Messages (CCMs), Loopback Messages (LBMs) and Link Trace Messages (LTMs). CFM uses standard Ethernet frames that can be sourced, terminated, processed and relayed by bridges. Routers support limited CFM functions.

Continuity Check Messages (CCMs) are multicast messages exchanged among MEPs. CCMs allow discovery of MEPs for other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a maintenance domain. CCMs are cataloged by MIPs are the same maintenance level and terminated by remote MEPs at the same maintenance level. They are unidirectional (no response solicitation) and carry the status of the port on which the MEP is configured. LBMs are similar to Ping or ICMP messages in that they indicate only whether a destination is reachable and do not allow discovery of each hop.

Link Trace Messages (LTMs) are multicast CFM frames sent by MEPs to identify adjacency relationships with remote MEPs and MIPs at the same maintenance level. The message body of an LTM includes a destination MAC address of a target MEP that terminates the linktrace. When a MIP or MEP receives an LTM, it generates a unicast Link Trace Reply (LTR) to the initiating MEP. It also forwards the LTM to the target MEP destination MAC address. An LTM effectively traces the path to the target MEP or MIP.

Loopback Messages (LBMs) are similar to Ping or ICMP messages in that they indicate only whether a destination is reachable and do not allow the discovery of each hop.

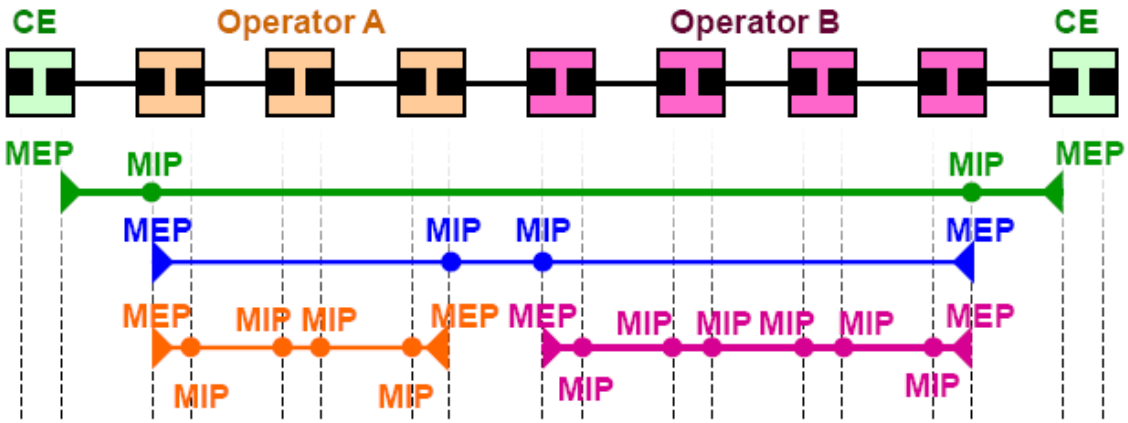


Figure 11-1 OAM Domain Architecture

- Maintenance Association (MA) – Boundaries of an Administrator's scope of monitoring part of the network
- Maintenance Domain (MD) – A level of monitoring within the hierarchy
- Maintenance End Points (MEP) – End Points of the MA or MD
- Maintenance Intermediate Points (MIP) – Intermediate Points within MA or MD
- Customer Equipment (CE).

CFM Settings

On this page the user can configure the CFM parameters.

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

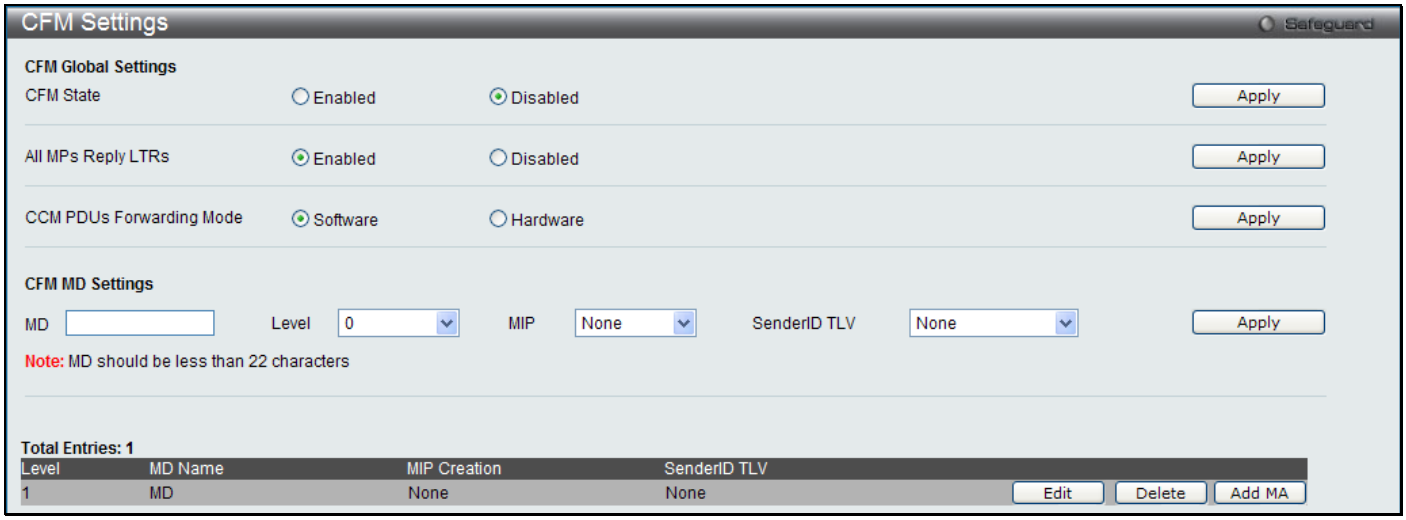


Figure 11-2 CFM Settings window

The fields that can be configured are described below:

Parameter	Description
CFM State	Here the user can enable or disable the CFM feature.
All MPs Reply LTRs	Here the user can enable or disable all MPs to reply LTRs.
CCM PDUs Forwarding Mode	Select the CCM PDU Forwarding mode that will be used. Options to choose from are *Software* and *Hardware*.
MD	Here the user can enter the maintenance domain name.
Level	Here the user can select the maintenance domain level.

MIP	This is the control creations of MIPs. *None* – Don't create MIPs. This is the default value. *Auto* – MIPs can always be created on any ports in this MD, if that port is not configured with a MEP of this MD. For the intermediate switch in a MA, the setting must be auto in order for the MIPs to be created on this device. *Explicit* – MIPs can be created on any ports in this MD, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MD.
SenderID TLV	This is the control transmission of the SenderID TLV. *None* – Don't transmit sender ID TLV. This is the default value. *Chassis* – Transmit sender ID TLV with chassis ID information. *Manage* – Transmit sender ID TLV with managed address information. *Chassis Manage* – Transmit sender ID TLV with chassis ID information and manage address information.

Click the **Apply** button to accept the changes made for each individual section.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

NOTE: The **MD Name** value should be less than 22 characters.

To add a maintenance association (MA), click on the **Add MA** button.

After clicking the **Add MA** button, the following page will appear:

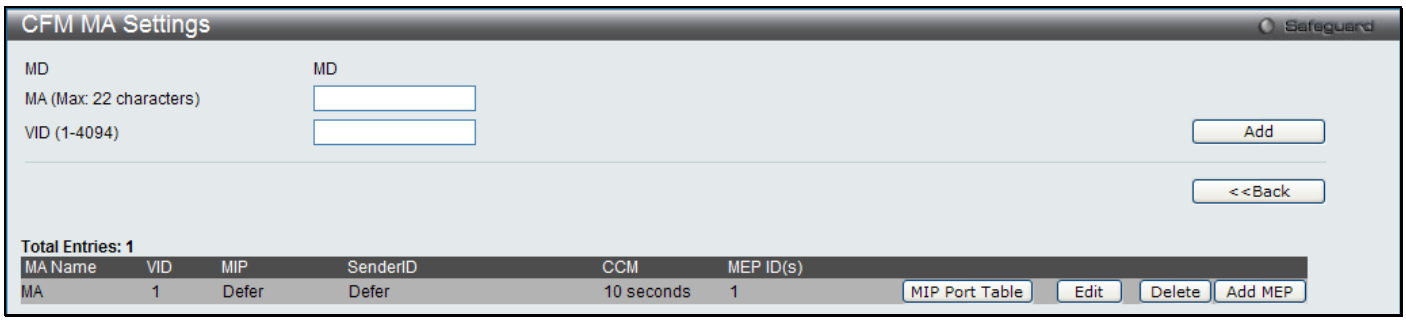


Figure 11-3 CFM MA Settings window

The fields that can be configured are described below:

Parameter	Description
MA	Here the user can enter the maintenance association name.
VID	VLAN Identifier. Different MA must be associated with different VLANs.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.
Click the **MIP Port Table** button to view the CFM MIP Table.
Click the **Add MEP** button to add a Maintenance End Point entry.

After clicking the **Edit** button, the following page will appear:

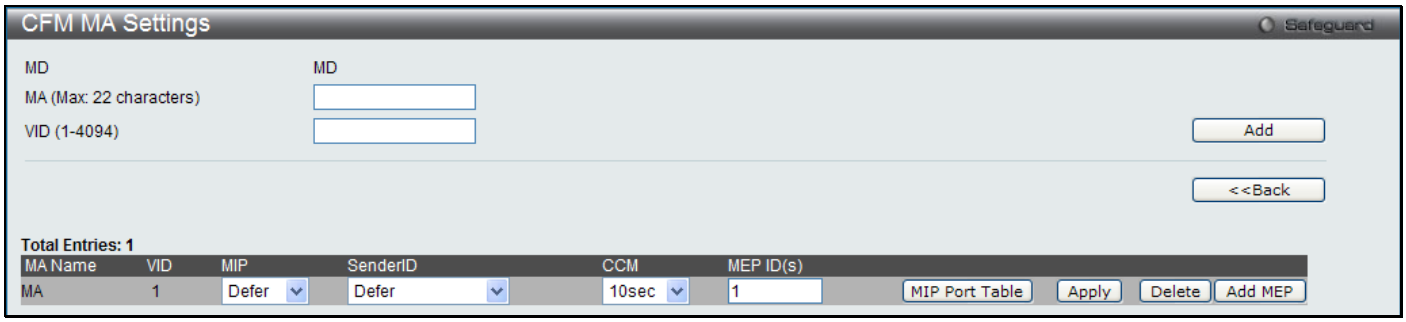


Figure 11-4 CFM MA Settings - Edit window

The fields that can be configured are described below:

Parameter	Description
MIP	This is the control creation of MIPs. *None* - Don't create MIPs. *Auto* - MIPs can always be created on any ports in this MA, if that port is not configured with a MEP of that MA. *Explicit* - MIP can be created on any ports in this MA, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MA. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
SenderID	This is the control transmission of the sender ID TLV. *None* - Don't transmit sender ID TLV. This is the default value. *Chassis* - Transmit sender ID TLV with chassis ID information. *Manage* - Transmit sender ID TLV with manage address information. *Chassis Manage* - Transmit sender ID TLV with chassis ID information and manage address information. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
CCM	This is the CCM interval. *10ms* - 10 milliseconds. Not recommended. For test purpose. *100ms* - 100 milliseconds. Not recommended. For test purpose. *1sec* - One second. *10sec* - Ten seconds. This is the default value. *1min* - One minute. *10min* - Ten minutes.
MEP ID(s)	This is to specify the MEP IDs contained in the maintenance association. The range of the MEP ID is 1-8191. *Add* - Add MEP ID(s). *Delete* - Delete MEP ID(s). By default, there is no MEP ID in a newly created maintenance association.

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

After clicking the **MIP Port Table** button, the following page will appear:

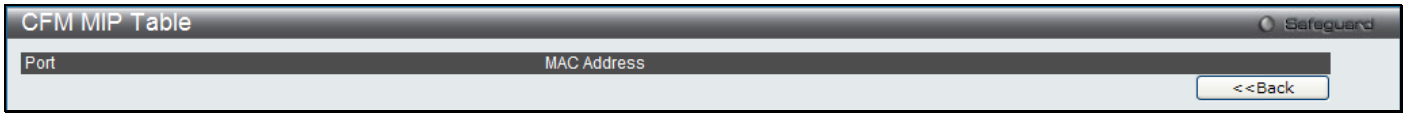


Figure 11-5 CFM MIP Table window

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

After clicking the **Add MEP** button, the following page will appear:

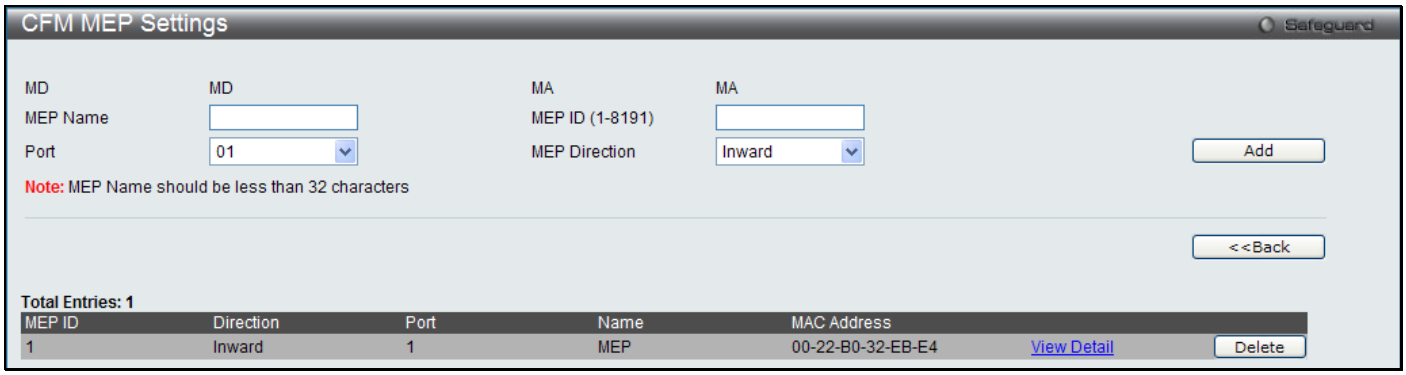


Figure 11-6 CFM MEP Settings window

The fields that can be configured are described below:

Parameter	Description
MEP Name	Enter the MEP name here. It is unique among all MEPs configured on the device.
MEP ID (1-8191)	Enter the MEP Identifier here. It should be configured in the MA's MEP ID list.
Port	Enter the port number used here. This port should be a member of the MA's associated VLAN.
MEP Direction	This is the MEP direction. *Inward* - Inward facing (up) MEP. *Outward* - Outward facing (down) MEP.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the View Detail link to view more information regarding the specific entry.
Click the **Delete** button to remove the specific entry.

NOTE: The **MEP Name** value should be less than 32 characters.

After clicking the View Detail link, the following page will appear:

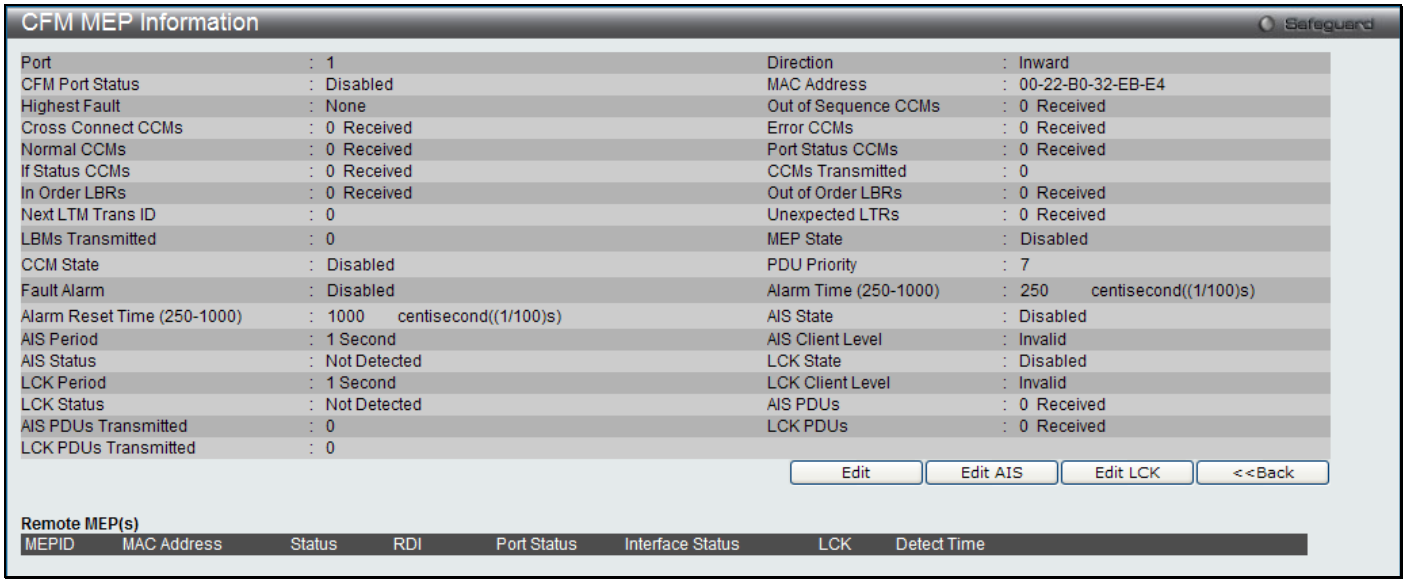


Figure 11-7 CFM MEP Information window

Click the **Edit** button to re-configure the specific entry.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Edit** button, the following page will appear:

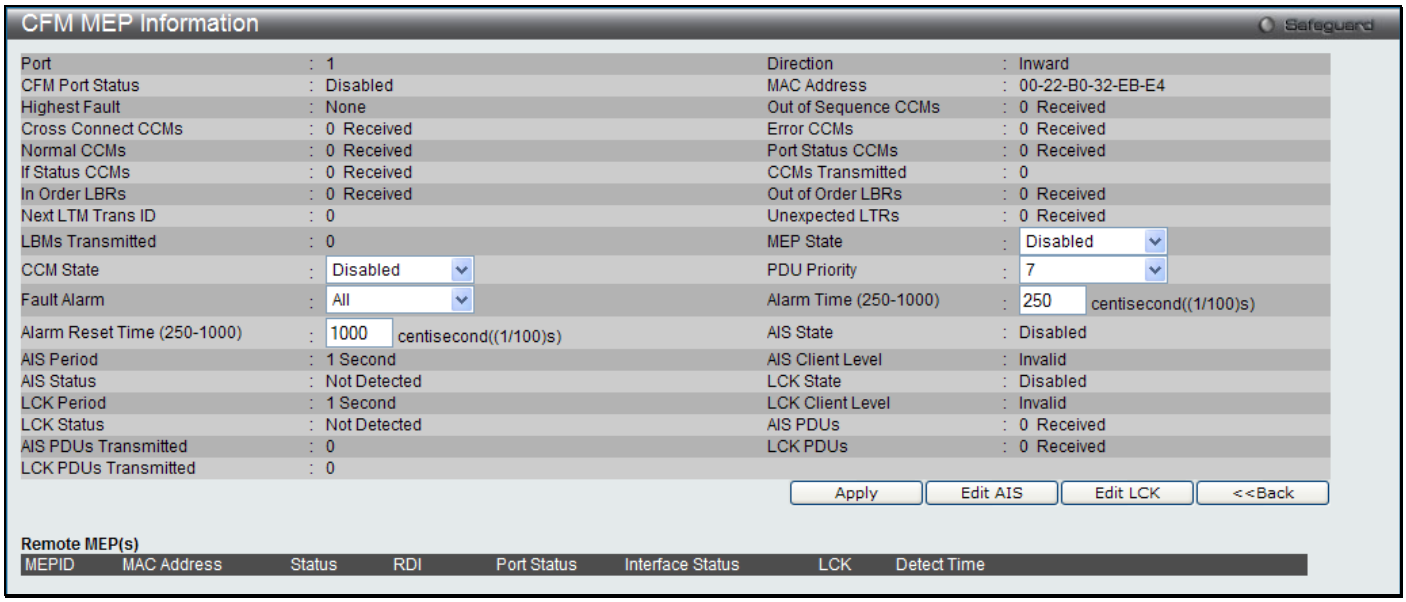


Figure 11-8 CFM MEP Information – Edit window

The fields that can be configured are described below:

Parameter	Description
MEP State	This is the MEP administrative state. *Enable* - MEP is enabled. *Disable* - MEP is disabled. This is the default value.
CCM State	This is the CCM transmission state. *Enable* - CCM transmission enabled. *Disable* - CCM transmission disabled. This is the default value.
PDU Priority	The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.
Fault Alarm	This is the control types of the fault alarms sent by the MEP. *All* - All types of fault alarms will be sent. *Mac Status* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Error” are sent. *Remote CCM* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP Down” are sent. *Errors CCM* - Only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent. *Xcon CCM* - Only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent. *None* - No fault alarm is sent. This is the default value.
Alarm Time (250-1000)	This is the time that a defect must exceed before the fault alarm can be sent. The unit is in centiseconds, the range is 250-1000. The default value is 250.
Alarm Reset Time (250-1000)	This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is in centiseconds, the range is 250-1000. The default value is 1000

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

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

Click the **Edit AIS** button to configure the AIS settings.

Click the **Edit LCK** button to configure the LCK settings.

After clicking the **Edit AIS** button, the following window will appear:

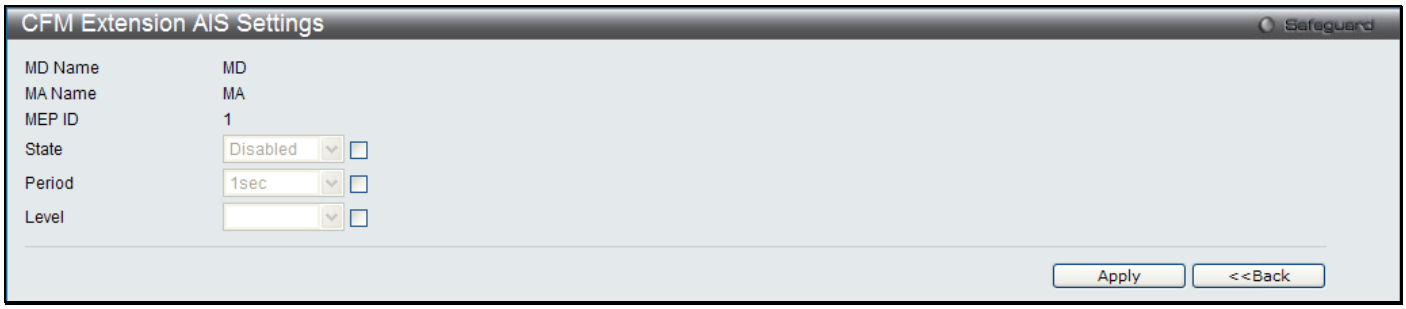


Figure 11-9 CFM Extension AIS window

The fields that can be configured are described below:

Parameter	Description
State	Tick the check box and use the drop-down menu to enable or disable the AIS function.
Period	Tick the check box and use the drop-down menu to select the transmitting interval of AIS PDU.
Level	Tick the check box and use the drop-down menu to select the client level ID to which the MEP sends AIS PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between 0 and 7.

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

After click the **Edit LCK** button, the following window will appear:

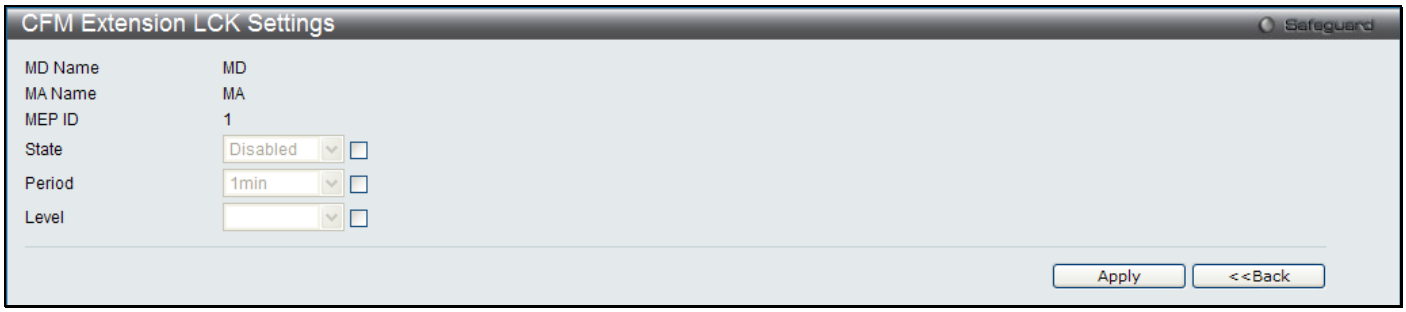


Figure 11-10 CFM Extension LCK Settings window

The fields that can be configured are described below:

Parameter	Description
State	Tick the check box and use the drop-down menu to enable or disable the LCK function.
Period	Tick the check box and use the drop-down menu to select the transmitting interval of LCK PDU.
Level	Tick the check box and use the drop-down menu to select the client level ID to which the MEP sends LCK PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between 0 and 7.

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

CFM Port Settings

On this page the user can enable and disable the CFM port state.

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

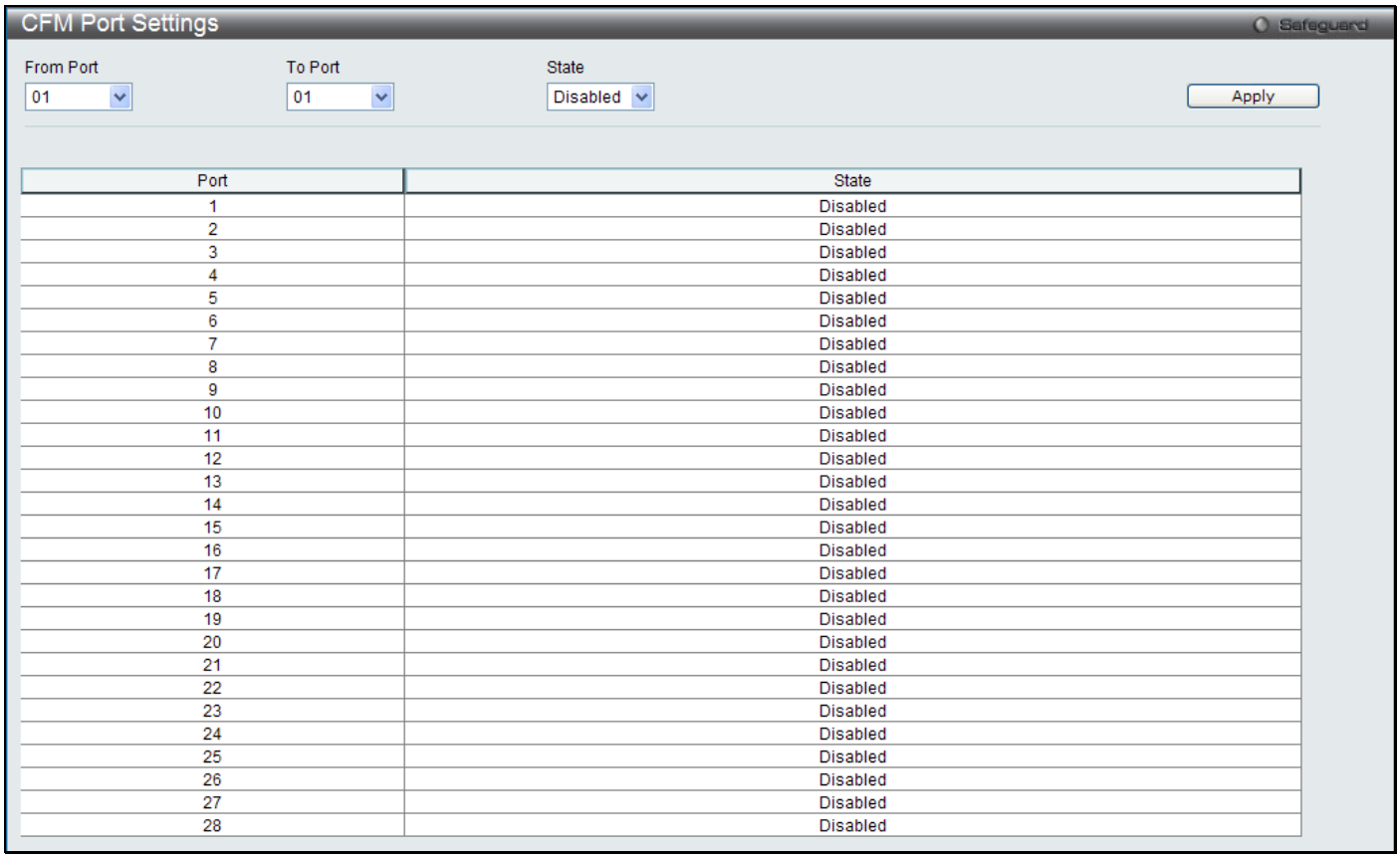


Figure 11-11 CFM Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select the port range used for this configuration.
State	Here the user can enable or disable the state of specific port regarding the CFM configuration.

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

CFM MIPCCM Table

On this page the user can view MIP CCM database entries.

To view the following window, click **OAM > CFM > CFM MIPCCM Table**, as shown below:

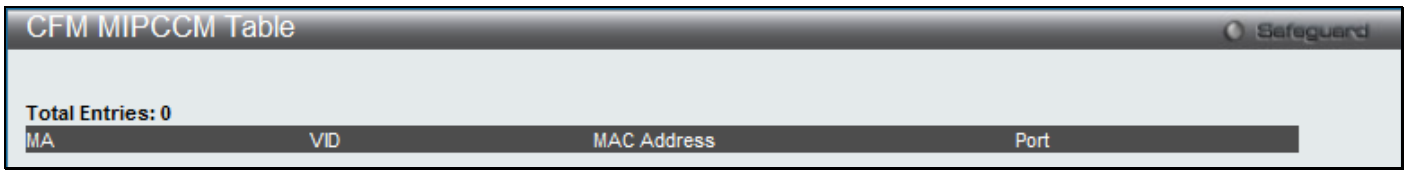


Figure 11-12 CFM MIPCCM Table window

CFM Loopback Settings

On this page the user can configure the CFM loopback parameters.

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

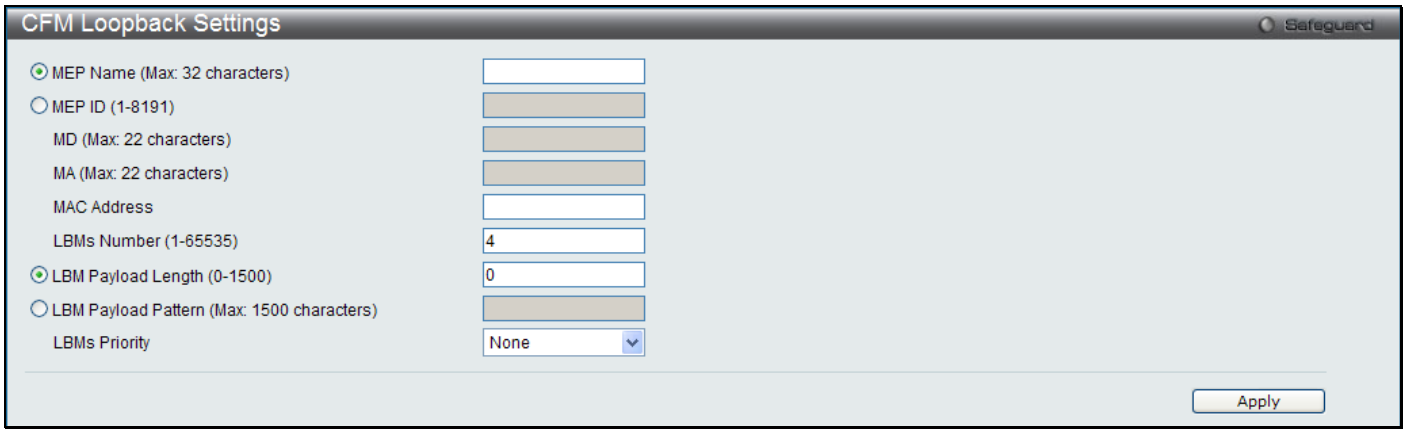


Figure 11-13 CFM Loopback Settings window

The fields that can be configured are described below:

Parameter	Description
MEP Name	Here the user can enter the MEP name.
MEP ID (1-8191)	Here the user can enter the MEP ID.
MD	Here the user can enter the maintenance domain name.
MA	Here the user can enter the maintenance association name.
MAC Address	Here the user can enter the destination MAC address.
LBMs Number (1-65535)	Number of LBMs to be sent. The default value is 4.
LBM Payload Length	The payload length of LBM to be sent. The default is 0.
LBM Payload Pattern	An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.
LBMs Priority	The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.

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

CFM Linktrace Settings

On this page the user can configure the CFM Linktrace message.

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

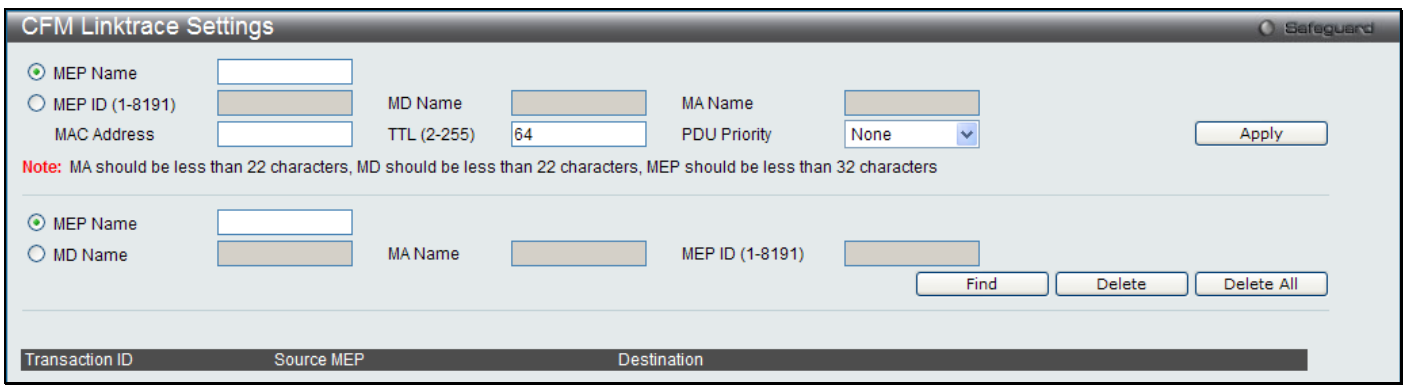


Figure 11-14 CFM Linktrace Settings window

The fields that can be configured are described below:

Parameter	Description
MEP Name	Here the user can enter the MEP name.
MEP ID (1-8191)	Here the user can enter the MEP ID.
MD Name	Here the user can enter the maintenance domain name.
MA Name	Here the user can enter the maintenance association name.
MAC Address	Here the user can enter the destination MAC address.
TTL (2-255)	Link-trace message TTL value. The default value is 64.
PDU Priority	The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.

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 specific entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.

CFM Packet Counter

On this page the user can view the CFM packet's RX and TX counters.

To view the following window, click **OAM > CFM > CFM Packet Counter**, as shown below:

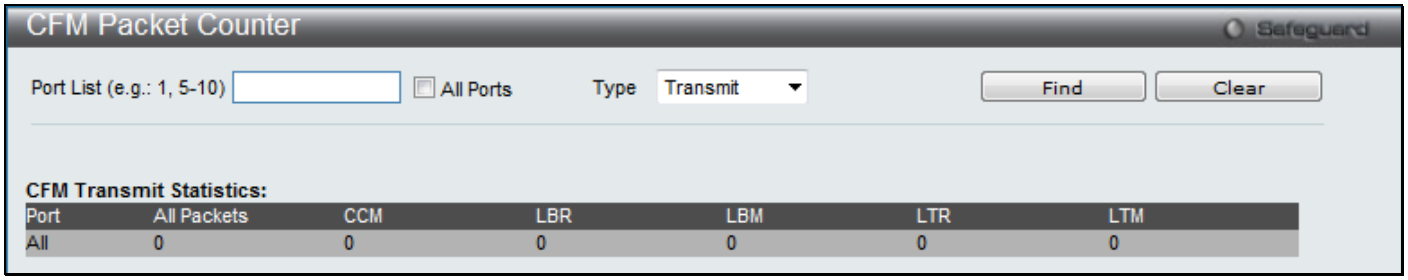


Figure 11-15 CFM Packet Counter window

The fields that can be configured are described below:

Parameter	Description
Port List	Which ports' counter to show. If not specified, all ports will be shown.
Type	*Transmit* – Selecting this option will display all the CFM packets transmitted. *Receive* – Selecting this option will display all the CFM packets received. *CCM* – Selecting this option will display all the CFM packets transmitted and received.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Clear** button to clear all the information entered in the fields.

CFM Fault Table

On this page the user can find the CFM fault table.

To view the following window, click **OAM > CFM > CFM Fault Table**, as shown below:

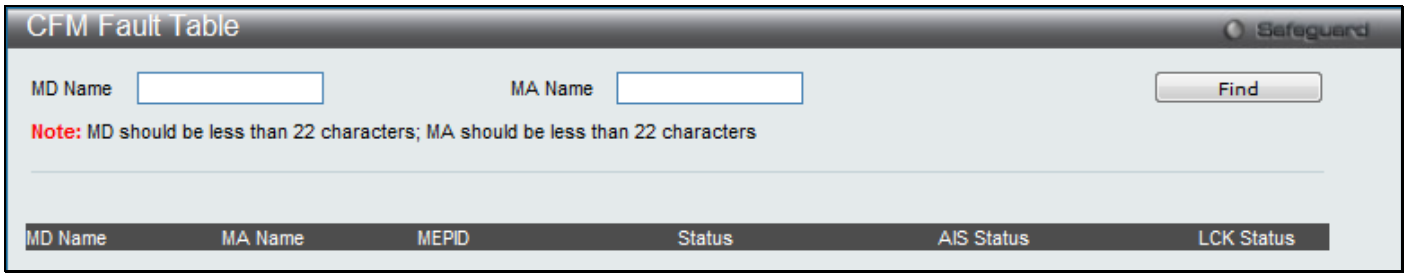


Figure 11-16 CFM Fault Table window

The fields that can be configured are described below:

Parameter	Description
MD Name	Here the user can enter the maintenance domain name.
MA Name	Here the user can enter the maintenance association name.

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

CFM MP Table

On this page the user can find the CFM MP table.

To view the following window, click **OAM > CFM > CFM MP Table**, as shown below:

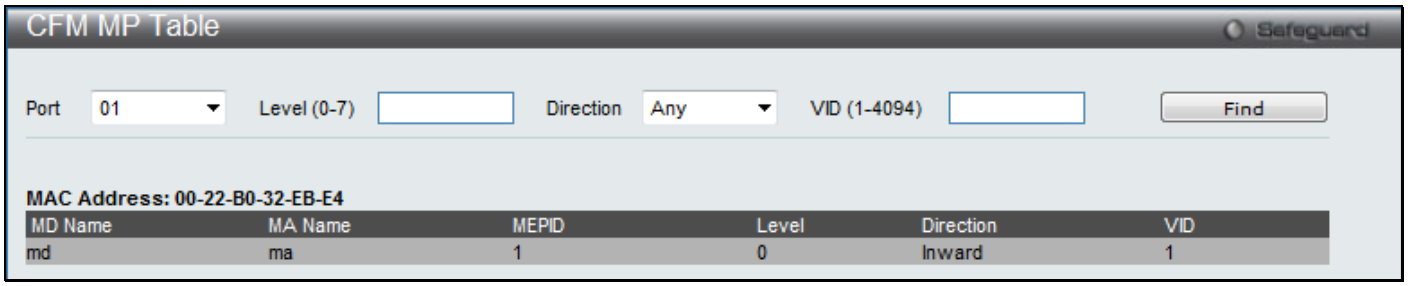


Figure 11-17 CFM MP Table window

The fields that can be configured are described below:

Parameter	Description
Port	Here the user can select the port number to view.
Level (0-7)	Here the user can enter the level to view.
Direction	Here the user can enter the direction to view. *Inward* - Inward facing (up) MP. *Outward* - Outward facing (down) MP.
VID (1-4094)	Here the user can enter the VID to view.

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

Ethernet OAM

Ethernet OAM (Operations, Administration, and Maintenance) is a data link layer protocol which provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions on point-to-point and emulated point-to-point Ethernet link.

OAMPDUs (OAM Protocol Data Units) contain the control and status information used to monitor, and also test and troubleshoots OAM-enabled links. OAMPDUs traverse a single link being passed between peer OAM entities, and as a result, are not forwarded by switches. OAM is a slow protocol, i.e. OAMPDU frame transmission rate is limited to a maximum of 10 frames per second.

The major features of Ethernet OAM are: OAM discovery, link monitoring, remote fault indication and remote loopbacks.

Ethernet OAM Settings

This window is used to configure the ports Ethernet OAM mode. In Active mode the ports can initiate OAM discovery and start or stop remote loopback. When a port in OAM enabled, any change to the OAM mode will cause the OAM discovery to be restarted.

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

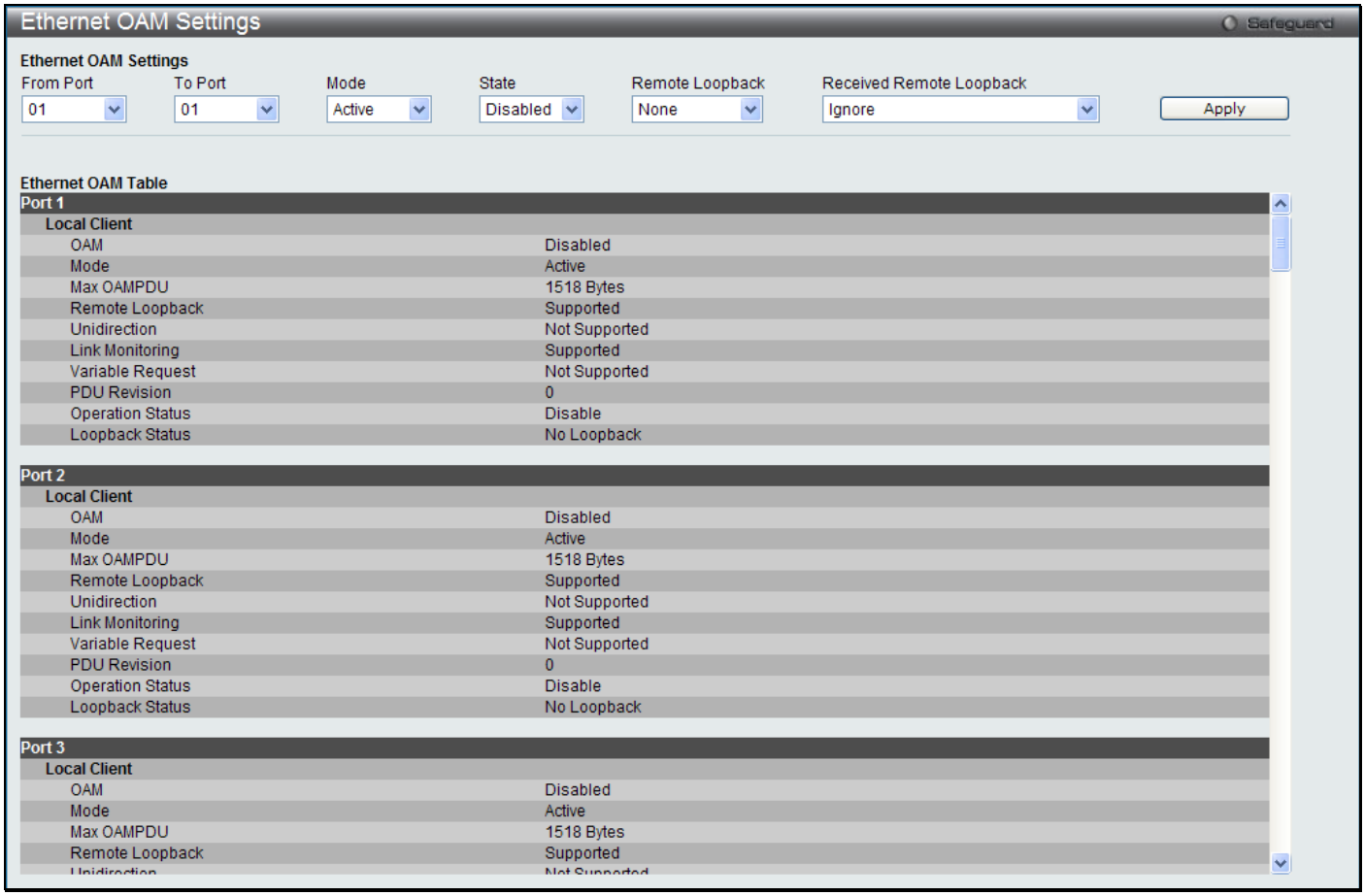


Figure 11-18 Ethernet OAM Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Specified a range of ports to be configured.
Mode	Specify to operate in either active mode or passive mode. The default mode is active.
State	Specify to enable or disable the OAM function. The default state is disabled.
Remote Loopback	If start is specified, it will request the peer to change to the remote loopback mode. If stop is specified, it will request the peer to change to the normal operation mode.
Received Remote Loopback	Specify whether to process or to ignore the received Ethernet OAM remote loopback command. The default method is *ignore*.

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

Ethernet OAM Configuration Settings

On this page the user can configure the Ethernet OAM parameters.

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

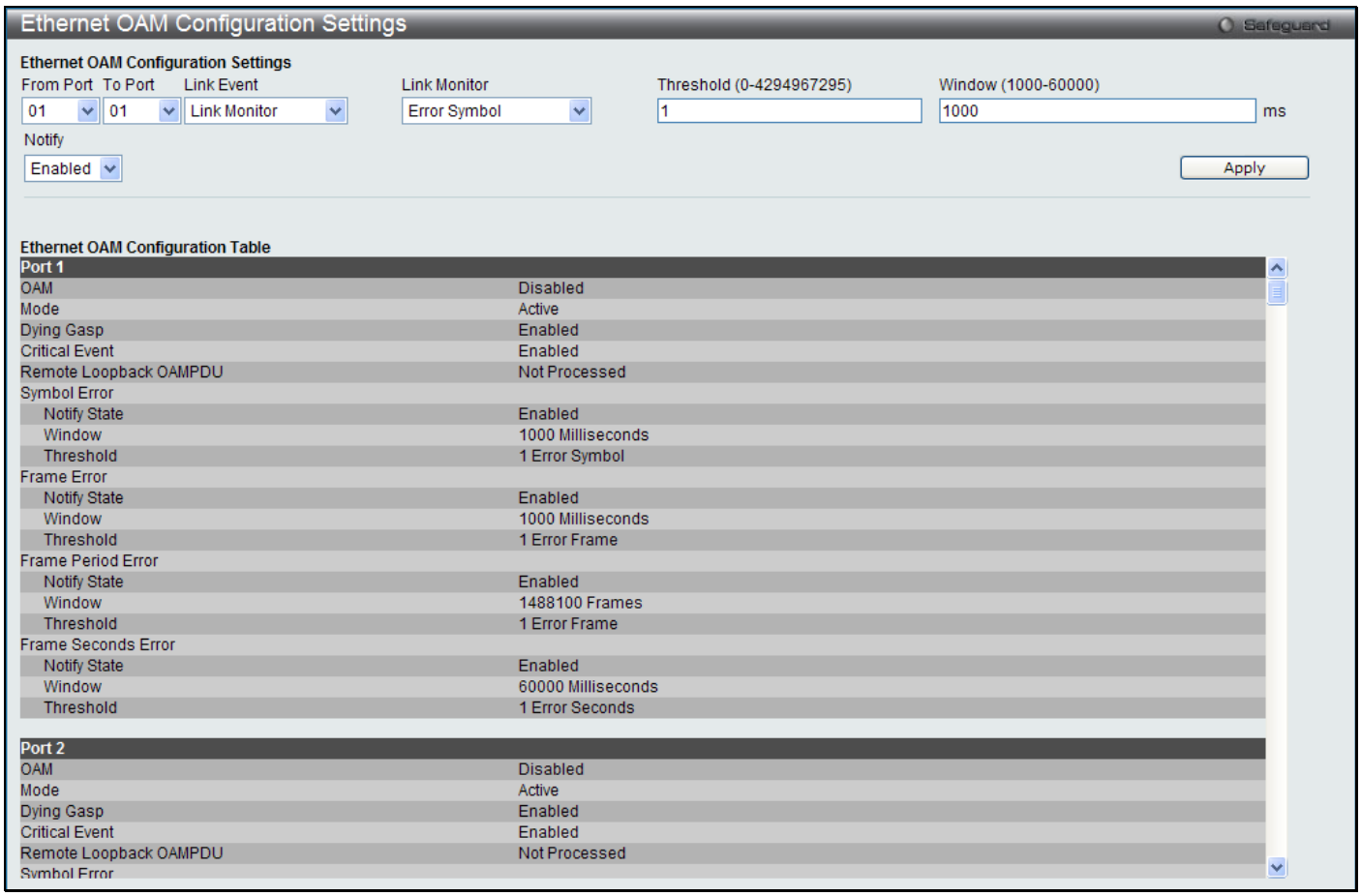


Figure 11-19 Ethernet OAM Configuration Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Specified a range of ports to be configured.
Link Event	The option used to configure the capability of Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event.
Link Monitor	The option is used to configure ports Ethernet OAM link monitoring error symbols. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer.
Critical Link Event	The option used to configure the capability of Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event.
Threshold (0-4294967295)	Specify the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 symbol error.
Window (1000-60000)	The range is 1000 to 60000ms. The default value is 1000ms.

Notify	Specify to enable or disable the event notification. The default state is enable.

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

Ethernet OAM Event Log

The page is used to show ports Ethernet OAM event log information. The switch can buffer 1000 event logs. The event log is different from sys-log. It provides more detailed information than the system log. Each OAM event will be recorded in both OAM event log and in the system log.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Event Log**, as shown below:

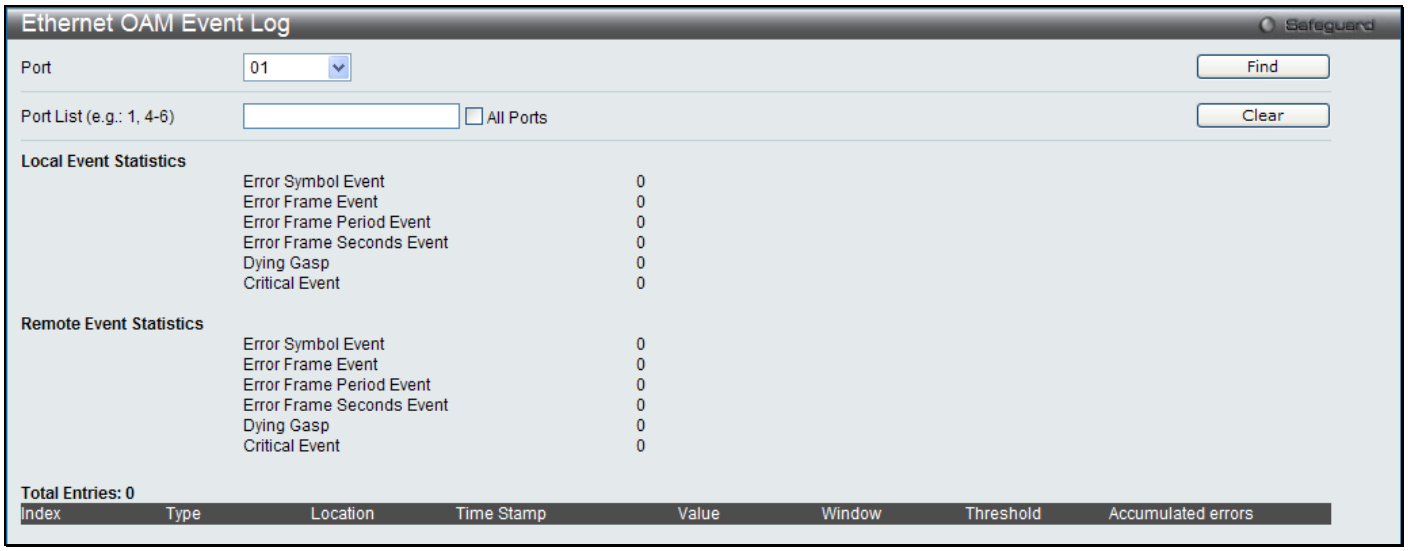


Figure 11-20 Ethernet OAM Event Log window

The fields that can be configured are described below:

Parameter	Description
Port	Here the user can select a specific port to view.
Port List	Here the user can enter a range of ports to view. Alternatively the user can select the **All Ports** option to view information of all the ports.

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

Click the **Clear** button to clear all the information entered in the fields.

Ethernet OAM Statistics

The page is used to show ports Ethernet OAM statistics information.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Statistics**, as shown below:

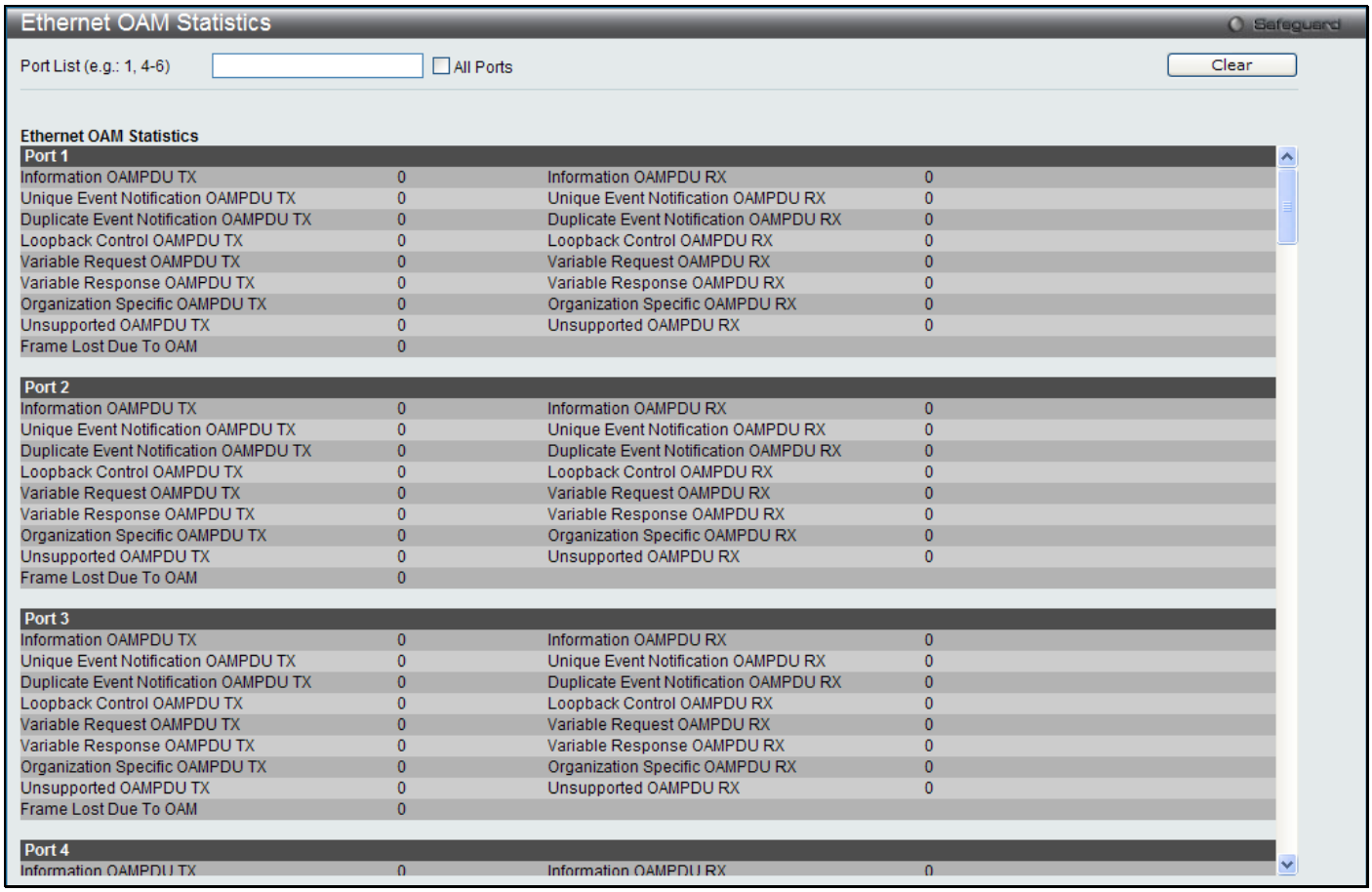


Figure 11-21 Ethernet OAM Statistics window

The fields that can be configured are described below:

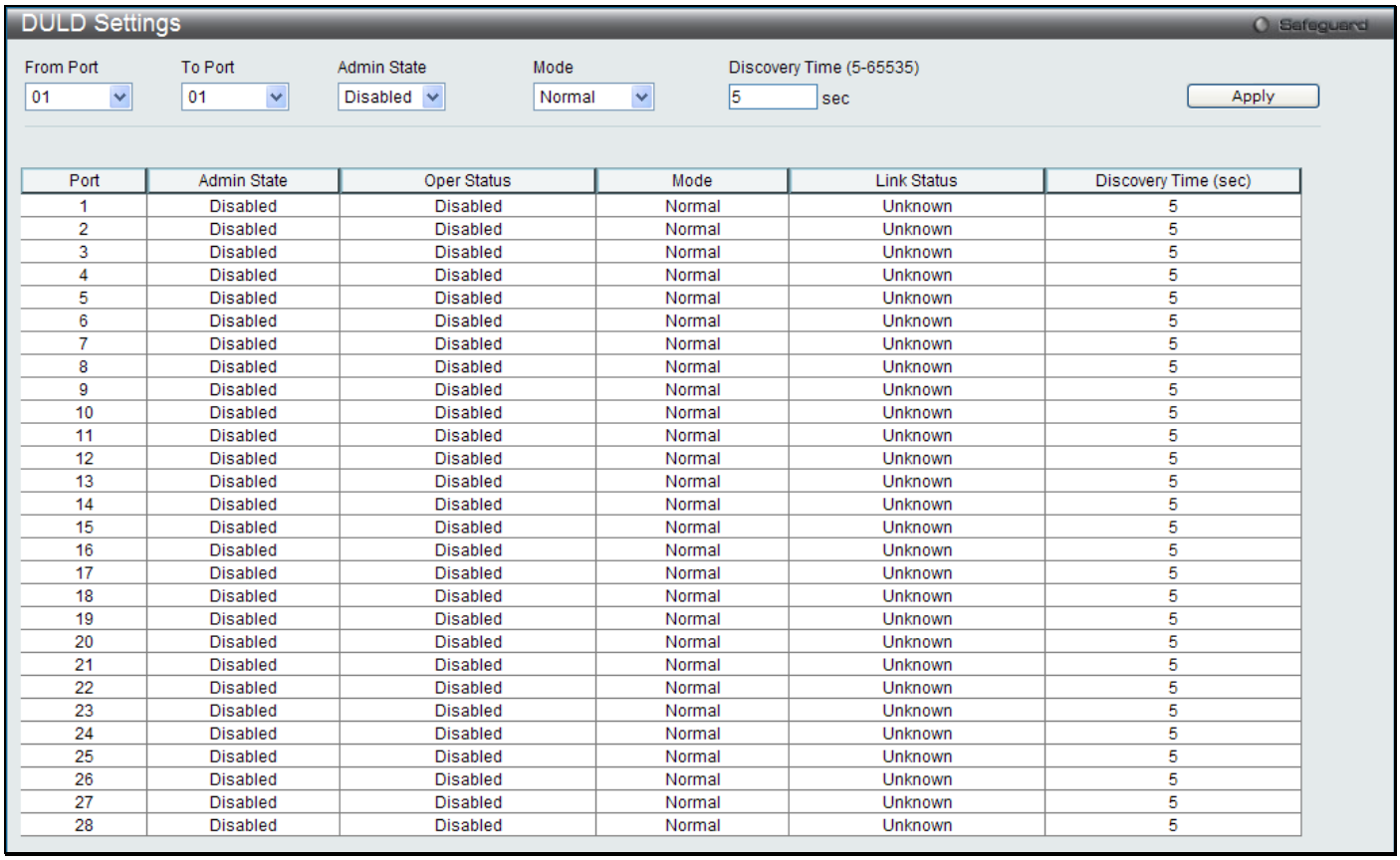
Parameter	Description
Port List	Here the user can enter a range of ports to view. Alternatively the user can select the **All Ports** option to view information of all the ports.

Click the **Clear** button to clear all the information entered in the fields.

DULD Settings

The Switch features a D-Link Unidirectional Link Detection (DULD) module. The unidirectional link detection provides a mechanism that can be used to detect unidirectional link for Ethernet switches whose PHYs do not support unidirectional OAM operation. This function is established based on OAM, so OAM should be enabled before starting detection.

To view this window, click **OAM > DULD Settings** as shown below:



Port	Admin State	Oper Status	Mode	Link Status	Discovery Time (sec)
1	Disabled	Disabled	Normal	Unknown	5
2	Disabled	Disabled	Normal	Unknown	5
3	Disabled	Disabled	Normal	Unknown	5
4	Disabled	Disabled	Normal	Unknown	5
5	Disabled	Disabled	Normal	Unknown	5
6	Disabled	Disabled	Normal	Unknown	5
7	Disabled	Disabled	Normal	Unknown	5
8	Disabled	Disabled	Normal	Unknown	5
9	Disabled	Disabled	Normal	Unknown	5
10	Disabled	Disabled	Normal	Unknown	5
11	Disabled	Disabled	Normal	Unknown	5
12	Disabled	Disabled	Normal	Unknown	5
13	Disabled	Disabled	Normal	Unknown	5
14	Disabled	Disabled	Normal	Unknown	5
15	Disabled	Disabled	Normal	Unknown	5
16	Disabled	Disabled	Normal	Unknown	5
17	Disabled	Disabled	Normal	Unknown	5
18	Disabled	Disabled	Normal	Unknown	5
19	Disabled	Disabled	Normal	Unknown	5
20	Disabled	Disabled	Normal	Unknown	5
21	Disabled	Disabled	Normal	Unknown	5
22	Disabled	Disabled	Normal	Unknown	5
23	Disabled	Disabled	Normal	Unknown	5
24	Disabled	Disabled	Normal	Unknown	5
25	Disabled	Disabled	Normal	Unknown	5
26	Disabled	Disabled	Normal	Unknown	5
27	Disabled	Disabled	Normal	Unknown	5
28	Disabled	Disabled	Normal	Unknown	5

Figure 11-22 DULD Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports you wish to configure.
Admin State	Use the drop-down menu to enable or disable the selected ports unidirectional link detection status.
Mode	Use the drop-down menu to select Mode between *Shutdown* and *Normal*. *Shutdown* – If any unidirectional link is detected, disable the port and log an event. *Normal* - Only log an event when a unidirectional link is detected.
Discovery Time (5-65535)	Enter these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start.

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

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:

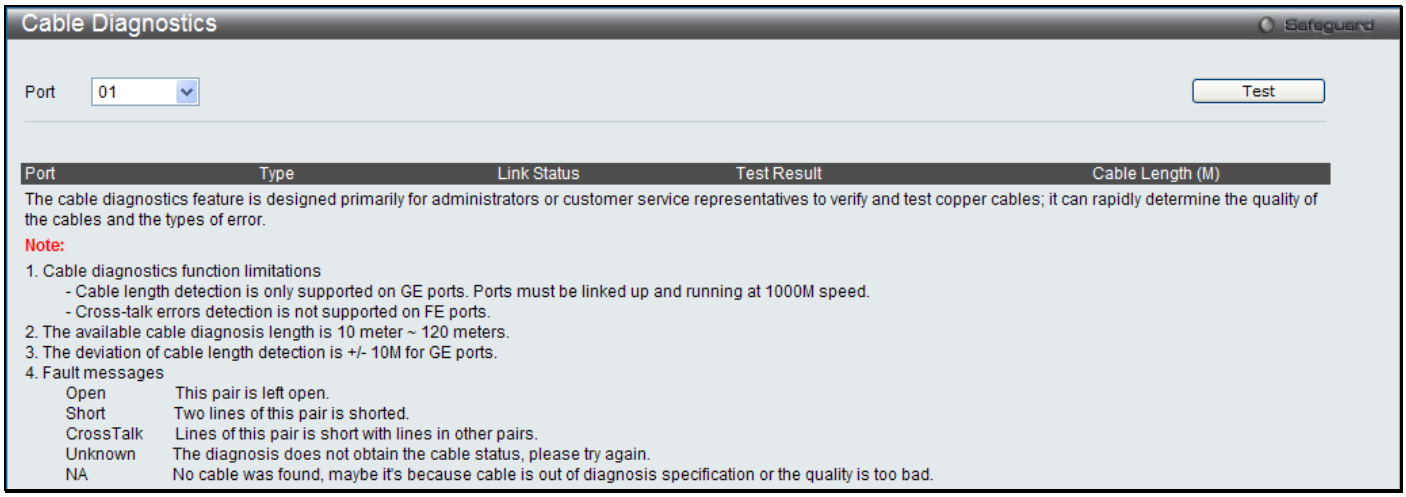


Figure 11-23 Cable Diagnostics window

To view the cable diagnostics for a particular port, use the drop-down menu to choose the port and click **Test** The information will be displayed in this window.

NOTE: Cable diagnostic function limitations: Cable length detection is only supported on GE ports. Ports must be linked up and running at 1000M speed. Cross-talk errors detection is not supported on FE ports.

NOTE: The available cable diagnosis length is from 10 meter to 120 meters.

NOTE: The deviation of cable length detection is +/- 10M for GE ports.

Fault messages:

- *Open* - This pair is left open.
- *Short* - Two lines of this pair is shorted.
- *CrossTalk* - Lines of this pair is short with lines in other pairs.
- *Unknown* - The diagnosis does not obtain the cable status, please try again.
- *NA* - No cable was found, maybe it's because cable is out of diagnosis specification or the quality is too bad.

Chapter 12 Monitoring

Utilization
Statistics
Mirror
sFlow
Ping Test
Trace Route
Device Environment

NOTE: The real time monitoring engine requires the JAVA runtime v1.6 or above platform. Please download the software from http://www.java.com/getjava

Utilization

CPU Utilization

Users can display the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

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

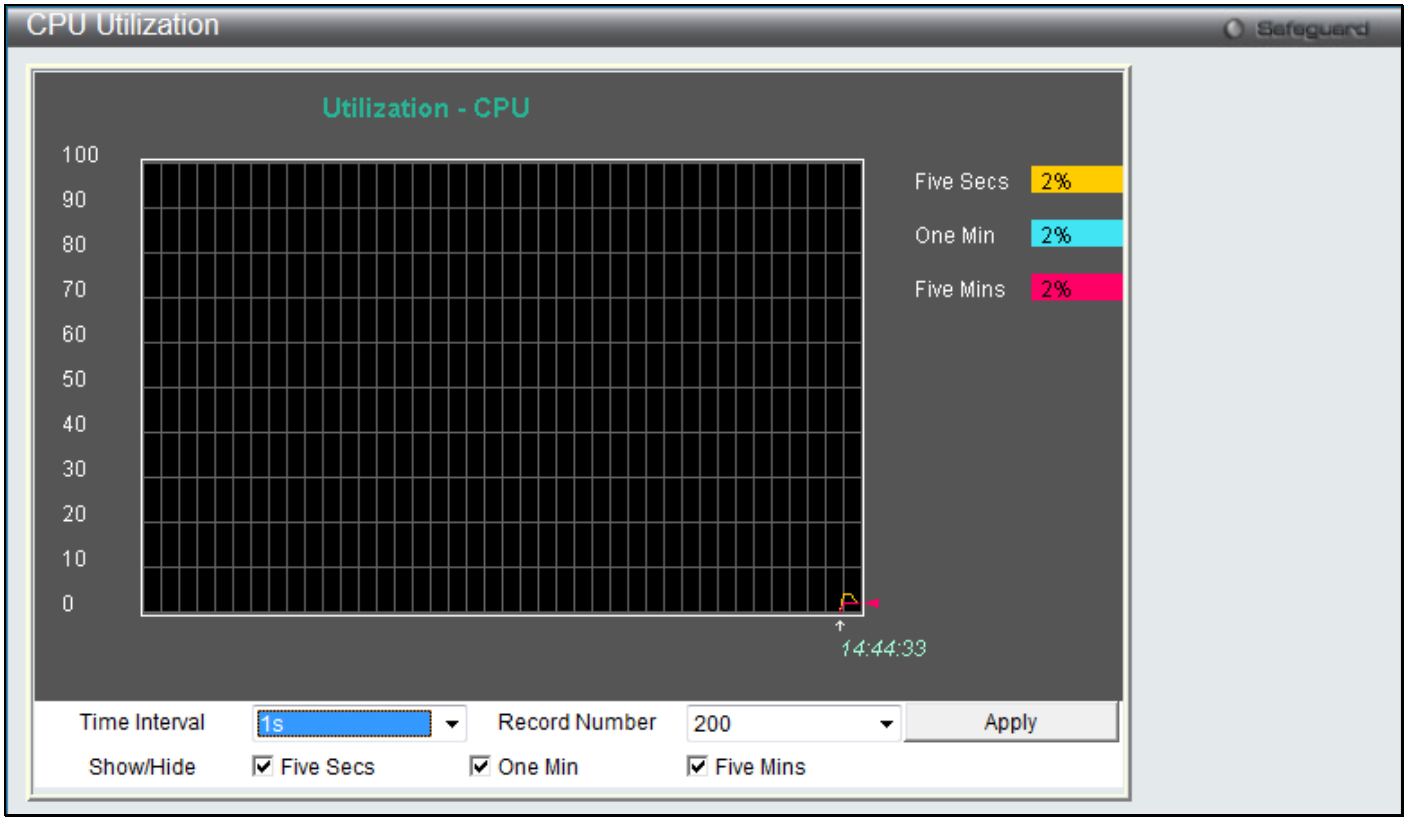


Figure 12-1 CPU Utilization window

To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

The fields that can be configured are described below:

Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default

	value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Five Seconds, One Minute, and Five Minutes.

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

DRAM & Flash Utilization

On this page the user can view information regarding the DRAM and Flash utilization.

To view the following window, click **Monitoring > Utilization > DRAM & Flash Utilization**, as shown below:

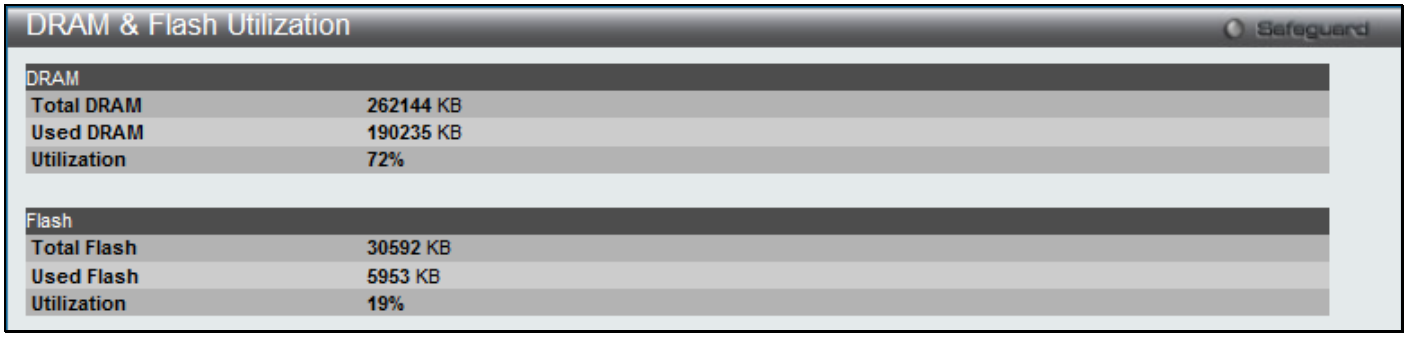


Figure 12-2 DRAM & Flash Utilization window

Port Utilization

Users can 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:

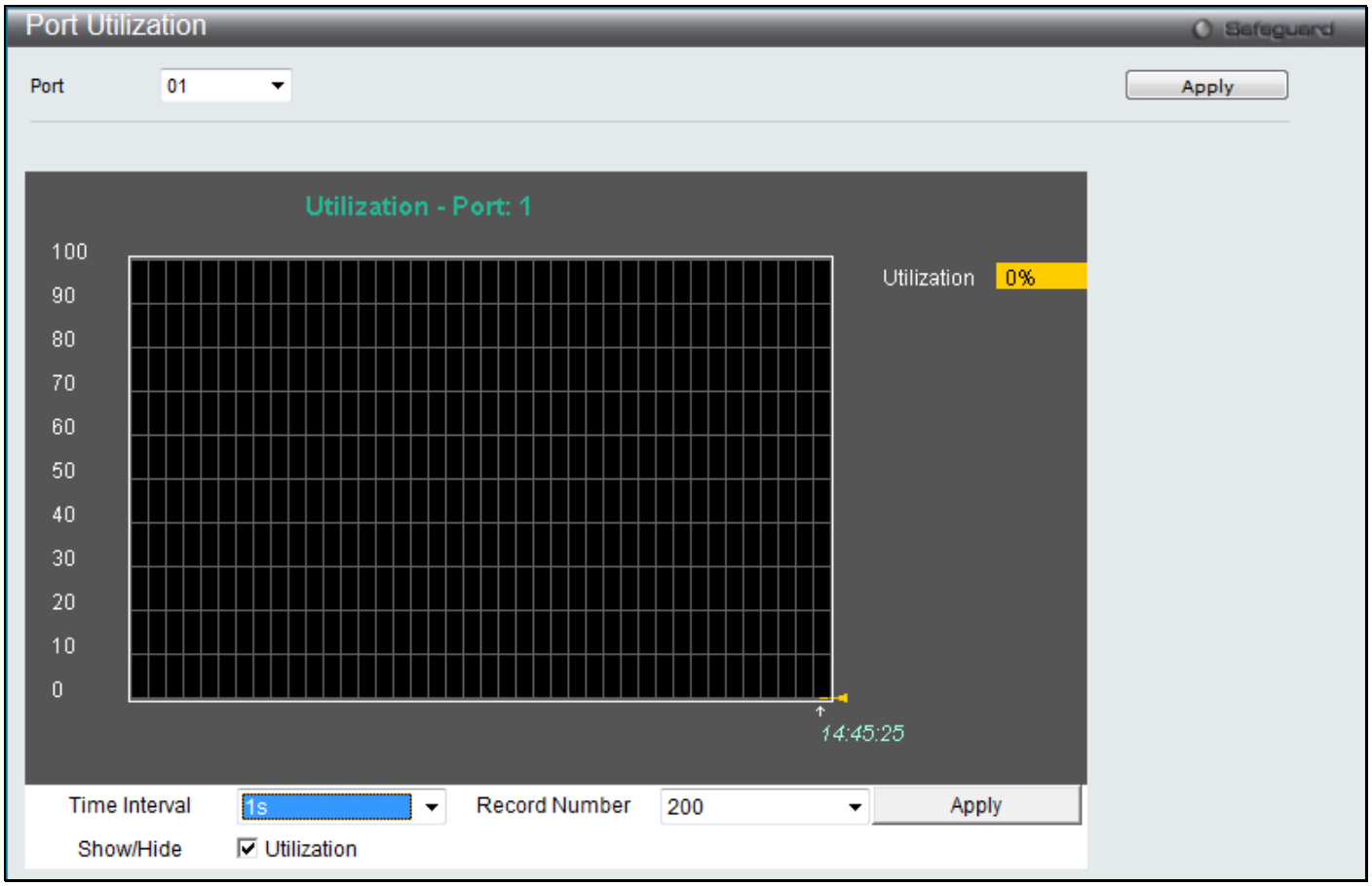


Figure 12-3 Port Utilization window

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Port Utilization.

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

Statistics

Packet Statistics

Packets

The Web manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following window, click **Monitoring > Statistics > Packet Statistics > Packets > Received (RX)**, as shown below:

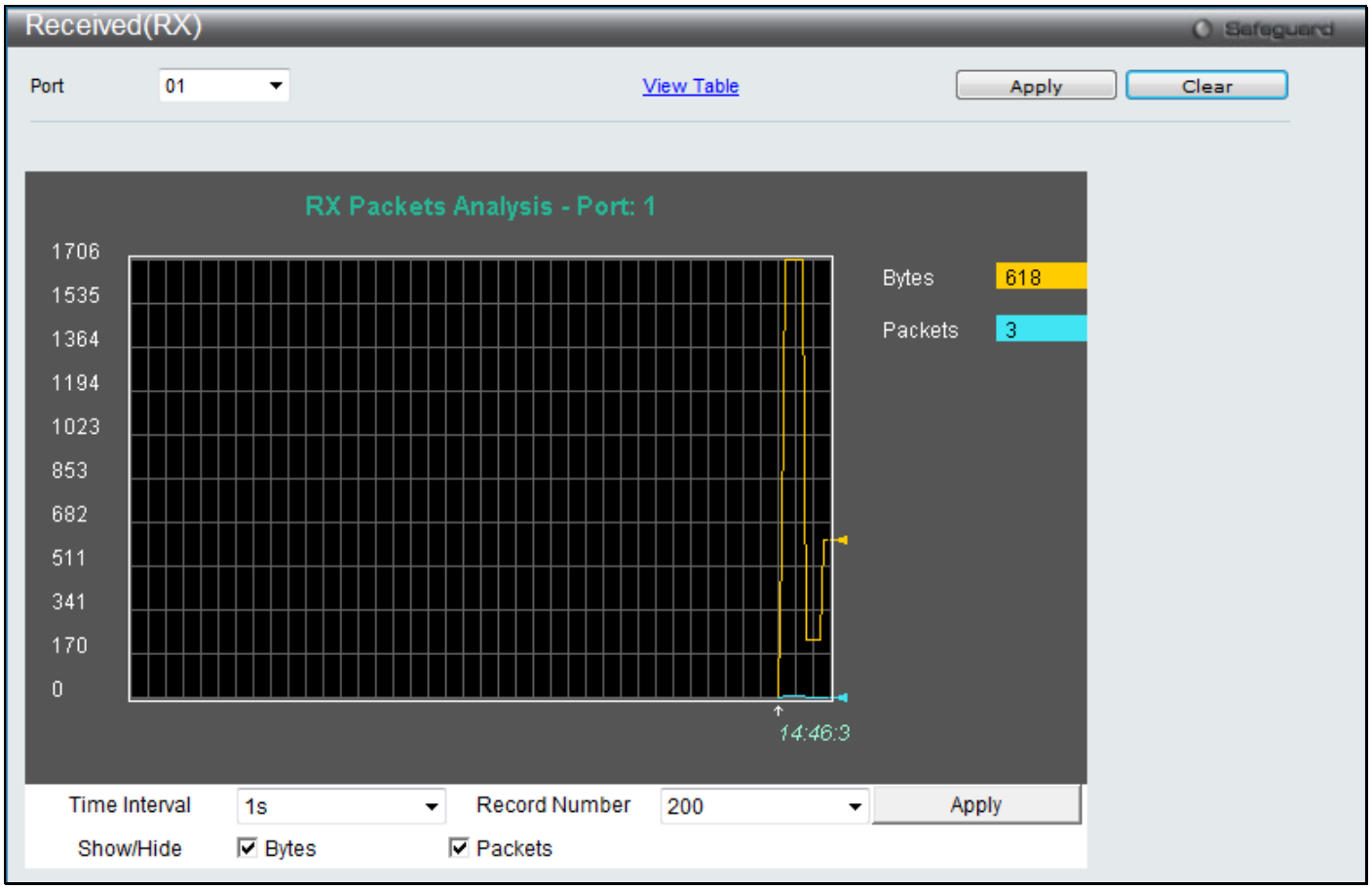


Figure 12-4 Received (RX) window

Click the View Table link to display the information in a table rather than a line graph.

Figure 12-5 RX Packets Analysis Table window

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.

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

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

UMB_Cast (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following window, click **Monitoring > Statistics > Packet Statistics > Packets > UMB_Cast (RX)**, as shown below:

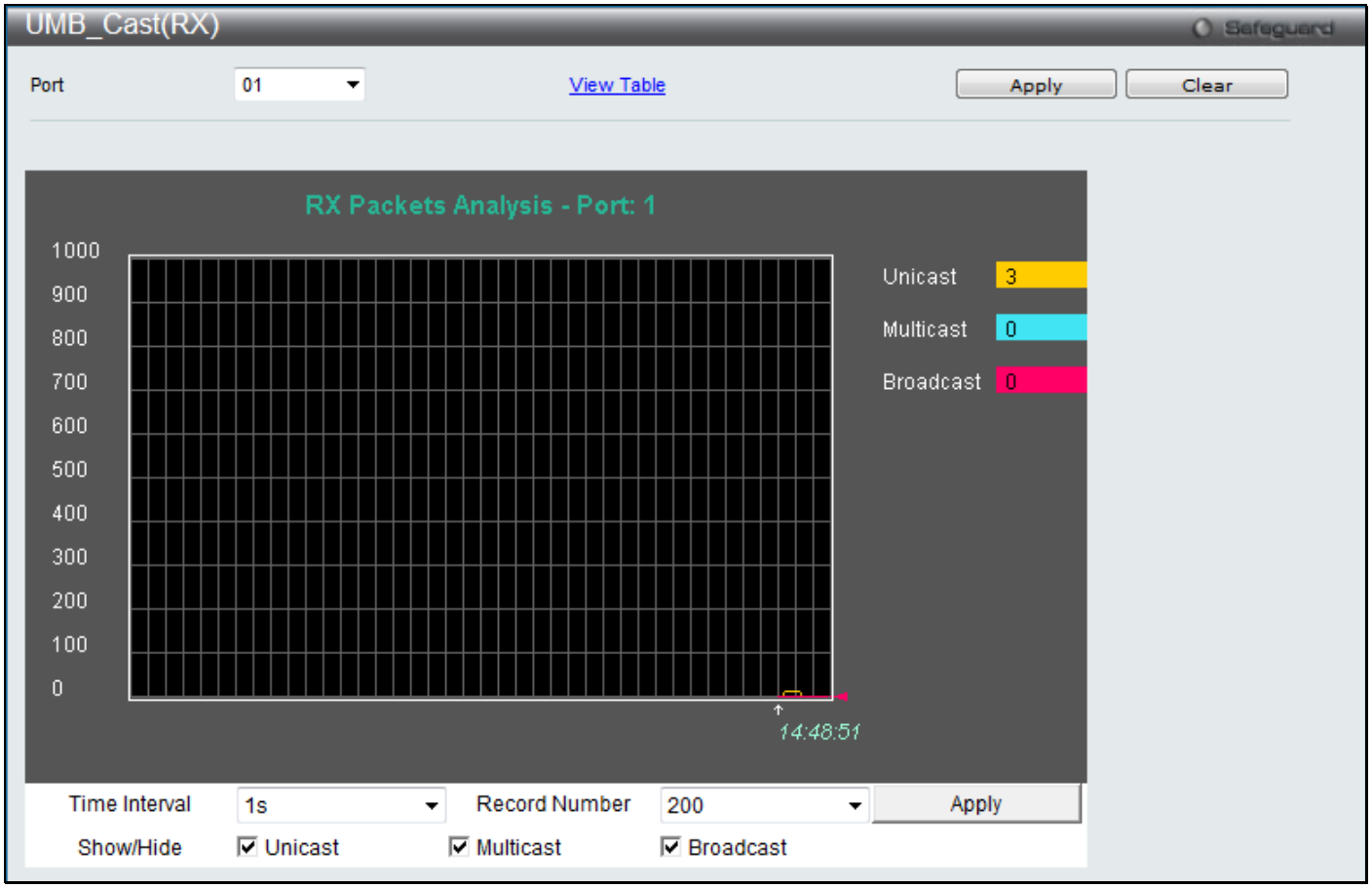


Figure 12-6 UMB_Cast (RX) window

Click the View Table link to display the information in a table rather than a line graph.

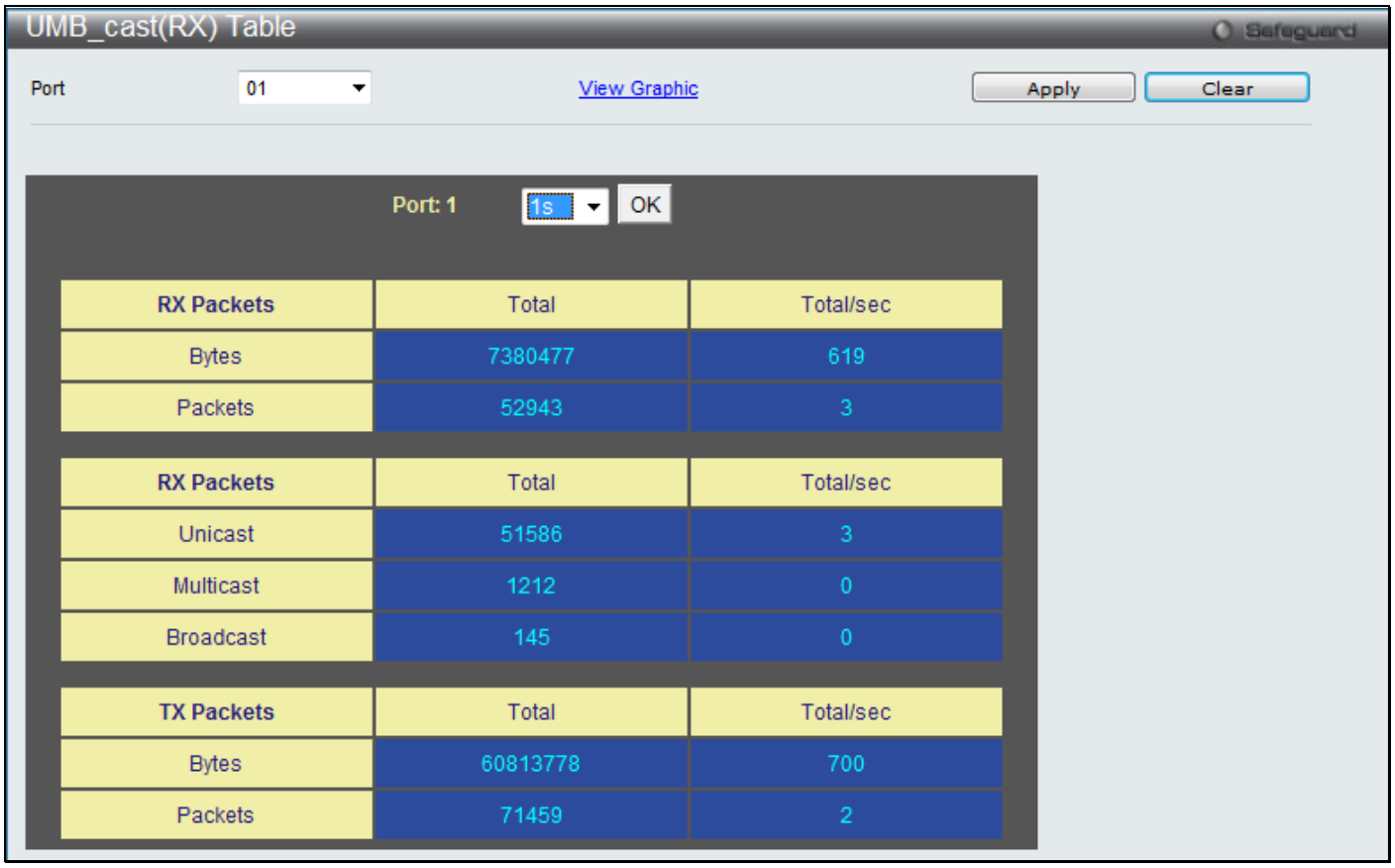


Figure 12-7 RX Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.

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

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following window, click **Monitoring > Statistics > Packet Statistics > Packets > Transmitted (TX)**, as shown below:

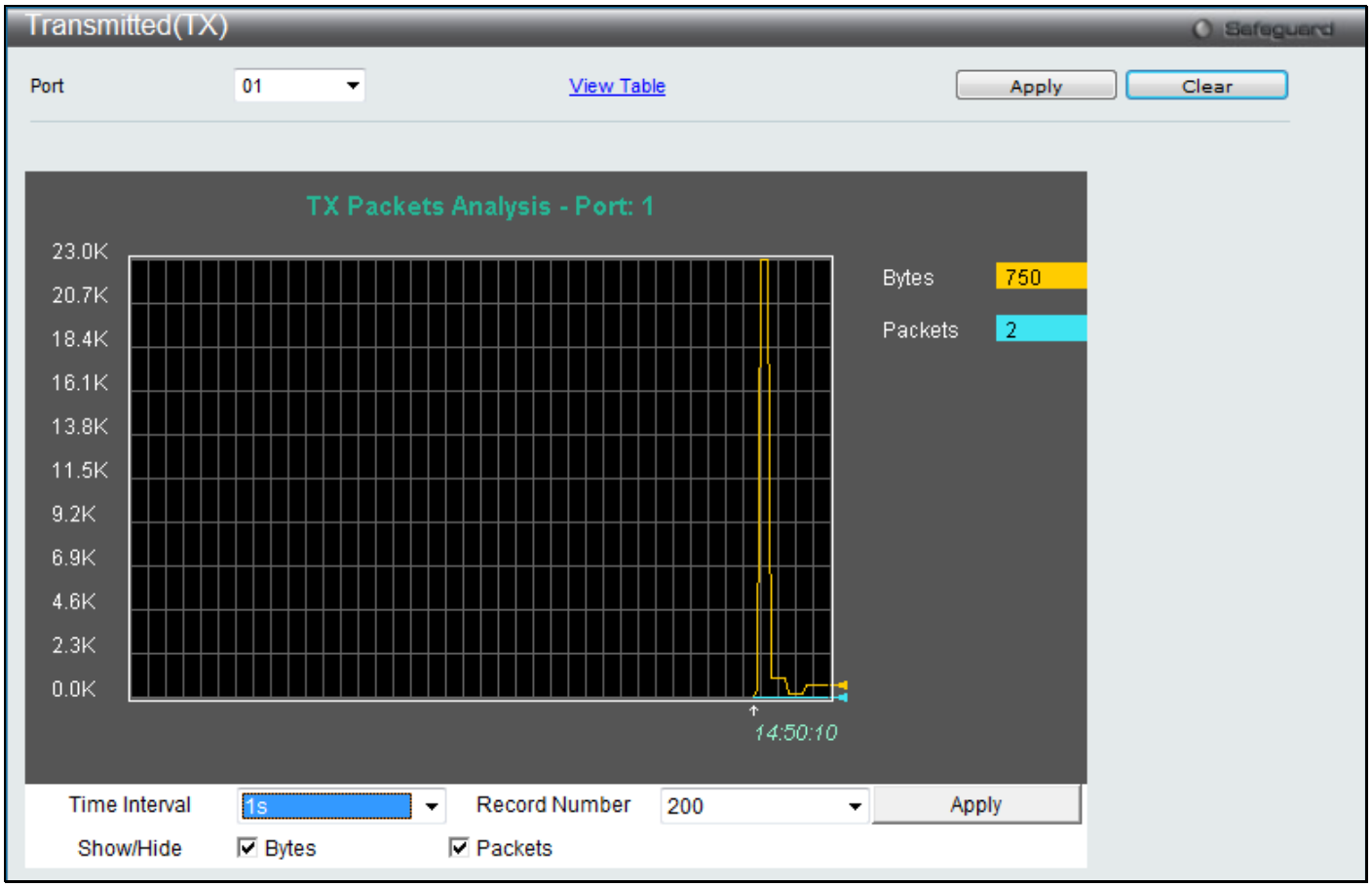


Figure 12-8 Transmitted (TX) window

Click the View Table link to display the information in a table rather than a line graph.

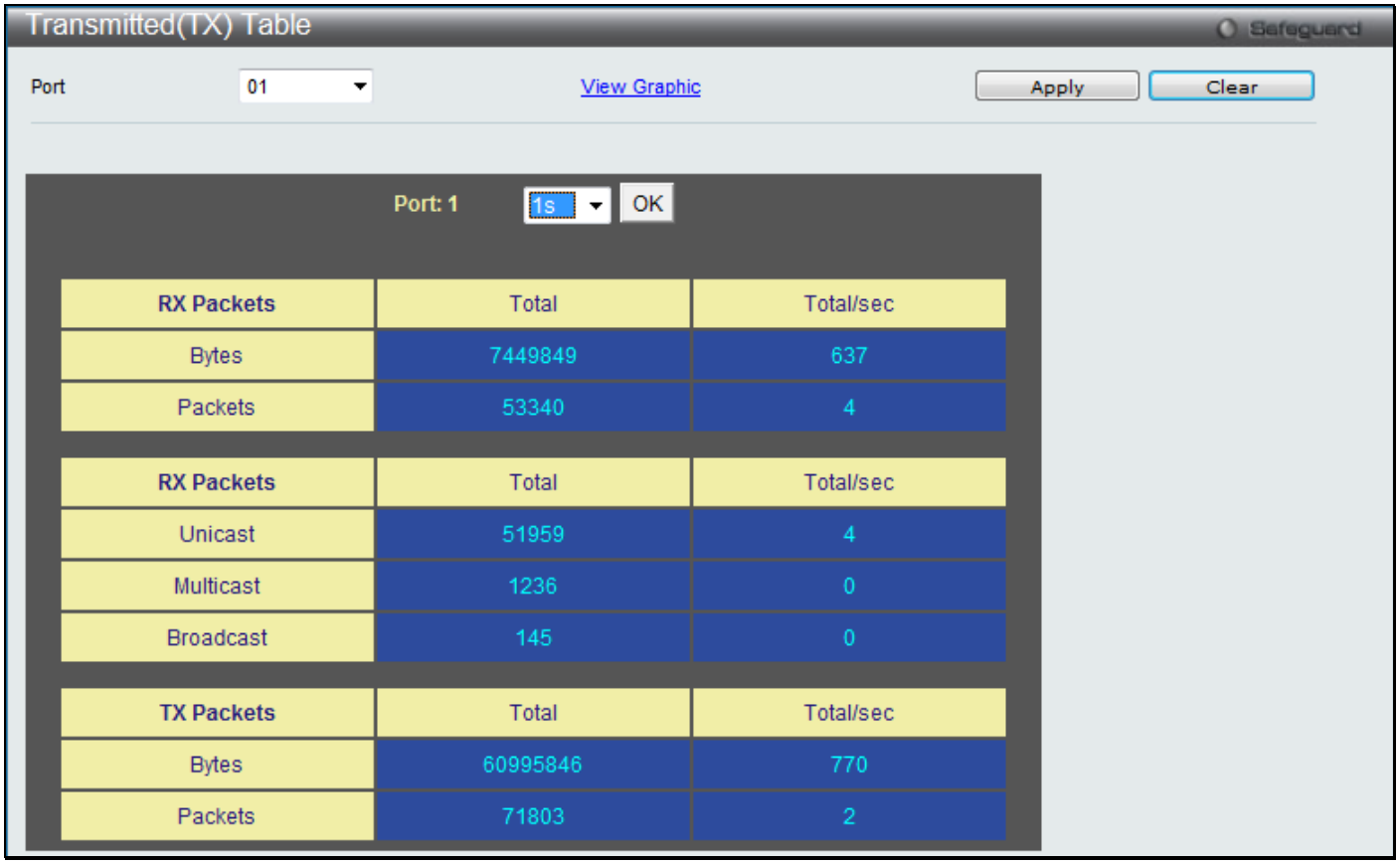


Figure 12-9 TX Packets Analysis window (table for Bytes and Packets)

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.

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

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Errors

The Web manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following window, click **Monitoring > Statistics > Packet Statistics > Errors > Received (RX)**, as shown below:

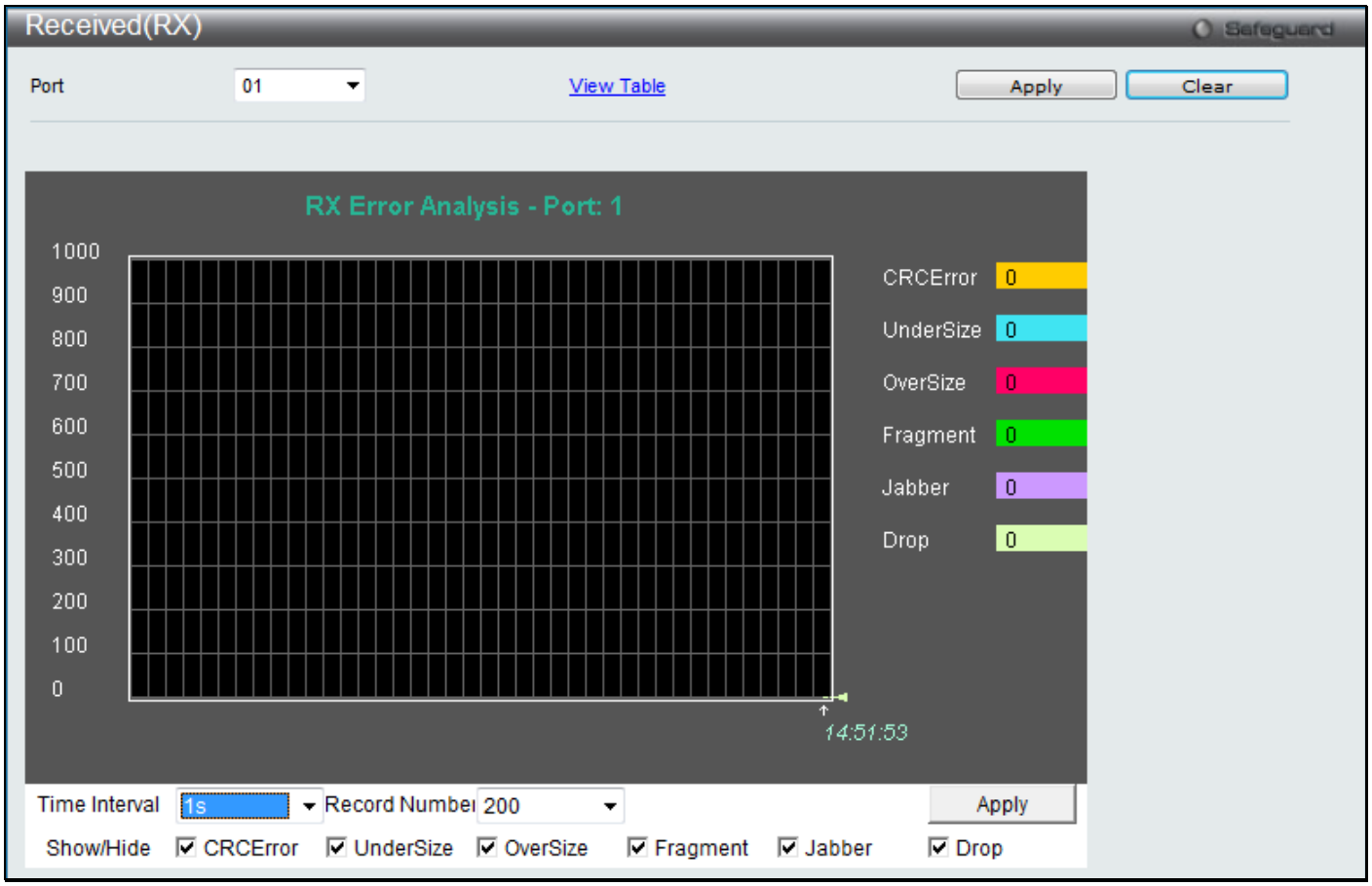


Figure 12-10 Received (RX) window

Click the View Table link to display the information in a table rather than a line graph.

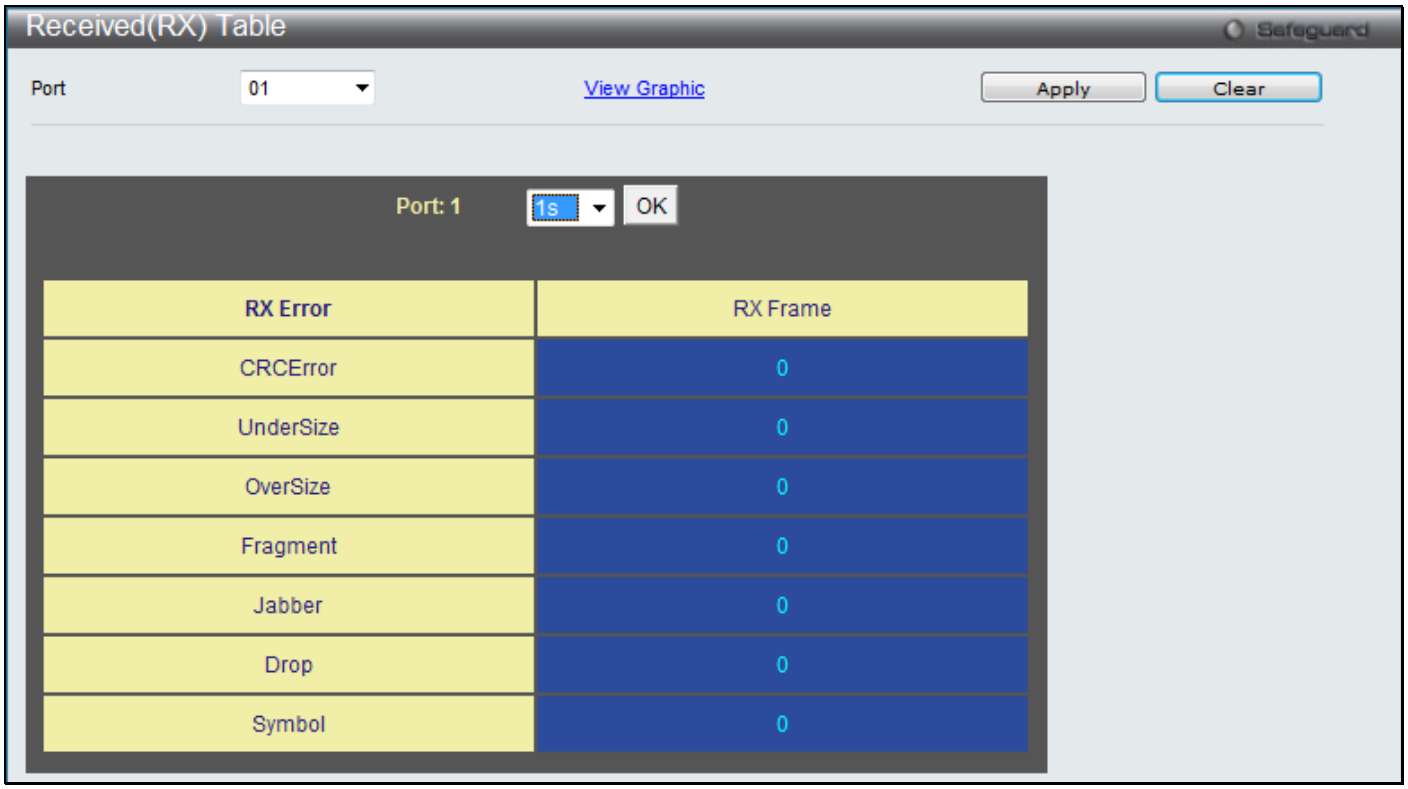


Figure 12-11 Received(RX) Table – View Table window

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Symbol	Counts the number of packets received that have errors received in the symbol on the physical labor.
Show/Hide	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.

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

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following window, click **Monitoring > Statistics > Packet Statistics > Errors > Transmitted (TX)**, as shown below:

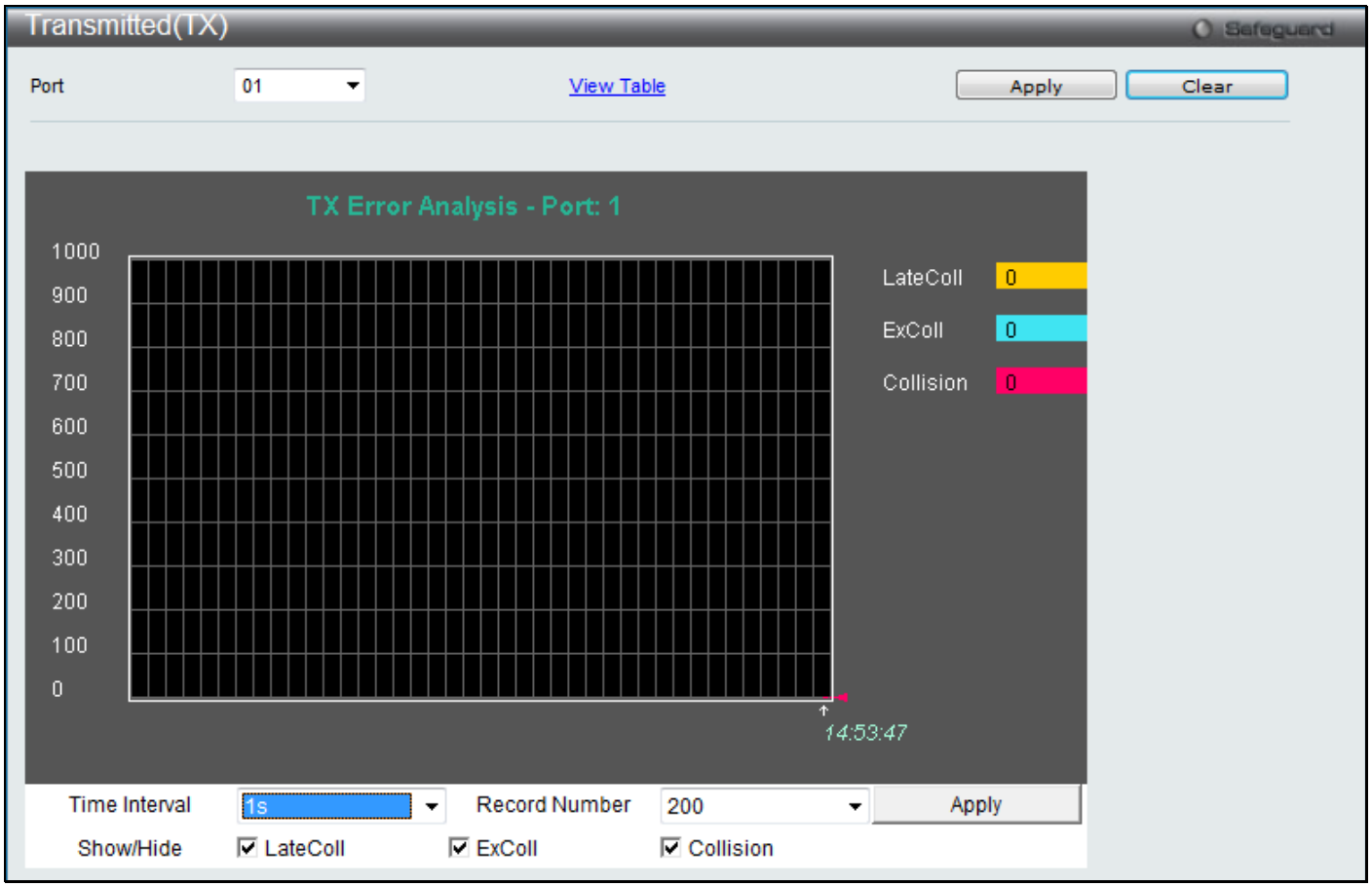


Figure 12-12 Transmitted (TX) window

Click the View Table link to display the information in a table rather than a line graph.

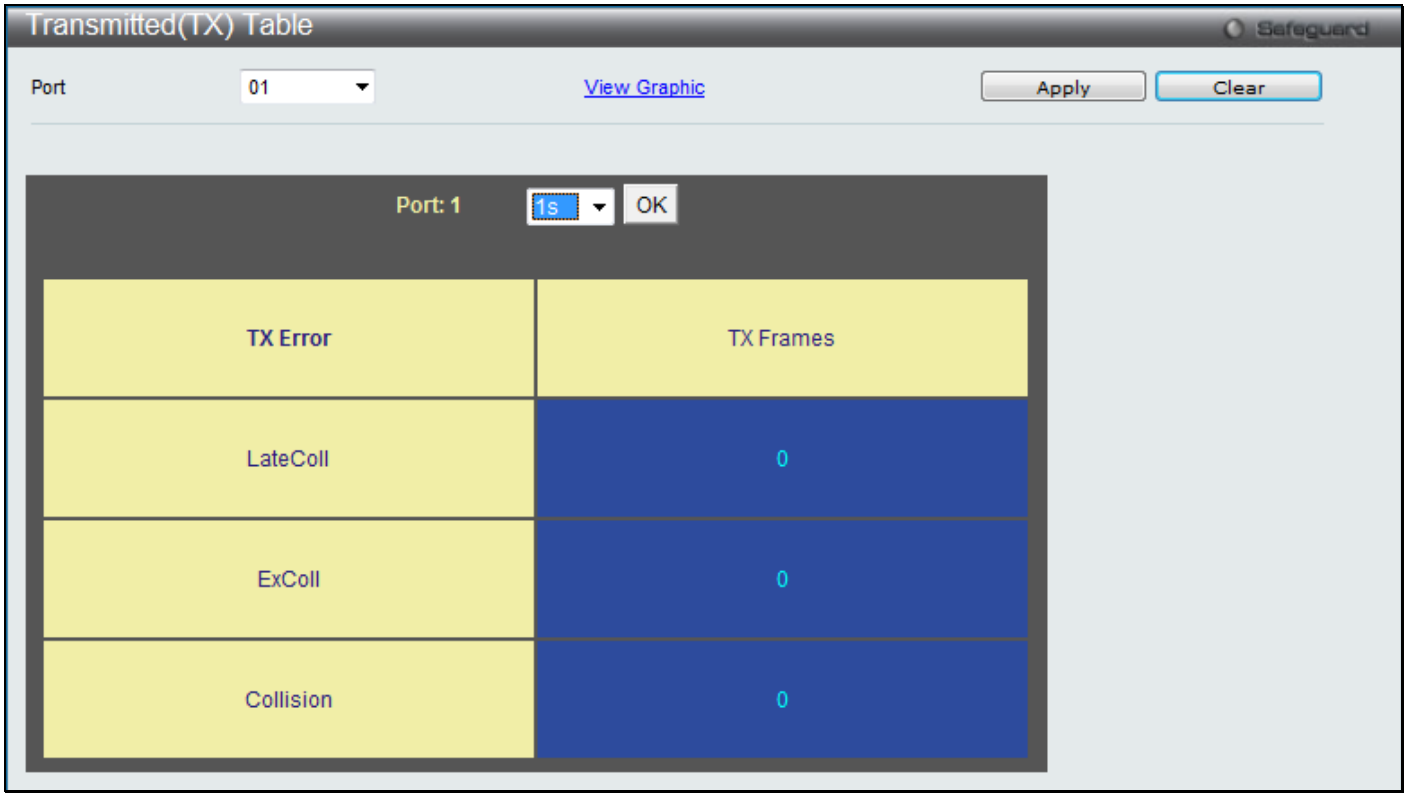


Figure 12-13 Transmitted (TX) –View Table window

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display LateColl, ExColl, and Collision errors.

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

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Packet Size

Users can display packets received by the Switch, arranged in six groups and classed by size, as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

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

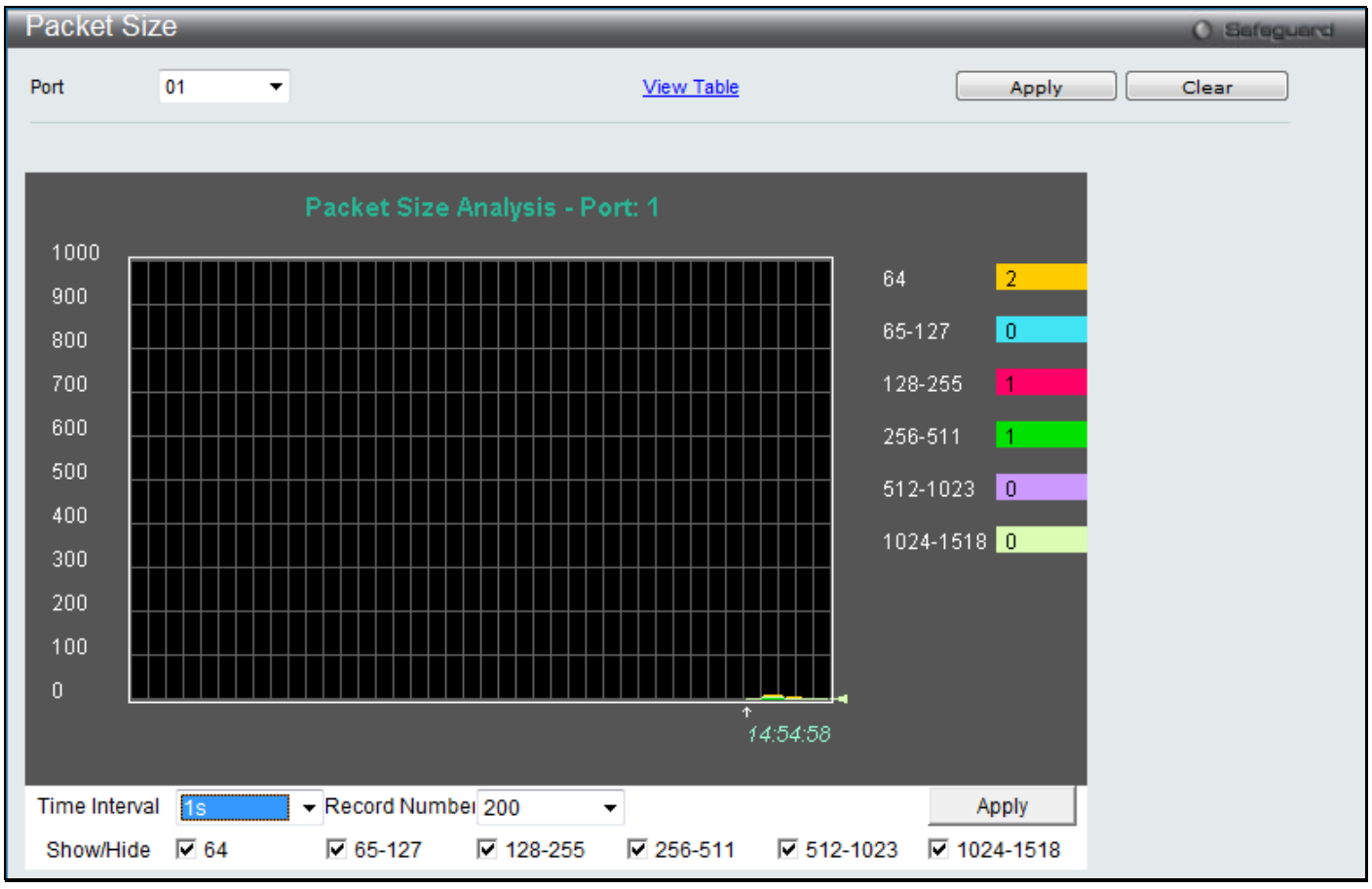


Figure 12-14 Packet Size window

Click the View Table link to display the information in a table rather than a line graph.

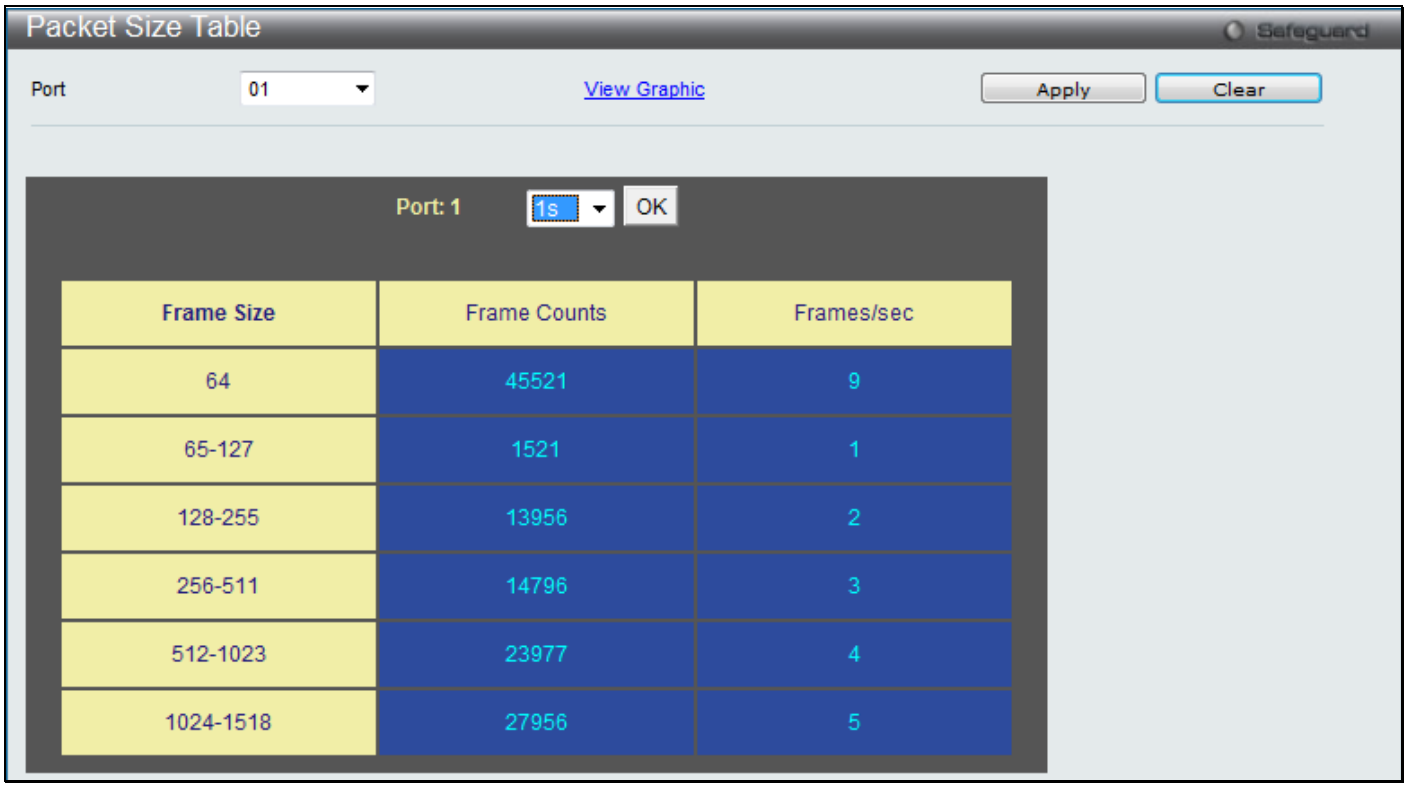


Figure 12-15 Packet Size – View Table window

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

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

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

VLAN Counter Statistics

On this page the user can view VLAN counter statistics.

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

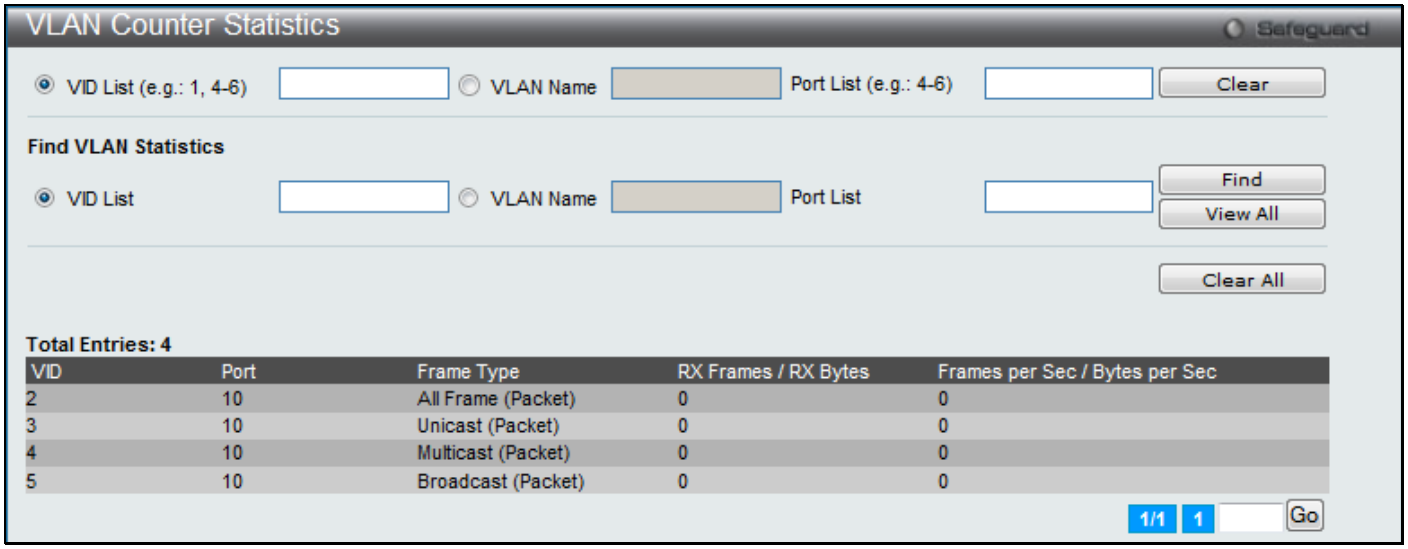


Figure 12-16 VLAN Counter Statistics window

The fields that can be configured are described below:

Parameter	Description
VID List	Here the user can enter a VID list to view.
VLAN Name	Here the user can enter VLAN Name to view.
Port List	Here the user can enter the appropriate port(s) to view.

Click the **Clear** button to clear all the information entered in the fields.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to display all the existing entries.
Click the **Clear All** button to remove all the entries listed in the table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Historical Counter & Utilization

Historical Counter

On this page the user can view information regarding the historical counter.

To view the following window, click **Monitoring > Statistics > Historical Counter & Utilization > Historical Counter**, as shown below:

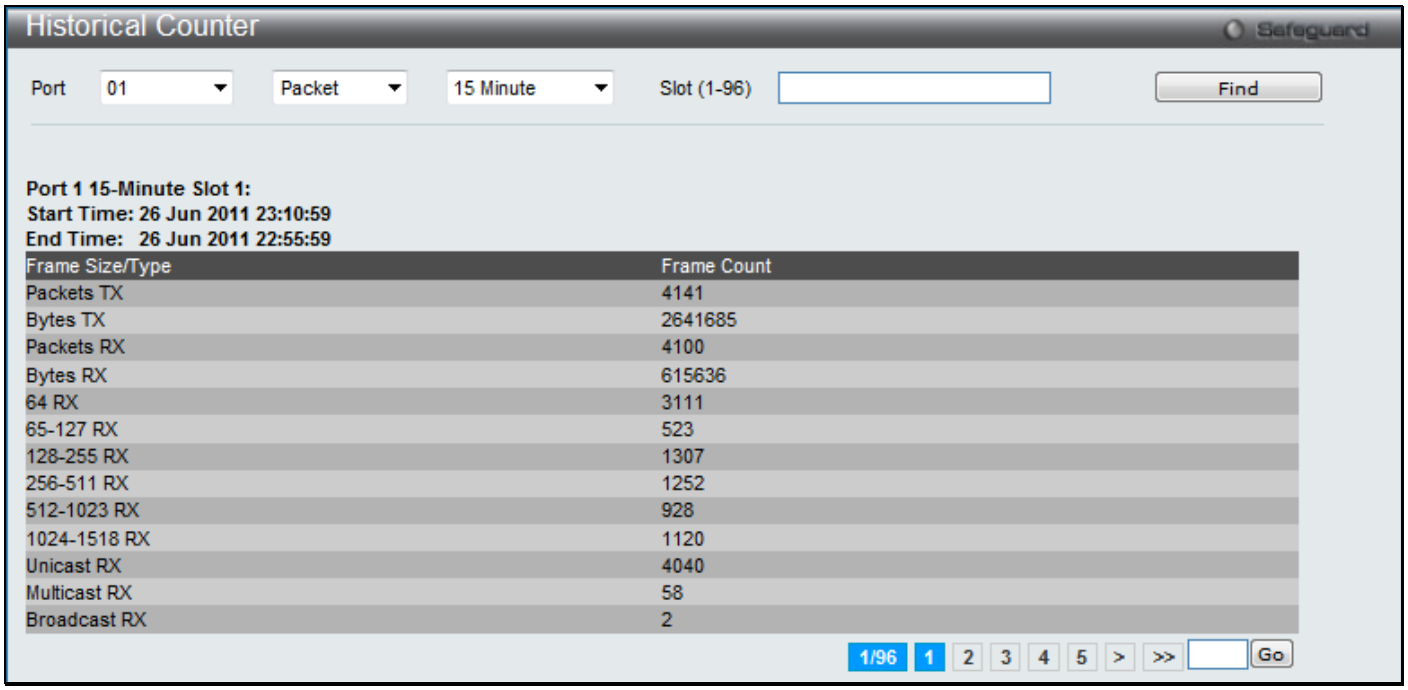


Figure 12-17 Historical Counter window

The fields that can be configured are described below:

Parameter	Description
Port	Here the user can select the appropriate port to view.
Packet	Selecting this option will display a frame count based on the packets send and received.
Error	Selecting this option will display a frame count based on the packet errors send and received.
Time	Here the user can select the time slot of how much information should be displayed based on the given time elapsed. Options to choose from are **15 Minute** and **1 Day**.
Slot (1-96)	Here the user can enter the slot number.

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.

Historical Utilization

On this page the user can view information regarding the historical utilization.

To view the following window, click **Monitoring > Statistics > Historical Counter & Utilization > Historical Utilization**, as shown below:

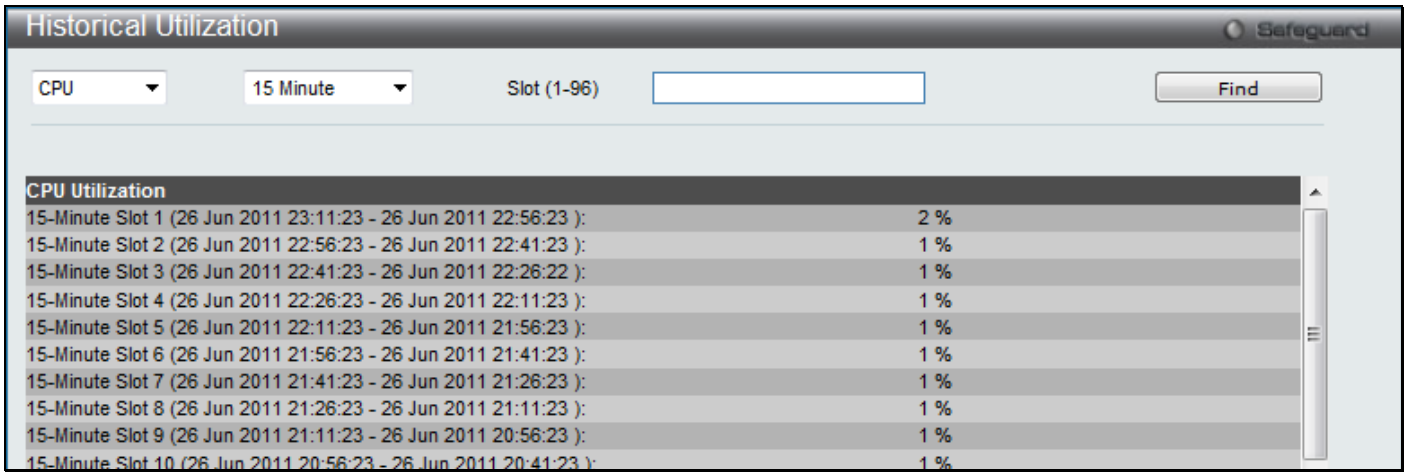


Figure 12-18 Historical Utilization – CPU window

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

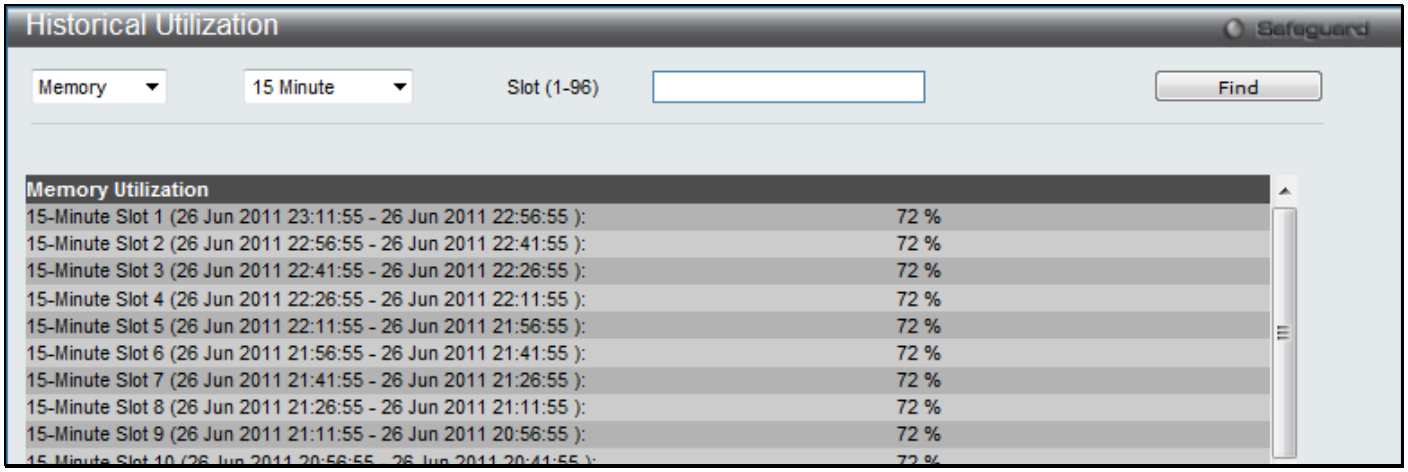


Figure 12-19 Historical Utilization – Memory window

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

Mirror

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored 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.

Port Mirror Settings

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

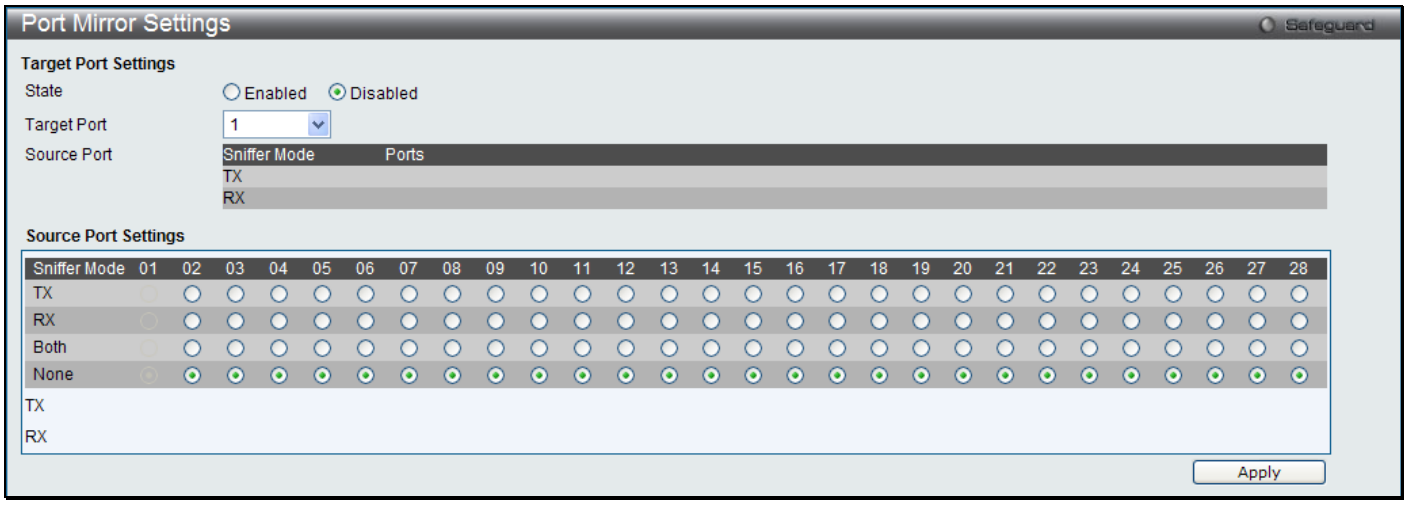


Figure 12-20 Port Mirror Settings window

The fields that can be configured are described below:

Parameter	Description
State	Here the user can *enable* or *disable* the Port Mirroring feature.
Target Port	Here the user can select the Target Port used for Port Mirroring.
TX	Here the user can select whether the port should include outgoing traffic.
RX	Here the user can select whether the port should include incoming traffic.
Both	Here the user can select whether the port should include both incoming and outgoing traffic.
None	Here the user can select whether the port should not include any traffic.

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

NOTE: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

RSPAN Settings

This page controls the RSPAN function. The purpose of the RSPAN function is to mirror packets to a remote switch. A packet travels from the switch where the monitored packet is received, passing through the intermediate switch, and then to the switch where the sniffer is attached. The first switch is also named the source switch.

To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source switch. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.

NOTE: RSPAN VLAN mirroring will only work when RSPAN is enabled (when one RSPAN VLAN has been configured with a source port). The RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

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

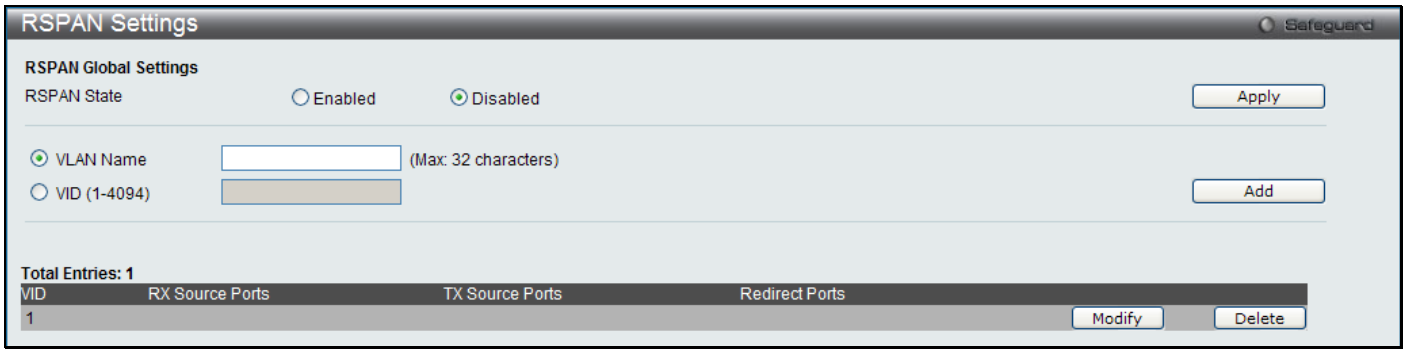


Figure 12-21 RSPAN Settings window

The fields that can be configured are described below:

Parameter	Description
RSPAN State	Here the user can enable or disable the RSPAN feature.
VLAN Name	Create the RSPAN VLAN by VLAN name.
VID (1-4094)	Create the RSPAN VLAN by VLAN ID.

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 **Modify** button to re-configure the specific entry.

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

After clicking the **Modify** button, the following page will appear:

Figure 12-22 RSPAN Settings – Modify window

The fields that can be configured are described below:

Parameter	Description
Source Ports	If the ports are not specified by option, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters. Select **RX, TX** or **Both** to specify in which direction the packets will be monitored. Tick **Add** or **Delete** to add or delete source ports.
Redirect Port List	Specify the output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets. Tick **Add** or **Delete** to add or delete redirect ports.

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

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

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 Global Settings

Here the user can enable or disable the sFlow feature.

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

Figure 12-23 sFlow Global Settings window

The fields that can be configured are described below:

Parameter	Description
sFlow State	Here the user can enable or disable the sFlow feature.

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

sFlow Analyzer Server Settings

On this page the user can configure the sFlow analyzer server parameters.

We can support 4 different Analyzer Servers at the same time and each sampler or poller can select a collector to send the samples. We can send different samples from different samplers or pollers to different collectors.

To view the following window, click **Monitoring > sFlow > sFlow Analyzer Server Settings**, as shown below:

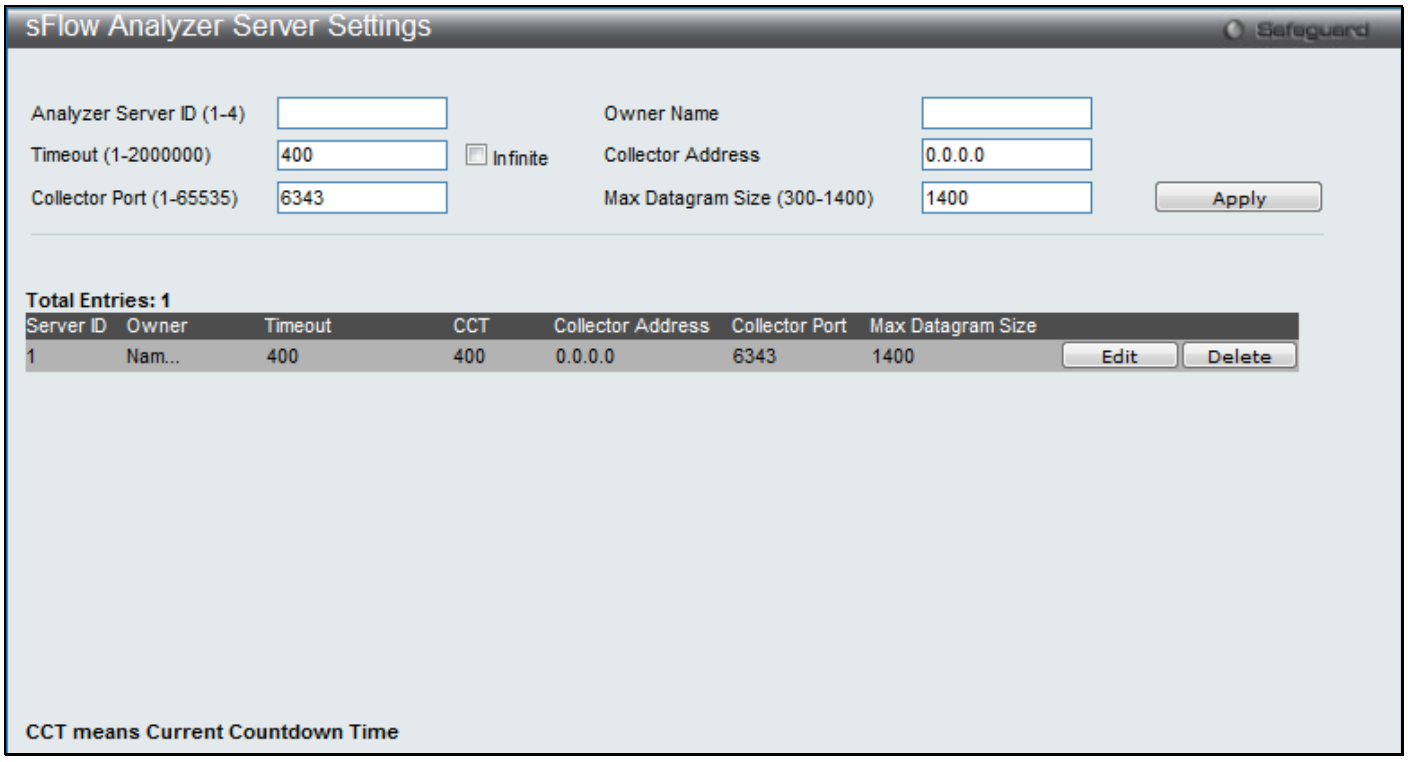


Figure 12-24 sFlow Analyzer Server Settings window

The fields that can be configured are described below:

Parameter	Description
Analyzer Server ID	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Owner Name	The entity making use of this sFlow analyzer server. When owner is set or modified, the timeout value will become 400 automatically.
Timeout	The length of time before the server times out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. If not specified, its default value is 400.
Collector Address	The IP address of the analyzer server. If not specified or set a 0 address, the entry will be inactive.
Collector Port	The destination UDP port for sending the sFlow datagrams. If not specified, the default value is *6343.*
Max Datagram Size	The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.

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.

sFlow Flow Sampler Settings

On this page the user can configure the sFlow flow sampler parameters. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.

NOTE: If the user wants to change the analyze server ID, he needs to delete the flow sampler and creates a new one.

To view the following window, click **Monitoring > sFlow > sFlow Flow Sampler Settings**, as shown below:

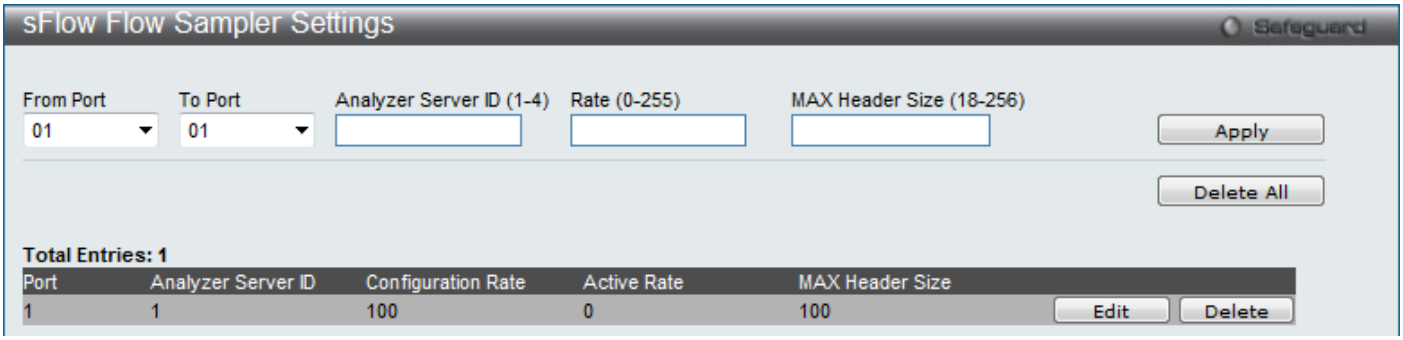


Figure 12-25 sFlow Flow Sampler Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Specifies the list of ports to be configured.
Analyzer Server ID (1-4)	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Rate (0-255)	The sampling rate for packet Rx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.
MAX Header Size (18-	The maximum number of leading bytes in the packet which has been sampled that will be

256)	encapsulated and forwarded to the server. If not specified, the default value is 128.

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

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

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

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

sFlow Counter Poller Settings

On this page the user can configure the sFlow counter poller parameters. If the user wants to change the analyzer server ID, he needs to delete the counter poller and create a new one.

To view the following window, click **Monitoring > sFlow > sFlow Counter Poller Settings**, as shown below:

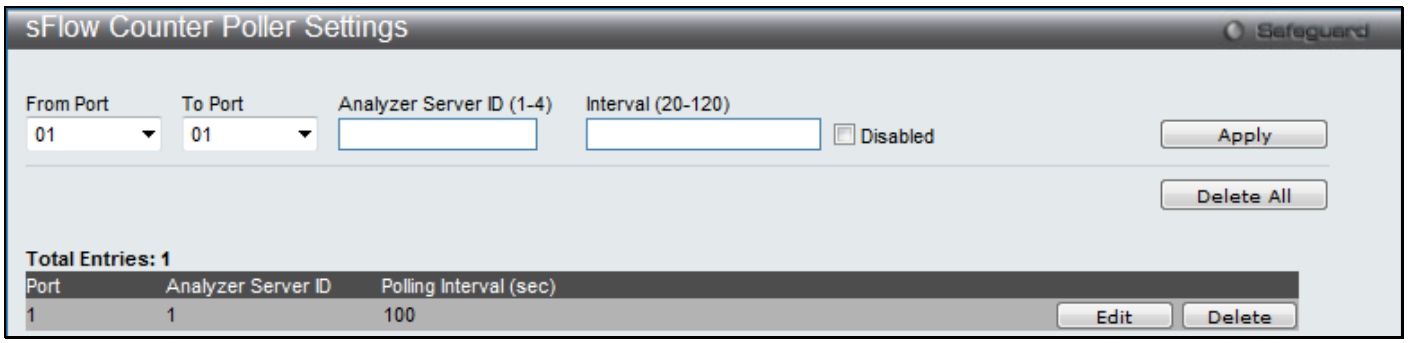


Figure 12-26 sFlow Counter Poller Settings window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Specifies the list of ports to be configured.
Analyzer Server ID (1-4)	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Interval (20-120)	The maximum number of seconds between successive samples of the counters. Tick the **Disable** check box to disable the polling interval.

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

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

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

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

Ping Test

Users can Ping either an IPv4 address or an IPv6 address. Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

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

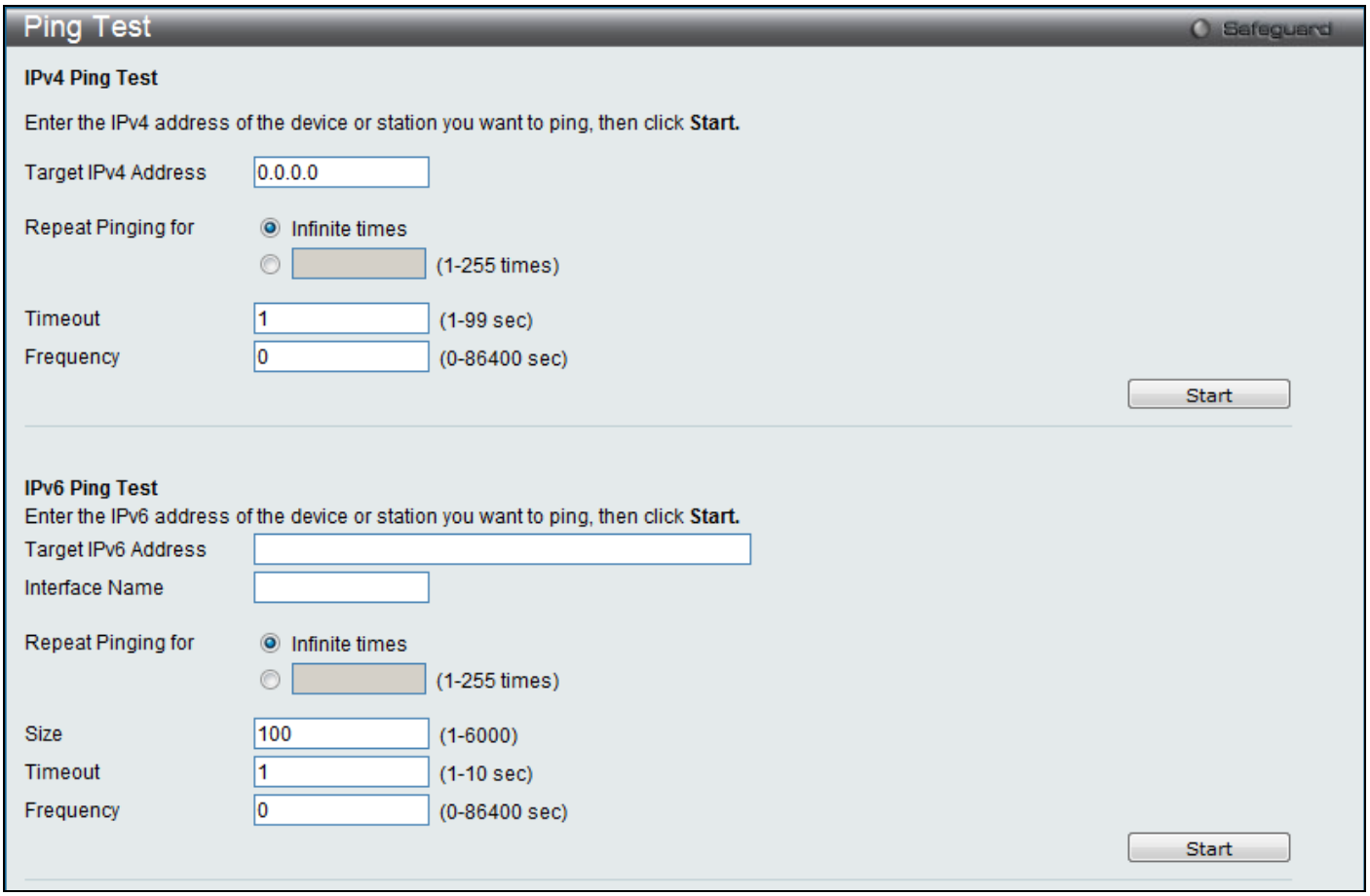


Figure 12-27 Ping Test window

The user may click the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between *1* and *255*.

The fields that can be configured are described below:

Parameter	Description
Target IP Address	Enter an IP address to be pinged.
Interface Name	For IPv6 Link local address only, enter the name of the interface to be Pinged.
Repeat Pinging for	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between *1* and *255*.
Size	For IPv6 only, enter a value between *1* and *6000*. The default is *100*.
Timeout	For IPv4, select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. For IPv6, select a timeout period between *1* and *10* seconds for this Ping message to reach its destination. In either case, if the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Frequency	Enter the ping test frequency value used here. This is the waiting time before repeating a ping test. This value must be between 0 and 86400 seconds.

Click the **Start** button to initiate the Ping Test

After clicking the **Start** button, the following page will appear:

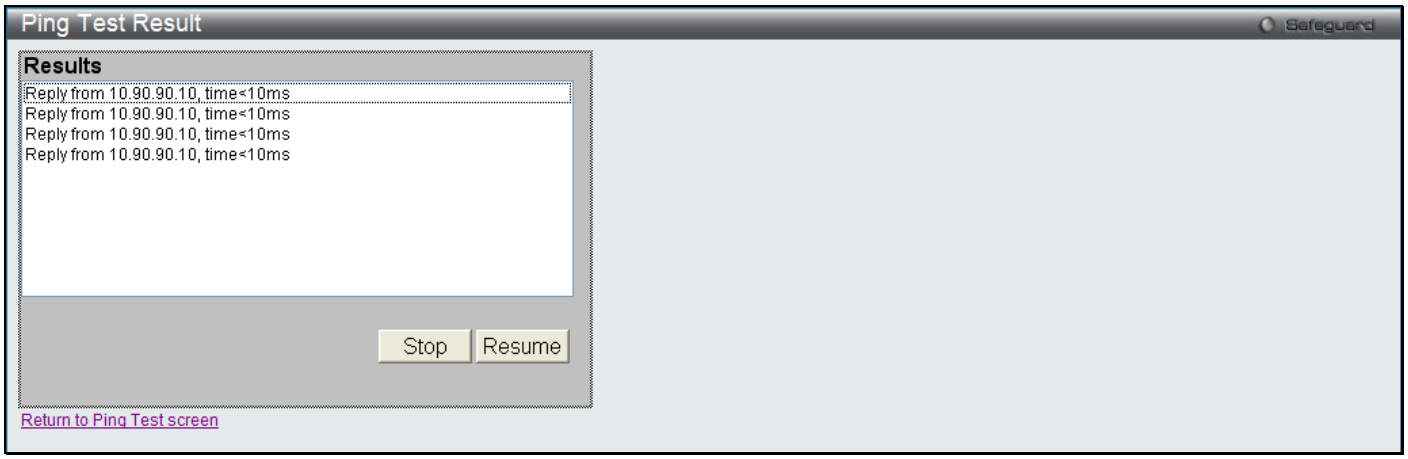


Figure 12-28 Ping Test – Result window

Click the **Stop** button to halt the Ping Test
Click the **Resume** button to resume the Ping Test

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 **Monitoring > Trace Route**, as shown below:

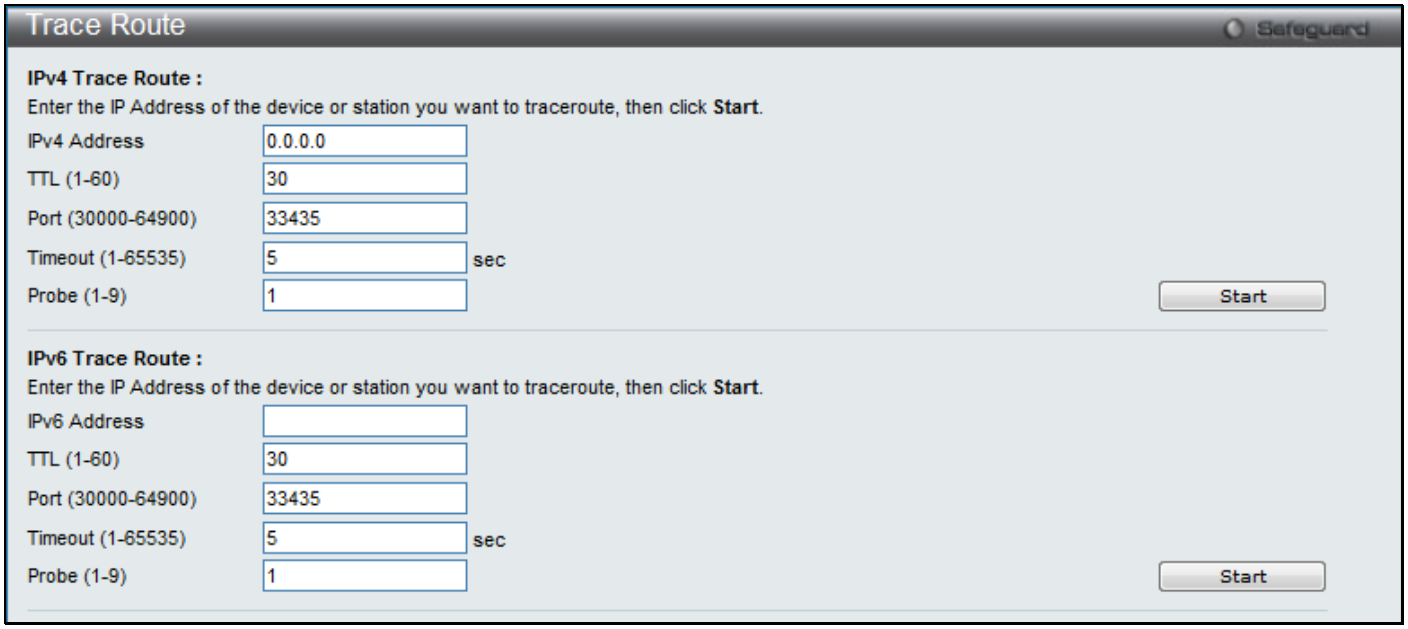


Figure 12-29 Trace Route window

The fields that can be configured are described below:

Parameter	Description
IPv4 Address / IPv6 Address	IP address of the destination station.
TTL (1-60)	The time to live value of the trace route request. 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 (30000-64900)	The port number. The value range is from 30000 to 64900.
Timeout (1-65535)	Defines the timeout period while waiting for a response from the remote device. A value of

	1 to 65535 seconds can be specified. The default is 5 seconds.
Probe (1-9)	The number of probing. The range is from 1 to 9. If unspecified, the default value is 1.

Click the **Start** button to initiate the Trace Route

After clicking the **Start** button, the following page will appear:

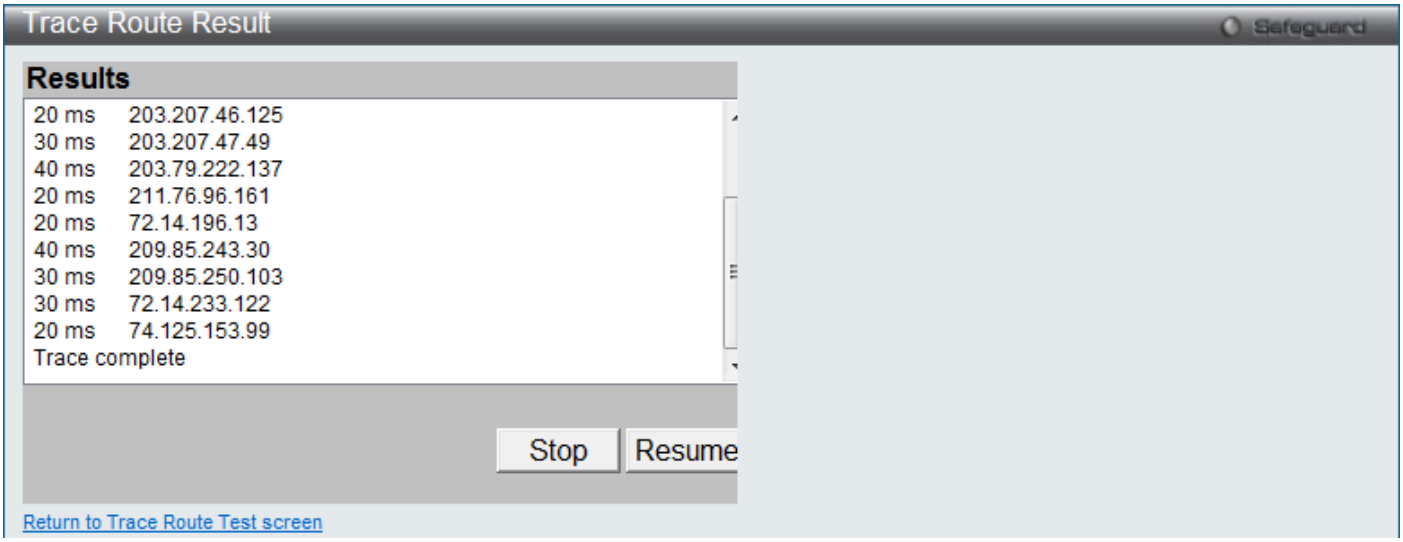


Figure 12-30 Trace Route – Result window

Click the **Stop** button to halt the Trace Route
Click the **Resume** button to resume the Trace Route

Device Environment

The device environment feature displays the Switch internal temperature status.

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

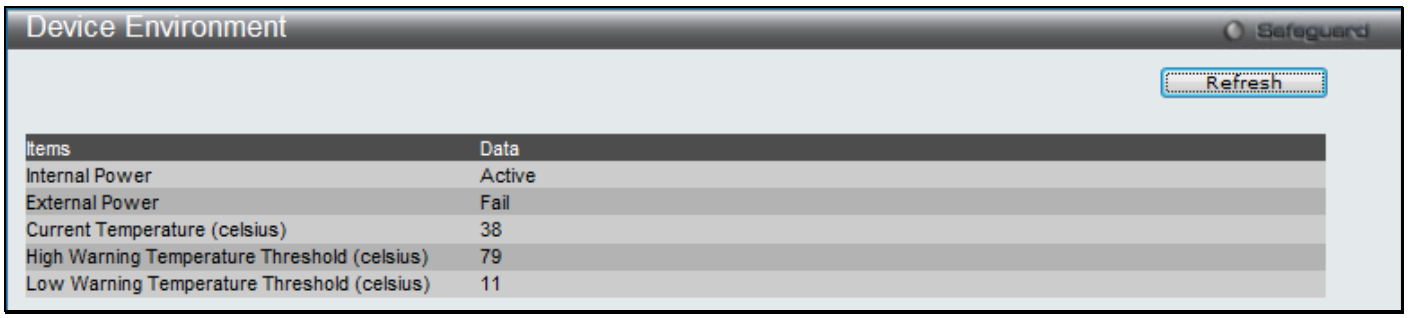


Figure 12-31 Device Environment window

Click the **Refresh** button to refresh the display table so that new entries will appear.

Chapter 13 Save and Tools

Save Configuration / Log
License Management
Download Firmware
Upload Firmware
Download Configuration
Upload Configuration
Upload Log File
Reset
Reboot System

Save Configuration / Log

Save Configuration allows the user to backup the configuration of the switch to a folder on the computer. Select **Configuration** from the **Type** field and enter the **File Path** in the space provided and click **Apply**.

To view the following window, click **Save > Save Configuration / Log**, as shown below:

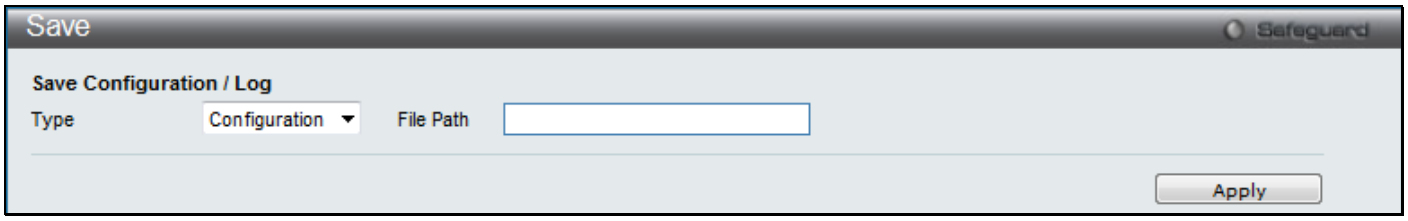


Figure 13-1 Save – Configuration window

Save Log allows the user to backup the log file of the switch. Select **Log** from the **Type** field and click **Apply**.

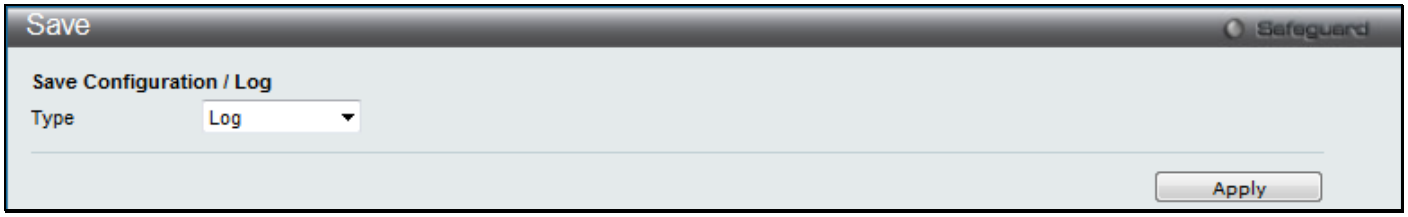


Figure 13-2 Save – Log window

Save All allows the user to permanently save changes made to the configuration. This option will allow the changes to be kept after the switch has rebooted. Select **All** from the **Type** field and click **Apply**.

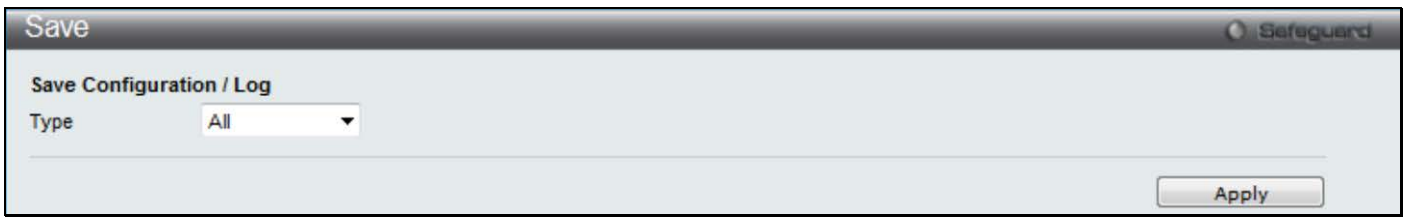


Figure 13-3 Save – All window

License Management

This window is used to install and display D-Link License Management System (DLMS) activation code.
To view this window, click **Tools > License Management**, as shown below.

Figure 13-4 License Management window

The fields that can be configured are described below:

Parameter	Description
Activation Code	Enter an activation code.

Click the **Install** button to install the DLMS activation code.

Download Firmware

The following window is used to download firmware for the Switch.
To view the following window, click **Tools > Download Firmware**, as shown below:

Download Firmware From TFTP

This page allows the user to download firmware from a TFTP Server to the Switch and updates the switch.

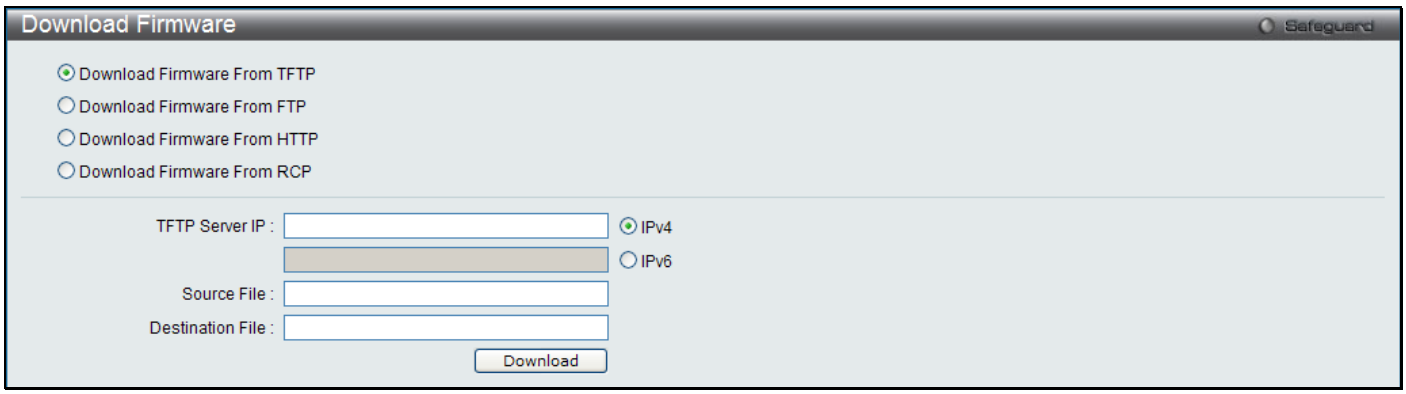


Figure 13-5 Download Firmware From TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Here the user can enter the TFTP Server IP Address used. The user can select **IPv4** to input an IPv4 address or select **IPv6** to input an IPv6 address in the space provided.
Source File	Here the user can enter the location and name of the Source File.
Destination File	Here the user can enter the location and name of the Destination File.

Click **Download** to initiate the download.

Download Firmware From FTP

This page allows the user to download firmware from a FTP Server to the Switch and updates the switch.

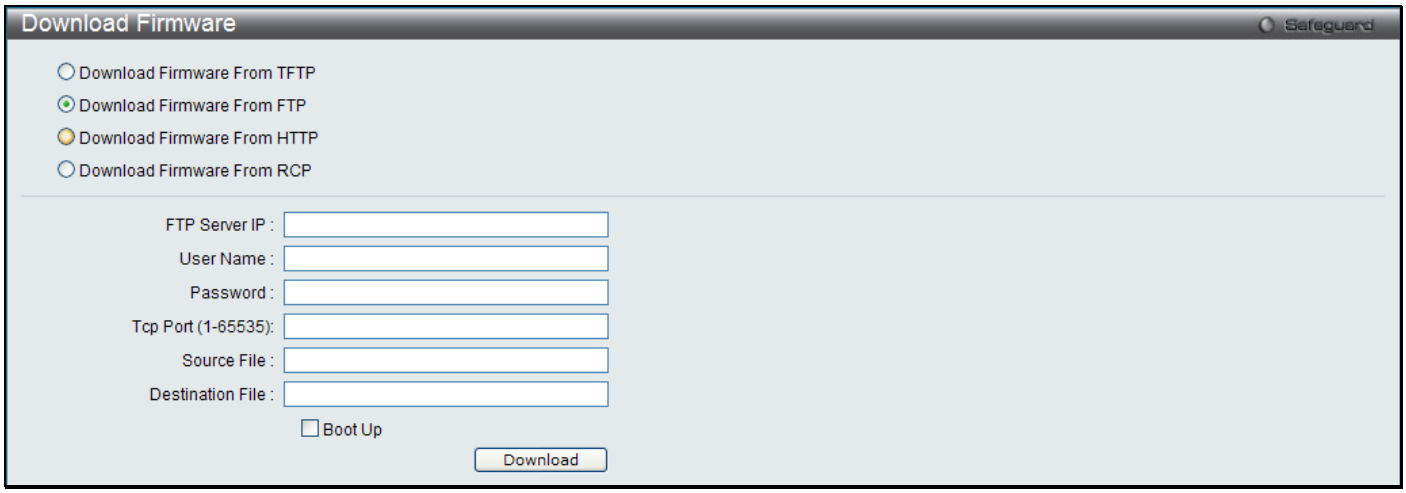


Figure 13-6 Download Firmware From TFTP window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Here the user can enter the FTP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Password	Here the user can enter the appropriate Password used.
TCP Port	Here the user can enter the TCP Port number used.
Source File	Here the user can enter the location and name of the Source File.
Destination File	Here the user can enter the location and name of the Destination File.
Boot U	Select this option to use this firmware as the boot-up firmware.

Click **Download** to initiate the download.

Download Firmware From HTTP

This page allows the user to download firmware from a computer to the Switch and updates the switch.

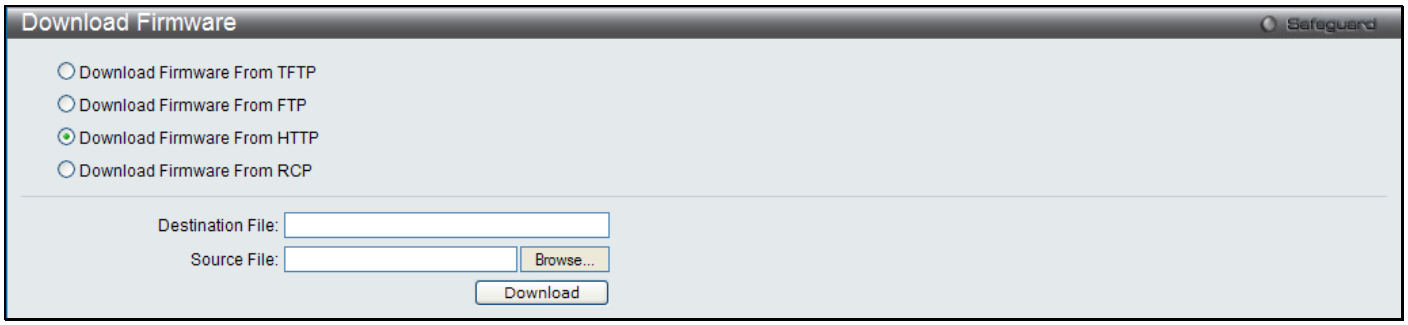


Figure 13-7 Download Firmware From HTTP window

The fields that can be configured are described below:

Parameter	Description
Destination File	Here the user can enter the location of the Destination File.
Source File	Here the user can enter the location of the Source File. Click on the **Browse** button to navigate to the firmware file for the download.

Click **Download** to initiate the download.

Download Firmware From RCP

This page allows the user to download firmware from a RCP Server to the Switch and updates the switch.

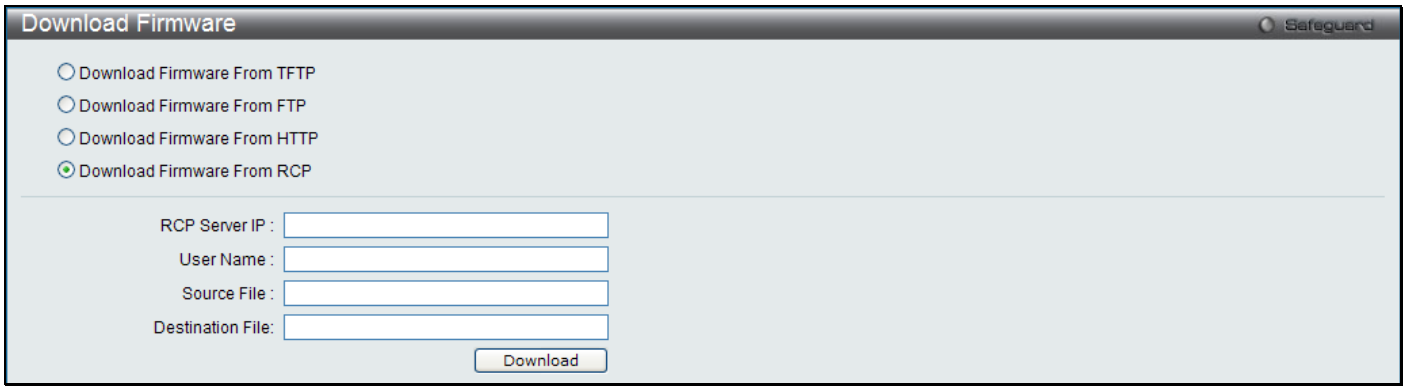


Figure 13-8 Download Firmware From RCP window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Here the user can enter the RCP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Source File	Here the user can enter the location and name of the Source File.
Destination File	Here the user can enter the location and name of the Destination File.

Click **Download** to initiate the download.

Upload Firmware

The following window is used to upload firmware from the Switch.
To view the following window, click **Tools > Upload Firmware**, as shown below:

Upload Firmware To TFTP

This page allows the user to upload firmware from the Switch to a TFTP Server.

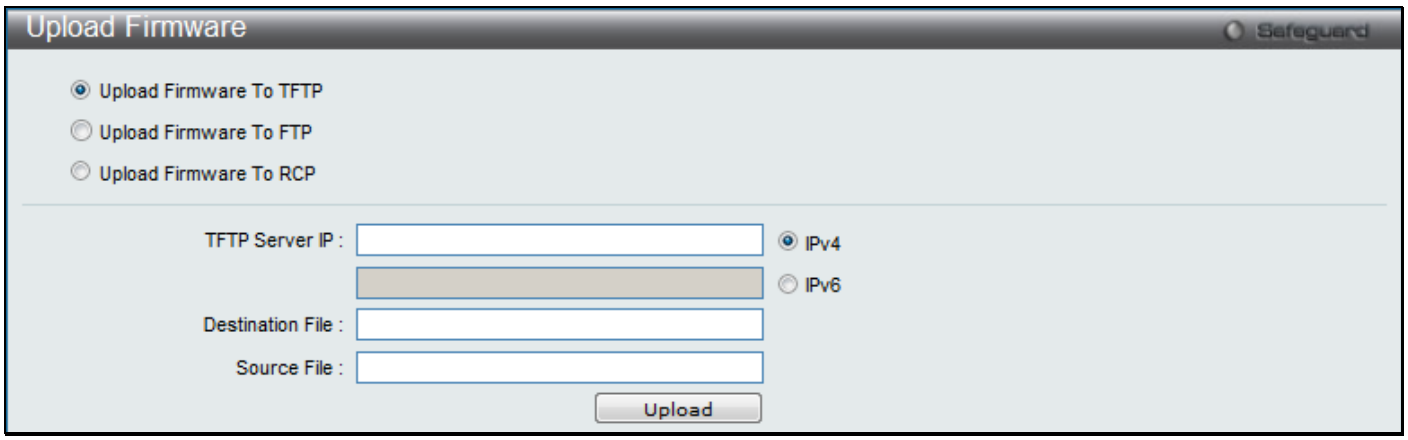


Figure 13-9 Upload Firmware To TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Here the user can enter the TFTP Server IP Address used. The user can select **IPv4** to input an IPv4 address or select **IPv6** to input an IPv6 address in the space provided.
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.

Click **Upload** to initiate the upload.

Upload Firmware To FTP

This page allows the user to upload firmware from the Switch to a FTP Server.

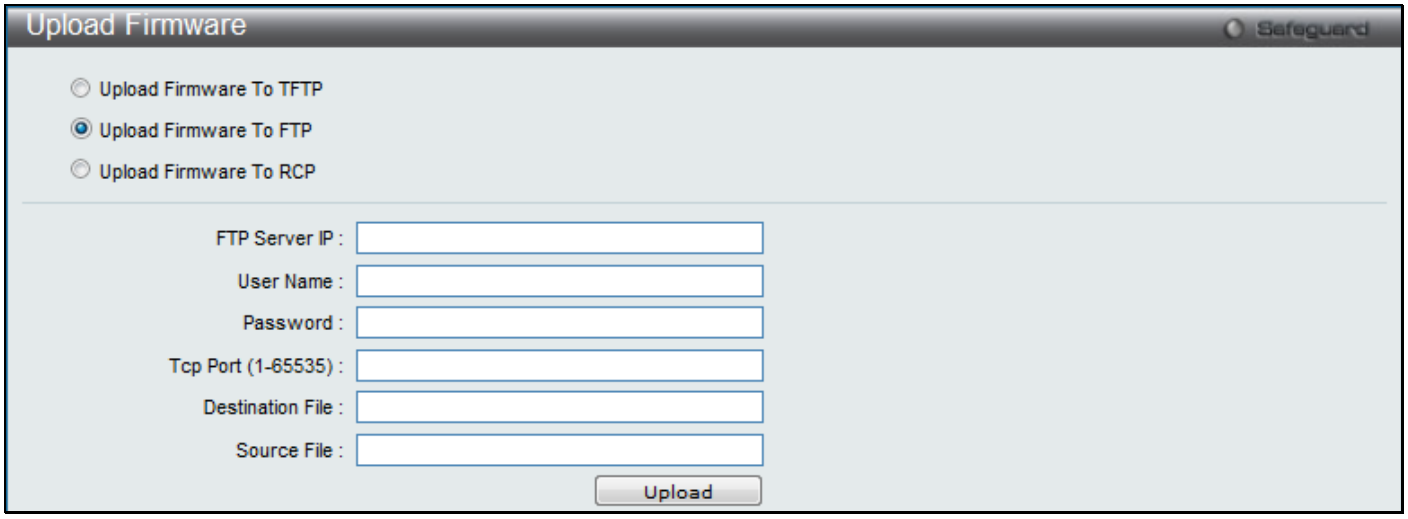


Figure 13-10 Upload Firmware To FTP window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Here the user can enter the FTP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Password	Here the user can enter the appropriate Password used.
TCP Port	Here the user can enter the TCP Port number used.
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.

Click **Upload** to initiate the upload.

Upload Firmware To RCP

This page allows the user to upload firmware from the Switch to a RCP Server.

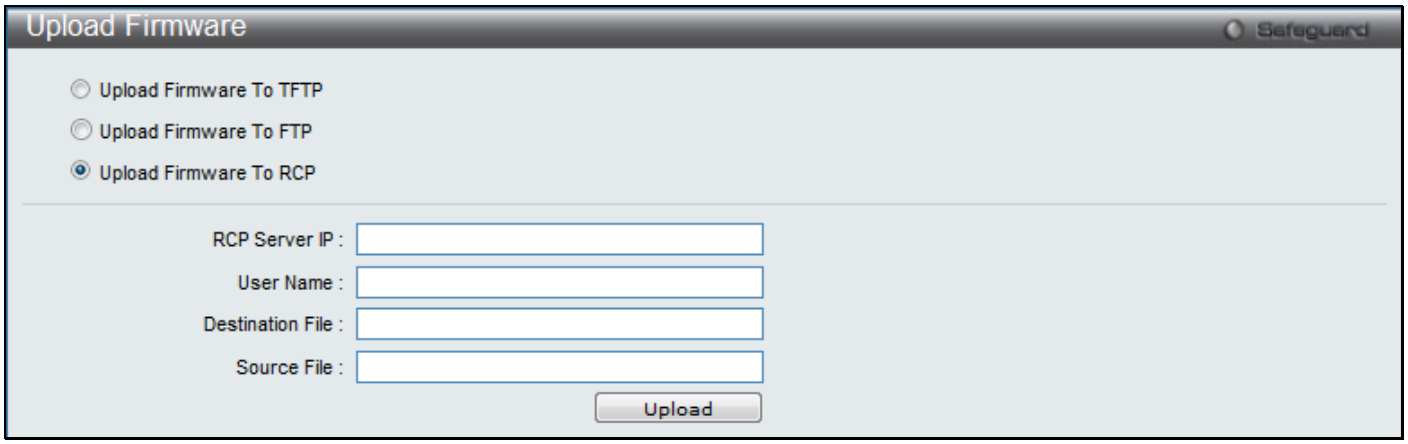


Figure 13-11 Upload Firmware To RCP window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Here the user can enter the RCP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.

Click **Upload** to initiate the upload.

Download Configuration

The following window is used to download the configuration file for the Switch.
To view the following window, click **Tools > Download Configuration**, as shown below:

Download Configuration From TFTP

This page allows the user to download the configuration file from a TFTP Server to the Switch and updates the switch.

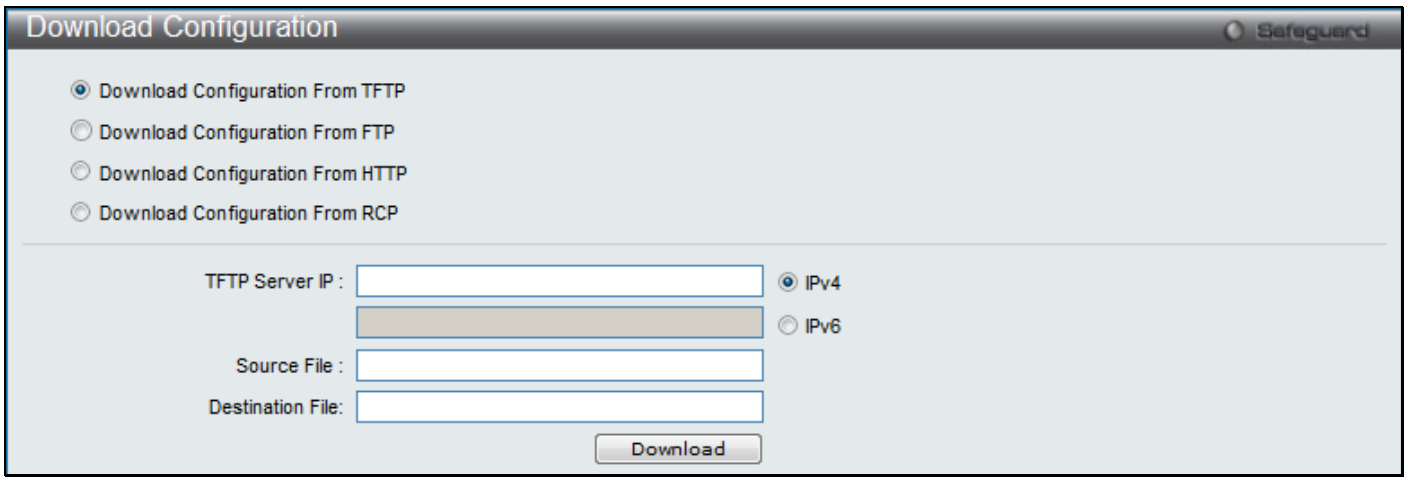


Figure 13-12 Download Configuration From TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Here the user can enter the TFTP Server IP Address used. The user can select **IPv4** to input an IPv4 address or select **IPv6** to input an IPv6 address in the space provided.

Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.

Click **Download** to initiate the download.

Download Configuration From FTP

This page allows the user to download the configuration file from a FTP Server to the Switch and updates the switch.

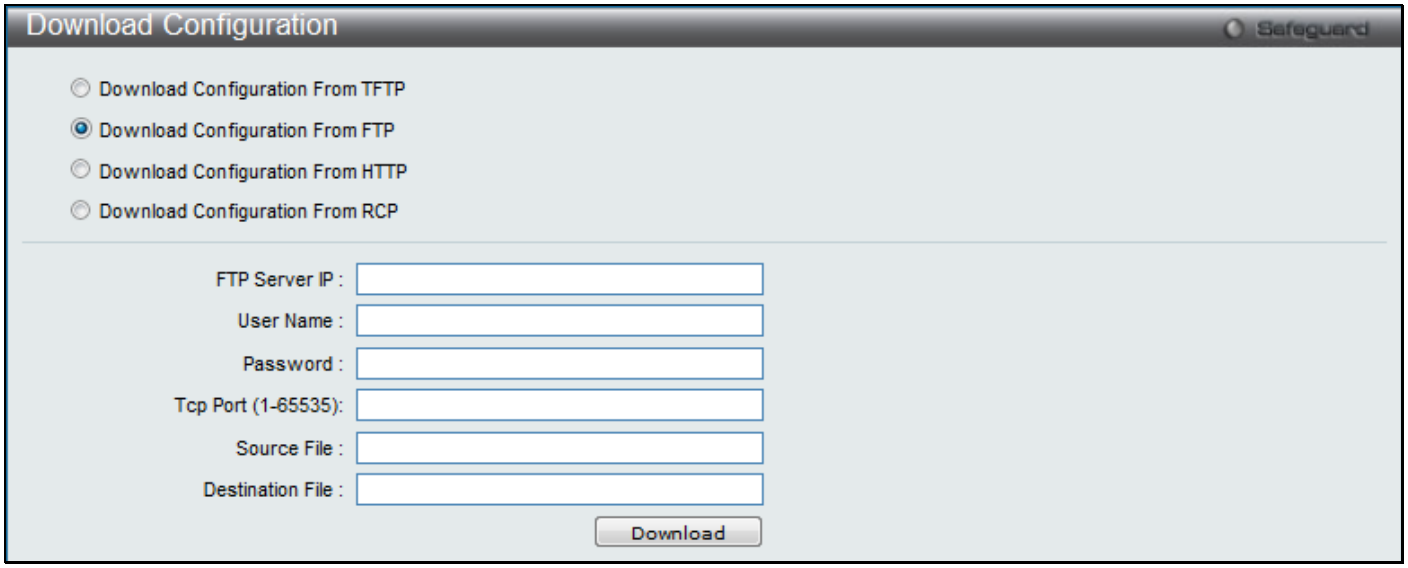


Figure 13-13 Download Configuration From FTP window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Here the user can enter the FTP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Password	Here the user can enter the appropriate Password used.
TCP Port	Here the user can enter the TCP Port number used.
Source File	Here the user can enter the location and name of the Source File.
Destination File	Here the user can enter the location and name of the Destination File.

Click **Download** to initiate the download.

Download Configuration From HTTP

This page allows the user to download the configuration file from a computer to the Switch and updates the switch.

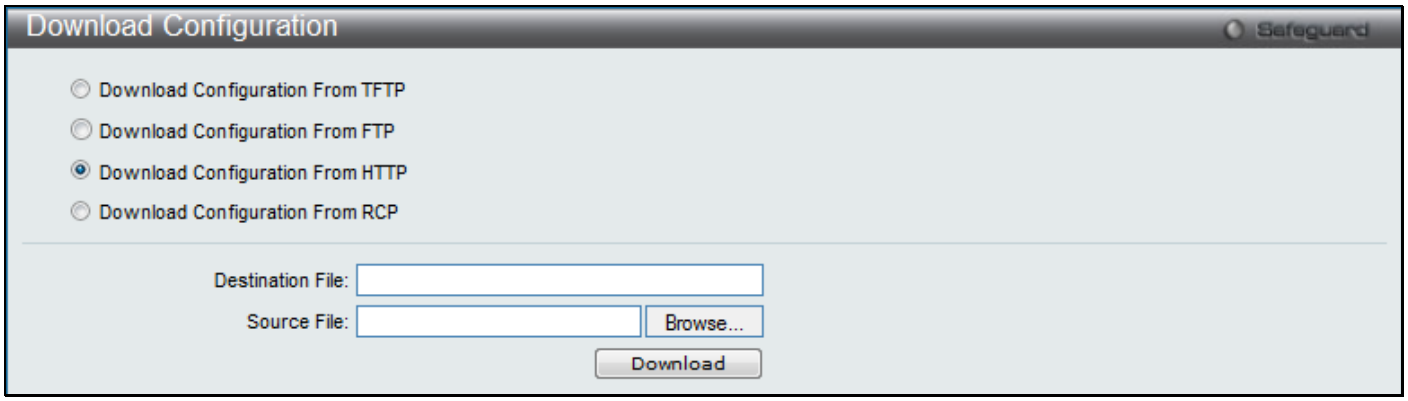


Figure 13-14 Download Configuration From HTTP window

The fields that can be configured are described below:

Parameter	Description
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File. Click on the **Browse** button to navigate to the configuration file for the download.

Click **Download** to initiate the download.

Download Configuration From RCP

This page allows the user to download the configuration file from a RCP Server to the Switch and updates the switch.

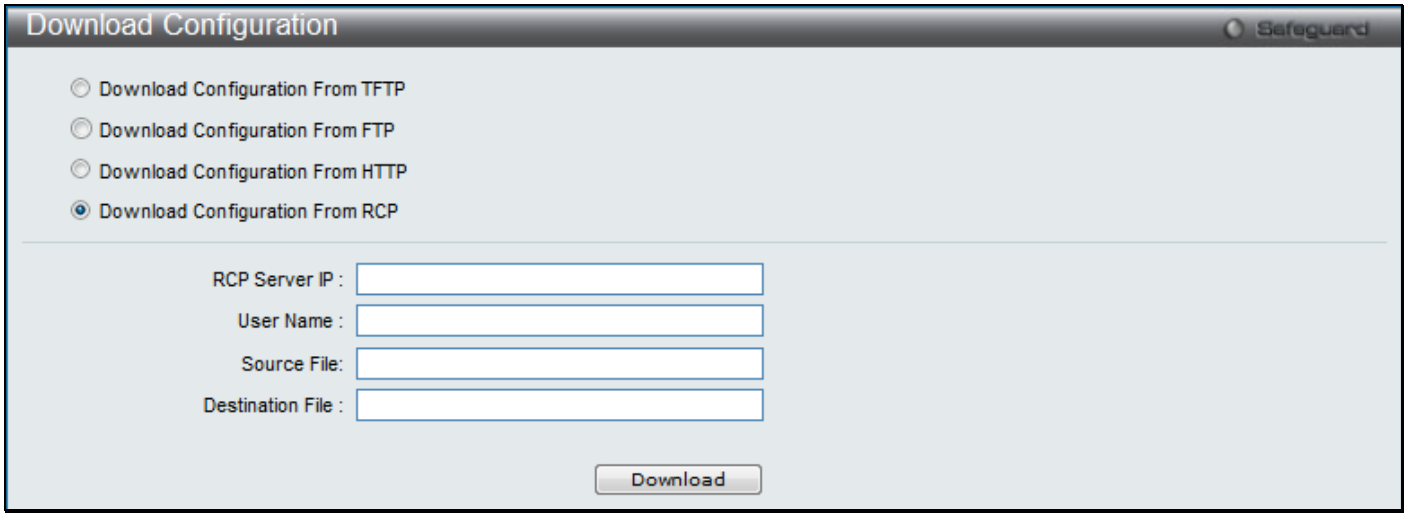


Figure 13-15 Download Configuration From RCP window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Here the user can enter the RCP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Source File	Here the user can enter the location and name of the Source File.
Destination File	Here the user can enter the location and name of the Destination File.

Click **Download** to initiate the download.

Upload Configuration

The following window is used to upload the configuration file from the Switch.
To view the following window, click **Tools > Upload Configuration**, as shown below:

Upload Configuration To TFTP

This page allows the user to upload the configuration file from the Switch to a TFTP Server.

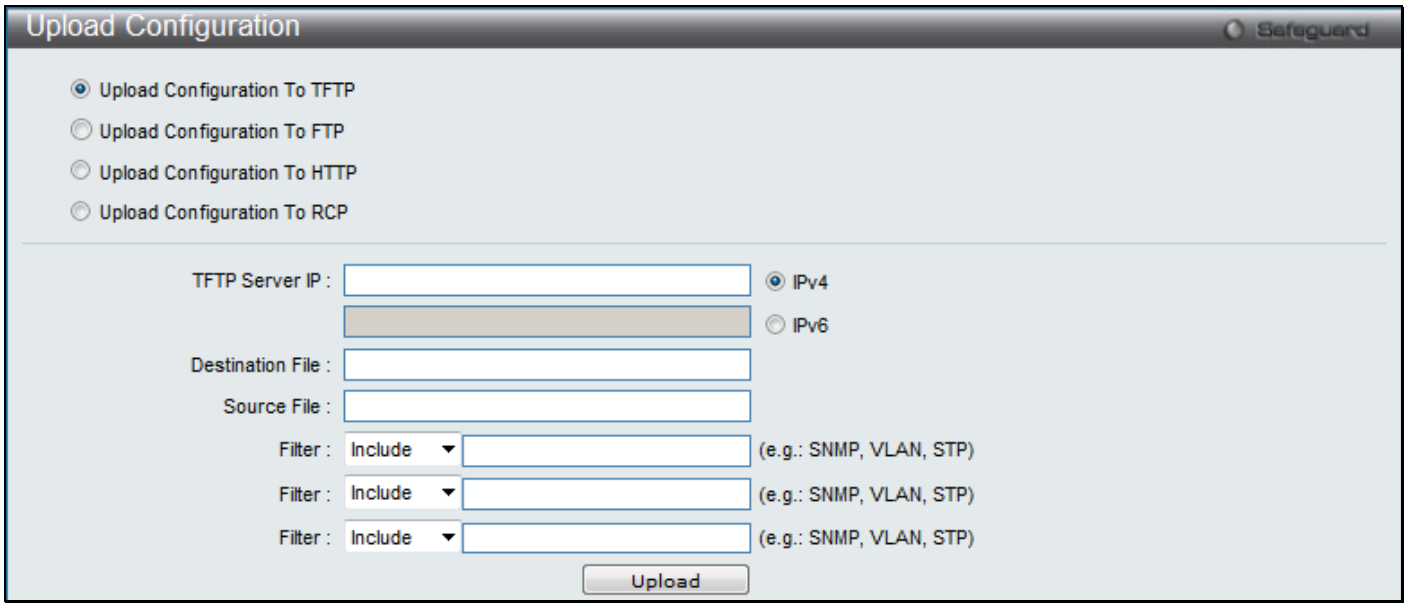


Figure 13-16 Upload Configuration To TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Here the user can enter the TFTP Server IP Address used. The user can select **IPv4** to input an IPv4 address or select **IPv6** to input an IPv6 address in the space provided.
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.
Filter	Here the user can specify to *include, begin* or *exclude* a filter like SNMP, VLAN or STP. Select the appropriate **Filter** action and enter the service name in the space provided.

Click **Upload** to initiate the upload.

Upload Configuration To FTP

This page allows the user to upload the configuration file from the Switch to a FTP Server.

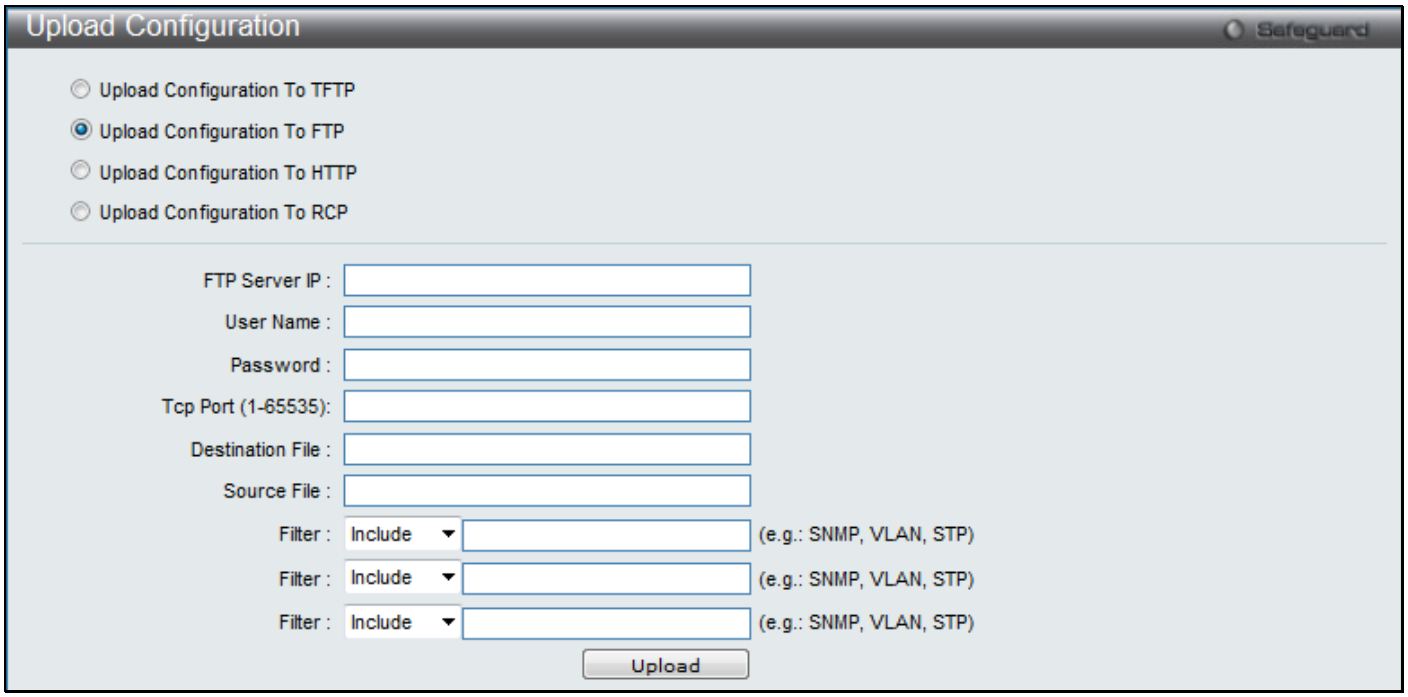


Figure 13-17 Upload Configuration To FTP window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Here the user can enter the FTP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Password	Here the user can enter the appropriate Password used.
TCP Port	Here the user can enter the TCP Port number used.
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.
Filter	Here the user can specify to *include, begin* or *exclude* a filter like SNMP, VLAN or STP. Select the appropriate **Filter** action and enter the service name in the space provided.

Click **Upload** to initiate the upload.

Upload Configuration To HTTP

This page allows the user to upload the configuration file from the Switch to a computer.

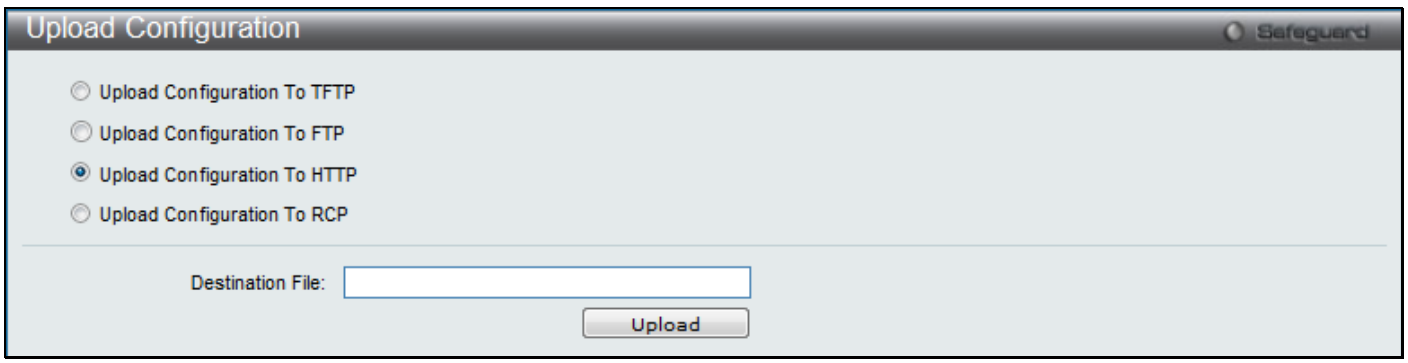


Figure 13-18 Upload Configuration To HTTP window

The fields that can be configured are described below:

Parameter	Description
Destination File	Here the user can enter the location and name of the Destination File.

Click **Upload** to initiate the upload.

Upload Configuration To RCP

This page allows the user to upload the configuration file from the Switch to a RCP Server.

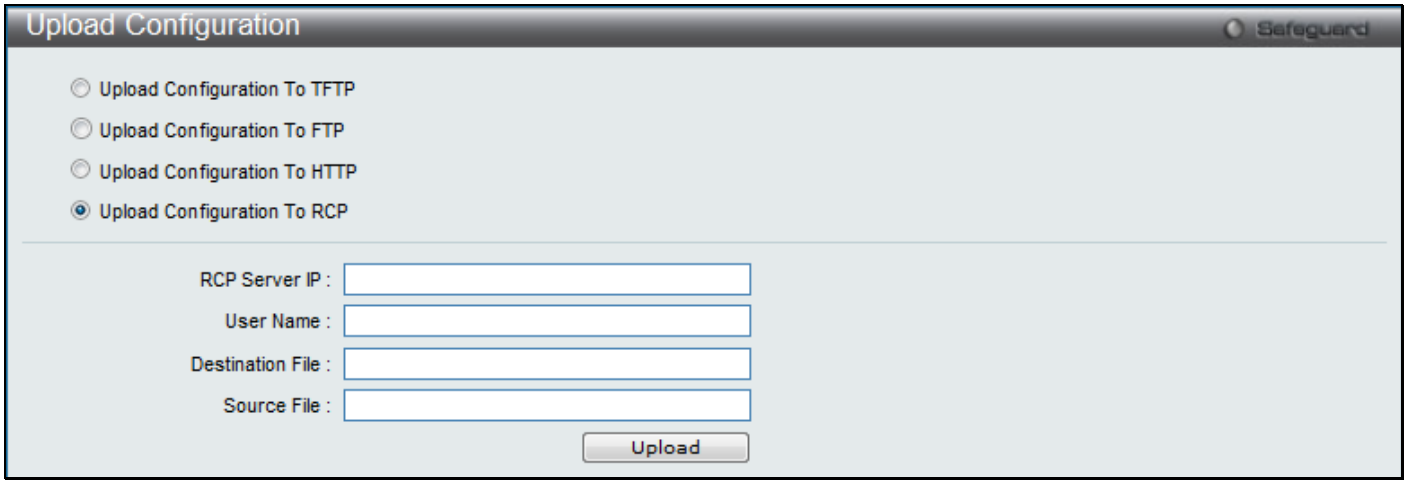


Figure 13-19 Upload Configuration To RCP window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Here the user can enter the RCP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Destination File	Here the user can enter the location and name of the Destination File.
Source File	Here the user can enter the location and name of the Source File.

Click **Upload** to initiate the upload.

Upload Log File

The following window is used to upload the log file from the Switch.
To view the following window, click **Tools > Upload Log File**, as shown below:

Upload Log To TFTP

This page allows the user to upload the log file from the Switch to a TFTP Server.

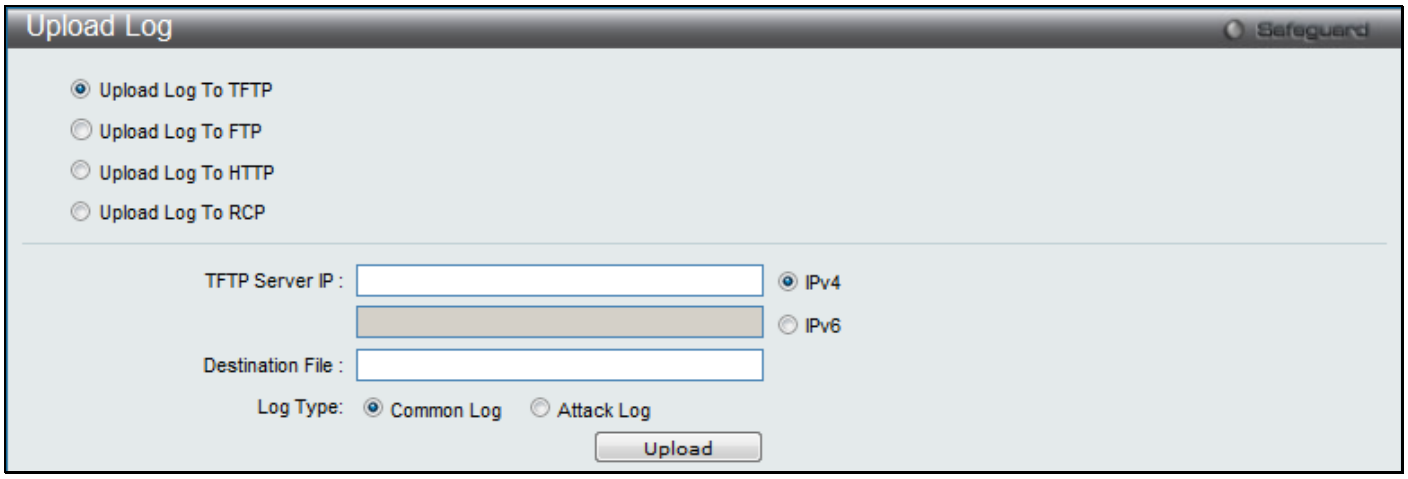


Figure 13-20 Upload Log To TFTP window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Here the user can enter the TFTP Server IP Address used. The user can select **IPv4** to input an IPv4 address or select **IPv6** to input an IPv6 address in the space provided.
Destination File	Here the user can enter the location and name of the Destination File.
Log Type	Here the user can select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Upload Log To FTP

This page allows the user to upload the log file from the Switch to a FTP Server.

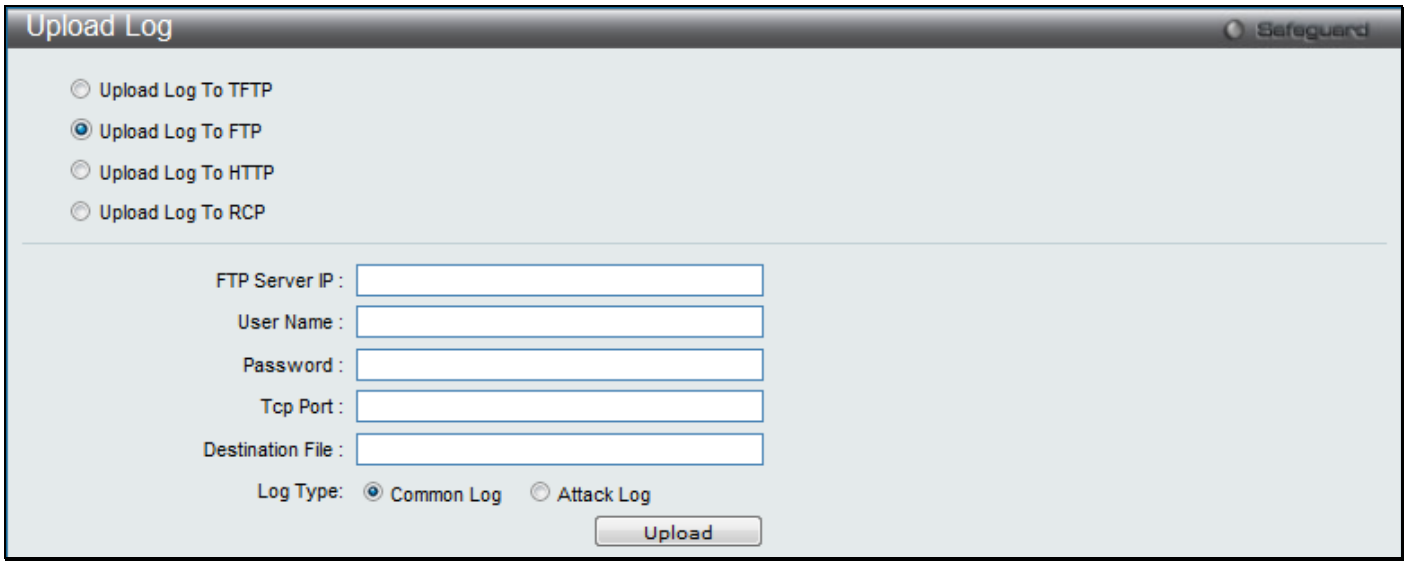


Figure 13-21 Upload Log To FTP window

The fields that can be configured are described below:

Parameter	Description
FTP Server IP	Here the user can enter the FTP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.

Password	Here the user can enter the appropriate Password used.
TCP Port	Here the user can enter the TCP Port number used.
Destination File	Here the user can enter the location and name of the Destination File.
Log Type	Here the user can select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Upload Log To HTTP

This page allows the user to upload the log file from the Switch to a computer.

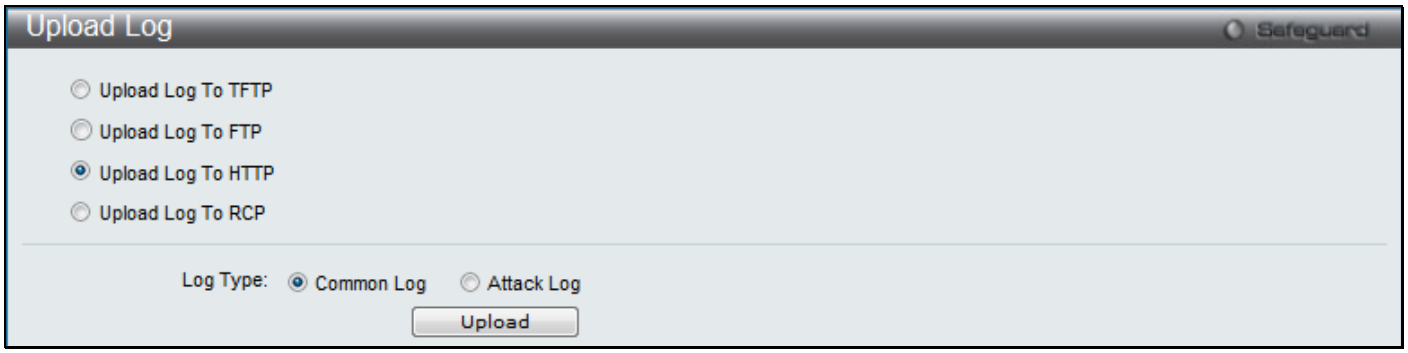


Figure 13-22 Upload Log To HTTP window

The fields that can be configured are described below:

Parameter	Description
Log Type	Here the user can select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Upload Log To RCP

This page allows the user to upload the log file from the Switch to a RCP Server.

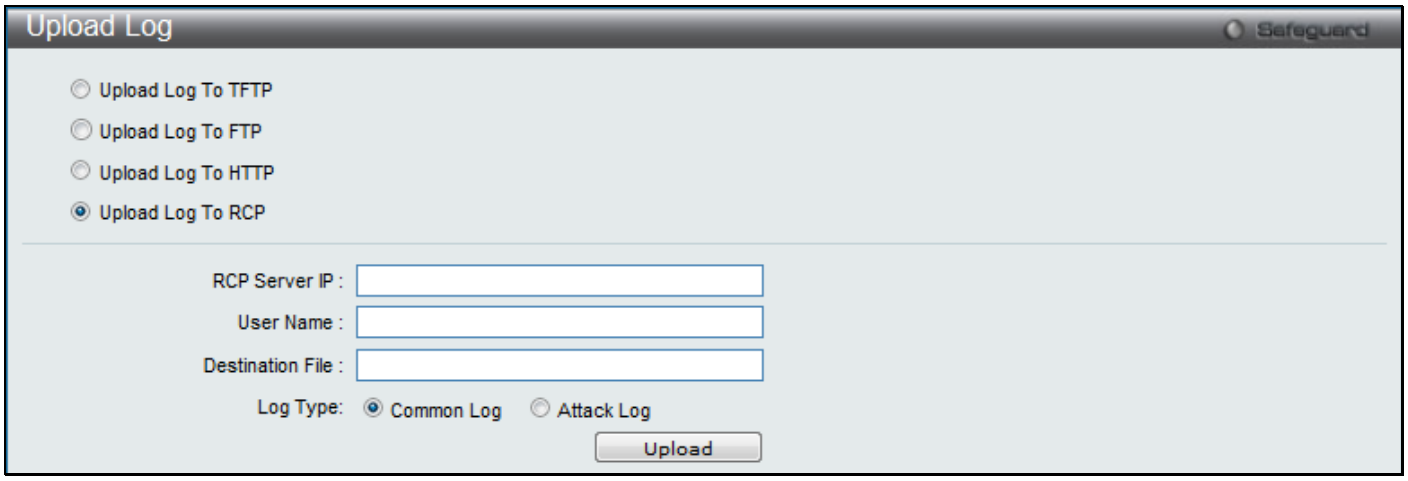


Figure 13-23 Upload Log To RCP window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Here the user can enter the RCP Server IP Address used.
User Name	Here the user can enter the appropriate Username used.
Destination File	Here the user can enter the location and name of the Destination File.
Log Type	Here the user can select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

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

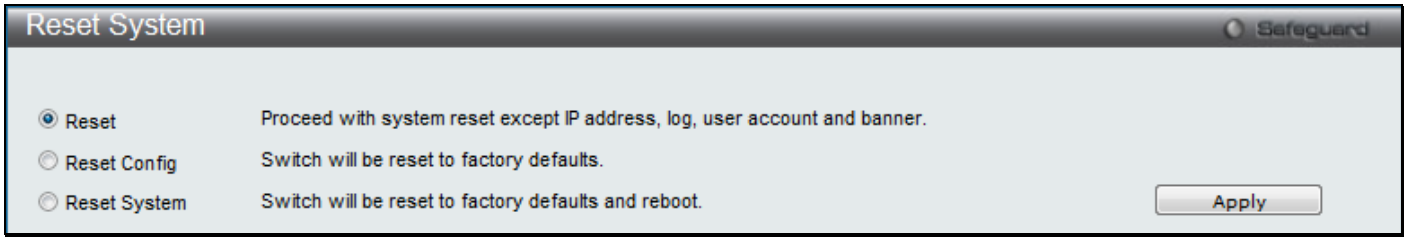


Figure 13-24 Reset System window

The fields that can be configured are described below:

Parameter	Description
Reset	Selecting this option will factory reset the Switch but not the *IP Address, log, user account* and the *banner*.
Reset Config	Selecting this option will factory reset the Switch but not perform a Reboot.
Reset System	Selecting this option will factory reset the Switch and perform a Reboot.

Click the **Apply** button to initiate the Reset action.

Reboot System

The following window is used to restart the Switch.

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

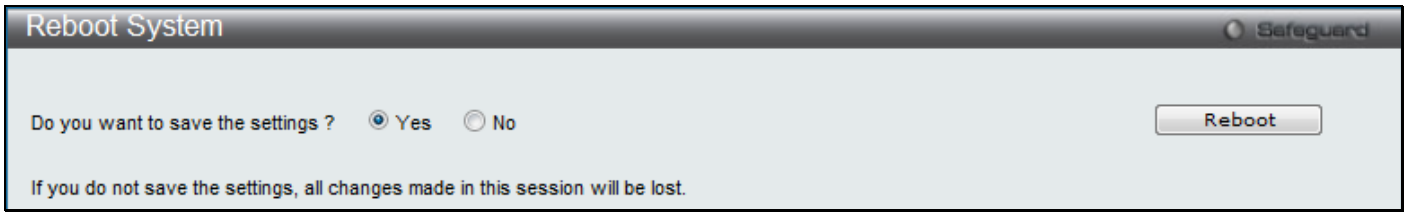


Figure 13-25 Reboot System window

Selecting the **Yes** radio button will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Selecting the **No** radio button instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Reboot** button to restart the Switch.

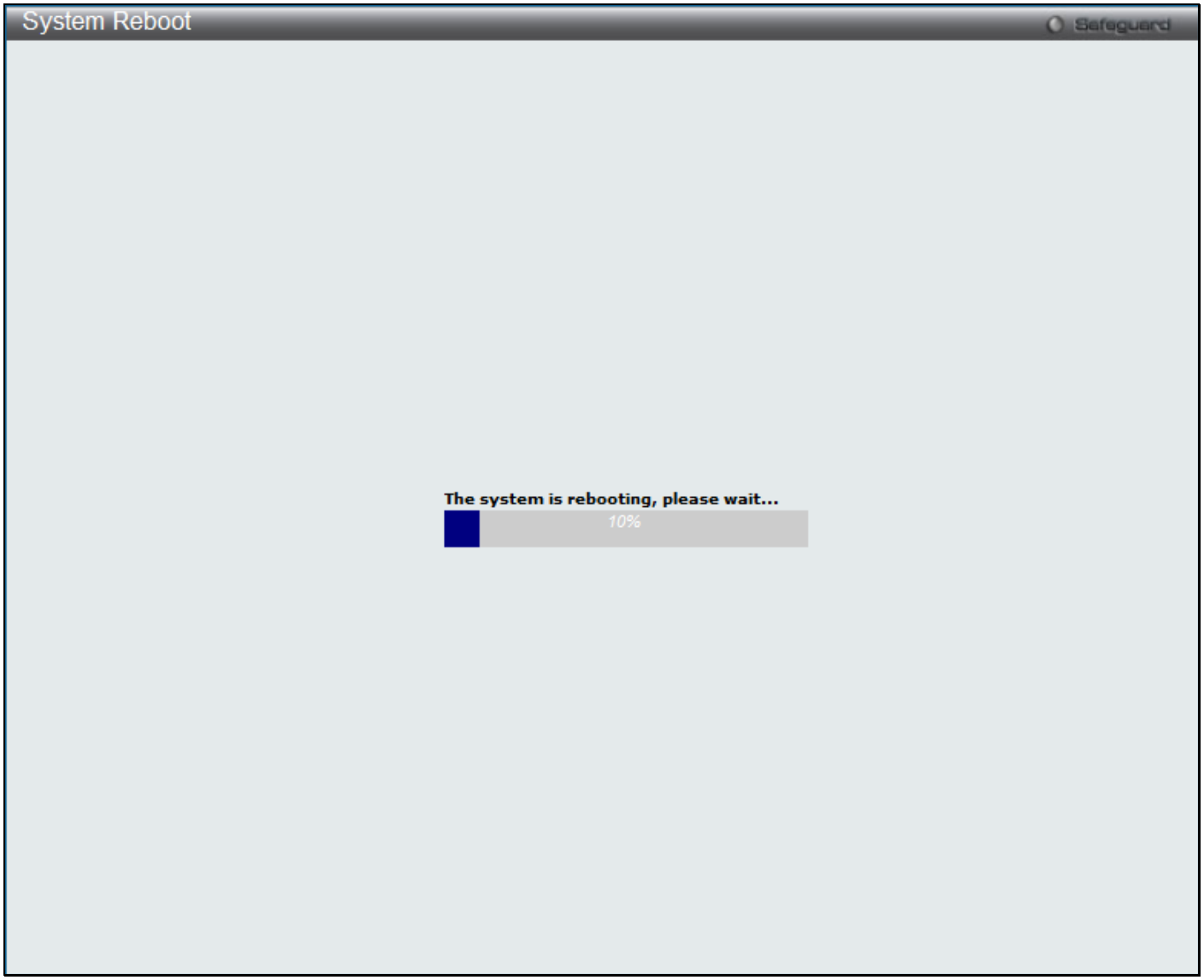


Figure 13-26 System Reboot window

Appendix A Mitigating ARP Spoofing Attacks Using Packet Content ACL

How Address Resolution Protocol works

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. However, this protocol is vulnerable because crackers can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce the ARP protocol, ARP spoofing attacks, and the countermeasures brought by D-Link's switches to thwart ARP spoofing attacks.

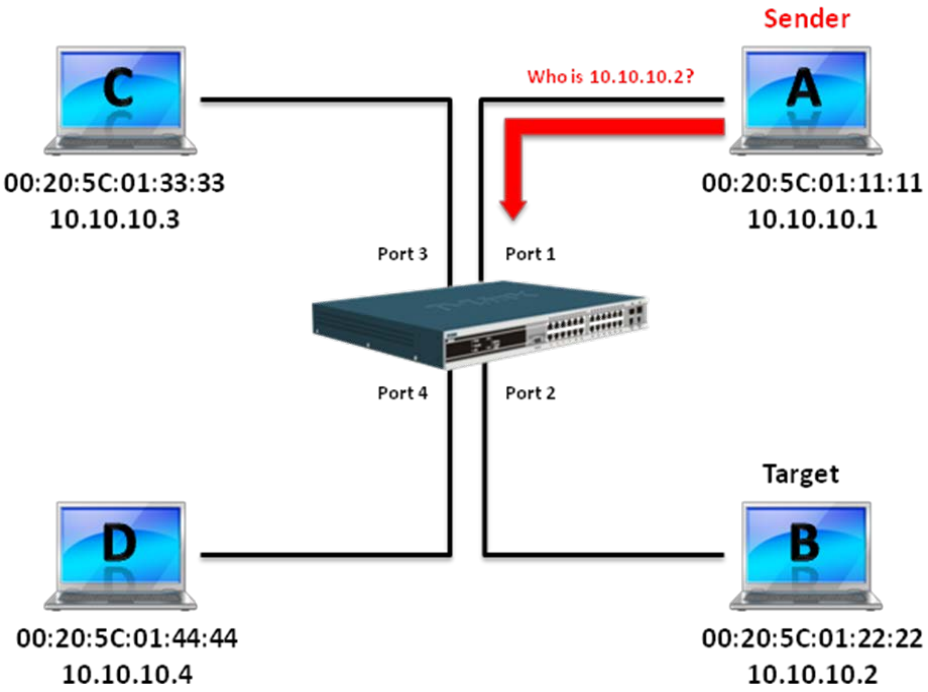


Figure 1 - ARP Request

In the process of ARP, PC A will first issue an ARP request to query PC B's MAC address. The network structure is shown in Figure 1.

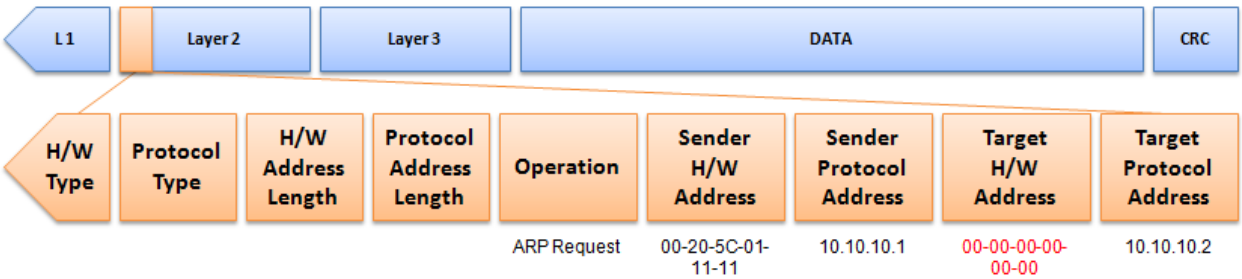


Figure 2 - ARP Payload

The ARP request will be encapsulated into an Ethernet frame and sent out. As can be seen in Figure 3, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via broadcast, the "Destination address" is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

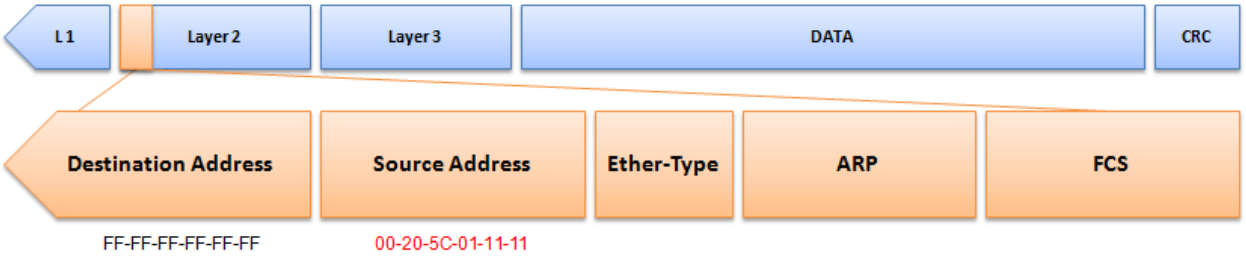


Figure 3 - Ethernet Frame Format

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.

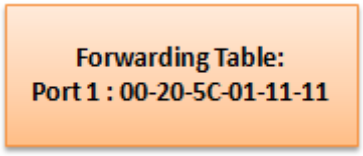


Figure 4 – Forwarding Table

In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure 5).

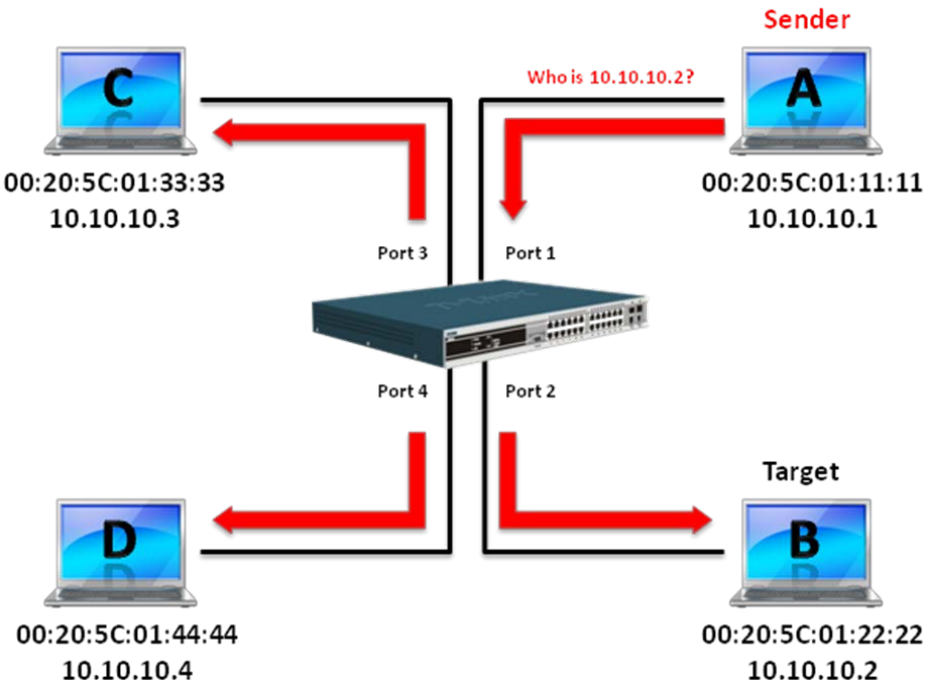


Figure 5 –Broadcast Request

When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload (see Figure 6). The ARP reply will be then encapsulated into an Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

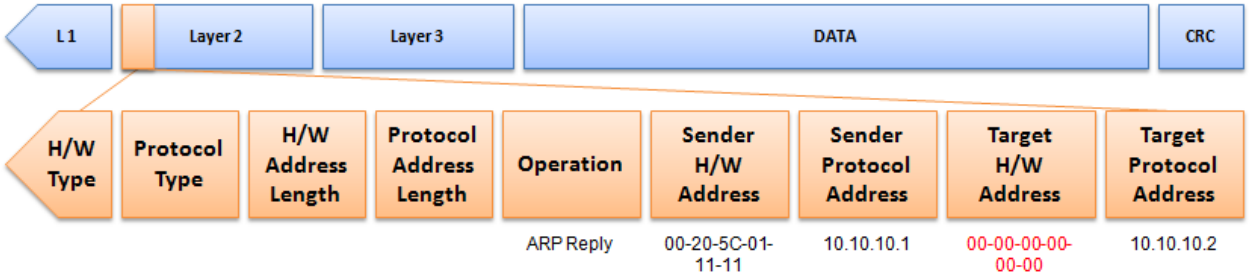


Figure 6 - ARP Payload

When PC B replies to the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Figure 7).

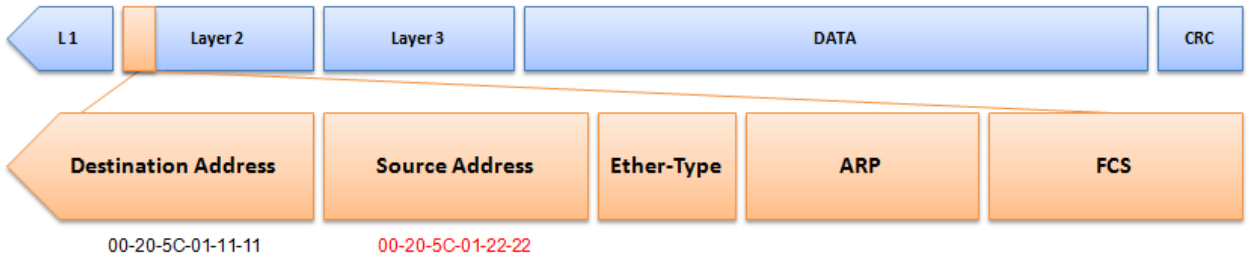


Figure 7 - Ethernet Frame Format

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

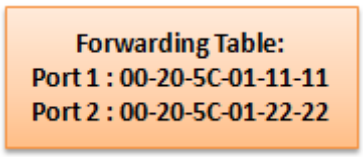


Figure 8 – Forwarding Table

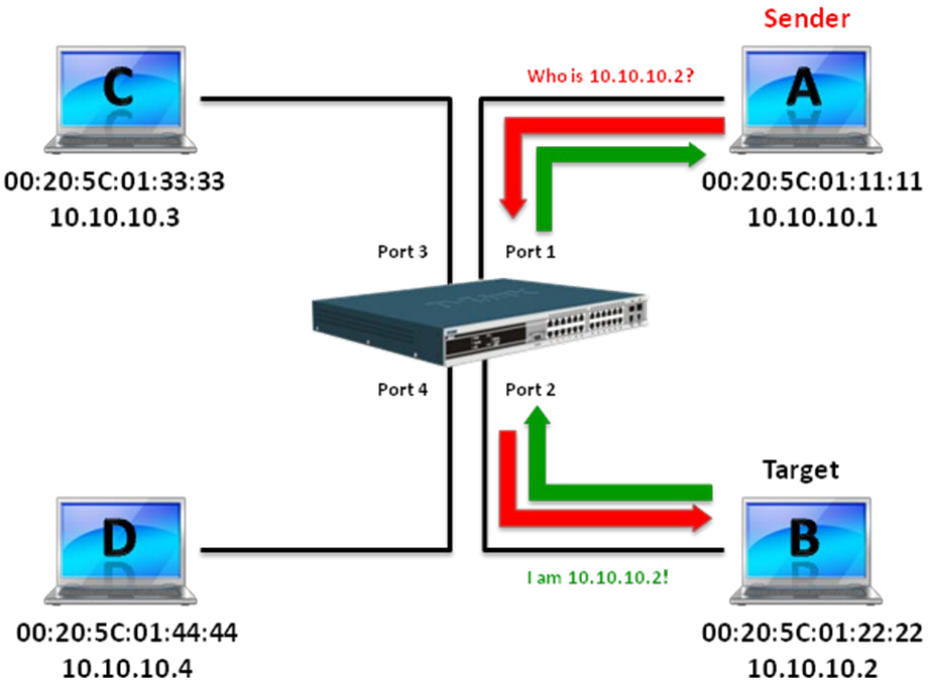


Figure 9 – Connection Established

How ARP Spoofing Attacks a Network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service – DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

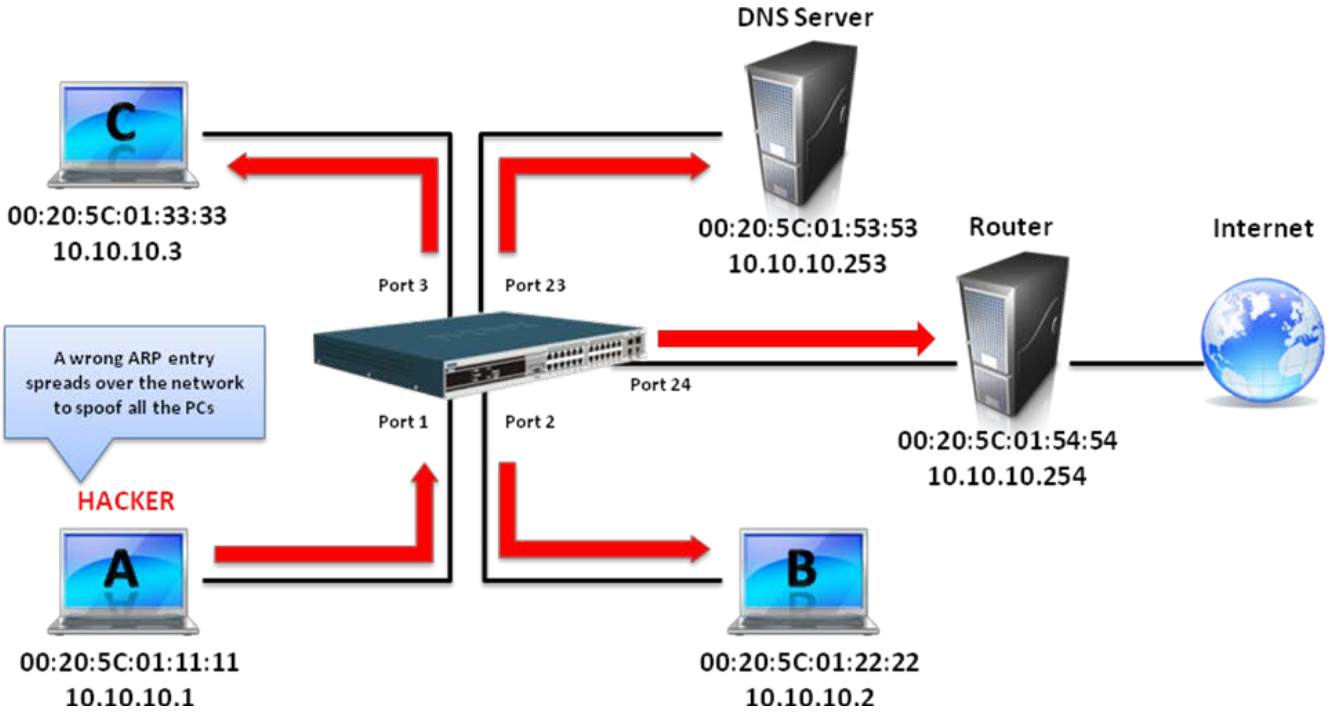


Figure 10 – ARP Spoofing

The IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure 10 shows a hacker within a LAN to initiate ARP spoofing attack.

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address itself. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of a Gratuitous ARP packet is shown in Figure 11.

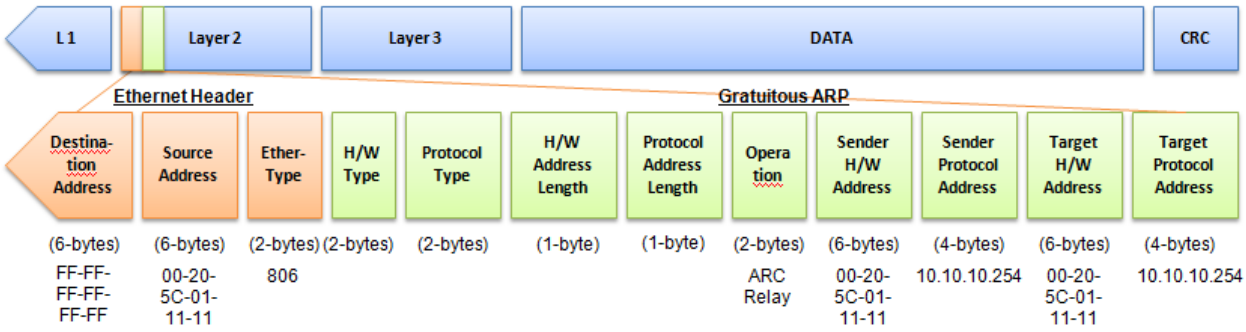


Figure 11 – Gratuitous ARP Packet

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network’s default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the

network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

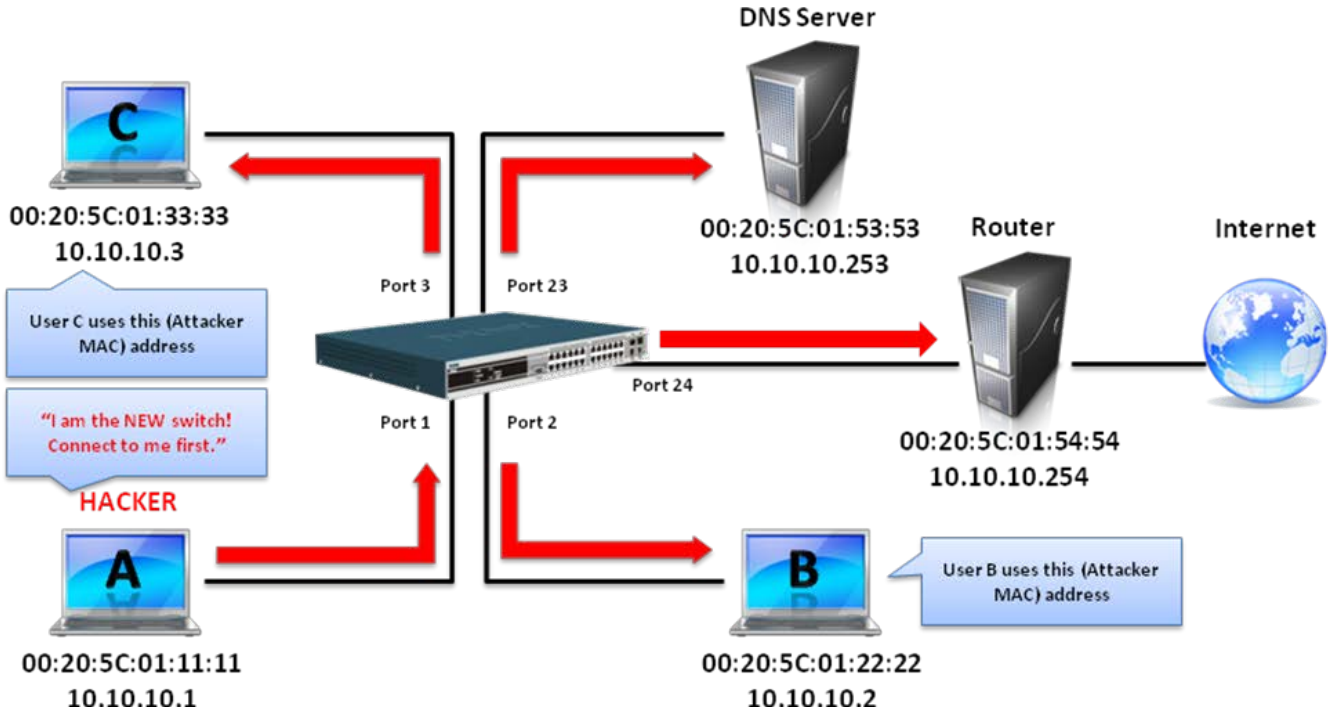


Figure 12 – Network Vulnerable

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim PC that it is a router and cheats the router that it is the victim. As can be seen in Figure 12 all traffic will be then sniffed by the hacker but the users will not discover.

Prevent ARP Spoofing using Packet Content ACL

D-Link managed switches can effectively mitigate common DoS attacks caused by ARP spoofing via a unique Package Content ACL.

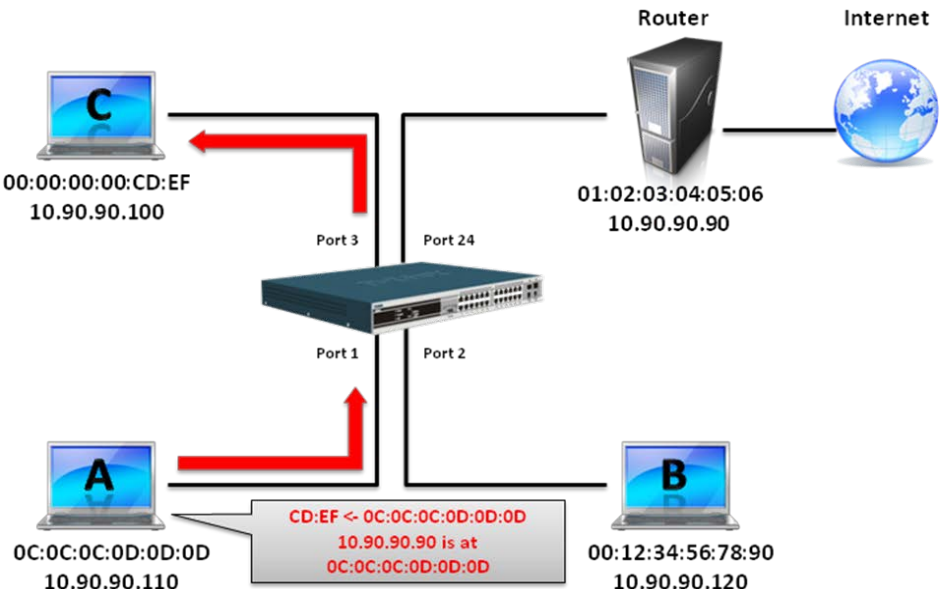


Figure 13 – Network with Packet Content ACL

For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source, and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here via using Packet Content ACL on the Switch to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

Configuration

The configuration logic is as follows:

1. Only if the ARP matches Source MAC address in Ethernet, Sender MAC address and Sender IP address in ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on the Switch enables users to inspect any offset chunk. An offset chunk is a 4-byte block in a HEX format, which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of four offset chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset chunks can be applied to each profile and a switch. Therefore, a careful consideration is needed for planning and configuration of the valuable offset chunks.

In Table 1, you will notice that the Offset_Chunk0 starts from the 127th byte and ends at the 128th byte. It also can be found that the offset chunk is scratched from 1 but not zero.

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Table 1 - Chunk and Packet Offset

The following figure indicates a completed ARP packet contained in Ethernet frame which is the pattern for the calculation of packet offset.

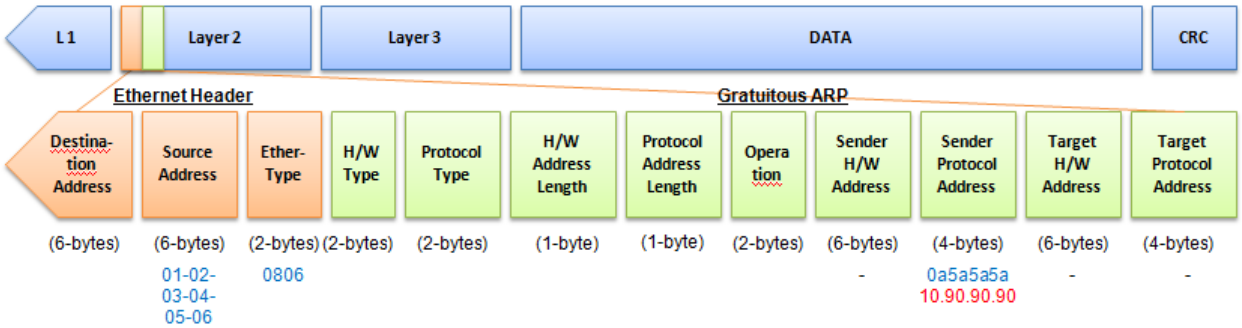


Figure 14 - A Completed ARP Packet Contained in an Ethernet Frame

	Command	Description
Step 1:	**create access_profile_id 1 profile_name 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type**	Create access profile 1 to match Ethernet Type and Source MAC address.
Step 2:	**config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit**	Configure access profile 1 Only if the gateway's ARP packet that contains the correct Source MAC in the Ethernet frame can pass through the switch.
Step 3:	**create access_profile profile_id 2 profile_name 2 packet_content_mask offset1 l2 0 0xFF offset2 l2 1 0xFF offset3 l2 16 0xFF offset4 l2 17 0xFF offset5 l2 18 0xFF offset6 l2 19 0xFF**	Create access profile 2 The first chunk starts from the offset 1 and offset 2 mask for the Ethernet Type. (Blue in Table 1, 13th and 14th bytes) The second chunk starts from the offset 3 and offset 4 mask for the Sender IP in the ARP packet. (Green in Table 1, 29th and 30th bytes) The third chunk starts from the offset 5 and offset 6 mask for the Sender IP in the ARP packet. (Brown in Table 1, 31st and 32nd bytes)
Step 4:	**config access_profile profile_id 2 add access_id 1 packet_content offset1 l2 0 0x08 offset2 l2 1 0x06 offset3 l2 16 0x0A offset4 l2 17 0x5A offset5 l2 18 0x5A offset6 l2 19 0x5A port 1-12 deny**	Configure access profile 2. The rest of the ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step 5:	**save**	Save configuration.

Appendix B Password Recovery Procedure

This document describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This document will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the Switch. After the UART init is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode.” Once the Switch enters the “Password Recovery Mode,” all ports on the Switch will be disabled.

```
  Boot Procedure                                        V1.00.013
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100%

  MAC Address   : 00-03-38-10-28-01
  H/W Version   : A1

  Please Wait, Loading V2.00.007 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
Password Recovery Mode
>
```

3. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config	The **reset config** command resets the whole configuration back to the default values.
reboot	The **reboot** command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.

Appendix C System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Log Description	Severity	Note
System	Event description: System started up Log Message: System started up	Critical	
	Event description: Configuration saved to flash Log Message: Configuration saved to flash (Username: <username>) Parameters description: username: The user name that save the configuration.	Informational	
	Event description: System log saved to flash Log Message: System log saved to flash(Username: <username>) Parameters description: username: The user name that save the configuration.	Informational	
	Event description: Configuration and log saved to flash Log Message: Configuration and log saved to flash (Username: <username>) Parameters description: username: The user name that save the configuration.	Informational	
Peripherals	Event description: Temperature sensor enters alarm state. Log Message: Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>) Parameters description: sensorID: The sensor ID. temperature: The temperature.	Informational	
	Event description: Temperature recovers to normal. Log Message: Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>) Parameters description: sensorID: The sensor ID. temperature: The temperature.	Informational	
	Event description: Internal Power failed. Log Message: Internal Power failed	Critical	
	Event description: Internal Power is recovered. Log Message: Internal Power is recovered	Critical	
	Event description: Redundant Power failed. Log Message: Redundant Power failed	Critical	
	Event description: Redundant Power is working. Log Message: Redundant Power is working	Critical	
SNMP	Event description: SNMP request received with invalid community string Log Message: SNMP request received from <ipAddress> with invalid community string! Parameters description: ipAddress: IP address.	Informational	
Interface	Event description: Port link up Log Message: Port <portNum> link up, <link state> Parameters description: portNum: The port number link state: port link status, for example: 100Mbps FULL duplex	Informational	
	Event description: Port link down Log Message: Port <portNum> link down Parameters description: portNum: The port number.	Informational	
Debug	Event description: System fatal error Log Message: System re-start reason: system fatal error	Emergency	
	Event description: CPU exception Log Message: System re-start reason: CPU exception	Emergency	
DDM	Event description: DDM exceeded or recover from DDM alarm threshold Log Message: Port <portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] alarm threshold Parameters description: portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power.	Critical	

	exceedType: indicate exceed threshold or recover to normal event, the value should be “recovered from” or “exceeded” thesholdSubType: the DDM threshold sub type, the value should be “high” or “low”.		
	Event description: DDM exceeded or recover from DDM warning threshold Log Message: Port <portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] warning threshold Parameters description: portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. exceedType: indicate exceed threshold or recover to normal event, the value should be “recovered from” or “exceeded” thesholdSubType: the DDM threshold sub type, the value should be “high” or “low”.	Warning	
DDM	Event description: DDM exceeded or recover from DDM alarm threshold Log Message: Port <portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] alarm threshold Parameters description: portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. exceedType: indicate exceed threshold or recover to normal event, the value should be “recovered from” or “exceeded” thesholdSubType: the DDM threshold sub type, the value should be “high” or “low”.	Critical	
	Event description: DDM exceeded or recover from DDM warning threshold Log Message: Port <portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] warning threshold Parameters description: portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. exceedType: indicate exceed threshold or recover to normal event, the value should be “recovered from” or “exceeded” thesholdSubType: the DDM threshold sub type, the value should be “high” or “low”.	Warning	
TFTP Client	Event description: Firmware upgraded successfully. Log Message: Firmware upgrade by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Firmware upgrade was unsuccessful. Log Message: Firmware upgrade by <session> was unsuccessful (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
	Event description: Firmware successfully uploaded. Log Message: Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Firmware upload was unsuccessful. Log Message: Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user’s session. Username: Represent current login user. Ipaddr: Represent client IP address.	Warning	
	Event description: Configuration successfully downloaded. Log Message: Configuration successfully downloaded by <session>	Informational	

	(Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.		
	Event description: Configuration download was unsuccessful. Log Message: Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
	Event description: Configuration successfully uploaded. Log Message: Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Configuration upload was unsuccessful. Log Message: Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
	Event description: Log message successfully uploaded. Log Message: Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational	
	Event description: Log message upload was unsuccessful. Log Message: Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) Parameters description: session: The user's session. Username: Represent current login user. Ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning	
RCP	Event description: Firmware downloaded successfully Log Message: Firmware download by RCP successfully (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Informational	
	Event description: Firmware download fail Log Message: Firmware download by RCP fail ! (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Warning	
	Event description: Firmware uploaded successfully Log Message: Firmware upload by RCP successfully (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Informational	
	Event description: Firmware upload fail Log Message: Firmware upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : server address.	Warning	

	Event description: Firmware applied successfully Log Message: Firmware applied successfully (Username: <username>, IP <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Informational	
	Event description: Firmware apply fail Log Message: Firmware apply fail ! (Username: <username>, IP <ipaddr>) Parameters description: username: user name. ipaddr : server address.	Warning	
	Event description: CFG downloaded successfully Log Message: Configuration download by RCP successfully (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Informational	
	Event description: CFG download fail Log Message: Configuration download by RCP fail ! (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr: RCP server address.	Warning	
	Event description: CFG upload successfully Log Message: Configuration uploaded by RCP successfully (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Informational	
	Event description: CFG upload fail Log Message: Configuration upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Warning	
	Event description: CFG applied successfully Log Message: configuration apply successfully (Username: <username>, IP: <ipaddr>) Parameters description: username: user name. ipaddr : server address.	Informational	
	Event description: CFG apply fail Log Message: configuration apply fail ! (Username: <username>, IP: <ipaddr>) Parameters description: username: user name. ipaddr : server address.	Warning	
	Event description: Log upload successfully Log Message: Log uploaded by RCP successfully (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Informational	
	Event description: Log upload fail Log Message: Log upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Warning	
	Event description: Attack log uploaded successfully Log Message: Attack log uploaded by RCP successfully (Username: <username>, RCP: <ipaddr>) Parameters description: username: user name. ipaddr : RCP server address.	Warning	
	Event description: Attack log upload fail Log Message: Attack log upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) Parameters description:	Warning	

	username: user name. ipaddr : RCP server address.		
MSTP Debug Enhancement	Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] ,port:<portNum> [,MAC: <macaddr>])] Parameters description: InstanceID: Instance ID. portNum:Port ID macaddr: MAC address	Informational	
	Event description: New Root selected Log Message: [CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <InstanceID>] MAC:<macaddr>, Priority: <value>) Parameters description: InstanceID: Instance ID. macaddr: root bridge MAC address value: root bridge priority	Informational	
	Event description: Spanning tree protocol is enabled Log Message: Spanning Tree Protocol is enabled.	Informational	
	Event description: Spanning tree protocol is disabled Log Message: Spanning Tree Protocol is disabled.	Informational	
	Event description: Spannnig Tree instance created. Log Message: Spanning Tree instance create (Instance:<InstanceID>) Parameters description: InstanceID: Instance ID.	Informational	
	Event description: Spannnig Tree instance deleted. Log Message: Spanning Tree instance delete (Instance:<InstanceID>) Parameters description: InstanceID: Instance ID.	Informational	
	Event description: Spanning Tree Version changed. Log Message: Spanning Tree version changed.(new version:<new_version>) Parameters description: new_version: New STP version.	Informational	
	Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level changed (name:<name> revision level <revision_level>). Parameters description: name : New name. revision_level:New revision level.	Informational	
	Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (Instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational	
	Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (Instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational	
	Event description: New root port Log Message: New root port selected [([Instance:<InstanceID>], port:< portNum>)] Parameters description: InstanceID: Instance ID. portNum:Port ID	Notice	
	Event description: Spanning Tree port status changed Log Message: Spanning Tree port status change [([Instance:<InstanceID>], port:<portNum>)] <old_status> -> <new_status> Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status new_status: New status	Notice	
	Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change [([Instance:<InstanceID>],	Informational	

	port:<portNum>)] <old_role> -> <new_role> Parameters description: InstanceID: Instance ID. portNum:Port ID old_role: Old role new_status:New role		
ERPS	Event description: Signal failure detected Log Message: Signal fail detected on node <macaddr> Parameters description: macaddr: The system MAC of the node	Notice	
	Event description: Signal failure cleared Log Message: Signal fail cleared on node <macaddr> Parameters description: macaddr: The system MAC of the node	Notice	
	Event description: RPL owner conflict Log Message: RPL owner conflicted on the ring <macaddr> Parameters description: macaddr: The system MAC of the node	Warning	
LLDP-MED	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) 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: Incompatible LLDP-MED TLV set detected Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum	Notice	

	>, 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.		
CFM	Event description: Cross-connect is detected Log Message: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters description: vlanid: Represents VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Critical	
	Event description: Error CFM CCM packet is detected Log Message: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters description: vlanid: Represents VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. portNum: Represents logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents MEPID of the MEP. macaddr: Represents MAC address of the MEP.	Warning	
	Event description: Can not receive remote MEP's CCM packet Log Message: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. portNum: Represents logical port number of the MEP. mepdirection: Can be "inward" or "outward".	Warning	
	Event description: Remote MEP's MAC reports an error status Log Message: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward".	Warning	
	Event description: Remote MEP detects CFM defects Log Message: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. portNum: Represents logical port number of the MEP. mepdirection: Can be "inward" or "outward".	Informational	
Voice VLAN	Event description: When a new voice device is detected in the port. Log Message: New voice device detected (MAC <macaddr>, Port <portNum>)	Informational	

	Parameters description: portNum : The port number. macaddr: Voice device MAC address		
	Event description: When a port which is in auto voice VLAN mode joins the voice VLAN Log Message: Port < portNum > add into voice VLAN <vid > Parameters description: portNum : The port number. vid:VLAN ID	Informational	
	Event description: When a port leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that port, the log message will be sent. Log Message: Port < portNum > remove from voice VLAN <vid > Parameters description: portNum : The port number. vid:VLAN ID	Informational	
MAC-based Access Control	Event description: A host fails to pass the authentication Log Message: MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>) Parameters description: macaddr: MAC address portNum: The port number. vid: VLAN ID on which the host exists	Critical	
	Event description: The authorized user number on a port reaches the max user limit. Log Message: Port <portNum> enters MAC-based Access Control stop learning state. Parameters description: portNum: The port number.	Warning	
	Event description: The authorized user number on a port is below the max user limit in a time interval (interval is project depended). Log Message: Port <portNum> recovers from MAC-based Access Control stop learning state. Parameters description: portNum: The port number.	Warning	
	Event description: The authorized user number on whole device reaches the max user limit. Log Message: MAC-based Access Control enters stop learning state. Parameters description: None	Warning	
	Event description: The authorized user number on whole device is below the max user limit in a time interval (interval is project depended). Log Message: MAC-based Access Control recovers from stop learning state. Parameters description: None	Warning	
	Event description: A host passes the authentication Log Message: MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>) Parameters description: macaddr: MAC address portNum: The port number. vid: VLAN ID on which the host exists	Informational	
	Event description: A host is aged out. Log Message: MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>) Parameters description: macaddr: MAC address portNum: The port number. vid: VLAN ID on which the host exists	Informational	
802.1X	Event description: 802.1X Authentication failure. Log Message: 802.1XAuthentication failure [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>) Parameters description: reason: The reason for failed authentication. username: The user that is being authenticated. portNum: The port number. macaddr: the MAC address of authenticated device.	Warning	
	Event description: 802.1X Authentication success. Log Message: 802.1X Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Informational	

	Parameters description: username: The user that being authenticated. portNum: The port number. macaddr: the MAC address of authenticated device.		
AAA and SSH	Event description: Successful login through a session. Log Message: Successful login through <Console | Telnet | Web | Web(SSL) | SSH>(Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Informational	The IP parameter not for Console.
	Event description: Login failed through a session. Log Message: Login failed through <Console | Telnet | Web | Web(SSL) |SSH> (Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Warning	The IP parameter not for Console.
	Event description: Logout through a session. Log Message: Logout through <Console | Telnet | Web | Web(SSL) | SSH> (Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Informational	The IP parameter not for Console.
	Event description: session timed out. Log Message: <Console | Telnet | Web | Web(SSL) | SSH> session timed out (Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Informational	The IP parameter not for Console session.
	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	
	Event description: Login failed through a session due to AAA server timeout or improper configuration. Log Message: Login failed through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>). Parameters description: ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning	The string "[from <ipaddr | ipv6address>]" not for console session.
	Event description: Enable Admin failed through a session due to AAA server timeout or improper configuration. Log Message: Enable Admin failed through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) Parameters description: ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning	The string "[from <ipaddr | ipv6address>]" not for console session.
	Event description: Enable Admin failed through a session authenticated by AAA local or server. Log Message: Enable Admin failed through <Console | Telnet | Web| Web(SSL) | SSH> [from <ipaddr | ipv6address>] authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: enable admin by AAA local method. server: enable admin by AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning	The string "[from <ipaddr | ipv6address>]" not for console session.
	Event description: Successful Enable Admin through a session authenticated by AAA local or none or server. Log Message: Successful Enable Admin through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>). Parameters description:	Informational	The string "[from <ipaddr | ipv6address>]" not for console session.

	local: enable admin by AAA local method. none: enable admin by AAA none method. server: enable admin by AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.		
	Event description: Login failed through a session authenticated by AAA local or server. Log Message: Login failed through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: specify AAA local method. server: specify AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning	The string "[from <ipaddr | ipv6address>]" not for console session.
	Event description: Successful login through a session authenticated by AAA local or none or server. Log Message: Successful login through <Console | Telnet | Web | Web(SSL) | SSH> [from < ipaddr | ipv6address >] authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: specify AAA local method. none: specify none method. server: specify AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Informational	The string "[from <ipaddr | ipv6address>]" not for console session.
	Event description: Authentication Policy is enabled Log Message: Authentication Policy is enabled (Module: AAA)		
	Event description: Authentication Policy is disabled Log Message: Authentication Policy is disabled (Module: AAA)		
Port Security	Event description: Address full on a port Log Message: Port security violation [([mac address:<macaddr>] on locking address full [port:< portNum>])] Parameters description: macaddr: The violation MAC address. portNum: The port number.	Warning	
IMPB	Event description: Dynamic IMPB entry conflicts with static ARP Log Message: Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>) Parameters description: ipaddr: IP address macaddr: MAC address portNum : The port number	Warning	
	Event description: Dynamic IMPB entry conflicts with static FDB. Log Message: Dynamic IMPB entry conflicts with static FDB(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <portNum>) Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address portNum : The port number	Warning	
	Event description: Dynamic IMPB entry conflicts with static IMPB. Log Message: Dynamic IMPB entry conflicts with static IMPB(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <portNum>). Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address portNum : The port number	Warning	
	Event description: Creating IMPB entry failed due to no ACL rule being available. Log Message: Creating IMPB entry failed due to no ACL rule being available(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <portNum>) Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address portNum : The port number	Warning	
	Event description: IMPB checks a host illegal. Log Message: Unauthenticated IP-MAC address and discarded by IMPB (IP:	Warning	

	[<ipaddr> | <ipv6addr>]], MAC :< macaddr >, Port <portNum >). Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address portNum : The port number		
	Event description: Dynamic IMPB entry conflicts with static NDP Log Message: Dynamic IMPB entry conflicts with static NDP (IP: [< ipaddr > | < ipv6addr >], MAC: <macaddr>, Port <portNum>) Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address portNum : The port number	Warning	
BPDU Attack Protection	Event description: BPDU attack happened. Log Message: Port <portNum> enter BPDU under protection state (mode: drop | block | shutdown) Parameters description: portNum : The port number drop / block / shutdown: There only one of they in a log entry.	Informational	
	Event description: BPDU attack automatically recover. Log Message: Port <portNum > recover from BPDU under protection state automatically Parameters description: portNum : The port number	Informational	
	Event description: BPDU attack manually recover. Log Message: Port <portNum > recover from BPDU under protection state manually Parameters description: portNum : The port number	Informational	
WAC	Event description: When a client host fail to authenticate. Log Message: WAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>) Parameters description: string: Username ipaddr: IP address macaddr: MAC address portNum : The port number	Warning	
	Event description: This log will be triggered when the authorized user number reaches the max user limit on whole device. Log Message: WAC enters stop learning state.	Warning	
	Event description: This log will be triggered when the authorized user number is below the max user limit on whole device in a time interval (interval is project depended). Log Message: WAC recovers from stop learning state.	Warning	
JWAC	Event description: When a client host authenticated successful. Log Message: JWAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>) Parameters description: string: Username ipaddr: IP address macaddr: MAC address portNum : The port number	Warning	
	Event description: When a client host fail to authenticate. Log Message: JWAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>). Parameters description: string: Username ipaddr: IP address macaddr: MAC address portNum : The port number	Warning	
	Event description: This log will be triggered when the authorized user number reaches the max user limit on whole device. Log Message: JWAC enters stop learning state.	Warning	
	Event description: This log will be triggered when the authorized user number is below the max user limit on whole device in a time interval (interval is project depended). Log Message: JWAC recovers from stop learning state.	Warning	
LBD	Event Description: Loop back is detected under port-based mode. Log Message: Port < portNum> LBD loop occurred. Port blocked. Parameters Description:	Critical	

	portNum: The port number.		
	Event Description: Port recovered from LBD blocked state under port-based mode. Log Message: Port< portNum> LBD port recovered. Loop detection restarted Parameters Description: portNum: The port number.	Informational	
	Event Description: Loop back is detected under VLAN-based mode. Log Message: Port <portNum> VID <vlanID> LBD loop occurred. Packet discard begun Parameters Description: portNum: The port number. vlanID: the VLAN ID number.	Critical	
	Event Description: Port recovered from LBD blocked state under VLAN-based mode. Log Message: Port < portNum> VID <vlanID> LBD recovered. Loop detection restarted Parameters Description: portNum: The port number. vlanID: the VLAN ID number.	Informational	
	Event Description: The number of VLAN in which loop back occurs hit the specified number. Log Message: Loop VLAN number overflow. Parameters Description: None	Informational	
Traffic Control	Event description: Broadcast storm occurrence. Log Message: Port <portNum> Broadcast storm is occurring. Parameters description: portNum: The port number.	Warning	
	Event description: Broadcast storm cleared. Log Message: Port <portNum> Broadcast storm has cleared. Parameters description: portNum: The port number.	Informational	
	Event description: Multicast storm occurrence. Log Message: Port <portNum> Multicast storm is occurring. Parameters description: portNum: The port number.	Warning	
	Event description: Multicast Storm cleared. Log Message: Port <portNum> Multicast storm has cleared. Parameters description: portNum: The port number.	Informational	
	Event description: Port shut down due to a packet storm Log Message: Port <portNum> is currently shut down due to a packet storm Parameters description: portNum: The port number.	Warning	
SafeGuard	Event description: Safeguard Engine is in normal mode Log Message: Safeguard Engine enters NORMAL mode	Informational	
	Event description: Safeguard Engine is in filtering packet mode Log Message: Safeguard Engine enters EXHAUSTED mode	Warning	
IP and Password Changed	Event description: Password change activity Log Message: Password was changed by console (Username: <username>) Parameters description: username: user name.	Informational	
DoS Attack Function	Event description: Spoofing attack: 1. The soure ip is same as switch's interface ip but the source mac is different 2. Source ip is the same as the switch's IP in ARP packet 3. Self IP packet dected Log Message: Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, port: <portNum> Parameters description: ipaddr: IP address macaddr: MAC address portNum : The port number	Critical	
Gratuitous ARP	Event description: IP conflict was detected Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: < intf-name>) Parameters description: ipaddr: IP address	Informational	

	macaddr: MAC address portNum : The port number intf-name: Interface name		
DHCP Server Screening	Event description: Detected untrusted DHCP server IP address. Log Message: Detected untrusted DHCP server(IP: <ipaddr>, Port <portNum>) Parameters description: ipaddr: The untrusted IP address which has beenis detected with our device. portNum : Represent the logic port number of the device.	Informational	
OSPF Debug Enhancement	Event description: OSPF interface link state changed. Log Message: OSPF interface <intf-name> changed state to <Up | Down> Parameters description: intf-name: Name of OSPF interface.	Informational	
	Event description: OSPF interface administrator state changed. Log Message: OSPF protocol on interface <intf-name> changed state to <Enabled | Disabled> Parameters description: intf-name: Name of OSPF interface.	Informational	
	Event description: One OSPF interface changed from one area to another. Log Message: OSPF interface <intf-name> changed from area <area-id> to area <area-id> Parameters description: intf-name: Name of OSPF interface. area-id: OSPF area ID.	Notice	
	Event description: One OSPF neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF neighbor state's dead timer expired. Log Message: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF virtual neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full Parameters description: nbr-id: Neighbor's router ID.	Notice	
	Event description: One OSPF virtual neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Full to Down Parameters description: nbr-id: Neighbor's router ID.	Notice	
	Event description: OSPF router ID was changed. Log Message: OSPF router ID changed to <router-id> Parameters description: router-id: OSPF router ID.	Informational	
	Event description: Enable OSPF. Log Message: OSPF state changed to Enabled	Informational	
	Event description: Disable OSPF. Log Message: OSPF state changed to Disabled	Informational	
VRRP Debug Enhancement	Event description: One virtual router state becomes Master. Log Message: VR <vr-id> at interface <intf-name> switch to Master Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational	
	Event description: One virtual router state becomes Backup. Log Message: VR <vr-id> at interface <intf-name> switch to Backup	Informational	

	Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.		
	Event description: One virtual router state becomes Init. Log Message: VR <vr-id> at interface <intf-name> switch to Init. Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational	
	Event description: Authentication type mismatch of one received VRRP advertisement message. Log Message: Authentication type mismatch on VR <vr-id> at interface <intf-name>. Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: Authentication checking fail of one received VRRP advertisement message. Log Message: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type>. Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based. Auth-type: VRRP interface authentication type.	Warning	
	Event description: Checksum error of one received VRRP advertisement message. Log Message: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name>. Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: Virtual router ID mismatch of one received VRRP advertisement message. Log Message: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>. Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: Advertisement interval mismatch of one received VRRP advertisement message. Log Message: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>. Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning	
	Event description: A virtual MAC address is added into switch L2 table Log Message: Added a virtual MAC <vrrp-mac-addr> into L2 table. Parameters description: vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: A virtual MAC address is deleted from switch L2 table. Log Message: Deleted a virtual MAC <vrrp-mac-addr> from L2 table. Parameters description: vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: A virtual MAC address is adding into switch L3 table. Log Message: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: A virtual MAC address is deleting from switch L3 table. Log Message: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice	
	Event description: Failed when adding a virtual MAC into switch chip L2 table. Log Message: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode>. Parameters description: vrrp-mac-addr: VRRP virtual MAC address	Error	

	vrrp-errcode: Errcode of VRRP protocol behavior.		
	Event description: Failed when deleting a virtual MAC from switch chip L2 table. Log Message: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode>. Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behavior.	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The L3 table is full. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-port: port number of VRRP virtual MAC.	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-intf: interface id on which VRRP virtual MAC address is based.	Error	
	Event description: Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-box: stacking box number of VRRP virtual MAC.	Error	
	Event description: Failed when adding a virtual MAC into switch chip's L3 table. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error	
	Event description: Failed when deleting a virtual MAC from switch chip's L3 table. Log Message: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode>. Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error	
CFM Extension	Event description: AIS condition detected Log Message: [CFM_EXT(1):]AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice	
	Event description: AIS condition cleared Log Message: [CFM_EXT(2):]AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP.	Notice	

	portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.		
	Event description: LCK condition detected Log Message: [CFM_EXT(3):]LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice	
	Event description: LCK condition cleared Log Message: [CFM_EXT(4):]LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice	
DULD	Event description: A unidirectional link has been detected on this port Log Message: Port: <portNum> is unidirectional. Parameters description: portNum: port number	Informational	
SRM	Event Description: SRM mode change Log Message: The SRM mode has been changed to <srm_mode> Parameters Description: srm_mode: the SRM mode, could be Routing or VPWS	Informational	
RADIUS	Event description: VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member. Log Message: RADIUS server <ipaddr> assigned VID :<vlanID> to port <portNum> (account :<username>) Parameters description: ipaddr: The IP address of the RADIUS server. vlanID: The VID of RADIUS assigned VLAN. portNum: The port number. Username: The user that is being authenticated.	Informational	
	Event description: Ingress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This Ingress bandwidth will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <portNum> (account : <username>) Parameters description: ipaddr: The IP address of the RADIUS server. ingressBandwidth: The ingress bandwidth of RADIUS assign. portNum: The port number. Username: The user that is being authenticated.	Informational	
	Event description: Egress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This egress bandwidth will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <portNum> (account: <username>) Parameters description: ipaddr: The IP address of the RADIUS server. egressBandwidth: The egress bandwidth of RADIUS assign. portNum: The port number. Username: The user that is being authenticated.	Informational	
	Event description: 802.1p default priority assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This 802.1p default priority will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <portNum> (account : <username>) Parameters description: ipaddr: The IP address of the RADIUS server. priority: Priority of RADIUS assign.	Informational	

	portNum: The port number. Username: The user that is being authenticated.		
	Event description: Failed to assign ACL profiles/rules from RADIUS server. Log Message: RADIUS server <ipaddr> assigns <username> ACL failure at port <portNum> (<string>) Parameters description: ipaddr: The IP address of the RADIUS server. portNum: The port number. Username: The user that is being authenticated. string: The failed RADIUS ACL command string.	Warning	
DHCPv6 Relay	Event description: DHCPv6 relay on a specific interface's administrator state changed. Log Message: [DHCPv6_RELAY(1):]DHCPv6 relay on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Name of the DHCPv6 relay agent interface.	Informational	
VPWS	Event description: Pseudowire link down Log Message: Pseudowire <vc_id> link down. Parameters description: vc_id: the link down pseudowire ID	Informational	
	Event description: Pseudowire link up Log Message: Pseudowire <vc_id> link up. Parameters description: vc_id: the link up pseudowire ID	Informational	
	Event description: Pseudowire is deleted Log Message: Pseudowire <vc_id> is deleted. Parameters description: vc_id: the deleted pseudowire ID	Informational	
LDP	Event description: the number of Session Initialization messages exceeds the value of the 'mplsLdpEntityInitSessionThreshold' Log Message: Session of peer <lsrid> initialization exceeded threshold < threshold > Parameters description: lsrid: LSR ID of peer threshold: LDP session initialization threshold.	Informational	
	Event description: Path vector limit mismatch Log Message: LDP entity path vector limit <value> does not match the peer <lsrid> path vector limit <value> Parameters description: lsrid: LSR ID of peer value: Path Vector limit	Informational	
	Event description: LDP session state enters the operational state Log Message: LDP session of peer <lsrid> is operational Parameters description: lsrid: LSR ID of peer	Informational	
	Event description: LDP session state restart Log Message: LDP session of peer <lsrid> restart Parameters description: lsrid: LSR ID of peer	Informational	
MPLS	Event description: LSP is up Log Message: LSP <lsp_id> is up Parameters description: lsp_id: The established LSP ID	Informational	
	Event description: LSP is down Log Message: LSP <lsp_id> is down Parameters description: lsp_id: The deleted LSP ID	Informational	
RIPng	Event description: The RIPng state of interface changed Log Message: RIPng protocol on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Interface name.	Informational	

Appendix D Trap Entries

This table lists the trap logs found on the Switch.

Category	Trap Name	Description	Note
SNMP	coldStart/1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	(RFC1907 SNMPv2-MIB)
	warmStart/1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is initializing itself such that its configuration is unaltered.	(RFC1907 SNMPv2-MIB)
	linkDown/1.3.6.1.6.3.1.1.5.3	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. This other state is indicated by the included value of ifOperStatus. Binding objects: (1)ifIndex (2)ifAdminStatus (3)ifOperStatus	(RFC2233 IF-MIB)
	linkUp/1.3.6.1.6.3.1.1.5.4	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. This other state is indicated by the included value of ifOperStatus. Binding objects: (1)ifIndex (2)ifAdminStatus (3)ifOperStatus	(RFC2233 IF-MIB)
	authenticationFailure/1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated.	(RFC1907 SNMPv2-MIB)
BRIDGE-MIB	newRoot/1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree	
	topologyChange/1.3.6.1.2.1.17.0.2	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.	
OAM	dot3OamNonThresholdEvent/1.3.6.1.2.1.158.0.2	A dot3OamNonThresholdEvent notification is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event. Binding objects: (1)dot3OamEventLogTimestamp (2)dot3OamEventLogOui (3)dot3OamEventLogType(olny support the value: dyingGaspEvent(257)) (4)dot3OamEventLogLocation (5)dot3OamEventLogEventTotal	(ie8023ah.mib)
MAC-based Access Control	swMacBasedAccessControlLoggedSuccess/ 1.3.6.1.4.1.171.12.35.11.1.0.1	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	
	swMacBasedAccessControlLoggedFail/ 1.3.6.1.4.1.171.12.35.11.1.0.2	The trap is sent when a MAC-based Access Control host login fails. Binding objects: (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	
	swMacBasedAccessControlAgesOut/ 1.3.6.1.4.1.171.12.35.11.1.0.3	The trap is sent when a MAC-based Access Control host ages out. Binding objects: (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	
RMON (RFC2819.mib)	risingAlarm/1.3.6.1.2.1.16.0.1	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	
	fallingAlarm/1.3.6.1.2.1.16.0.2	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	
LLDP (lldp.mib)	lldpRemTablesChange/1.0.8802.1.1.2.0.0.1	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding objects： (1)lldpStatsRemTablesInserts, (2)lldpStatsRemTablesDeletes, (3)lldpStatsRemTablesDrops, (4)lldpStatsRemTablesAgeouts	
LLDP-MED	lldpXMedTopologyChangeDetected/1.0.8802.1.1.2.1.5.4795.0.1	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	
Port Security	swL2PortSecurityViolationTrap/1.3.6.1.4.1.171.11.115.1.2.2.100.1.2.0.2	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)swPortSecPortIndex (2)swL2PortSecurityViolationMac	
FDB	swL2macNotification/1.3.6.1.4.1.171.11.115.1.2.2.100.1.2.0.1	This trap indicates the MAC addresses variation in address table Binding objects: (1)swL2macNotifyInfo	
Peripherals	swHighTemperature/ /1.3.6.1.4.1.171.12.11.2.2.4.0.1	When Temperature High. Binding objects： (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swHighTemperatureRecover /1.3.6.1.4.1.171.12.11.2.2.4.0.2	When Temperature recover from High. Binding objects： (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swLowTemperature /1.3.6.1.4.1.171.12.11.2.2.4.0.3	When Temperature Low. Binding objects: (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swLowTemperatureRecover/ /1.3.6.1.4.1.171.12.11.2.2.4.0.4	When Temperature recover from Low. Binding objects: (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swPowerStatusChg/ /1.3.6.1.4.1.171.12.11.2.2.2.0.1	When Power Status Change. Binding objects: (1) swPowerUnitIndex (2) swPowerID (3) swPowerStatus	
	swPowerFailure /1.3.6.1.4.1.171.12.11.2.2.2.0.2	When Power Fail. Binding objects: (1) swPowerUnitIndex (2) swPowerID (3) swPowerStatus	
	swPowerRecover /1.3.6.1.4.1.171.12.11.2.2.2.0.3	When Power Recover. Binding objects: (1) swPowerUnitIndex (2) swPowerID (3) swPowerStatus	
SafeGuard	swSafeGuardChgToExhausted /1.3.6.1.4.1.171.12.19.4.1.0.1	This trap indicates System change operation mode from normal to exhausted. Binding objects: (1) swSafeGuardCurrentStatus	
	swSafeGuardChgToNormal /1.3.6.1.4.1.171.12.19.4.1.0.2	This trap indicates System change operation mode from exhausted to normal. Binding objects: (1) swSafeGuardCurrentStatus	
Traffic Control	swPktStormOccurred/ /1.3.6.1.4.1.171.12.25.5.0.1	This trap is sent when a packet storm is detected by a packet storm mechanism and a shutdown action is taken. Binding objects: (1) swPktStormCtrlPortIndex	
	swPktStormCleared /1.3.6.1.4.1.171.12.25.5.0.2	The trap is sent when the packet storm is cleared by the packet storm mechanism. Binding objects: (1) swPktStormCtrlPortIndex	
IMPB	swIpMacBindingViolation	When the IMPB trap is enabled, if there's a new MAC that violates the	

	Trap/ /1.3.6.1.4.1.171.12.23.5.0.1	predefined port security configuration, a trap will be sent out. Binding objects: swIpMacBindingPortIndex swIpMacBindingViolationIP swIpMacBindingViolationMac	
	swIpMacBindingIPv6ViolationTrap/ 1.3.6.1.4.1.171.12.23.5.0.4	When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined IPv6 IMPB configuration, a trap will be sent out. Binding objects: (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIPv6Addr (3) swIpMacBindingViolationMac	
Gratuitous ARP	agentGratuitousARPTrap/1.3.6.1.4.1. 171.12.1.7.2.0.5	This trap is sent when there is an IP address conflict. Binding objects: (1)agentGratuitousARPIpAddr (2)agentGratuitousARPMacAddr (3)agentGratuitousARPPortNumber (4)agentGratuitousARPInterfaceName	
DDM	swDdmAlarmTrap/1.3.6.1.4.1.171.12. 72.4.0.1	The trap is sent when any parameter value exceeds the alarm threshold value, depending on the configuration of the trap_log action. Binding objects: (1)swDdmPort (2)swDdmThresholdType (3)swDdmThresholdExceedType	
	swDdmWarningTrap/1.3.6.1.4.1.171.1 2.72.4.0.2	The trap is sent when any parameter value exceeds the warning threshold value, depending on the configuration of the trap_log action. Binding objects: (1)swDdmPort (2)swDdmThresholdType (3)swDdmThresholdExceedType	
DHCP Server Screening	swFilterDetectedTrap /1.3.6.1.4.1.171.12.37.100.0.1	Send trap when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration. Binding objects: (1) swFilterDetectedIP (2) swFilterDetectedport	
LBD	swPortLoopOccurred /1.3.6.1.4.1.171.12.41.10.0.1	The trap is sent when a port loop occurs. Binding objects: (1) swLoopDetectPortIndex	
	swPortLoopRestart /1.3.6.1.4.1.171.12.41.10.0.2	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) swLoopDetectPortIndex	
	swVlanLoopOccurred /1.3.6.1.4.1.171.12.41.10.0.3	The trap is sent when a port loop occurs under LBD VLAN-based mode. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	
	swVlanLoopRestart /1.3.6.1.4.1.171.12.41.10.0.4	The trap is sent when a port loop restarts under LBD VLAN-based mode after the interval time. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	
BPDU Attack Protection	swBpduProtectionUnderAttackingTra p /1.3.6.1.4.1.171.12.76.4.0.1	When the BPDU Protection trap is enabled, if the specific port changes from a normal state to an under attack state, a trap will be sent out. Binding objects: (1)swBpduProtectionPortIndex (2)swBpduProtectionPortMode	
	swBpduProtectionRecoveryTrap /1.3.6.1.4.1.171.12.76.4.0.2	When the BPDU Protection trap is enabled, if the specific port changes from an under attack state to a normal state, a trap will be sent out. Binding objects: (1)swBpduProtectionPortIndex (2)swBpduProtectionRecoveryMethod	
ERPS	swERPSSFDetectedTrap /1.3.6.1.4.1.171.12.78.4.0.1	When a signal failure occurs, a trap will be generated. Binding objects: (1)swERPSNodeId	
	swERPSSFClearedTrap /1.3.6.1.4.1.171.12.78.4.0.2	When the signal failure clears, a trap will be generated. Binding objects: (1)swERPSNodeId	
	swERPSRPLOwnerConflictTrap /1.3.6.1.4.1.171.12.78.4.0.3	When a conflict occurs, a trap will be generated. Binding objects: (1)swERPSNodeId	
CFM	dot1agCfmFaultAlarm /1.3.111.2.802.1.1.8.0.1	A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Binding objects: (1)dot1agCfmMepHighestPrDefect	
CFM Extension	swCFMExtAISOccurred / 1.3.6.1.4.1.171.12.86.100.0.1	A notification is generated when local MEP enters AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtAISCleared / 1.3.6.1.4.1.171.12.86.100.0.2	A notification is generated when local MEP exits AIS status. Binding objects:	

		(1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtLockOccurred / 1.3.6.1.4.1.171.12.86.100.0.3	A notification is generated when local MEP enters lock status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtLockCleared / 1.3.6.1.4.1.171.12.86.100.0.4	A notification is generated when local MEP exits lock status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
MPLS	mplsXCUp /1.3.6.1.2.1.10.166.2.0.1	This notification is generated when the mplsXCOperStatus object for one or more contiguous entries in the mplsXCTable is about to enter the up state from another state.	
	mplsXCDown /1.3.6.1.2.1.10.166.2.0.2	This notification is generated when the mplsXCOperStatus object for one or more contiguous entries in the mplsXCTable is about to enter the up state from another state.	
LDP	mplsLdpInitSessionThresholdExceed ed /1.3.6.1.2.1.10.166.4.0.1	This notification is generated when the number of Session Initialization messages exceeds the value of the 'mplsLdpEntityInitSessionThreshold'	
	mplsLdpPathVectorLimitMismatch /1.3.6.1.2.1.10.166.4.0.2	This notification is sent when the'mplsLdpEntityPathVectorLimit' does NOT match the value of the 'mplsLdpPeerPathVectorLimit' for a specific Entity.	
	mplsLdpSessionUp /1.3.6.1.2.1.10.166.4.0.3	If this notification is sent when the value of 'mplsLdpSessionState' enters the 'operational(5)' state	
	mplsLdpSessionDown /1.3.6.1.2.1.10.166.4.0.4	This notification is sent when the value of 'mplsLdpSessionState' leaves the 'operational(5)' state	
VPWS	pwUp /1.3.6.1.2.1.10.246.0.1	This notification is generated when the pwOperStatus object for one or more contiguous entries in the pwTable which are about to enter the up(1) state from some other state except the notPresent(5) state and given that the pwDown notification issued for these entries.	
	pwDown /1.3.6.1.2.1.10.246.0.2	This notification is generated when the pwOperStatus object for one or more contiguous entries in the pwTable which are about to enter the down(2) or lowerLayerDown(6) state from any other state, except for transition from the notPresent(5) state.	
	pwDeleted /1.3.6.1.2.1.10.246.0.3	This notification is generated when the PW has been deleted, i.e., when the pwRowStatus has been set destroy(6) or the PW has been deleted by a non-MIB application or due to an auto-discovery process.	