User Manual

Product Model: DAS-3626

VDSL2 Switch

Release 1.00

October 2009 P/N 651EV3726015G

Table of Contents

Preface

The ***DAS-3626 User Manual*** is divided into sections that describe the system installation and operating instructions. Section 2 through Section 13 corresponds to a menu folder in the web management interface presented in the same order they appear in the web interface.

Section 1, Introduction to Web-based Switch Management – Describes how to connect to and use the Web-based switch management feature on the switch.

Section 2, System Configuration – Details for configuring some of the basic functions of the switch including System Information, IP Settings, Interface Settings, IPv6 Neighbor Settings, User Accounts, SNTP Settings and System Log Configuration. The Quick Configuration section of the home page includes a few menus that are not accessable in the main menu folders; these menus are featured in this section as well.

Section 3, Switch Configuration – This section describes menus common to Layer 2 switching for configuration of MAC Address Aging, Port Mirroring, Ethernet Settings, Traffic Segmentation, Forwarding Database configuration, CLI Paging, Port Mirroring, Port Trunks, LACP Port configuration, Loopback Detection setting, GVRP, DHCP Relay and Spanning Tree Protocol/Multiple Spanning Tree and CFM settings.

Section 4, VDSL Configuration – Settings for configuration of VDSL Profiles, VDSL Ports and various VDSL Status display menus are located here.

Section 5, Multicasting – Configuration menus for IGMP Snooping, Multicast Profile, Limited Range, Group settings and Multicast Listener Discovery (MLD) configuration.

Section 6, Storm Control – Configuration menus for multicast and broadcast storm control.

Section 7, QoS – Information for Quality of Service configuration. Menus include Bandwidth Control, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Mechanism, QoS Scheduling and In Band Manage Settings.

Section 8, ACL Configuration – Menus for configuration of ACL including the ACL Configuration Wizard, Access Profile List and ACL Finder.

Section 9, VLAN – Information for configuration of 802.1Q VLANs, 802.1v Protocol VLAN configuration.

Section 10, Security – Features information on security functions, including Safeguard Engine, Trusted Host, Port Security , MAC Spoofing Access, SSL setting, SSH setting and Access Authentication Control settings.

Section 11, CPE Management – Menus for configuration, upgrade and testing of remote CPE equipment and client LAN settings.

Section 12, Status – Features information about the monitoring switch and network functions including CPU Utilization, Port Utilization, Packet Size, Memory Utilization, Packets, Errors, System Log, Ping Test, VDSL monitoring and system Firmware Information.

Section 13, Maintenance – Menus for Firmware Upgrade, Configuration File Backup and restore, as well as the SNMP Settings menu folder are also located in the Maintenance folder.

Appendix A, System Log Entries – This table lists all the possible entries and their corresponding meanings that will appear in the System Log of this switch.

Appendix B, Glossary – Lists definitions for terms and acronyms used in this document.

Appendix C, Password Recovery Procedure - This section describes the procedure for resetting passwords on D-Link switches.

Intended Readers

The ***DAS-3626 User Manual Manual*** 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 your 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 you should type the actual filename 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.

Notes, Notices, and Cautions

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

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

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

Section 1

Web-based Switch Configuration

Introduction

All software functions of the switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The switch can be managed from remote stations anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The web-based management module and command line interface (console program or 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 command line interface (CLI).

Out-of-Band Access to System Management

Management access to the System can be done out-of-band with a physical connection directly to the switch. Connect to the RS-232 **Console** serial port on the front panel, or use the **Mangament** Ethernet port located next to the **Console** port. Use standard terminal emulation software for **Console** port access as described in the CLI Command Reference Manual. Use of the **Management** port provides the options of using either the web-based management module or the command line interface via Telnet. The **Management** port must reside on a different subnet than the in-band System interface. The default IP settings for the **Management** port are 192.168.1.10/255.255.255.0 while the default IP settings for the in-band network interface are 10.90.90.90/255.0.0.0. See below for instructions on how to change the IP settings for the in-band and out-of-band interfaces used for switch management. For more information about physical ports and other hardware information please see the Hardware Manual.

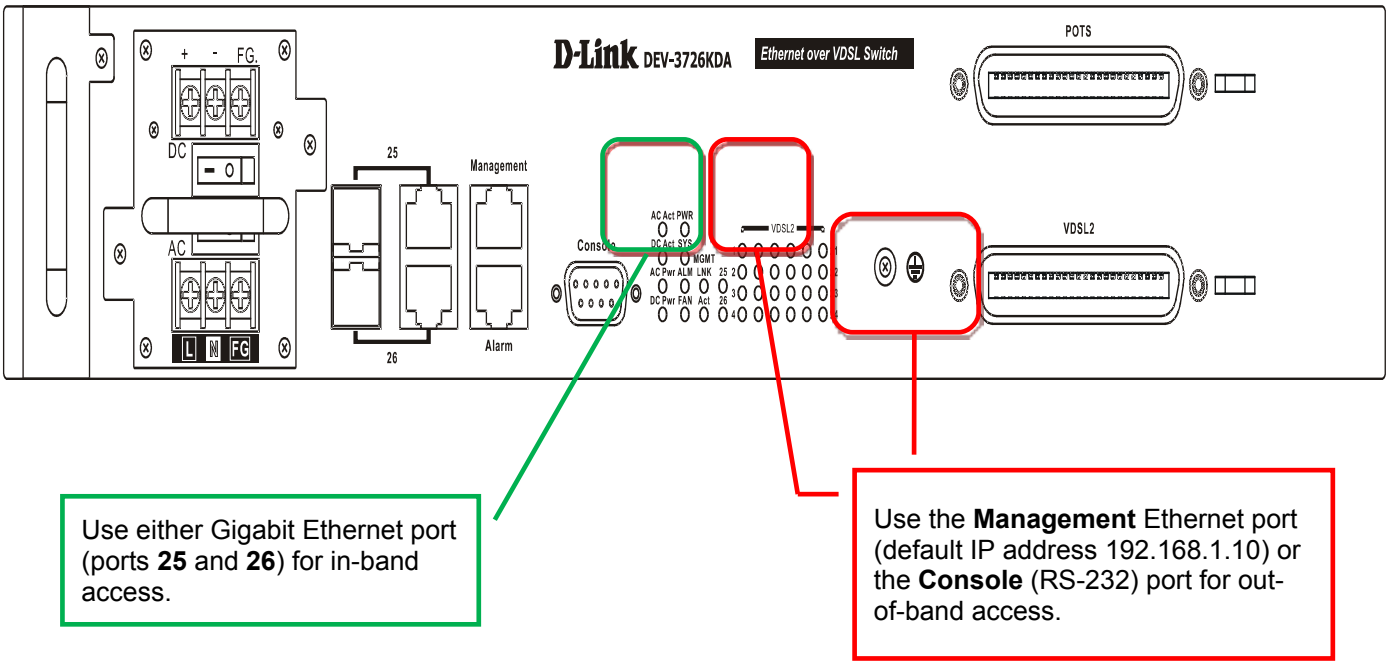


Figure 1. Front panel in-band and out-of-band ports

Interface IP Settings for Switch Management

The switch maintains two IP interfaces used for management, one in-band IP interface named **System**, and one out-of-band IP interface named **outband**. These IP interfaces cannot reside within the same subnet. If the **outband** interface is configured with IP settings that place it within the same subnet as the **System** IP interface, the IP interface for **outband** is invalidated.

The default IP settings of the in-band IP interface **System** are 10.90.90.90/255.0.0.0. The default IP settings for the ou-of-band IP interface outband are 192.168.1.10/255.255.255.0. The CLI command syntax used to change the IP settings of the in-band IP interface is **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy** where the x's represent the IP address to be assigned to the IP interface named **System** and the y's represent the corresponding subnet mask. The CLI command syntax used to change the IP settings of the out-of-band IP interface is **config ipif outband ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Alternatively you can use CIDR notation for the IP settings, **xxx.xxx.xxx.xxx/z**, where the x's represents the corresponding number of subnets.

Connection to the switch using Telnet can be done by connecting to the Management Ethernet port and launching the Windows Command Prompt or similar software. Make sure your computer's IP settings allow connection to the switch default IP subnet of the **outband** interface (192.168.1.0) and Telnet to 192.168.1.10. You will be prompted for a User Name and Password, there is no default user name or password, simply press the Enter at each prompt to obtain the administrator's prompt **DAS-3626:admin#** as seen in the example below. The switch is not ready for configuration.

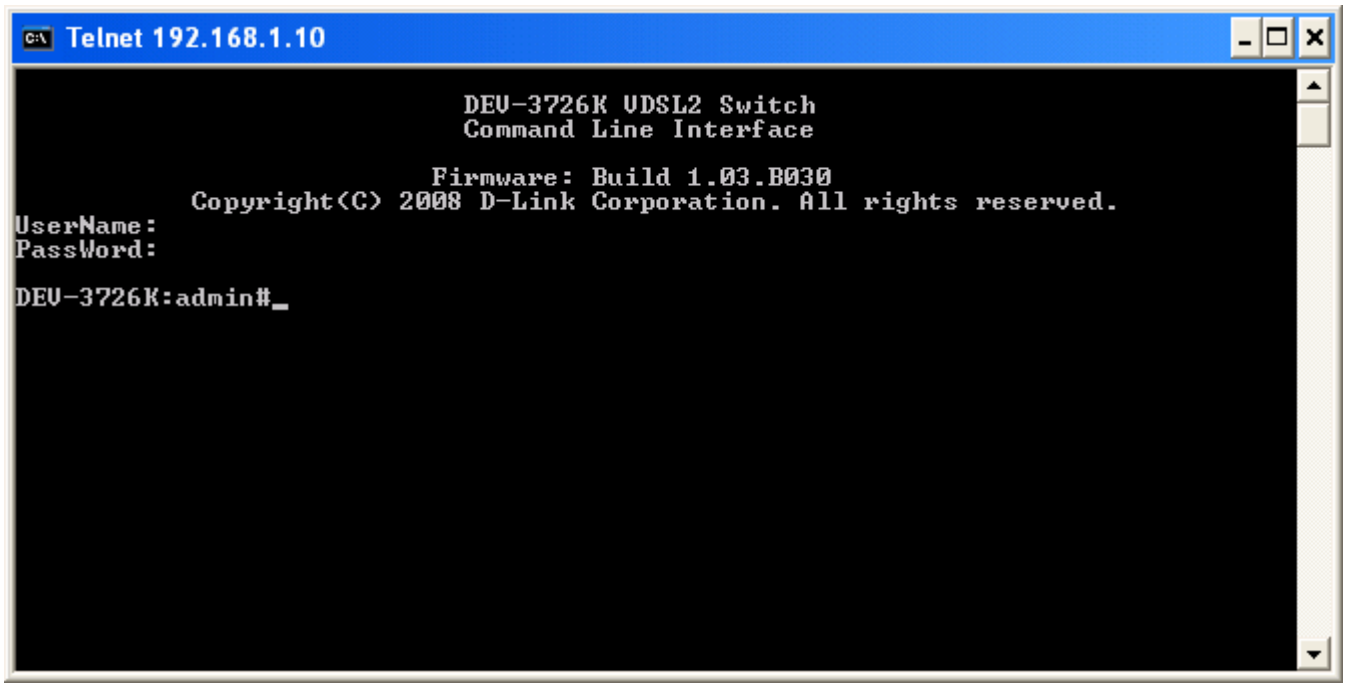


Figure 2. Menus Command Prompt using out-of-band Telnet connection

NOTE: Telnet can also be used in-band by connecting through port 25 or 26. The Factory default IP address of the in-band interface "System" is 10.90.90.90.

Login to Web Manager

To use the web-based management module for switch management, run the browser you have 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; this opens the management module's user authentication window, as seen below.

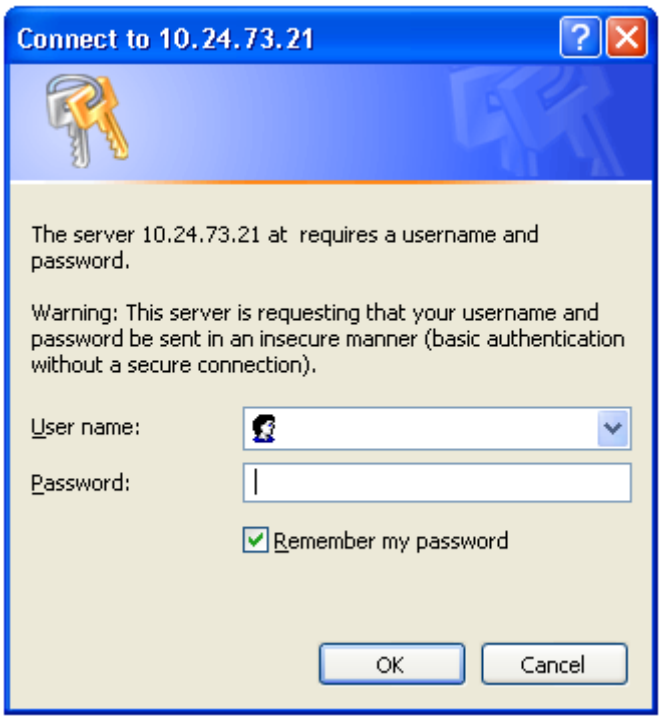


Figure 3. Enter Network Password dialog

There is no default user name or password. At the User Name and Password fields, click on **OK**. This opens the web-based management interface. 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 windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into three distinct areas as described in the table.

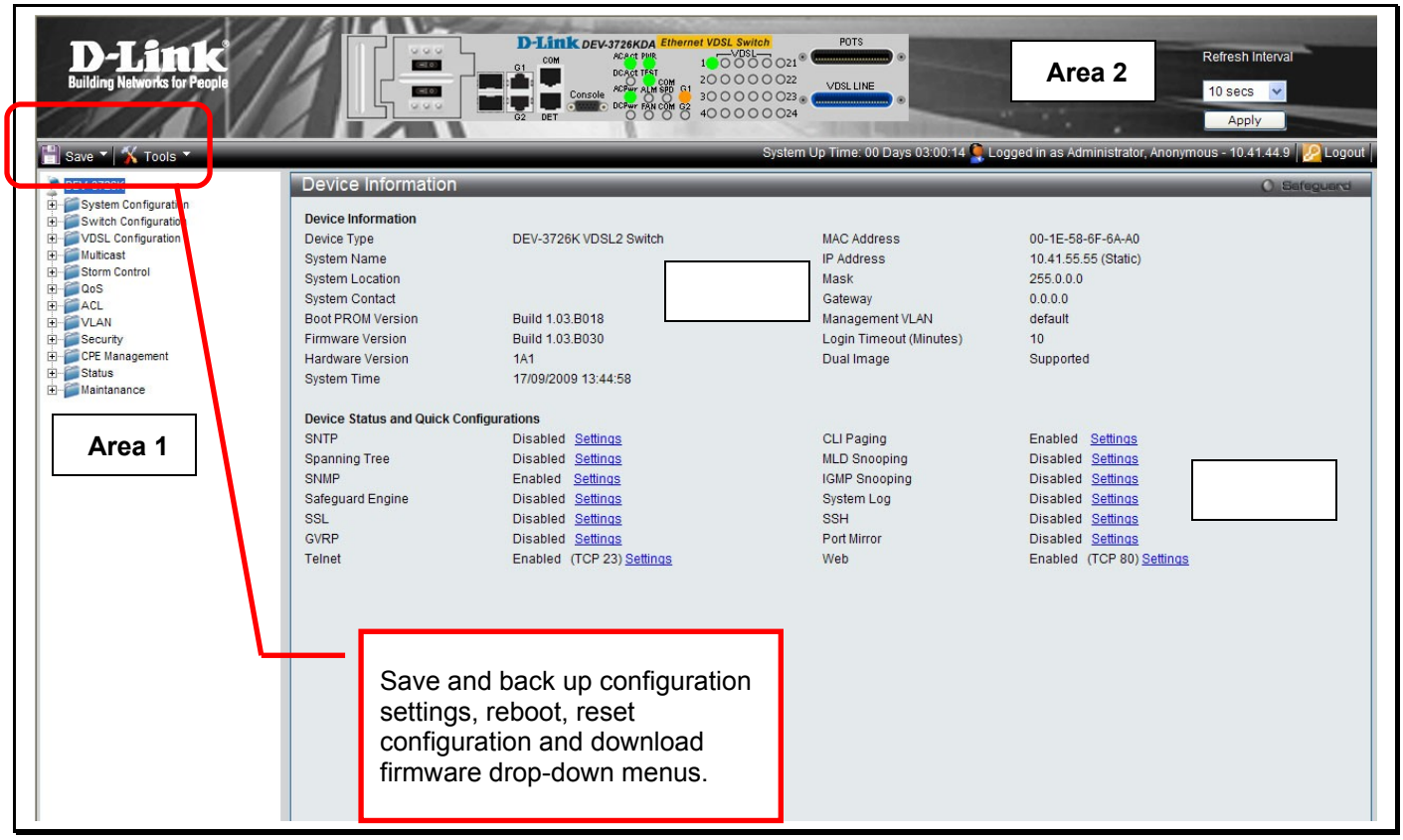


Figure 4. Main Web-Manager page

Area	Function
Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyper-linked window buttons and subfolders contained within them. 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 and expansion modules showing port activity. Various areas of the graphic can be selected for performing management functions, including port configuration.
Area 3	Presents switch information based on your selection and the entry of configuration data.
Area 4	Links to configuration menus, some of which are not accessable in the configuration menu folders (displayed in Area 1) are located here.

NOTICE: Any changes made to the switch configuration during the current session must be saved using the drop-down **Save** menu or use the command line interface (CLI) command **save**.

System Save Menus

The web interface for the switch includes two drop-down menus, the **Save** and **Tools** menus, located just above the menu folders. The Save menu includes options to save switch configuration settings and switch log.

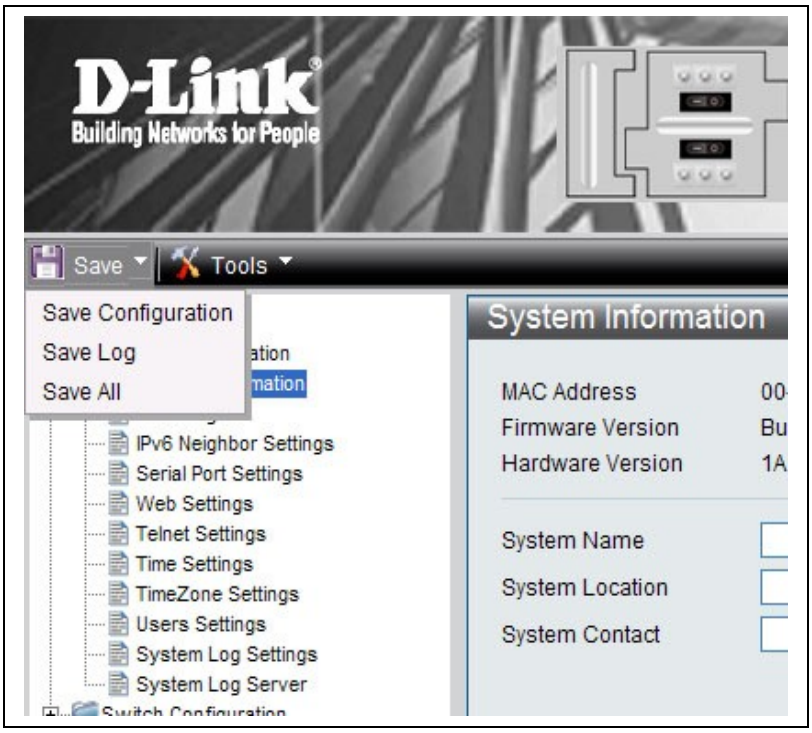


Figure 5. Save Configuration drop-down menu

To save the current configuration, from the Save drop-down menu, pull the cursor down to the **Save Configuration** option. The Save Configuration menu display appears during the saving process. Upon successfully saving the configuration, a message informs you the save is completed.

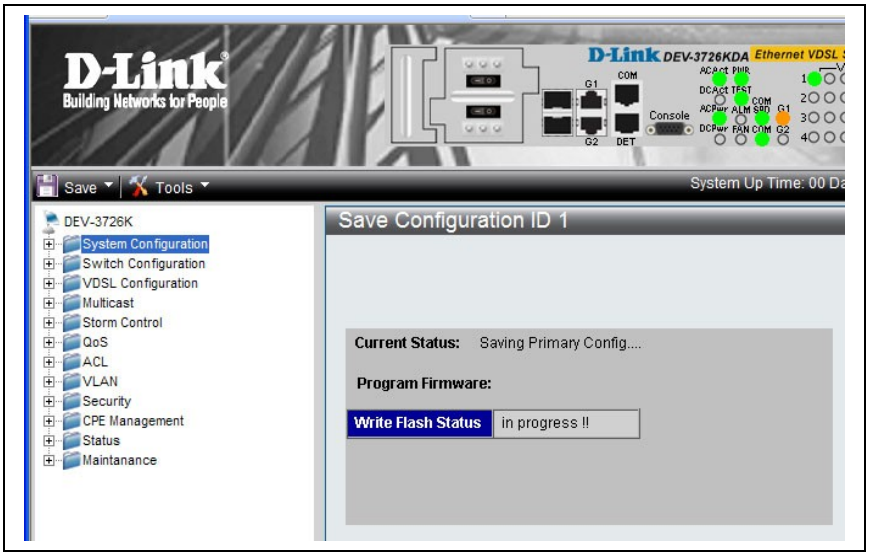


Figure 6. Save Configuration display

In addition to the Save Configuration option, the Save menus offer a **Save Log** and **Save All** option. The **Save All** option saves both the **System Log** and the current configuration file.

System Tools Menus

The Tools drop-down menu includes links **Configuration File Backup & Restore**, **Upload Log File**, **Reset**, **Download Firmware** and **Reboot System menus**.

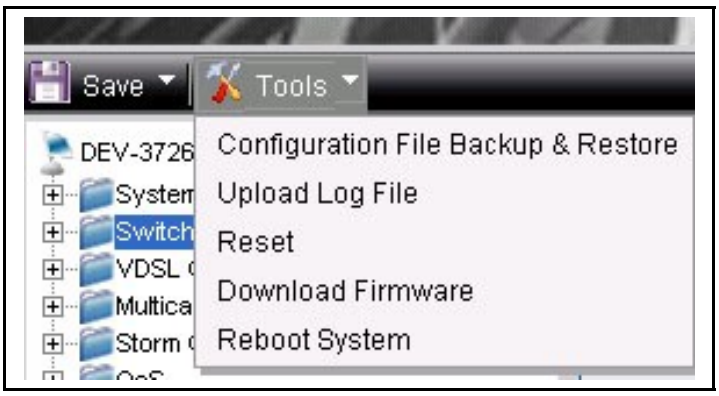


Figure 7. Tools drop-down menu

These menus are described below.

Configuration File Backup & Restore

The switch supports dual image storage for configuration file backup and restoration. The firmware and configuration images are indexed by ID number 1 or 2. To change the boot firmware image, use the Configuration ID drop-down menu to select the desired configuration file to backup or restore. The default switch settings will use image ID 1 as the boot configuration or firmware.

To backup the configuration file, enter the Server IP (either IPv4 or IPv6), interface name, file/path name, desired Configuration ID, and click **Backup**.

To restore the configuration file, enter the Server IP (either IPv4 or IPv6), interface name, file/path name, desired Configuration ID, and click **Restore**.

Figure 8. Configuration File Backup & Restore menu

Upload Log File

A history and attack log can be uploaded from the switch to a TFTP server. To upload a log file, enter a Server IP address, Interface Name and file/path name and then click **Upload** or **Upload Attack Log**.

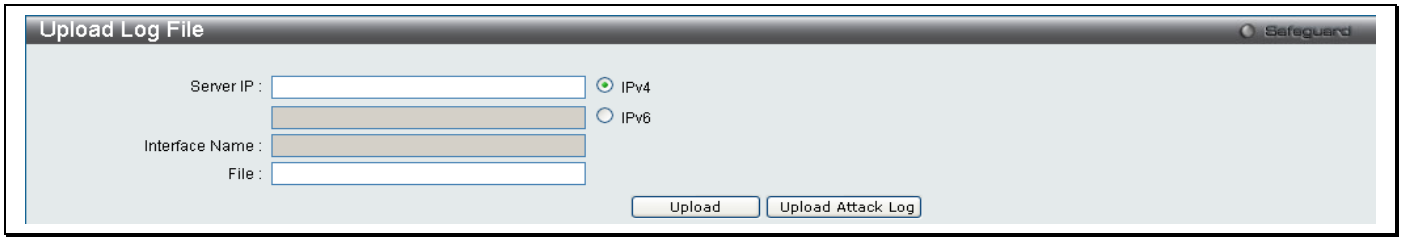


Figure 9. Upload Log File menu

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

NOTE: The serial port's baud rate will not be changed by the reset command. It will not be restored to the factory default setting.

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.

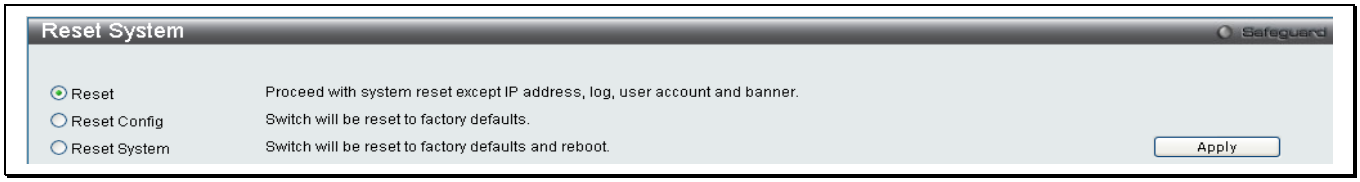


Figure 10. Reset System menu

Download Firmware

The following window is used to download firmware for the switch.

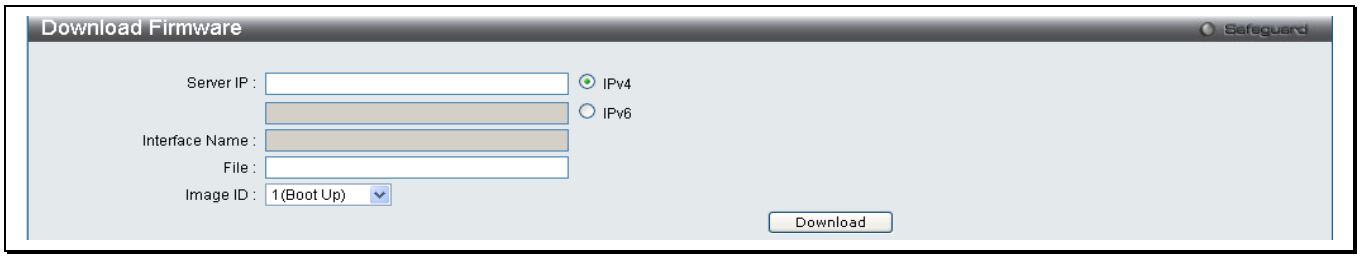


Figure 11. Download Firmware menu

Enter the Server IP address, the Interface Name, the path/file name and select the desired Image ID. Click **Download** to initiate the file transfer.

Reboot System

The following window is used to restart the switch.

Figure 12. Reboot System menu

Clicking the Yes radio button will instruct the switch to save the current configuration to non-volatile RAM before restarting the switch.

Clicking 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.

Device Information and Quick Configuration Links

This window contains the main settings for all major functions on the switch and appears automatically when you log on. To return to the **Device Information** and **Quick Configuration** likns, click the **DAS-3626** device name above the menu folders. The **Device Information** display shows the switch's **MAC Address** (assigned by the factory and unchangeable), the **Boot PROM Version**, **Firmware Version** and **Hardware Version** as well as other information about different settings on the switch. This information 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. Some functions are hyper-linked to their configuration window for easy access from the **Device Information** window.

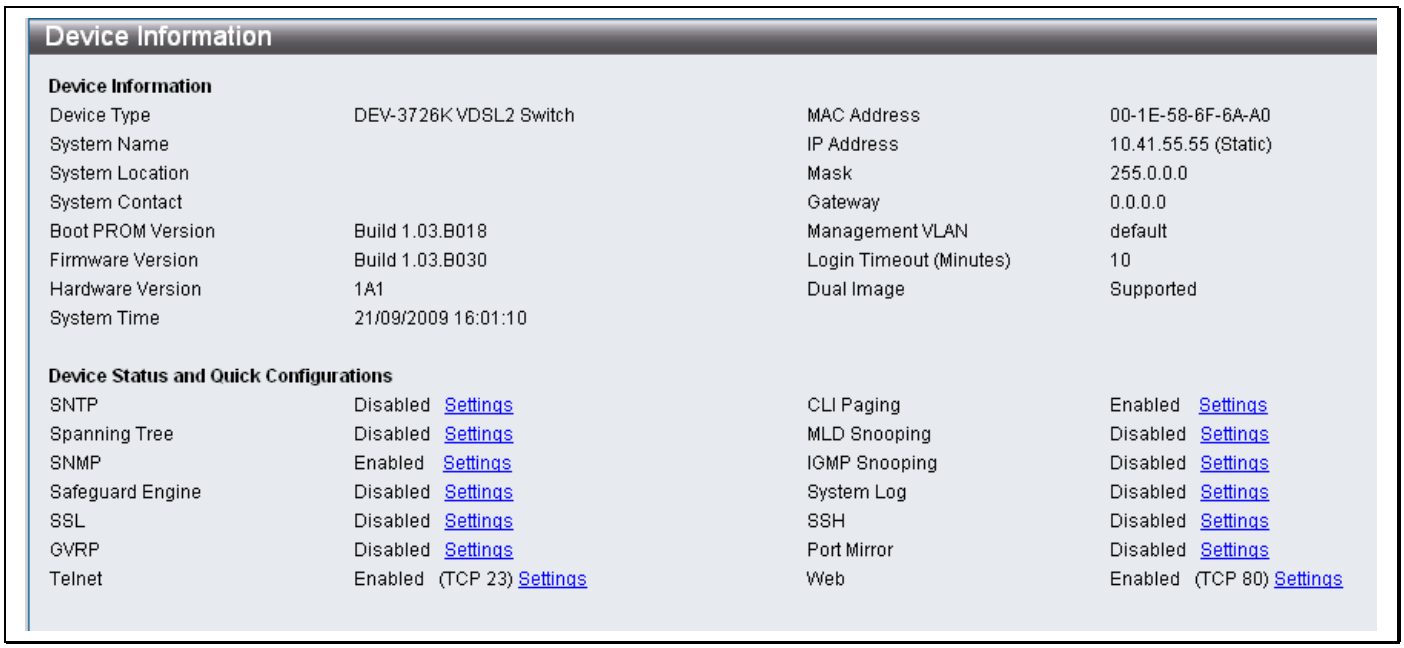


Figure 13. Device Information display and Quick Configuration links

Section 2

System Configuration

System Information

IP Settings

IPv6 Neighbor Settings

Serial Port Settings

Web Settings

Telnet Setting

Time Setting

TimeZone Setting

Users Setting

System Log Setting

System Log Server

Configuration menus in the System Configuration folder are used to change general system settings sucha as IP settings for the two switch IP interfaces, system time settings and user account settings.This section describes the menus contained in the System Configuration menu directory.

System Information

Use the System Information menu to add name, location and administrator contact information.

To view the menu, click **System Configuration > System Information** as shown below:

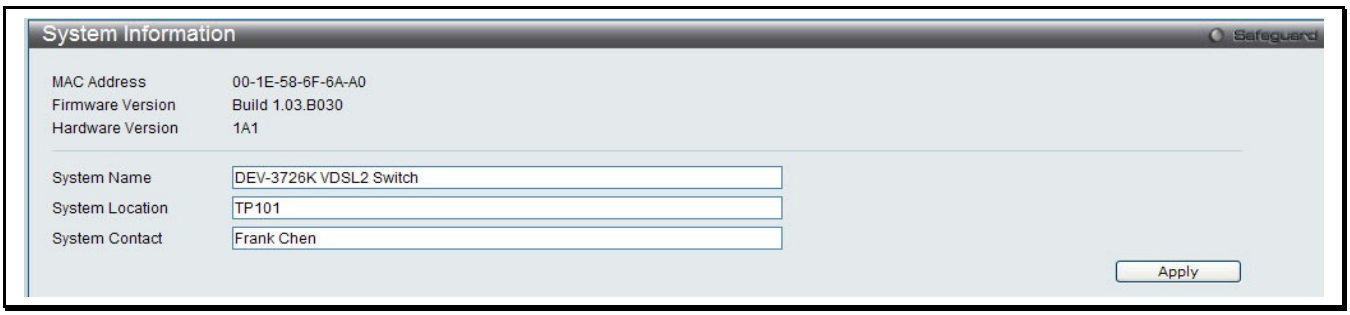


Figure 14. System Information menu

Interface Settings

The **Interface Settings** menu is used to access the IP settings for the two IP interefaces of the switch.

To view the menu, click **System Configuration > IP Settings** as shown below:

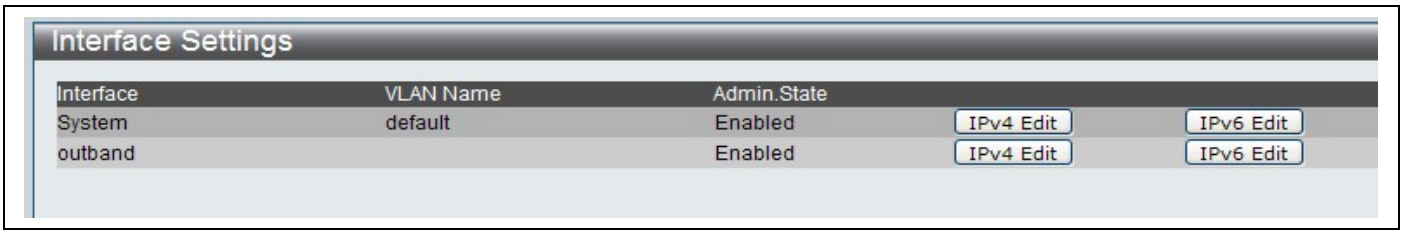


Figure 15. Interface Settings menu

The parameter values below are displayed in the **Interface Settings** menu:

Parameter	Description
Interface	The name of the IP interfaces used to manage the switch.
VLAN Name	The name of the VLAN that includes the System interface. This can be configured in the **IPv4** or **IPv6 Interface Settings** menu for the interface.
Admin. State	Displays the current state of the interface. Access the **IPv4** or **IPv6 Interface Settings** menu to enable or disable the interface.

To change the IP settings, *VLAN Name,* or *Admin.State,* click on the **IPv4 Edit** or **IPv6 Edit** button for the interface to be configured.

In the new menu, enter the new *VLAN Name, IPv4 Address* and *Subnet Mask*, select the *IPv4 State* and click **Apply**. To edit an entry for IPv4 features click the corresponding **IPv4 Edit** button.

Figure 16. IPv4 Interface Settings Edit menu

The following parameters can be configured:

Parameter	Description
Interface Name	Displays the interface being edited.
VLAN Name	Enter the name of the VLAN corresponding to the interface. (System interface only)
IPv4 Address	Enter an alternative IPv4 address. Currently an interface can only have one IPv4 address defined. Therefore multinetting configuration of IPv4 must be done through creation of a secondary interface on the same VLAN, instead of directly configuring multiple IPv4 addresses on the same interface.
Subnet Mask	Enter the corresponding subnet mask.
IPv4 State	This function allows user to enable the IPv4 address on the IP interface.

Click **Apply** to implement changes made.

To edit an entry for IPv6 features click the corresponding **IPv6 Edit** button.

Figure 17. IPv6 Interface Settings Edit menu

The following parameters can be configured:

Parameter	Description
Interface Name	Displays the interface being edited.
VLAN Name	Enter the name of the VLAN corresponding to the interface. (System interface only)
IPv6 Network Address	Enter the IPv6 Network Address to be configured. The interface can have multiple IPv6 addresses defined. Configuration of IPv6 addresses must be done through the command config ipif.
IPv6 State	Allows the user to enable or disable the IPv6 state on the interface.
NS Retransmit time (0-4294967295)	This field is used to set the interval, in milliseconds that the switch will produce neighbor solicitation packets to be sent out over the local network. This is used to discover IPv6 neighbors on the local network. The user may select a time between *0* and *4294967295* milliseconds. The default is *0*.
Automatic Link Local Address	Enables or disables the automatic configuration of link local addresses when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

Click **Apply** to implement changes made.

IPv6 Neighbor Settings

This window allows the user to create and configure IPv6 Neighbor settings on the switch. The switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

To view this window, click **System Configuration > IPv6 Neighbor Settings** as shown below:

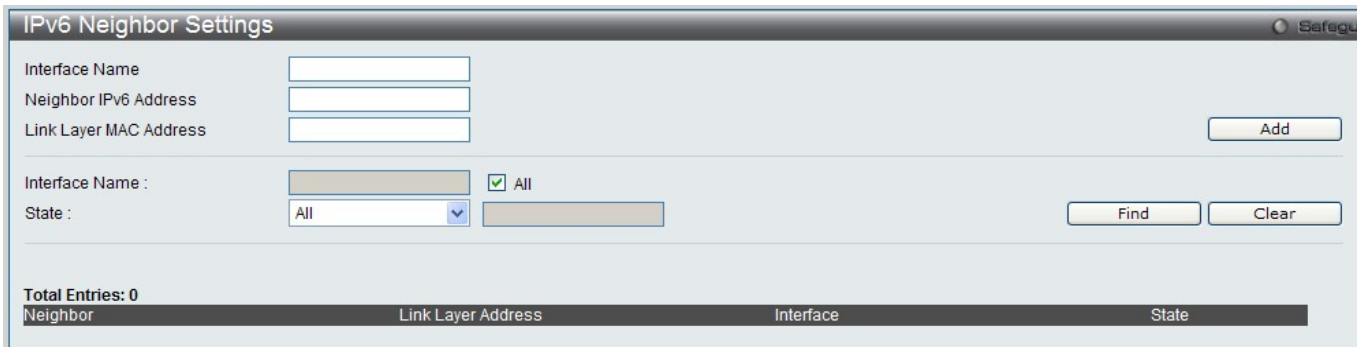


Figure 18. IPv6 Neighbor Settings menu

The following parameters can be configured:

Parameter	Description
Interface Name	Enter the interface name of the IPv6 neighbor you wish to configure.
Neighbor IPv6 Address	Enter the neighbor IPv6 address of the entry you wish to configure.
Link Layer MAC Address	Enter the MAC address of the neighbor device to be added as an IPv6 neighbor on the IP interface.
Interface Name	In order to search for a previously configured Interface name enter the appropriate information and click **Find**. To remove a previously configured Interface enter the Interface name and click **Clear**.
State	To find or delete specific entries use the pull down menu to select *All*, *Address*, *Static*, or *Dynamic*. *All* – Select **All** to view all configured neighbor devices which are IPv6 neighbors of the IP interface previously created. *Address* – Select **Address** and enter the IPv6 address of the entry you wish to find. *Static* – Select **Static** to view all statically entered IPv6 neighbors on the switch. *Dynamic* – Select **Dynamic** to view all dynamically configured neighbor devices which are IPv6 neighbors of the IP interface previously created.

Click **Add** to add a new entry, click **Find** to search for a specific entry or click **Clear** to remove an entry.

Serial Port Setting

Use the **Serial Port Setting** window to console serial port setting, config Baud Rate and Auto Logout setting.

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

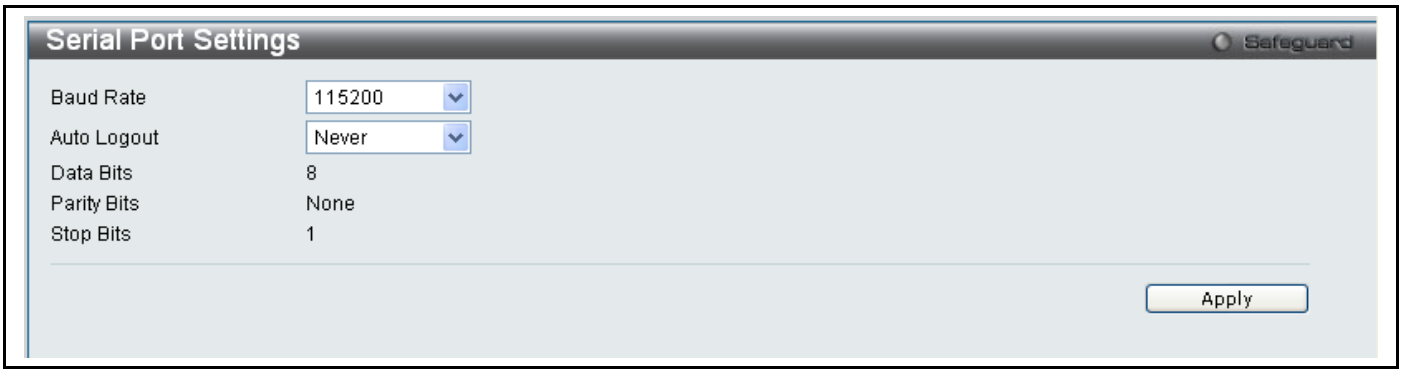


Figure 19. Serial Port Settings

The following fields can be set:

Parameter	Description
Baud Rate	Select the baud rate used for the console serial port.
Auto Logout	To configure console logout time, choose 2, 5, 10, 15 minutes or never logout from the pull-down menu.

Web Settings

Web-based management is *Enabled* by default. If you choose to disable this by selecting *Disabled*, you will lose the ability to configure the system through the web interface as soon as these settings are applied.

To view this menu, click the **Web Settings** link in the Quick Configuration menu as shown below:

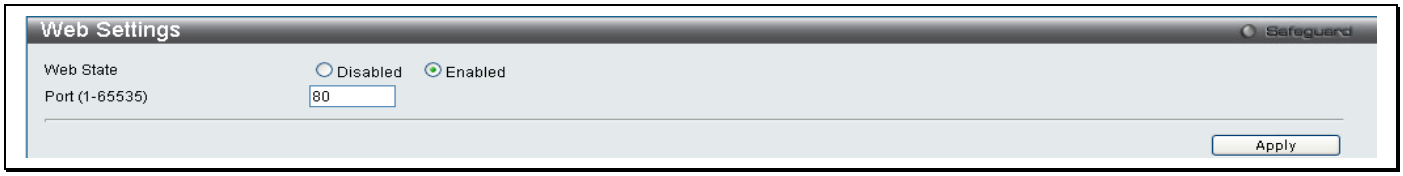


Figure 20. Web Settings menu

Telnet Settings

Telnet configuration is *Enabled* by default. If you do not want to allow configuration of the system through Telnet choose *Disabled*. The TCP ports are numbered between *1* and *65535*. The "well-known" TCP port for the Telnet protocol is *23*.

To view this menu, click the **Telnet Settings** link in the Quick Configuration menu as shown below:

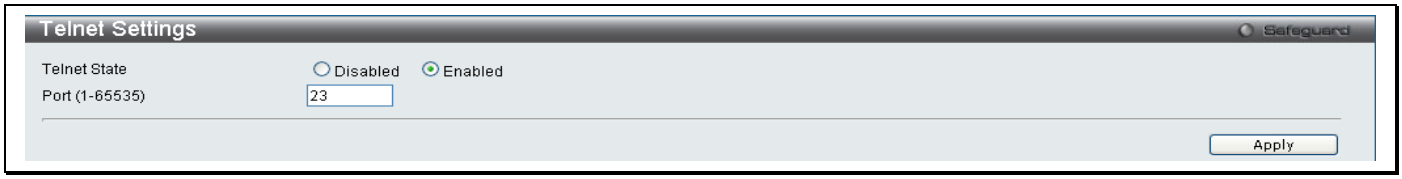


Figure 21. Telnet Settings menu

System Time and SNTP Settings

Simple Network Time Protocol Settings used to set system time are configured in two menus, the Time Settings and Time Zone Settings menus.

Time Settings

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

To view this window, click **System Configuration > Time Settings** (alternatively this menu is also displayed by clicking the **SNTP Settings** link in the Quick Configuration menu in the Device Information page) as shown below:

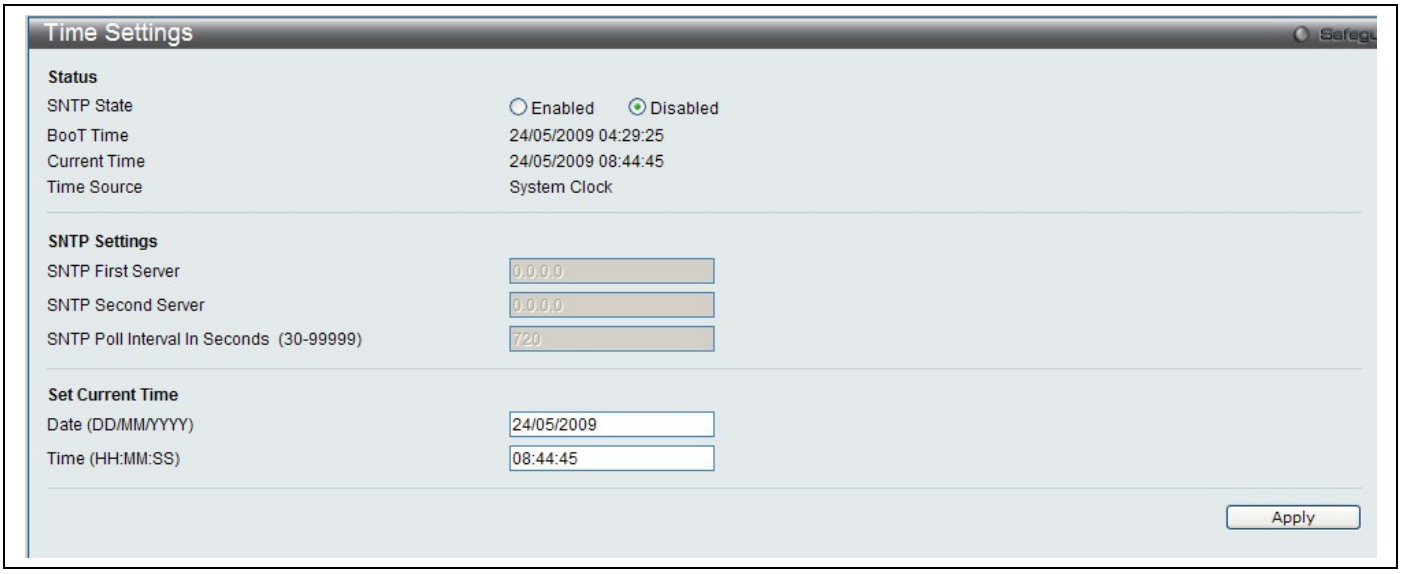


Figure 22. Time Settings menu

The following parameters can be set or are displayed:

Parameter	Description
Status	
SNTP State	Use the radius button to select an *Enabled* or *Disabled* SNTP state.
Current Time	Displays the Current Time set on the switch.
Time Source	Displays the time source for the system.
SNTP Settings	
SNTP First Server	This is the IP address of the primary server the SNTP information will be taken from.
SNTP Second Server	This is the IP address of the secondary server the SNTP information will be taken from.
SNTP Poll Interval in Seconds (30-99999)	This is the interval, in seconds, between requests for updated SNTP information.
Set Current Time	
Date (DD/MM/YYYY)	Enter the current date in day, month and year to update the system clock.
Time in (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.

Click **Apply** to implement changes made.

Time Zone Settings

The following window is used to configure time zones and Daylight Savings time settings for SNTP.

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

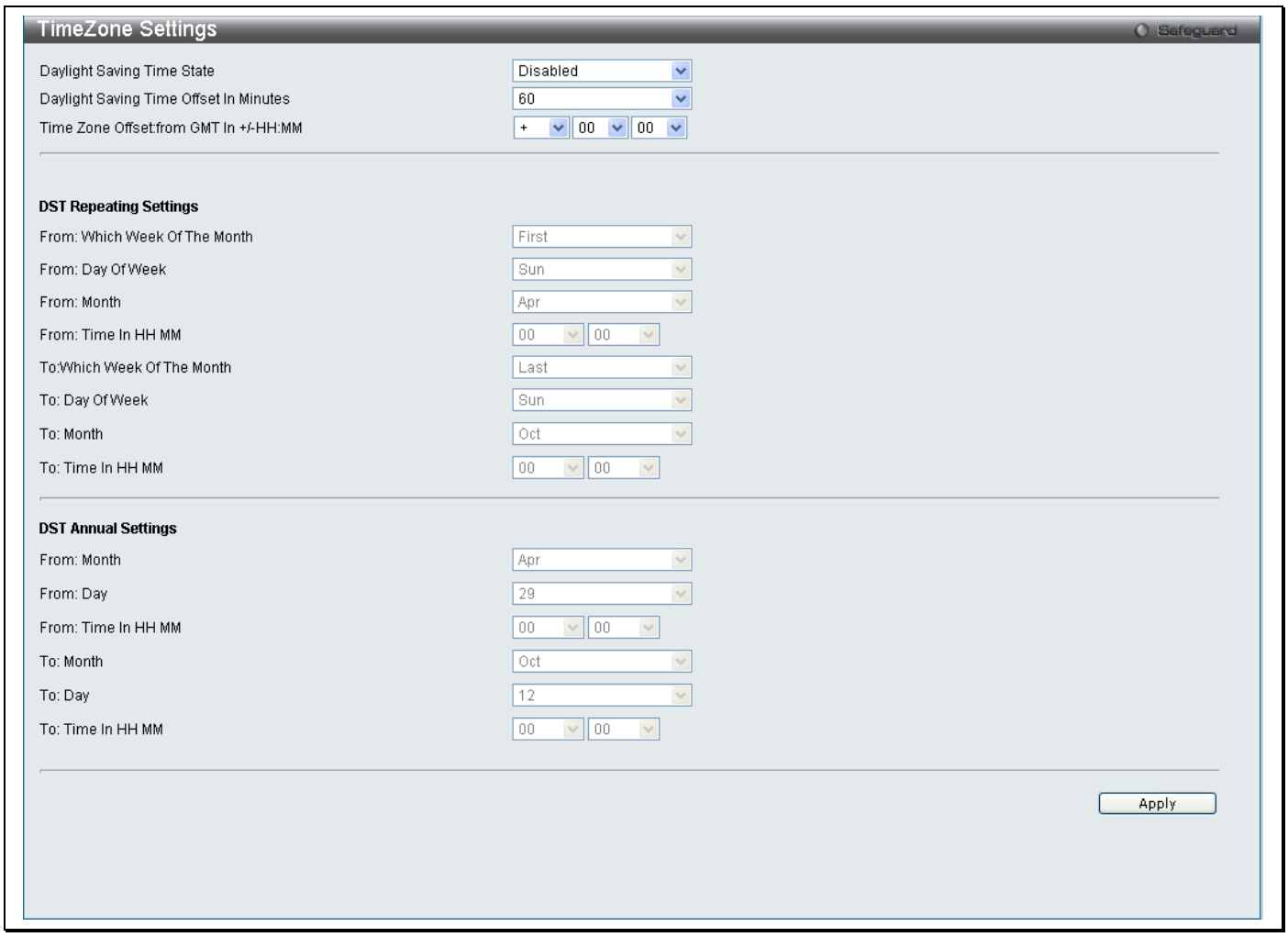


Figure 23. Time Zone and DST Settings menu

The following parameters can be set:

Time Zone and DST	
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.)

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 the 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 the 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.

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 week 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 date DST will end on, each year.
To: Time in HH:MM	Enter the time of day that DST will end on, each year.

Click **Apply** to implement changes made to the **Time Zone and DST** window.

User Account Settings

The **User Accounts** menu is used to control user privileges, create new users and view existing User Accounts.

To view the menu, click **System Configuration > User Settings**:

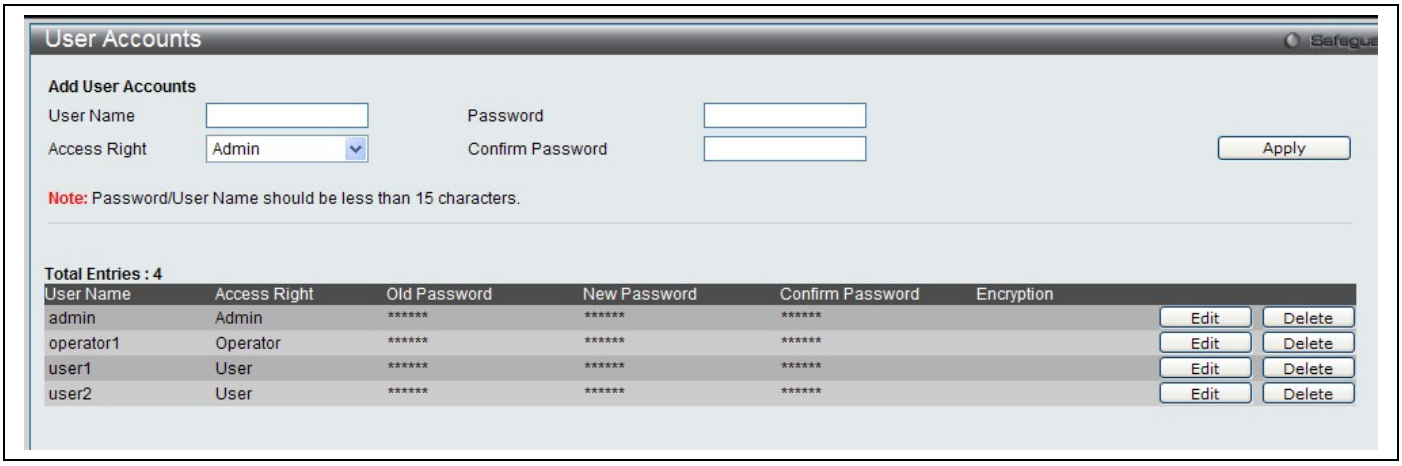


Figure 24. User Accounts menu

The following fields can be set:

Parameter	Description
User Name	The name of the user, an alphanumeric string of up to 15 characters.
Access Right	There are three levels of user privileges, **Admin**, **Operator** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** or **Operator** level privileges. There are 3 levels of security offered on the switch, the **Operator** level privilege will allow users to configure and view configurations on the switch, except for those involving security features, which are still left to the **Admin** level privilege. **Operator** level users can be authenticated through either the local authentication method of the switch, or through the Access Authentication Control feature, discussed later in this document. Once the user has logged in to the switch in the **Operator** level, certain security screens and windows will not be made available to view, or to configure. Only **Admin** level users have access to these features. (Ошибка: источник перекрестной ссылки не найден below summarizes **Admin**, **Operator** and **User** level privileges)
New Password	Enter a password for the new user.
Confirm New Password	Retype the new password.

To add a new user, enter the appropriate information and click **Apply**. To delete an account click the corresponding **Delete** button. To modify an existing user account, click **Edit** as shown below.

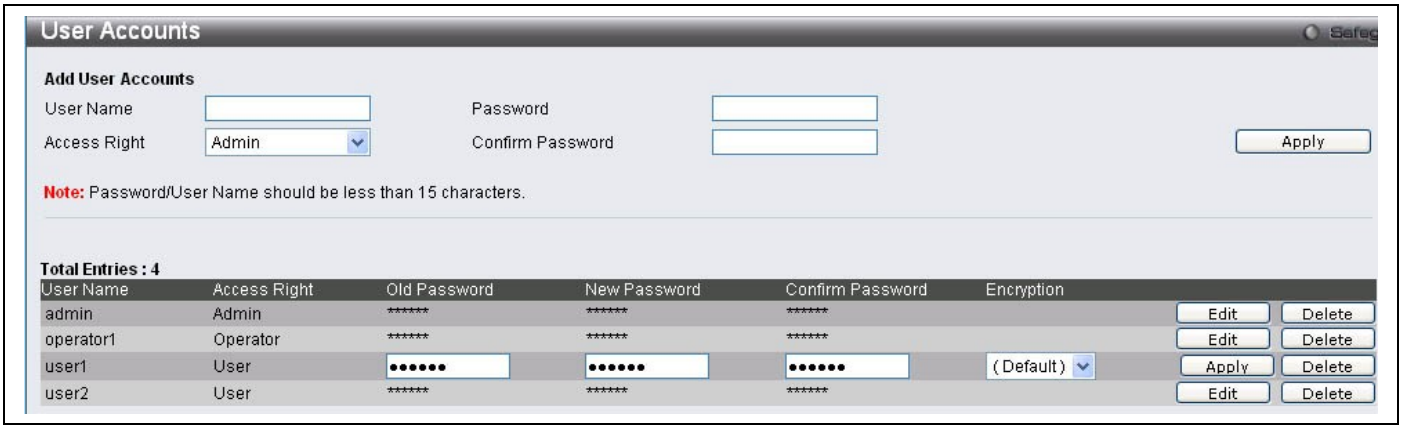


Figure 25. User Accounts menu

Enter the Old Password for the account, the New Password you wish to use, and retype the new password in the Confirm Password field. Use the drop-down menu to select the type of encryption (*Default, Plain Text* or *Sha 1*), and click **Apply**.

NOTICE: In case of lost passwords or password corruption, please refer to the D-Link website and the White Paper entitled "Password Recovery Procedure", which will guide you through the steps necessary to resolve this issue.

Admin, Operator and User Privileges

Recently added to the levels of security offered on the switch, the **Operator** level privilege will allow users to configure and view configurations on the switch, except for those involving security features, which are still left to the **Admin** privilege. Operator users can be authenticated through either the local authentication method of the switch, or through the Access Authentication Control feature, discussed later in this document. Once the user has logged in to the switch in the Operator level, certain security screens and windows will not be made available to view, or to configure. Only Admin level users have access to these features.

There are three levels of user privileges, **Admin**, **Operator** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** or **Operator** privileges.

The following table summarizes the Admin, Operator and User privileges:

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

Figure 26. Admin, Operator and User Privileges

System Log Configuration

This section contains information for configuring various attributes and properties for System Log Configurations, including System Log Settings and System Log Host.

System Log Settings

This window allows the user to enable or disable the System Log and specify the System Log Save Mode Settings.

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

Figure 27. System Log Settings menu

The following parameters can be set:

Parameter	Description
System Log	To activate the System Log select *Enabled* or *Disabled*.
Save Mode	Use this drop-down menu to specify the method that will trigger a log entry. You can choose between *On Demand*, *Time Interval* and *Log Trigger*. *On Demand* – This method will only save log files when they manually tell the switch to do so, using the **Save Log** link in the **Save** folder. *Time Interval* – This method configures a time interval by which the switch will save the log files. The user may set a time between *1* and *65535* minutes. *Log Trigger* – This method will save log files to the switch every time a log event occurs on the switch.
Minutes (1-65535)	Enter a time interval, in minutes, for which you would like a log entry to be made.

To add a new entry, enter the appropriate information and click **Apply**.

System Log Server

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

To view this window, click **System Configuration > System Log Configuration > System Log Server** as shown below:

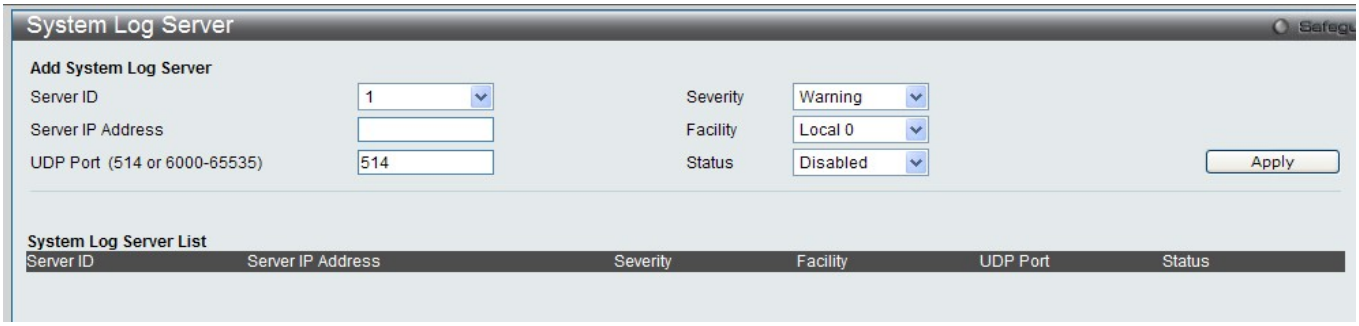


Figure 28. System Log Server menu

The following parameters can be set:

Parameter	Description
Server ID	Syslog server settings index (1-4).
Server IP Address	The IP address of the Syslog server.
UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is *514*.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *All*.
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values that the switch is currently employing.

Numerical	Facility Code	Numerical	Facility Code
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	**16**	**local use 0 (local0)**
5	messages generated internally by syslog line printer subsystem	**17**	**local use 1 (local1)**
		18	**local use 2 (local2)**
7	network news subsystem	**19**	**local use 3 (local3)**
8	UUCP subsystem	**20**	**local use 4 (local4)**
9	clock daemon	**21**	**local use 5 (local5)**
10	security/authorization messages	**22**	**local use 6 (local6)**
11	FTP daemon	**23**	**local use 7 (local7)**

Status	Choose *Enabled* or *Disabled* to activate or deactivate.

Section 3

Switch Configuration

MAC Address Aging Time

Ethernet Settings

FDB

Traffic Segmentation

CLI Paging

Port Mirror

LACP Port Settings

Loopback Detection Settings

QinQ Settings

GVRP

DHCP/BOOTP Relay Settings

Spanning Tree Settings

Multiple Spanning Tree Settings

CFM

The Switch Configurtion Section includes these functions discussed in detail.

MAC Address Aging Time

This table 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, enter a value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1,000,000* seconds. The default setting is *300* seconds.

To view this window, click **Switch Configuration > MAC Address Aging Time** as shown below:

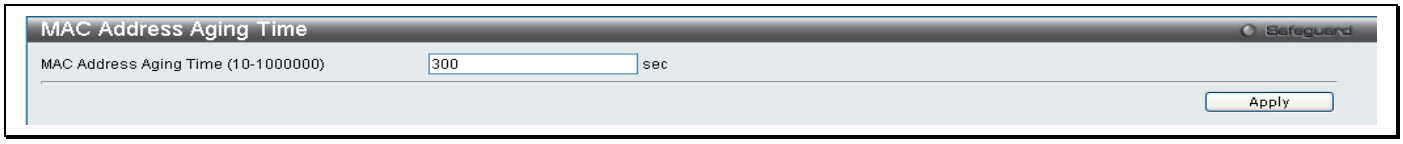


Figure 29. MAC Address Aging Time menu

Ethernet Settings

Figure 30. (Ethernet) Port Settings

Users may configure the speed and duplex of Ethernet port 1 here.

Auto negotiate – Turning on this feature will automatically adjust the speed and duplex of this port to its optimum settings.

Speed – Users may set the port speed here, as 10, 100 or 1000Mbps.

Duplex – Users may set the duplex settings for the port her, as half or full.

FDB

Use the MAC Address Table menu to view or clear entries from the switch's MAC address forwarding data base (FDB)

To view this menu, click **Switch Configuration > FDB** as shown below:

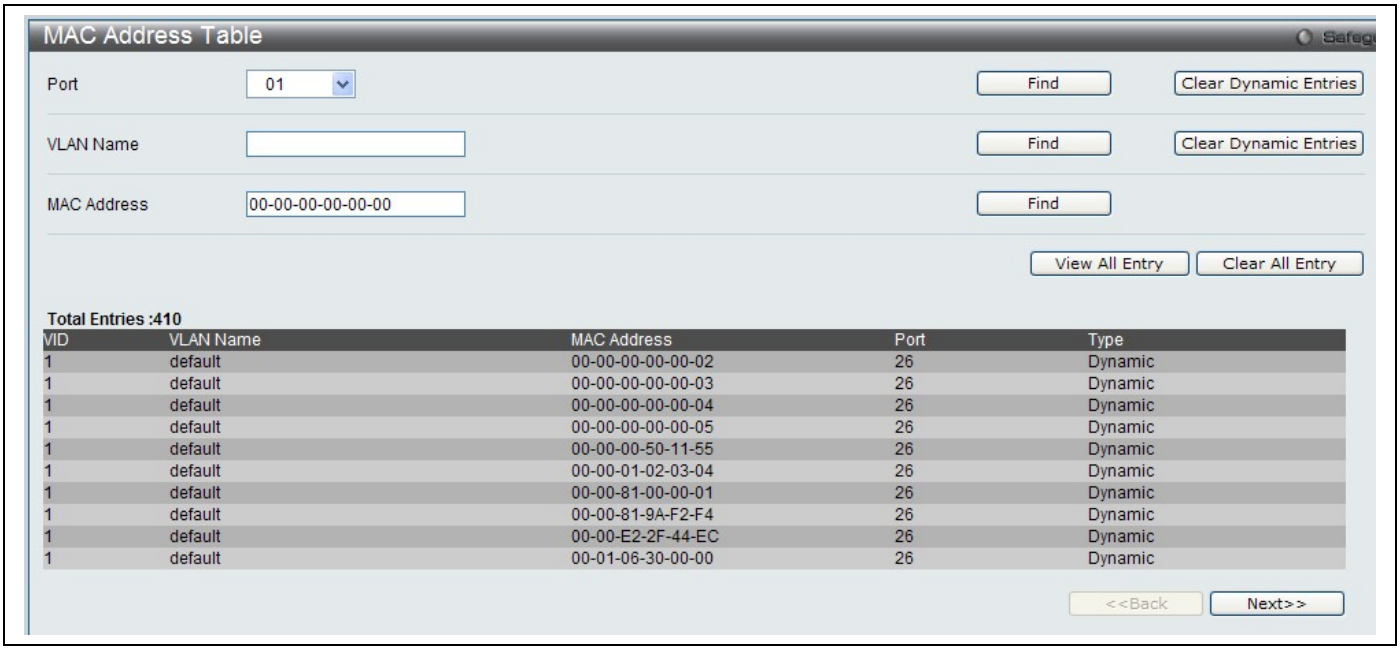


Figure 31. Forwarding Database entry table

Search options include searching by **Port** number, **VLAN Name** or specific **MAC Address**. To search the FDB, select the entry menu for the type of search to conduct (Port, VLAN Name or MAC Address), enter or select the port, VLAN name or MAC address, and click on the **Find** button.

To scroll through the FDB list manually, click on the **Next** and **Back** buttons.

To clear FDB entries choose to clear dynamic entries for a specified Port or VLAN by clicking on the **Clear Dynamic Entries** button for the search option used. Alternatively, to clear all entries in the FDB, click on the **Clear All Entries** button.

The MAC Address Table lists the following information:

Parameter	Description
VID	The VID of the VLAN from which packets are forwarded.
Port	The corresponding VDSL line of which the VID is a member.
MAC Address	The MAC address that resides on the port where traffic is forwarded.
Type	The type of FDB entry, Dynamic or Static.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on either a single switch or a group of ports on another switch in a switch stack. 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. This page allows you to view which port on a given switch will be allowed to forward packets to other ports on that switch. Select a port number from the drop down menu to display the forwarding ports. To configure new forwarding ports for a particular port, select a port from the menu and click **Apply**.

To view this window, click **Switch Configuration > Traffic Segmentation** as shown below:

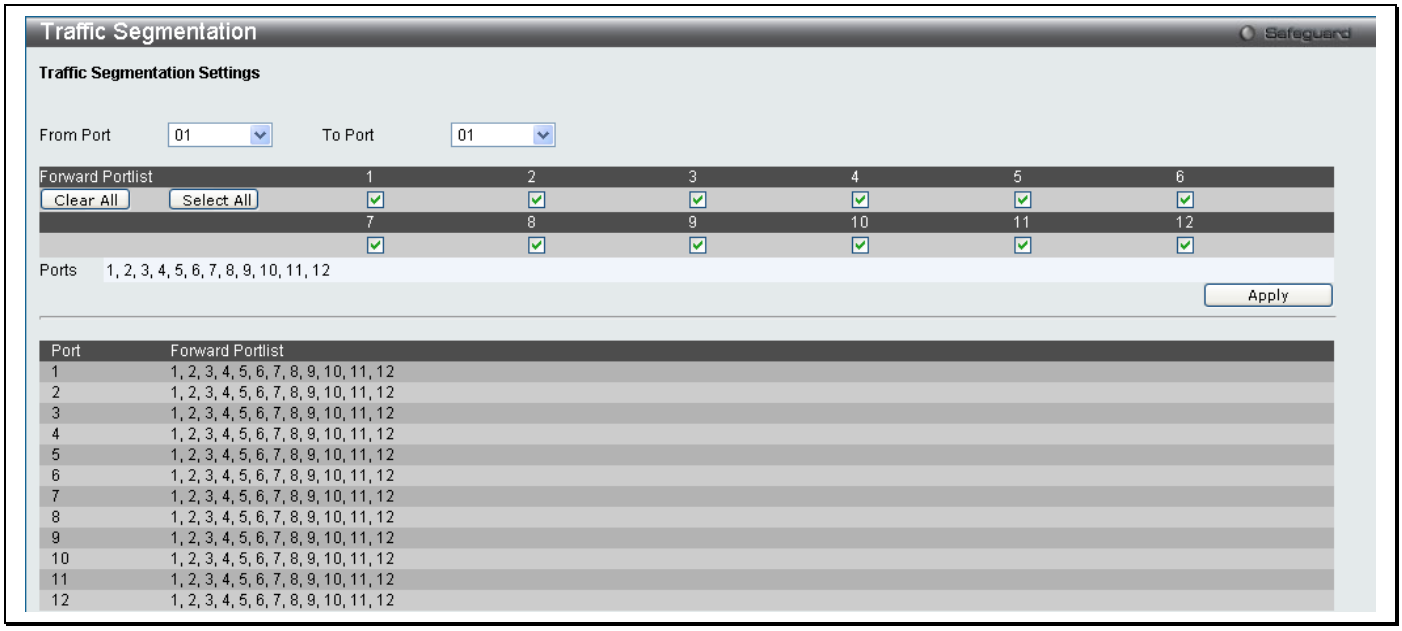


Figure 32. Traffic Segmentation menu

The following fields can be set

Parameter	Description
From Port / To Port	Check the corresponding boxes for the port(s) to transmit packets.
Forward Portlist	Check the boxes to select which of the ports on the switch will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the switch's **Current Traffic Segmentation Table**.

CLI Paging Settings

Clipaging Status can be *Enabled* or *Disabled* in this window, it is *Enabled* by default. Clipaging settings are used when issuing a command which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page.

To view this menu, click the **CLI Paging** link in the Quick Configuration menu as shown below:

Figure 33. CLI Paging Settings menu

Port 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.

To view this window, click **Switch Configuration > Port Mirror** as shown below:

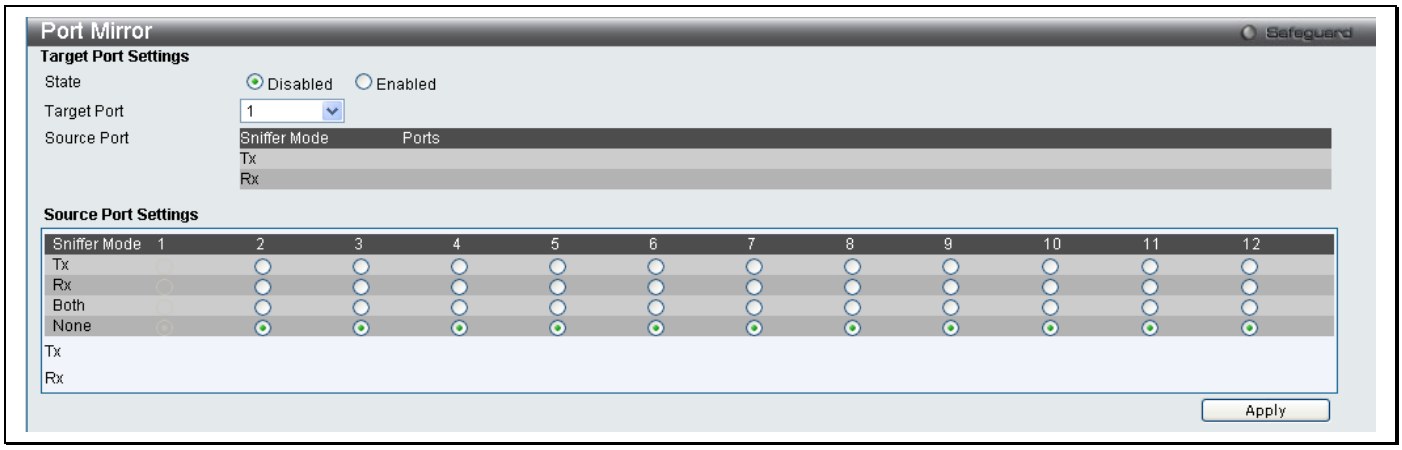


Figure 34. Port Mirror menu

To configure a mirror port:

1. Change the status to *Enabled*.
2. Select the Source Port from where you want to the frames to come from.
3. Select the Target Port, which receives the copies from the source port.
4. Click **Apply** to let the changes take effect.

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. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

Port Trunking

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 DAS-3626 supports single trunk group for the two Gigabit Ethernet (ports Ports 25 and 26). A potential bit rate of 2000 Mbps can be achieved.

The switch treats both ports in the 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.

NOTE: If either port within the trunk group becomes disconnected, packets intended for the disconnected port are load shared among the other unlinked ports of the link aggregation group.

Link aggregation is supported for the Gigabit Ethernet ports only. Both 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 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.

To view this window, click **Switch Configuraiton > Port Trunking** as shown below:

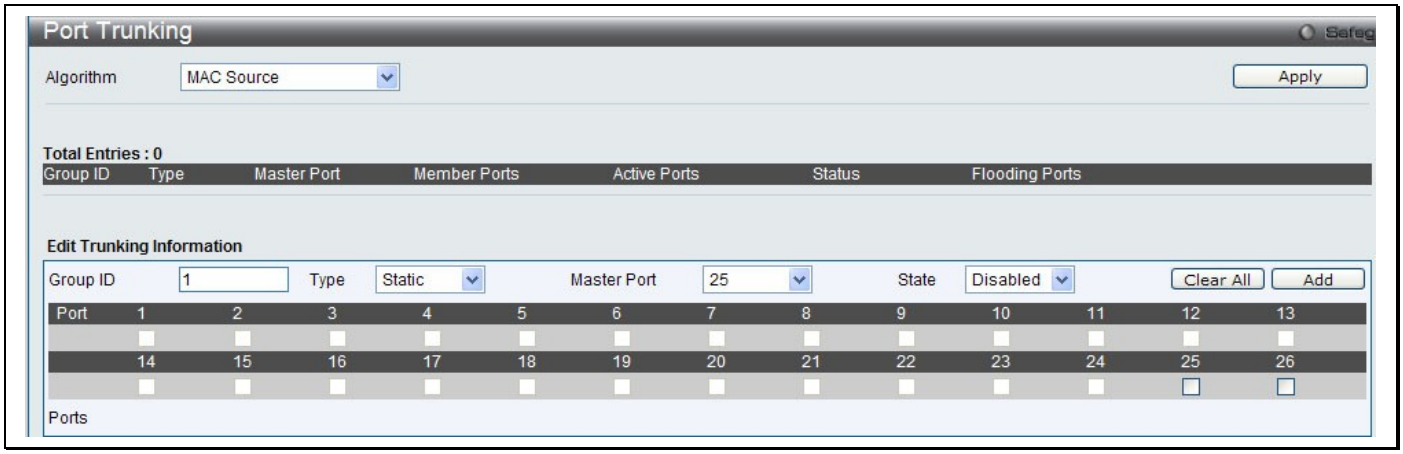


Figure 35. Port Trunking menu

To create a port trunk with Gigabit Ethernet ports 25 and 26, click to checkmark the boxes 25 and 26, configure the menu options and click the **Apply** button.

Configurable options and and display information in the Port Trunking menu include the following:

Parameter	Description
Algorithm	The algorithm that the switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *MAC Source*, *MAC Destination*, *MAC Source Dest*, *IP Source, IP Destination* or *IP Source Dest* (See the Link Aggregation section of this manual).
Group ID	Select an ID number for the group.
Type	This pull-down menu allows you 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	Toggle Enabled and Disabled to enable or disable the port trunk. 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.

Click **Apply** to implement changes made.

LACP Port Settings

The **LACP Port Settings** window is used to 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 this window, click **Switch Configuration > LACP Port Settings** as shown below:

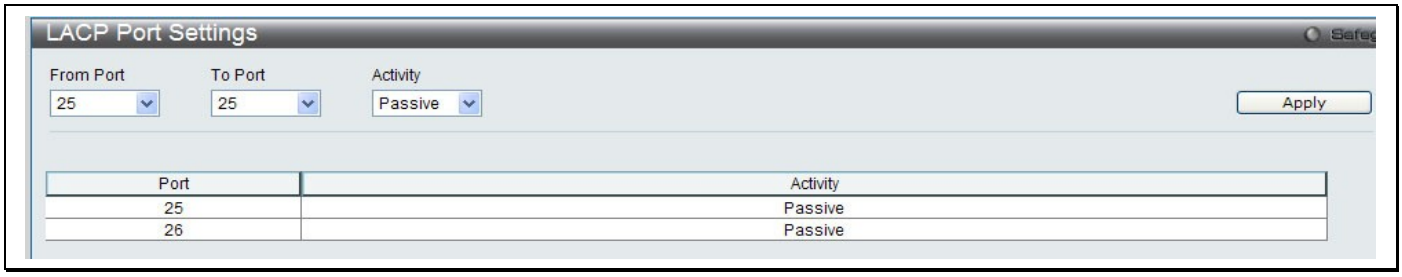


Figure 36. LACP Port Settings menu

The following fields can be set

Parameter	Description
From Port / To Port	Ports 25 and 26 are the only ports on the DAS-3626 available for LACP.
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 **Apply** to implement changes made.

Loopback Detection Settings

The Loopback Detection function is used to detect the loop created by a specific port. This feature is used to temporarily shutdown a port on the Switch when a loop detecting packet has been looped back to the switch. When the Switch detects that these packets are received from a port or a VLAN, it 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 this window, click **Switch Configuration > Loopback Detection Settings** as shown below:

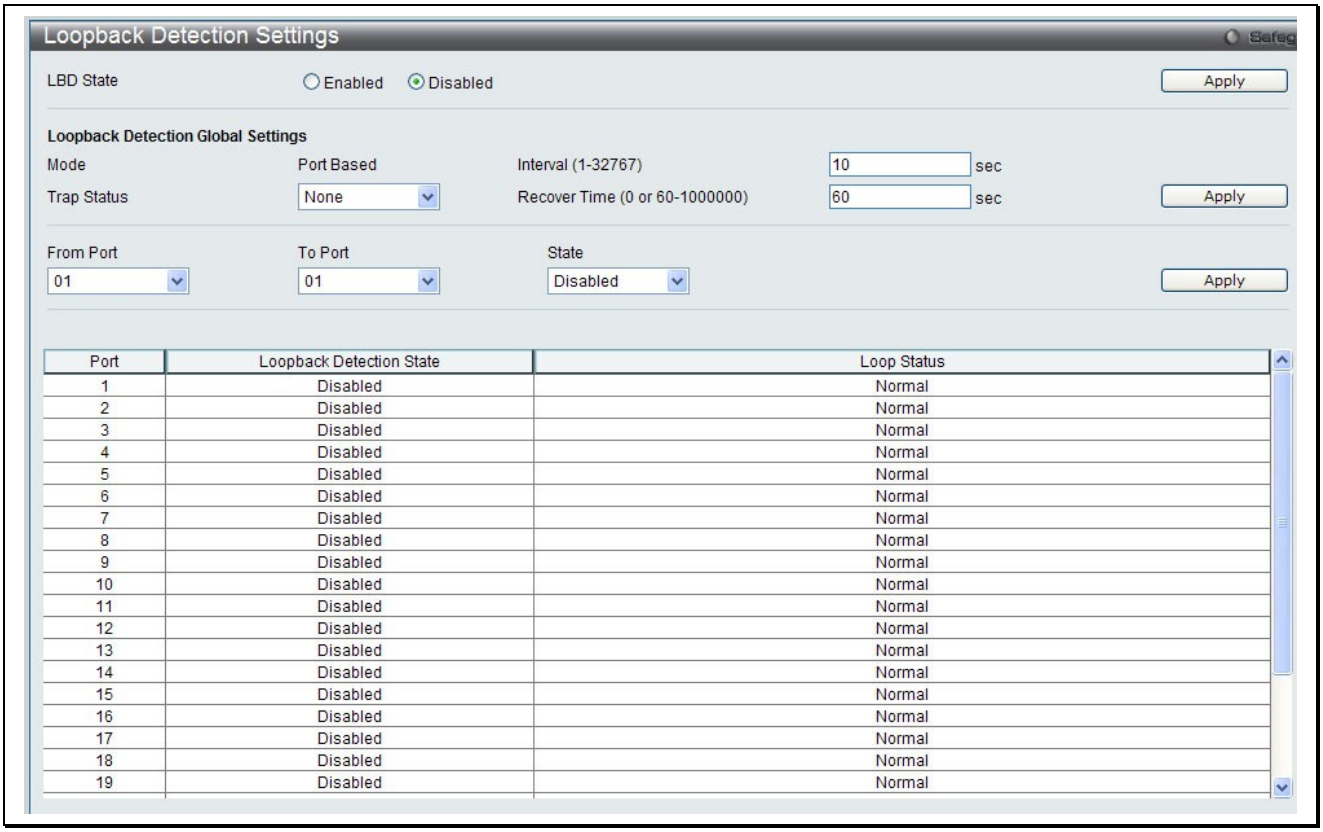


Figure 37. Loopback Detection Settings menu

The following parameters can be configured:

Parameter	Description
LBD State	Used to *Enable* or *Disable* loopback detection. The default is *Disabled.*
Mode	Use the drop-down menu to toggle between *Port Based* and *VLAN Based*.
Interval (1-32767)	Set a Loopdetect Interval between *1* and *32767* seconds. The default is *10* seconds.
Trap Status	Select the trap status, choose *None, Loop Detected, Loop Cleared* or *Both*.
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	Use the drop-down menu to select a beginning and ending port number.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*

Click **Apply** to implement changes made.

Q-in-Q Settings

This function allows the user to enable or disable the Q-in-Q function. Q-in-Q is designed for service providers to carry traffic from multiple users across a network. Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SPVLAN tags to each new frame.

To view this window, click **Switch Configuration > QinQ** as shown below:

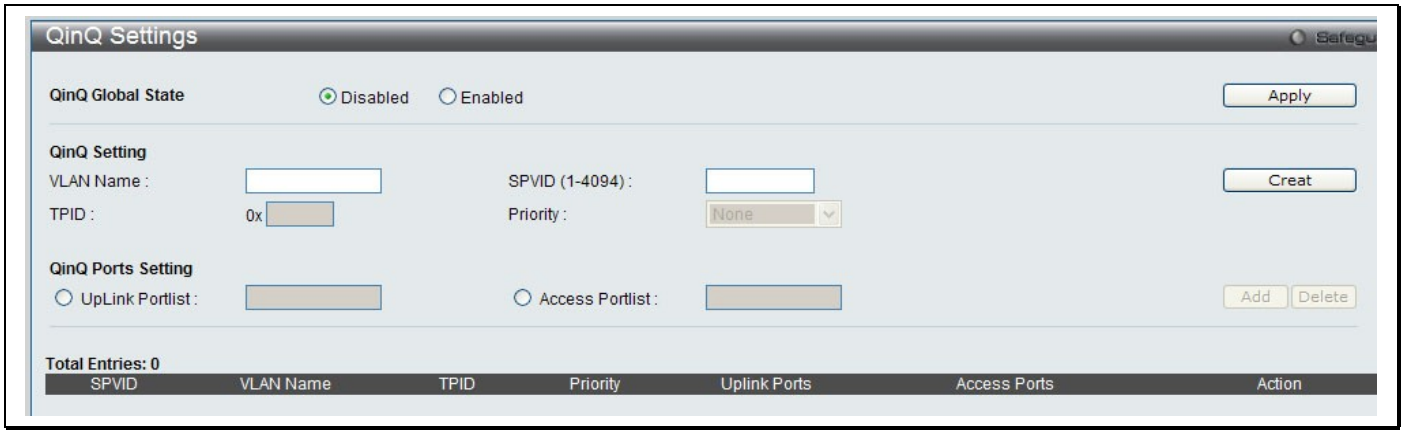


Figure 38. QinQ Settings menu

The following fields can be set:

Parameter	Description
From Port / To Port	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
Role	The user can choose between UNI or NNI role. *UNI* – To select a user-network interface which specifies that communication between the specified user and a specified network will occur. *NNI* – To select a network-to-network interface specifies that communication between two specified networks will occur.
Missdrop	Use the drop down menu to enable or disable missdrop. If missdrop is enabled, the packet that does not match any assignment rule in the Q-in-Q profile will be dropped. If disabled, then the packet will be assigned to the PVID of the receiving port.
Outer TPID	The Outer TPID is used for learning and switching packets.
Use Inner Priority	The priority given to the inner tag will be copied to the outer tag if this setting is enabled.
Add Inner Tag(hex: 0x1-0xffff)	Specify whether to add inner tag for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and thus the packets egress to the NNI port will be double tagged.

Click **Apply** to implement changes.

GVRP Global Settings

The GVRP allows interoperability with other switches, so the values of the GVRP timers can be configured. This table is used to set the GVRP Global Settings.

To view this window, click **Switch Configuration > GVRP Global Settings** as shown below:

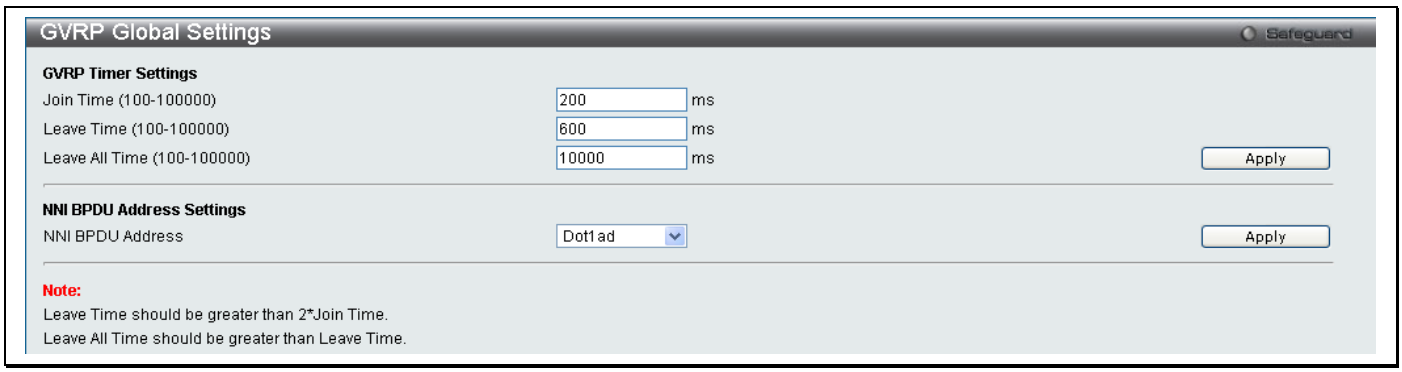


Figure 39. GVRP Global Settings menu

The following fields can be set:

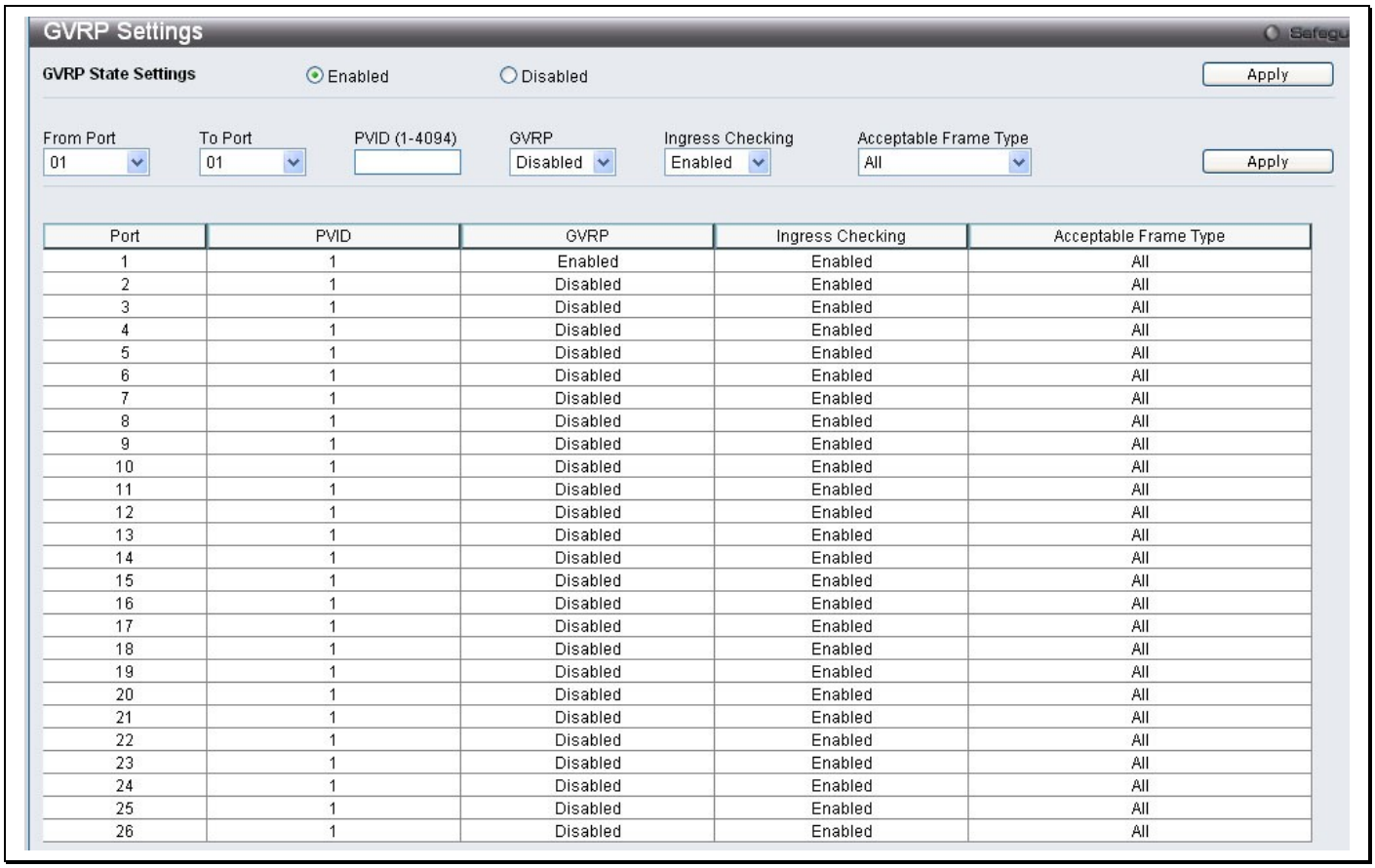
Parameter	Description
Join Time (100-100000)	The time in milliseconds that specifies the amount of time between the Switch receiving the information about becoming a member of the group and actually joining the group. The default is *200*.
Leave Time (100-100000)	The time in milliseconds that specifies the maximum amount of time between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. The default is *600*. The **Leave Time** must be greater than 2 join times.
Leave All Time (100-100000)	The time in milliseconds that specifies the amount of time the Switch will take to Leave All groups. The default is *10000*. The **Leave All Time** must be greater than the **Leave Time**.
NNI BPDU Address	This specifies the GVRP's pdu MAC address of the NNI port. *Dot1d* – Specifies GVRP's pdu MAC address of NNI port using 802.1d. *Dot1ad* – Specifies GVRP's pdu MAC address of NNI port using 802.1ad.

Click **Apply** to implement changes made.

GVRP Settings

The table allows the user to 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 do not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

To view this window, click **Switch Configuration > GVRP Settings** as shown below:



Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Enabled	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

Figure 40. GVRP Settings menu

The following fields can be set:

Parameter	Description
From Port / To Port	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** window.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
PVID	The read-only field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. 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.
Ingress Checking	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables 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 *Disabled* 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 *Admit_All*, which mean both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.

Click **Apply** to implement changes made.

DHCP Relay

The DHCP Relay folder contains six windows regarding the DHCP relay functions on the switch. The DHCP menus include **DHCP Relay Global Settings**, **DHCP Relay Interface Settings**, **DHCP Relay Option 60 Default Settings**, **DHCP Relay Option 82 Settings Remote ID**, **DHCP Realy Option 82 Settings Circuit ID** and **DHCP Relay Option 82 Settings**.

DHCP Relay Global Settings

This window is used to enable and configure **DHCP Relay Global Settings** on the switch. 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 more 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 *65,536* seconds, with a default value of *0* seconds.

To view this window, click **System Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings** as shown below:

Figure 41. DHCP Relay Global Settings menu

The following fields can be set:

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 across. The default hop count is *4*.
DHCP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum 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.

Click **Apply** to implement any changes that have been made.

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, you might configure a client with the option-82 field. In this situation, you should disable the information-check feature so that the switch does not remove the option-82 field from the packet. You can 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**. See the table below for a description of Option 82 settings as they relate to DSCP Relay.

Configure the following Option 82 settings in the DHCP/BOOTP Global Settins menu:

Parameter	Description
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 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 to the 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* – If 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 switch's ability to check the validity of the packet's option 82 field. *Enabled* – When the field is toggled to *Enable*, 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 switch's policy for handling packets when the **DHCP 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 Interface Settings

This window allows the user to set up a server, by IP address, for relaying DHCP information to the switch. The user may enter a previously configured IP interface on the switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **DHCP Relay Interface Table** at the bottom of the following window. The user may add up to four server IP's per IP interface on the switch.

To view this window, click **System Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings** as shown below:

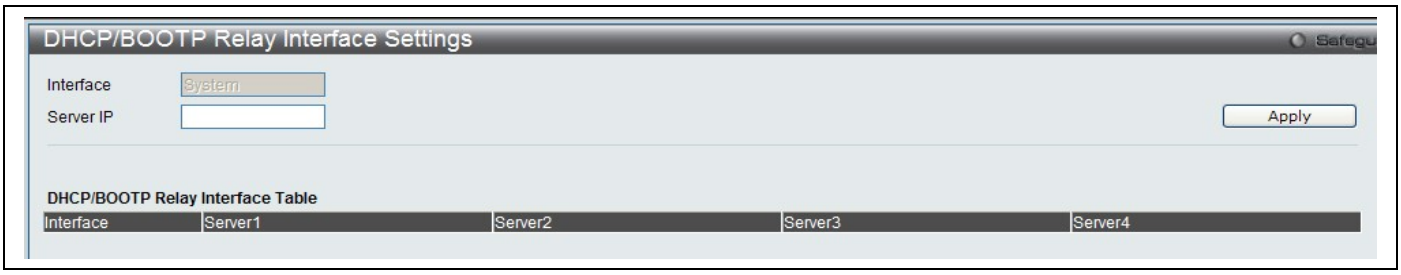


Figure 42. DHCP/BOOTP Relay Interface Settings and DHCP/BOOTP Relay Interface Table menu

The following parameters may be configured or viewed:

Parameter	Description
Interface	The IP interface on the switch that will be connected directly to the Server.
Server IP	Enter the IP address of the DHCP server. Up to four server IPs can be configured per IP Interface.

Click **Apply** to implement changes made.

Spanning Tree

This switch supports three versions of the Spanning Tree Protocol; 802.1D-2004 STP compatible, 802.11d-2004 Rapid STP and 802.1q-2005 MSTP. 802.1D STP will be familiar to most networking professionals. However, since 802.1w RSTP has 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 STP and 802.1w RSTP.

802.1w Rapid Spanning Tree

The switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1D STP. RSTP can operate with legacy equipment implementing IEEE 802.1D, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D 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. RSTP combines the transition states disabled, blocking and listening used in 802.1D and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 6-2 below compares how the two 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 is this absence of immediate feedback from adjacent bridges.

802.1w RSTP	802.1D STP	Forwarding	Learning
Discarding	Disabled	No	No
Discarding	Blocking	No	No
Discarding	Listening	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Comparing Port States

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, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1D and 802.1w Compatibility

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D format when necessary. However, any segment using 802.1D STP will not benefit from the rapid transition and rapid topology change detection of 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.

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

This window is used to enable and configure the STP bridge global settings on the Swtich.

To view this window, click **Switch Configuration > Spanning Tree > STP Bridge Global Settings** as shown below:

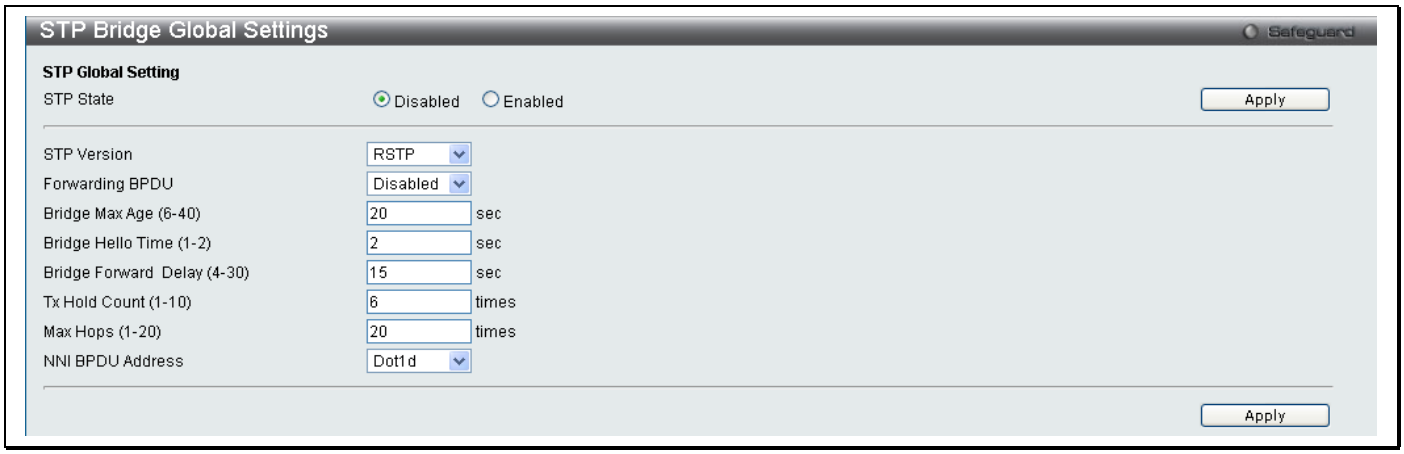


Figure 43. STP Bridge Global Settings menu

The following parameters can be set:

Parameter	Description
STP State	Use the radio buttons to enable or disable the STP Status.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the switch. There are three choices: *STPCompatability* – 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 Sec)	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. If the value ages out and a BPDU has still not been received from the Root Bridge, the switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between *6* and *40* seconds. The default value is *20*.
Bridge Hello Time (1-10 Sec)	The Hello Time can be set from *1* to *10* 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.
Bridge Forward Delay (4-30 Sec)	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.
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 (1-20)	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 BPDU packet and the information held for the port will age out. The user may set a hop count from *1* to *20*. The default is *20*.
NNI BPDU Address	Configure NNI port address. *dot1d* – Specifies GVRP's bpdu MAC address of NNI port using the definition of 802.1d. *dot1ad* – Specifies GVRP's pdu MAC address of NNI port using the definition of 802.1ad.

Click **Apply** to implement changes made.

NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

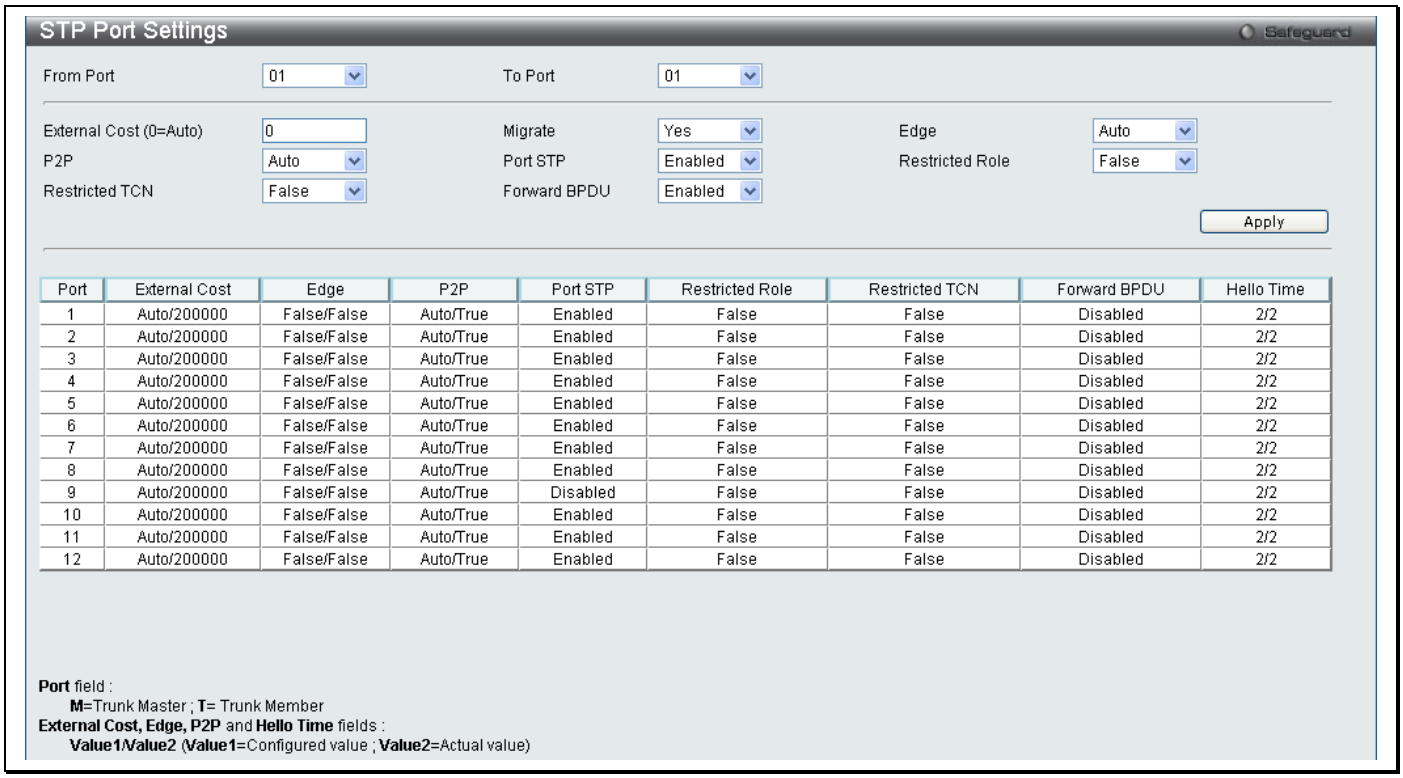
Max. Age ≤ 2 x (Forward Delay - 1 second)

Max. Age ≥ 2 x (Hello Time + 1 second)

STP Port Settings

This window is used to configure the STP Port Settings on the Swtich. STP can be set up on a port per port basis.

To view this window, click **Switch Configuration > Spanning Tree > STP Port Settings** as shown below:



Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	Hello Time
1	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
2	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
3	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
4	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
5	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
6	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
7	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
8	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
9	Auto/200000	False/False	Auto/True	Disabled	False	False	Disabled	2/2
10	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
11	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2
12	Auto/200000	False/False	Auto/True	Enabled	False	False	Disabled	2/2

Figure 44. STP Port Settings menu

In addition to setting Spanning Tree parameters for use on the switch level, the switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

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

The following fields can be set:

Parameter	Description
From Port / To Port	A consecutive group of ports may be configured starting with the selected port.
External Cost (0=Auto)	The external cost 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). *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. Default port cost: 100Mbps port = *200000*. Gigabit port = *20000*. *value 1-200000000* – Define 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.
Migrate	Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting If the switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.
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 *Auto* parameter will indicate that the port will be able to automatically enable edge port status if needed.
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 *True*. The default value *True* is equivalent to the *Auto* value.
Port STP	Allows STP to be *Enabled* or *Disabled* for the ports.
Restricted Role	Toggle between *True* and *False* to set whether this port is restricted to be selected as a root port. The default value is *False*.
Restricted TCN	Toggle between *True* and *False* to set whether this port is restricted to be selected as a propagate topology change. The default value is *False*.
Forward 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 *Enabled*.

Click **Apply** to implement changes made.

MST Configuration Identification

The following windows in the **MST Configuration Identification** section allow 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 this window, click **Switch Configuration > Spanning Tree > MST Configuration Identification** as shown below:

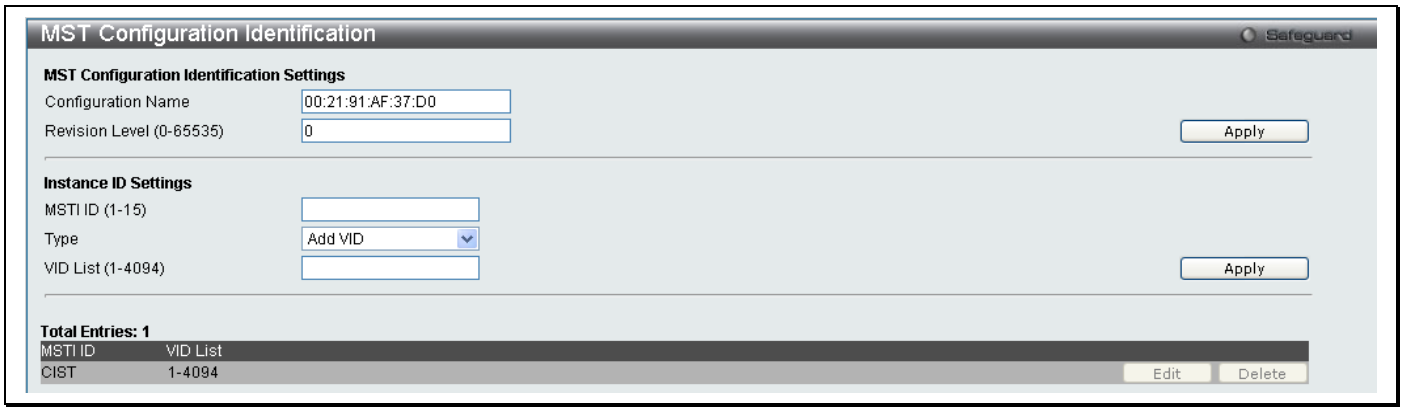


Figure 45. MST Configuration Identification menu

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the switch to uniquely identify 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. This field can be set in the **STP Bridge Global Settings** window.
Revision Level (0-65535)	This value, along with the Configuration Name will identify the MSTP region configured on the switch. The user may choose a value between *0* and *65535* with a default setting of *0*.
MSTI ID	This field shows the MSTI IDs currently set on the switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
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 (1-4094)	This field displays the VLAN IDs associated with the specific MSTI.

Click **Apply** to implement changes. Click **Edit** to modify an entry and **Delete** to remove an entry.

STP Instance Settings

This table is used to create STP Instance Settings on the switch. An STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.

To view this window, click **Switch Configuration > Spanning Tree > STP Instance Settings** as shown below:

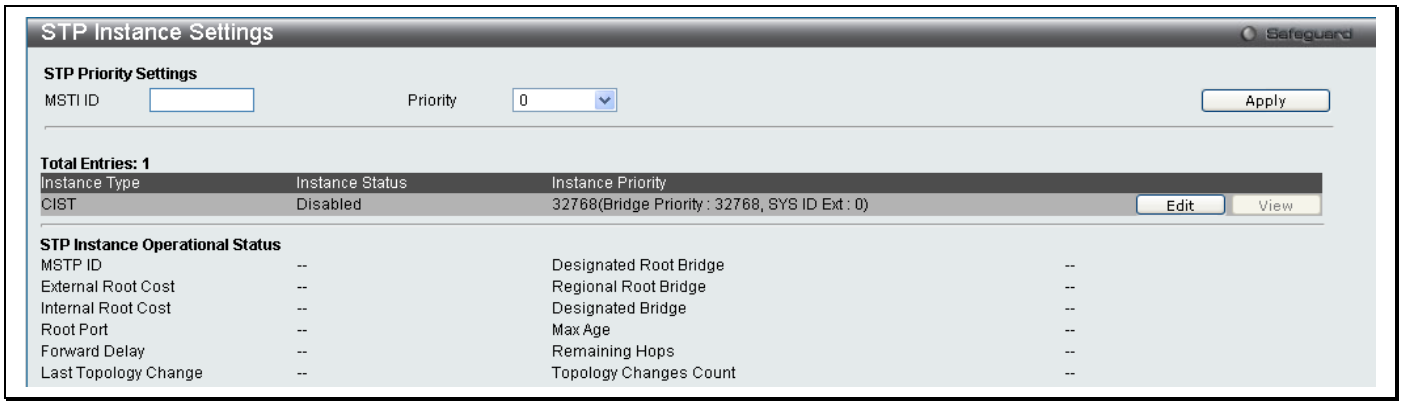


Figure 46. STP Instance Settings menu

The following information can be set:

Parameter	Description
MSTI ID	Displays the MSTI ID of the instance being modified. An entry of *0* in this field denotes the CIST (default MSTI).
Priority	Enter the new priority in the Priority field. The user may set a priority value between *0* and *61440*.

To modify an entry click the **Edit** button, to see the STP Instance Operational Status of a previously configured setting click **View**, the following window will be displayed.

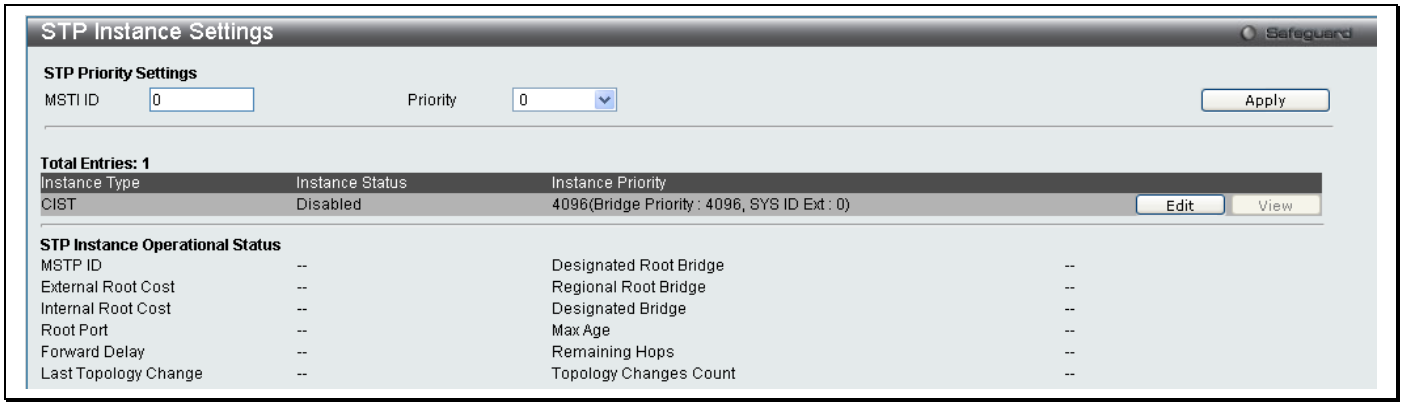


Figure 47. STP Instance Settings - View menu

MSTP Port Information

This window displays the current MSTP Port 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 this window, click **Switch Configuration > Spanning Tree > MSTP Port Information** as shown below:

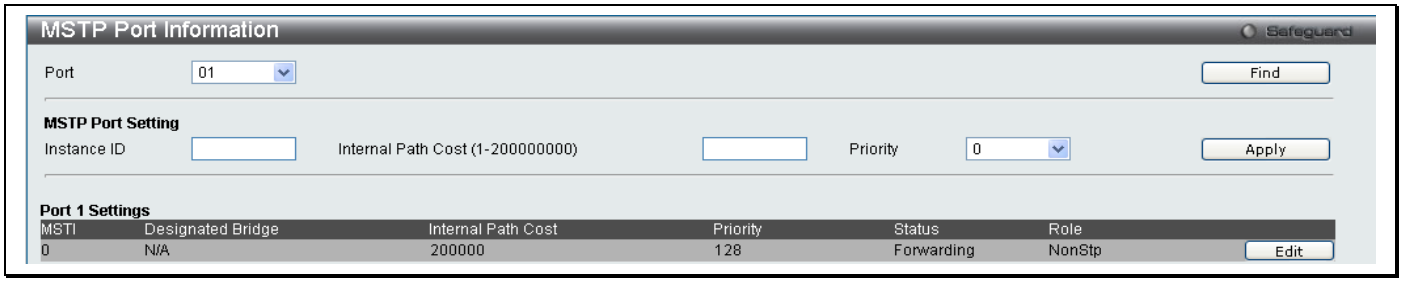


Figure 48. MSTP Port Information menu

The following parameters can be viewed or set:

Parameter	Description
Port	Use the drop-down menu to select a port.
Instance ID	Displays the MSTI ID of the instance being configured. The range is from 0 to 15. An entry of *0* in this field denotes the CIST (default MSTI).
Internal Path cost (1-200000000)	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *0* (auto). There are two options: *0 (auto)* – Selecting this parameter for the *internalCost* will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. *value 1-200000000* – 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.
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 **Apply** to implement changes made.

CFM

Connectivity Fault Management (CFM) is defined by IEEE 802.1ag, which is a standard for detecting, isolating and reporting connectivity faults in a network. CFM is an end-to-end per-service-instance Ethernet layer operation, administration, and management (OAM) function. CFM functions include path discovery, fault detection and fault verification and isolation as defined by 802.1ag.

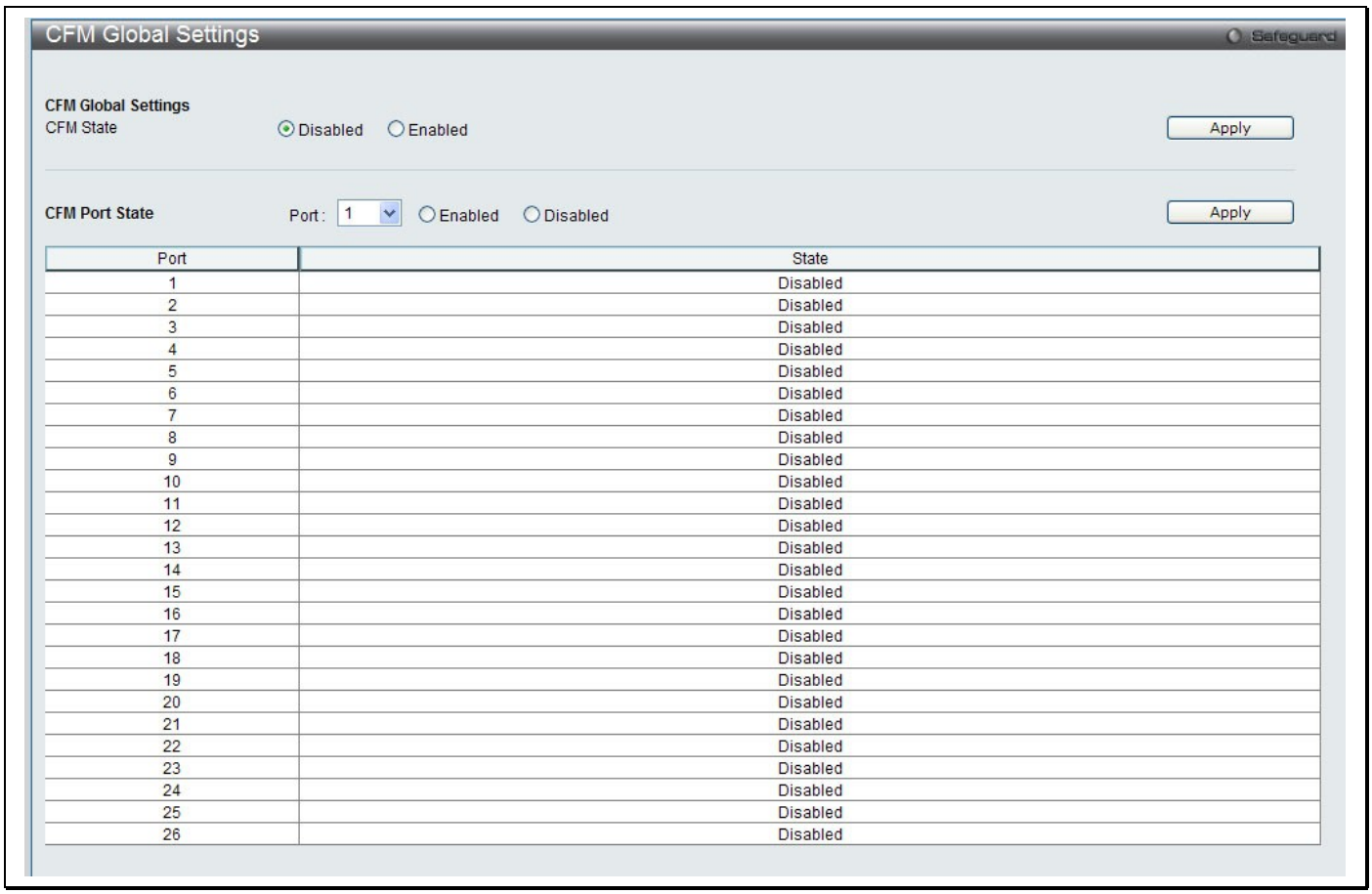
Ethernet CFM frames have a special Ether Type (0x8902). All CFM messages are confined to a maintenance domain per VLAN basis. There are different message types which are identified by unique Opcode of the CFM frame payload.

CFM message types that are supported include; Continuity Check Message (CCM), Loopback Message and Response (LBM, LBR) and Linktrace Message and Response (LTM and LTR).

CFM Global Settings

This table is used to enable or disable the connectivity fault management function on a per port basis. CFM is disabled on all ports by default.

To view this window, click **Switch Configuration > CFM > CFM Global Settings** as shown below:



Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Figure 49. CFM Global Settings menu

Enter the port list you wish to *Enable* and click **Apply**.

CFM MD Settings

This window is used to configure the CFM CCM PDU forwarding mode on the Switch. By default the CCM message is handled and forwarded by software. The software can handle the packet based on behaviour defined by the standard. Under a strict environment, there may be substantial amount of CCM packets, and it will consume a substantial amount of CPU resources. To meet the performance requirement, the handling of CCM can be changed to hardware mode.

To view this window, click **Switch Configuration > CFM > CFM MD Settings** as shown below:

Figure 50.CFM MD Settings menu

Use the drop down menu to forward by *Software* or *Hardware* and click **Apply**.

CFM MA Settings

This window is used to enable the CFM maintenance point reply Linktrace Response on the Switch.

To view this window, click **Switch Configuration > CFM > CFM MA Settings** as shown below:

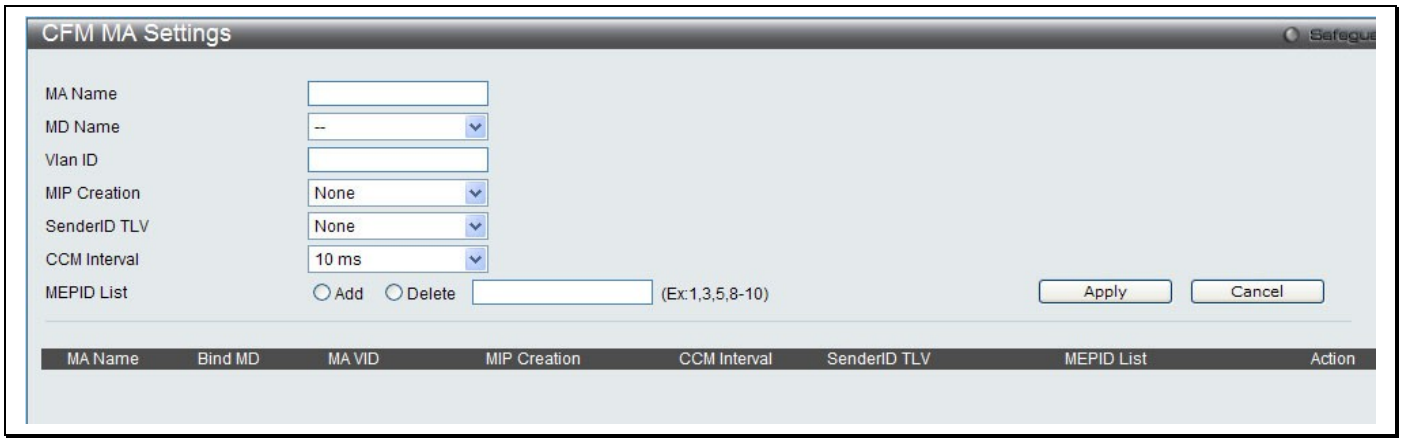


Figure 51. CFM MA Settings menu

Select *Enable* or *Disable* and click **Apply**.

CFM Mep Settings

This window is used to display the CFM, maintenance intermediate point and continuity check message on the Switch.

To view this window, click **Switch Configuration > CFM > CFM Mep Settings** as shown below:

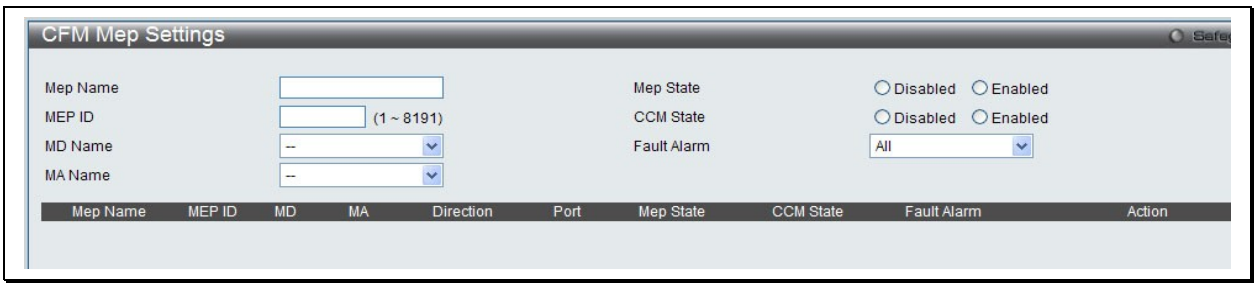


Figure 52. CFM Mep Settings menu

CFM Remote Mep

This window is used to configure the CFM settings on the Switch.

To view this window, click **Switch Configuration > CFM > CFM Remote Mep** as shown below:

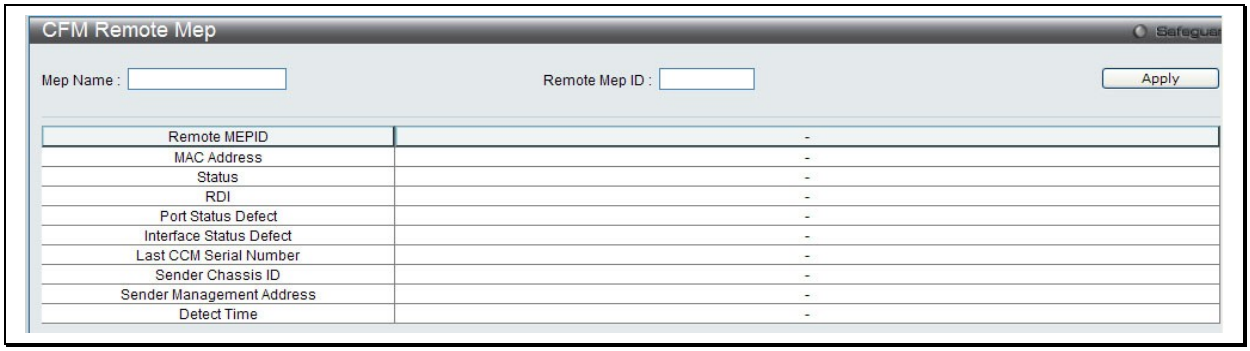


Figure 53. CFM Remote Mep menu

The following parameters can be set or are displayed:

Parameter	Description
CFM State	Used to *Enable* or *Disable* the CFM State.
Connectivity Fault Management Create(MD)	
MD	Enter the maintenance domain name you wish to create.
Level	Enter the maintenance domain level.
Connectivity Fault Management Settings(MD)	
MD	Enter the maintenance domain name you wish to configure.
MIP	This setting controls the creation of MIPs. *None* – Means that no MIPs will be created. This is the default value. *Auto* – MIPs are created when the next lower active MD-level on the port is reached or there are no lower active MD levels. *Explicit* – MIPs are created when the next lower active MD-level on the port is reached.
SenderID TLV	Used to define the TLV data types of the maintenance domain. The user can choose between *None*, *Chassis*, *Manage* or *Chassis Manage*.

To create a new entry enter the appropriate information and click **Add**. To configure the settings enter the appropriate information and click **Apply**.

CFM Loopback Settings

This window is used to configure the CFM Loopback settings on the Switch.

To view this window, click **L2 Features > CFM > CFM Loopback Settings** as shown below:

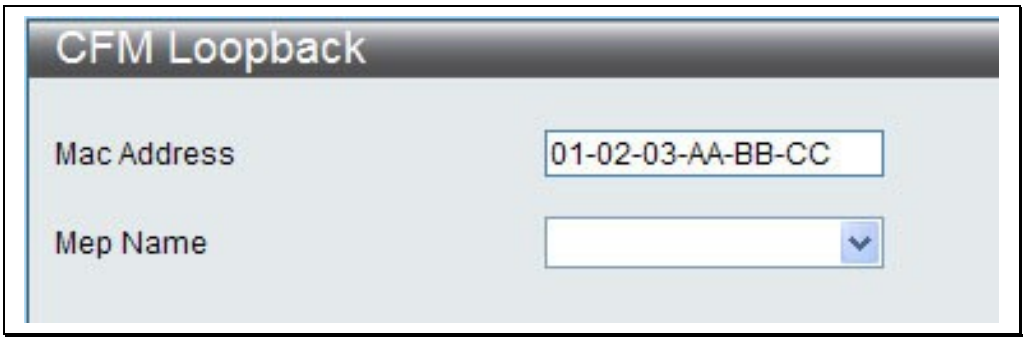


Figure 54. CFM Loopback menu

The following parameters can be configured:

Parameter	Description
MEP Name (Max:32 characters)	The name of the Maintenance End Point.
MEP ID (1-8191)	The ID for the Maintenance End Point between *1* and *8191*.
MD (Max:22 characters)	The Maintenance Domain Name.
MA (Max:22 characters)	The Maintenance Association Name.
MAC Address	The destination MAC address.
LBMs Number (1-65535)	The number of LBMs to be sent the default value is 4.
LBM Payload Length (0-1500)	The payload length of the LBM to be sent, the default value is O.
LBM Payload Pattern (Max:1500 characters)	The arbitary amount of data to be included in a Data TLV, along with the indication of 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 MEP.

Click **Apply** to implement changes made.

CFM Linktrace Settings

This window is used to configure the CFM linktrace settings on the Switch.

To view this window, click **Switch Configuration > CFM > CFM Linktrace Settings** as shown below:

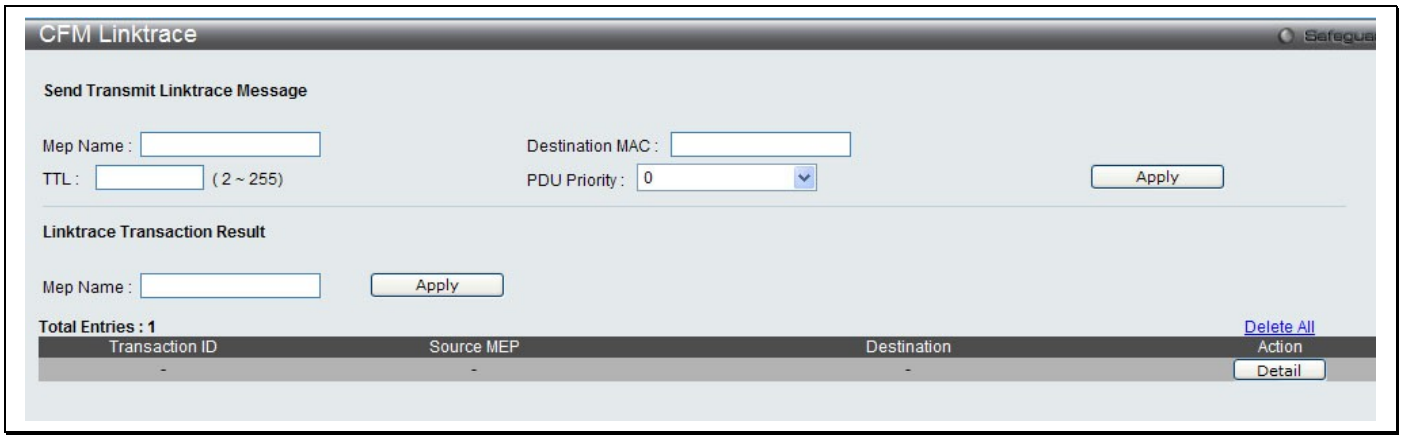


Figure 55. CFM Linktrace menu

The following parameters can be configured:

Parameter	Description
MEP Name	The name of the Maintenance End Point.
MEP ID (1-8191)	The ID for the Maintenance End Point between *1* and *8191*.
MD Name	The Maintenance Domain Name.
MA Name	The Maintenance Association Name.
MAC Address	The destination MAC address.
TTL (2-255)	The linktrace message TTL value. The default value is *64*.
PDU Priority	The 802.1p priority to be set in the transmitted LTM. If the PDU Priority is not specified, it uses the same priority as CCMs sent by the MA.

Click **Apply** to implement changes made.

Section 4

VDSL Configuration

VDSL Profiles

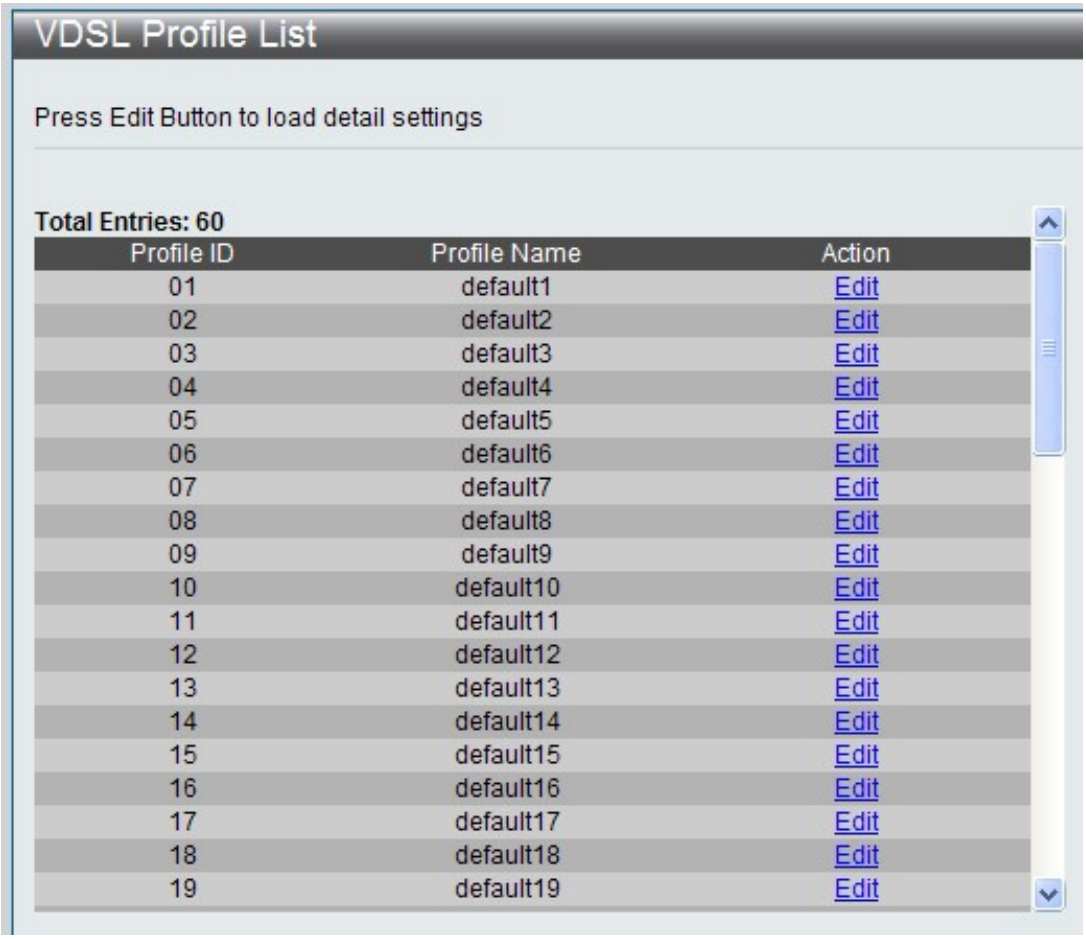
VDSL Ports

VDSL Status

The VDSL Configuration section will allow users to adjust the configuration settings for VDSL lines connected to the switch. This section has two divisions for configuration, **VDSL Profiles**, **VDSL Ports** and **VDSL Status** which are described below.

VDSL Profiles

The **VDSL Profile** window allows users to configure the settings for VDSL profiles of the switch. These profiles, once configured, may be set to individual VDSL lines on the switch, using the **VDSL Ports** window. Features such as upstream and downstream rates and power settings can be configured per profile. Click the **VDSL Profile** link to access the following window.



Profile ID	Profile Name	Action
01	default1	Edit
02	default2	Edit
03	default3	Edit
04	default4	Edit
05	default5	Edit
06	default6	Edit
07	default7	Edit
08	default8	Edit
09	default9	Edit
10	default10	Edit
11	default11	Edit
12	default12	Edit
13	default13	Edit
14	default14	Edit
15	default15	Edit
16	default16	Edit
17	default17	Edit
18	default18	Edit
19	default19	Edit

Figure 56. VDSL Profile list

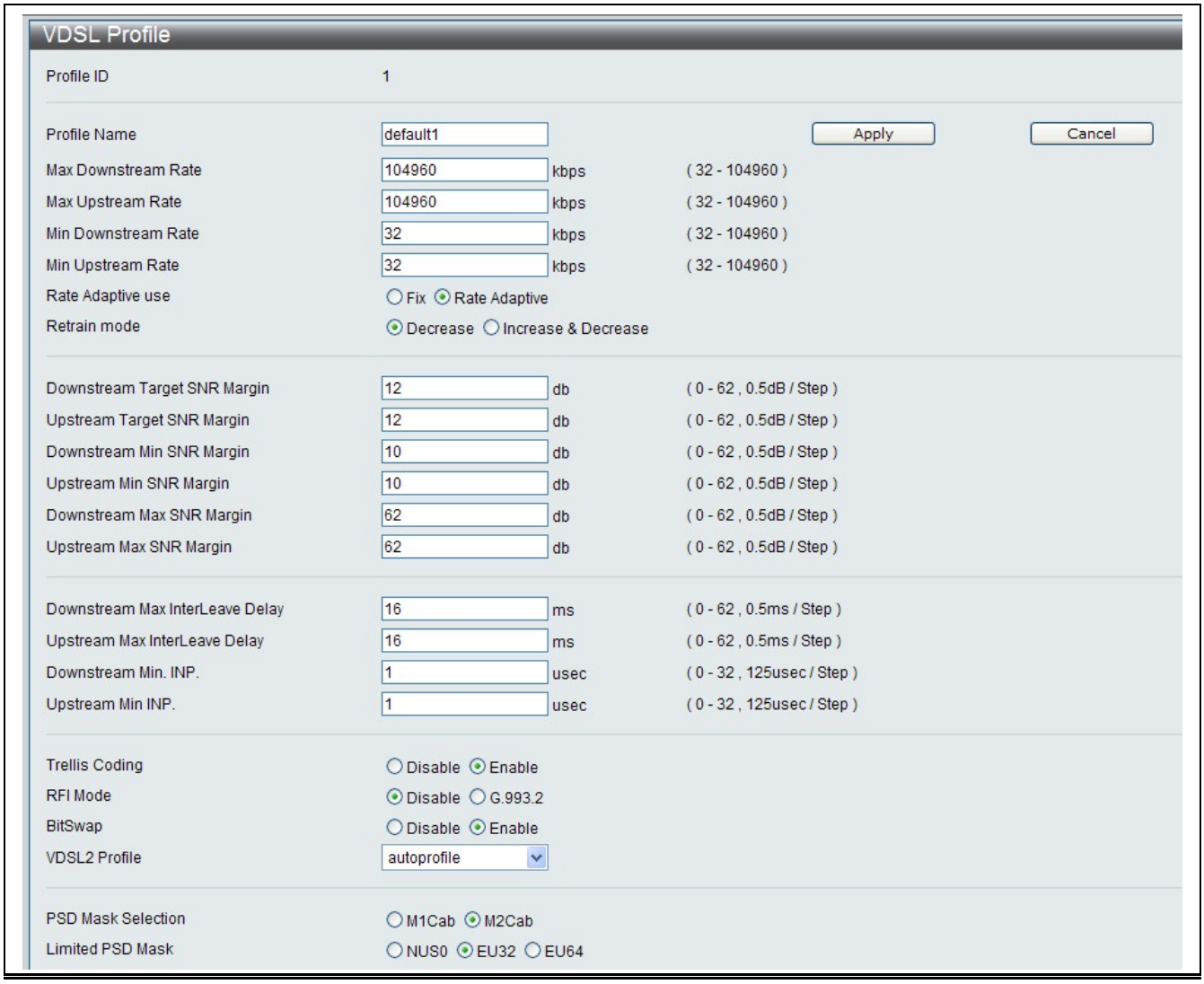


Figure 57. VDSL Profile menu – Edit

Parameter	Description
Profile Name	Enter a name to define the profile configured here. This name is used for configuration profiles applied to individual ports in the VDSL Ports menu.
Max Downstream/Upstream Rate	Enter a figure, in Kbps, that will set the maximum rate of packets of the VDSL line to which this profile will be added.
Min Downstream/Upstream Rate	Enter a figure, in Kbps, that will set the minimum rate of packets of the VDSL line to which this profile will be added.
Rate Adaptive Use	Choose if the downstream mode is **Rate Adaptive** in which the switch automatically adjusts the downstream rate depending on the line conditions such as FEXT, band plan limit or noise, or **Fixed** to statically set the transfer rate above in the Max Downstream Rate field. If a bad link is detected, the **Adaptive** setting implements a shorter loop profile to achieve a steady link. The default mode is **Adaptive** with the ability to decrease rates as needed.
Retrain Mode	*decrease*–The vdsl line will retrain if line condition is below minimum SNR. *increase-decrease*– The vdsl line will retrain if line condition is above maximum SNR or below minimum SNR.

Parameter	Description
Downstream/Upstream Target SNR Margin	Configure the target amount of increased noise that tolerated while maintaining the designed BER (bit error rate). If the SNR Margin is increased, bit error rate performance will improve, but the data rate will decrease. Conversely, if the SNR Margin is decreased, bit error rate performance will decrease, but the data rate will increase. This field is to be set for the maximum upstream rate SNR Margin and is to be set in dB. (decibals)
Downstream/Upstream Min SNR Margin	Configure the minimum amount of increased noise that can be tolerated while maintaining the designed BER (bit error rate).
Downstream/Upstream Max SNR Margin	Configure the maximum amount of increased noise that can be tolerated while maintaining the designed BER (bit error rate).
Downstream/Upstream Max InterLeave Delay	Adjust DS/US maximum interleave download delay settings (in ms) allowed Max from 0 to 62 ms.
Trellis Coding	Enable or disable Trellis coding.
RFI Mode	Enable or disable G.993.2 RFI cancellation.
BitSwap	Enable or disable BitSwap.
VDSL2 Profile	Select VDSL2 Profile ??????????
PSD Mask Selection	Environmental conditions, especially radio interference can cause significant problems in any or all bands. These masks will limit crosstalk between VDSL lines on the switch. Choosing one of these masks will filter noise from other VDSL lines on the switch.
Limited PSD Mask	
DS Reduced PSD Mode	
US Reduced PSD Mode	
Upstream/Downstream Virtual Noise State	
SRA Mode	
SOS Mode	
Robust EOC Ratte	
UPBO	Users may enable or disable the UPBo function using the corresponding radio buttons. Upstream Power Back Off (UPBO) is used to avoid lowering the performance in long loops due to strong FEXT which was generated by a short loop. The result of enabling this feature should result in higher upstream bit rates.
DPBO	
US0 Band	When the US0 Band is enabled, VDSL lines can be connected over longer distances.

Need information for descriptions, please give me reference documents if available or other D-Link manuals that have this.

Click on the **Apply** button to set these configurations in the memory of the switch.

VDSL Ports

The following window is used to attach profiles, configured in the VDSL Profiles section, with VDSL lines on the switch.

VDSL Ports

Port	Line Name	Profile	Status	Link State	Action	Detail
1	vdsl1	default1	Enabled	Training	Attach	Detail
2	vdsl2	default1	Enabled	Training	Attach	Detail
3	vdsl3	default1	Enabled	Training	Attach	Detail
4	vdsl4	default1	Enabled	Training	Attach	Detail
5	vdsl5	default1	Enabled	Training	Attach	Detail
6	vdsl6	default1	Enabled	Training	Attach	Detail
7	vdsl7	default1	Enabled	Training	Attach	Detail
8	vdsl8	default1	Enabled	Training	Attach	Detail
9	vdsl9	default1	Enabled	Training	Attach	Detail
10	vdsl10	default1	Enabled	Training	Attach	Detail
11	vdsl11	default1	Enabled	Training	Attach	Detail
12	vdsl12	default1	Enabled	Training	Attach	Detail
13	vdsl13	default1	Enabled	Training	Attach	Detail
14	vdsl14	default1	Enabled	Training	Attach	Detail
15	vdsl15	default1	Enabled	Training	Attach	Detail
16	vdsl16	default1	Enabled	Training	Attach	Detail
17	vdsl17	default1	Enabled	Training	Attach	Detail
18	vdsl18	default1	Enabled	Training	Attach	Detail
19	vdsl19	default1	Enabled	Training	Attach	Detail
20	vdsl20	default1	Enabled	Training	Attach	Detail
21	vdsl21	default1	Enabled	Training	Attach	Detail
22	vdsl22	default1	Enabled	Training	Attach	Detail
23	vdsl23	default1	Enabled	Training	Attach	Detail
24	vdsl24	default1	Enabled	Training	Attach	Detail

Figure 58. VDSL Port table

To attach a profile to a VDSL line, use the pull-down menu under the **Profile** heading, select a pre-configured profile and click the **Attach** button located under the **Action** heading. To view the settings of a VDSL Port, click the corresponding Port's **Detail** button which will produce the following read-only window.

VDSL Ports Detail

Back Clear

Port	1
Line Name	vdsl1
Link State	Training
Line TYPE	Interleaved
Band Plan	N/A
VDSL2 Profile	N/A
Line Uptime	-- days -- hours -- minutes -- seconds

	Downstream	Upstream
Line Rate	N/A Mbps	N/A Mbps
Payload Rate	N/A Mbps	N/A Mbps
Attainable Payload Rate	N/A Mbps	N/A Mbps
SNR Margin US0	N/A	N/A dB
SNR Margin DS1/US1	N/A dB	N/A dB
SNR Margin DS2/US2	N/A dB	N/A dB
SNR Margin DS3/US3	N/A dB	N/A dB
Average SNR Margin	N/A dB	N/A dB
Interleave Delay	N/A ms	N/A ms
INP (in DMT symbols)	N/A	N/A
Transmit power	N/A dBm	N/A dBm
Line Attenuation US0	N/A	N/A dB
Line Attenuation DS1/US1	N/A dB	N/A dB
Line Attenuation DS2/US2	N/A dB	N/A dB
Line Attenuation DS3/US3	N/A dB	N/A dB
Signal Attenuation US0	N/A	N/A dB
Signal Attenuation DS1/US1	N/A dB	N/A dB
Signal Attenuation DS2/US2	N/A dB	N/A dB
Signal Attenuation DS3/US3	N/A dB	N/A dB
Average Attenuation	N/A dB	N/A dB
Loop Length Estimate		N/A m
CRC error packets	N/A	N/A
Rs correctable packets	N/A	N/A
Errored Seconds	N/A	N/A
Severely Errored Seconds	N/A	N/A
Unavailable Seconds	86664	86664
LOF Detect	N/A	N/A
LOS Detect	N/A	N/A
LOL Detect	N/A	N/A
Error status report		No error
Lower VDSL Payload Rate Alarm		N/A

Layer2 switch statistcs	Outgoing	Incoming
CO Side Receive Frames	----	N/A
CO Side Drop Frames	----	N/A
CO Side FCS Error Frames	----	N/A
CO Side Transmit Frames	N/A	----

Figure 59. VDSL Port – details menu

VDSL Ports Config

The following window is used to config vdsl port status and action.

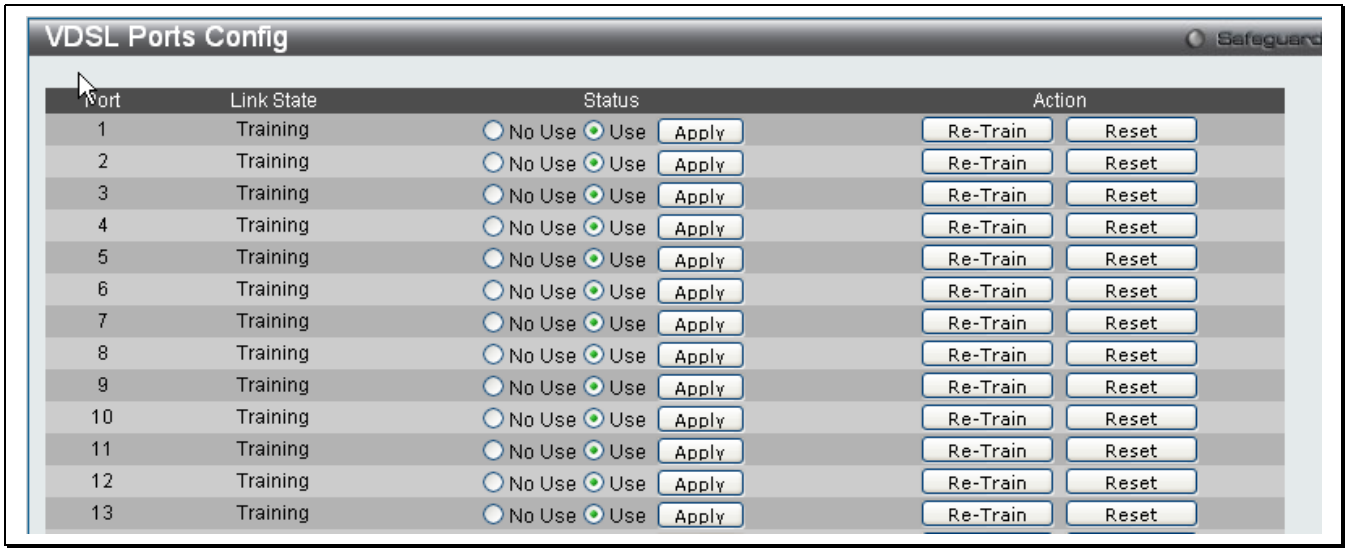


Figure 60. VDSL Ports config table

VDSL Loopback

The following window is used to run vdsl port loopback function.

Figure 61. VDSL loopback

The following parameters can be viewed or set:

Parameter	Description
Line	Specifies vdsl line to do loop back function
Choose Side	*co side* –Specifies that loop back test is internal . *eoc* –Specifies that loop back test is external via VDSL EOC channel. *cpe side*–Specifies that loop back test is external via VDSL DATA channel..
Times	How many times to run loop back test
Packet size	Specifies pcket size

Click **Apply** to implement changes made.

VDSL Status

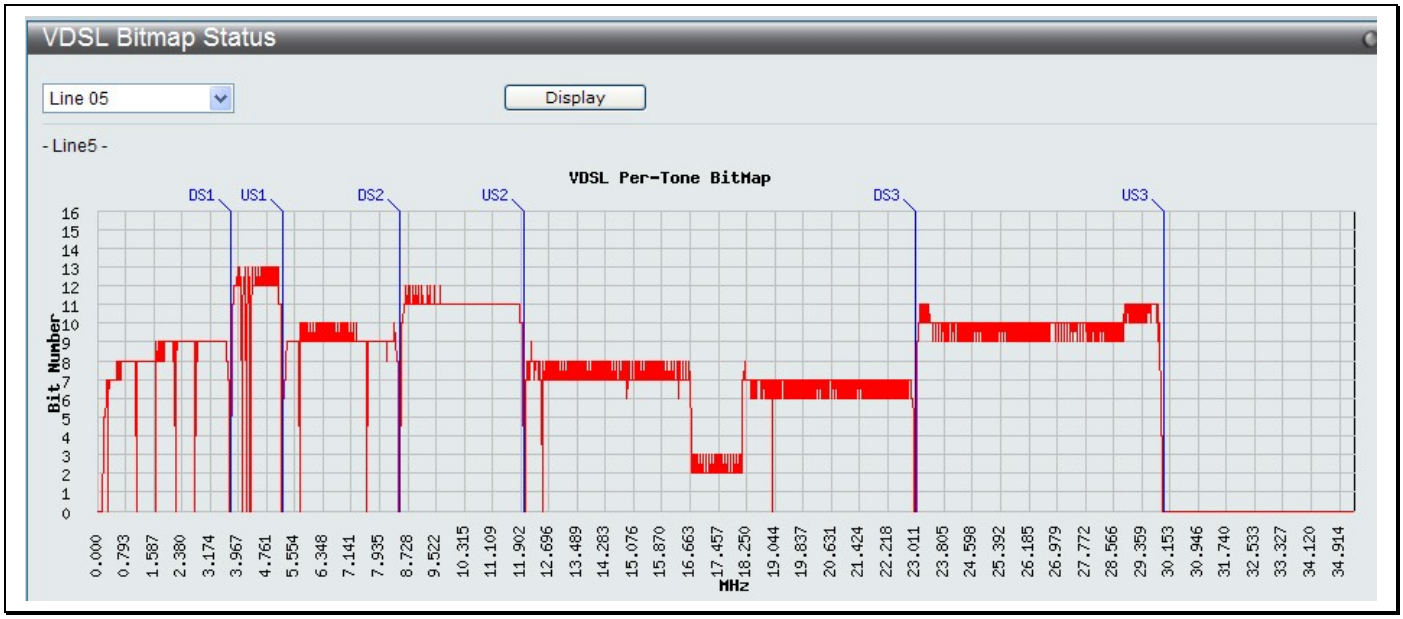


Figure 62. VDSL Bitmap Status display

Section 5

Multicasting

IGMP Snooping Settings

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.

In order to use IGMP Snooping it must first be enabled for the entire switch. You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link in the **Switch Configuration** folder. 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.

IGMP Snooping Settings

Use the **IGMP Snooping Settings** window to enable or disable IGMP Snooping on the switch. To modify the settings, click the **Edit** button under Parameter Settings and a new table will appear for the user to configure.

To view this window, click **Switch Configuration > IGMP Snooping > IGMP Snooping Settings** as shown below:

Figure 63. IGMP Snooping Settings menu

Clicking the **Edit** button will open the **IGMP Snooping Parameters Settings** window, shown below:

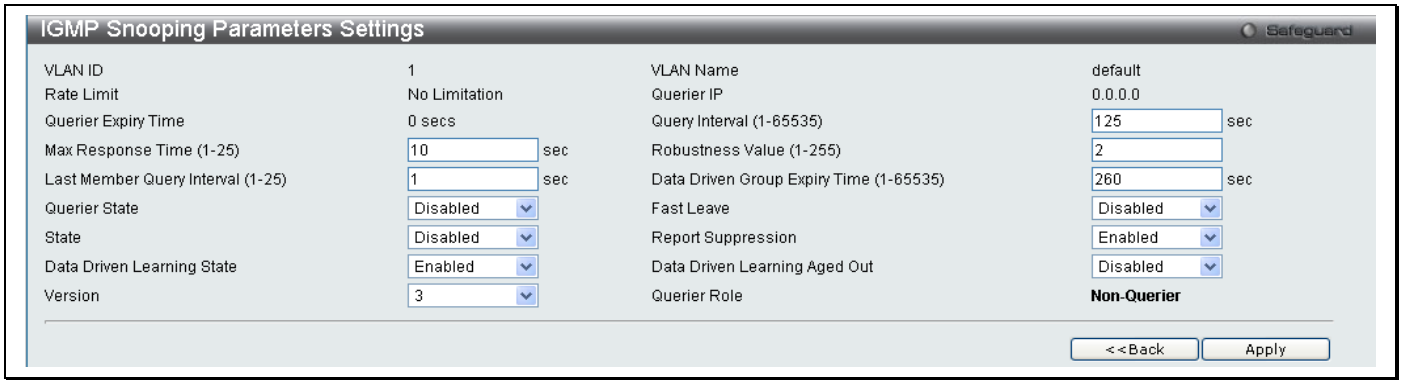


Figure 64. IGMP Snooping Parameters Settings - Edit menu

The following fields can be set:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
Rate Limit	Displays the rate limitation.
Querier IP	The querier IP address to send IGMP queries.
Querier Expiry Time	Displays the querier expiry time.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between *1* and *65535* seconds are allowed. Default = *125*.
Max Response Time (1-25)	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = *10*.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. Default = *2*.
Last Member Query Interval (1-25 Sec)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = *1*.
Querier State	Choose Enabled to enable transmitting IGMP Query packets or Disabled to disable. The default is Disabled.
Fast Leave	This parameter allows the user to enable the Fast Leave function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the switch. The default is Disabled.
State	Select Enabled to implement IGMP Snooping. This field is Disabled by default.
Report Suppression	Select Enable or Disable for IGMP Snooping report suppression for specified VLANs.
Version	Allows the user to configure the IGMP version used on the switch. The default value is *3*.
Querier Role	This read-only field describes the behavior of the router for sending query packets. Querier will denote that the router is sending out IGMP query packets. Non-Querier will denote that the router is not sending out IGMP query packets. This field will only read Querier when the Querier State and the State fields have been Enabled.

To modify the IGMP Snooping Router IP Settings click on the hyperlinked Modify Router Port which will show the following window for the user to configure:

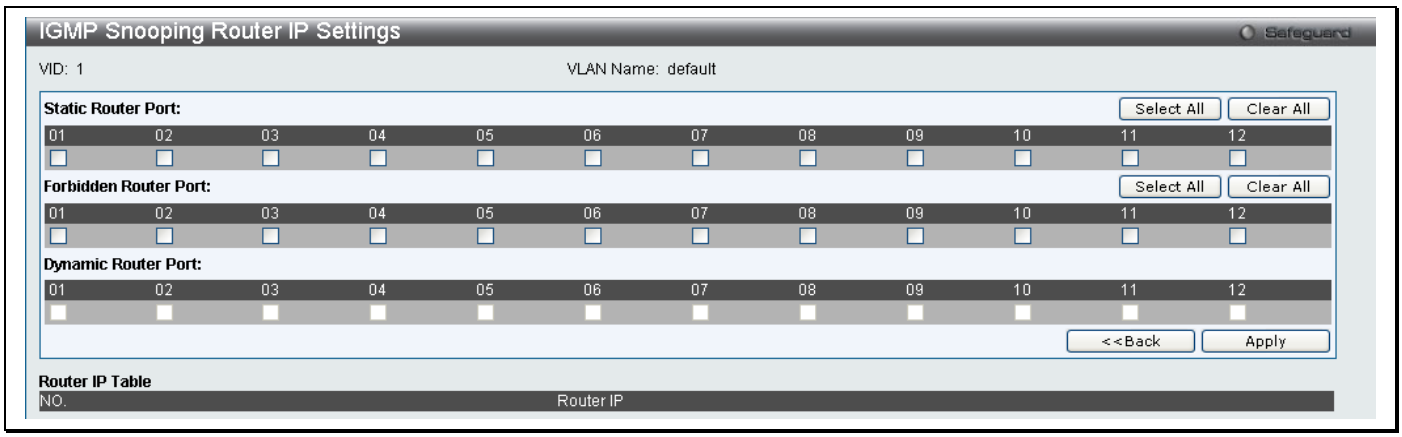


Figure 65. IGMP Snooping Router IP Settings – Edit menu

IGMP Snooping Rate Limit Settings

This table allows the user to configure the rate of IGMP snooping control packets that are allowed per port or VLAN.

To view this window, click **Switch Configuration > IGMP Snooping > IGMP Snooping Rate Limit Settings** as shown below:

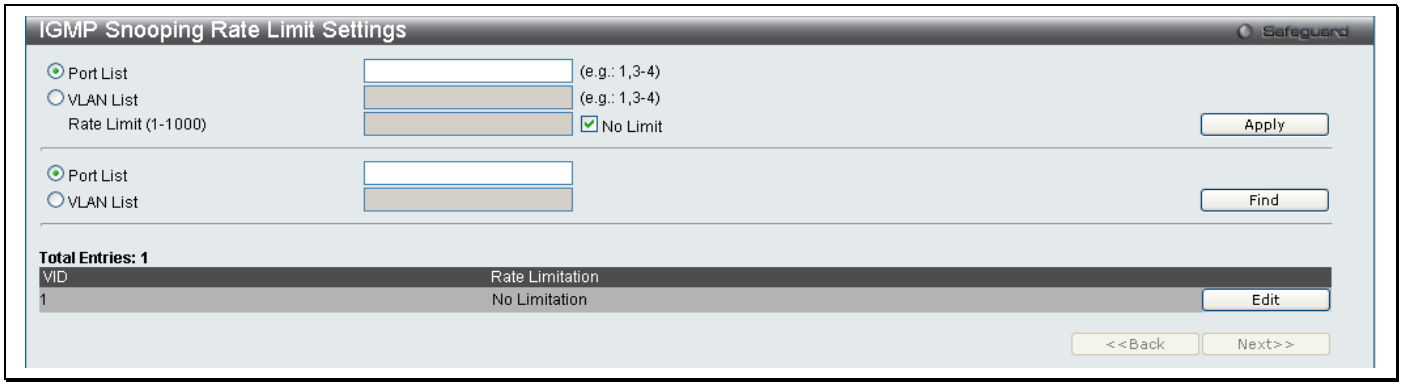


Figure 66. IGMP Snooping Rate Limit Settings menu

The following parameters can be configured:

Parameter	Description
Port List	Specifies a port or range of ports that will be configured.
VLAN List	Specifies a VLAN or range of VLANs that will be configured.
Rate Limit (1-1000)	Configures the rate of IGMP control packets that are allowed per port or VLAN.

Click **Apply** to implement changes made.

IGMP Snooping Static Group Settings

This table is used to configure the current IGMP snooping static group information on the switch.

To view this window, click **Switch Configuration > IGMP Snooping > IGMP Snooping Static Group Settings** as shown below:

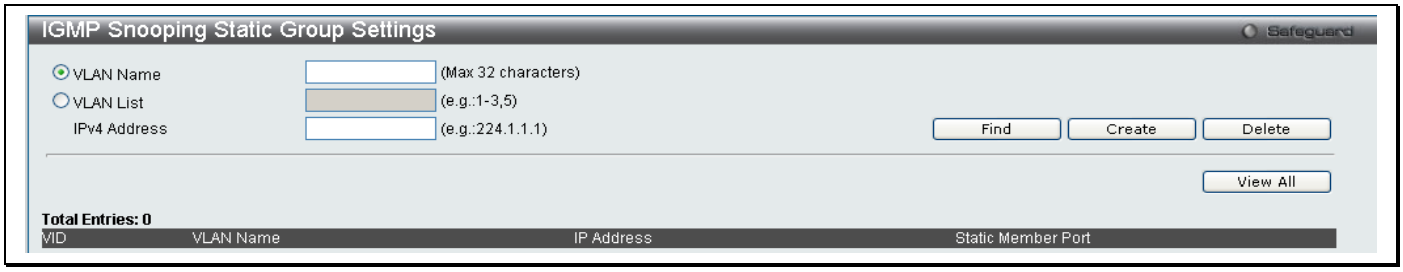


Figure 67. IGMP Snooping Static Group Settings menu

The following parameters can be configured:

Parameter	Description
VLAN Name	The name of the VLAN for which to create IGMP snooping static group information.
VLAN List	The list of the VLAN IDs for which to create IGMP snooping static group information.
IPv4 Address	The static group address for which to create IGMP snooping static group information.

Click **Apply** to implement changes made. To search for an entry enter the appropriate information and click **Find**, to remove and entry enter the appropriate information and click **Delete**.

IGMP Multicast Group Profile Settings

This table allows the user to create igmp multicast group profiles and specify multicast address lists on the switch.

To view this window, click **Switch Configuration > IGMP Snooping > IGMP Multicast Group Profile Settings** as shown below:

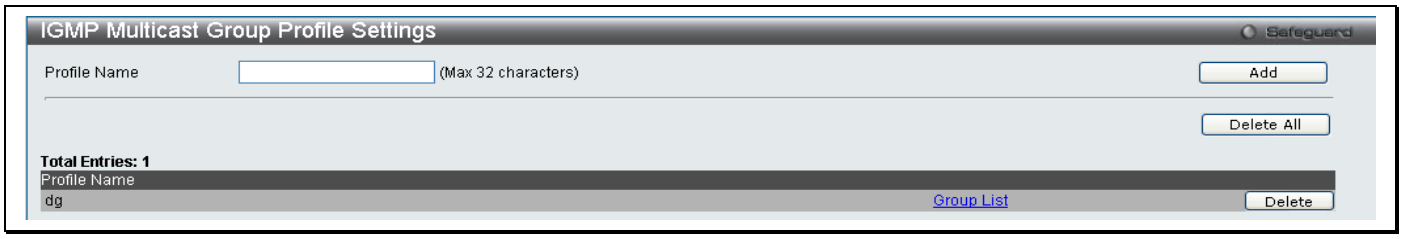


Figure 68. IGMP Multicast Group Profile Settings menu

To configure the multicast address list once a profile has been created, click on the hyperlinked Group List to reveal the following window:

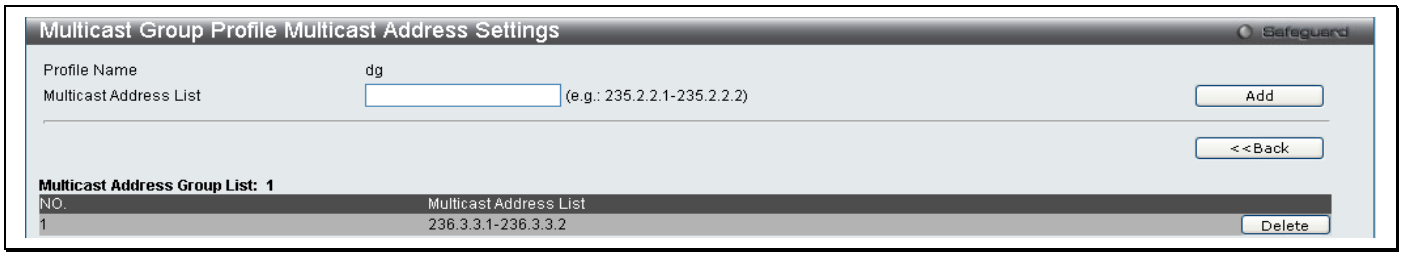


Figure 69. IGMP Multicast Group Profile Settings menu – Group List

Enter the Multicast Address List and click **Add** the new information will be displayed in the table. Click **<<Back** to return to the **IGMP Multicast Group Profile Settings** window and click **Delete** to remove an entry.

IGMP Snooping Multicast VLAN Settings

This window is used to configure the IGMP Snooping Multicast VLAN settings on the switch.

To view this window, click **Switch Configuration > IGMP Snooping > IGMP Snooping Multicast VLAN Settings** as shown below:

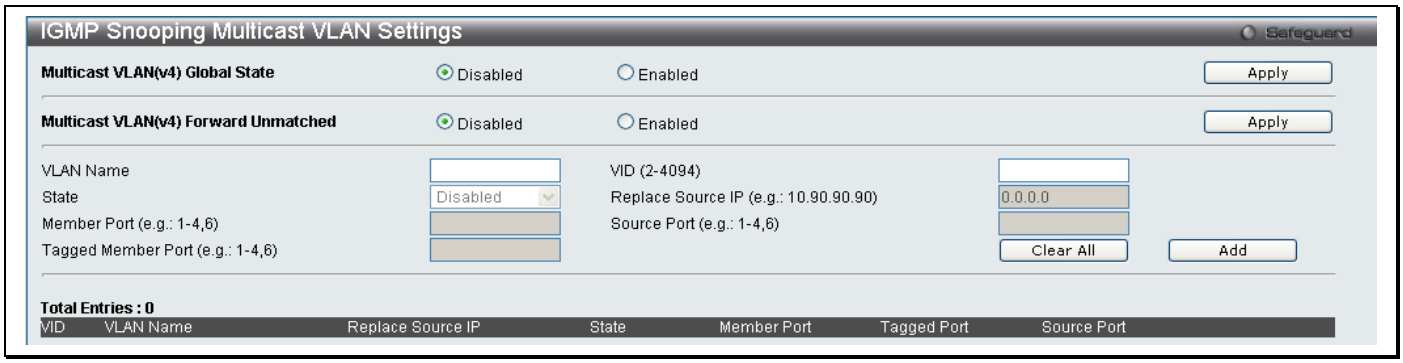


Figure 70.IGMP Snooping Multicast VLAN Settings menu

The following fields can be set

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
VID (2-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*
Replace Source IP	Enter an IP address that new IP address to be used.
Member Port (e.g.:1-4,6)	Select the ports that will be members of the Multicast VLAN. (Eg. Ports 1 to 4 and port 6)
Source Port (e.g.:1-4,6)	Select the source Port for the Multicast VLAN.
Tagged Member Port (e.g.:1-4,6)	Select the ports that will be tagged as members of the VLAN.

To modify an entry click the corresponding **Modify**, To edit and entry click the corresponding **Edit** button and to delete an entry click the corresponding **Delete** button.

IPv4 Multicast Profile Settings

The **IPv4 Multicast Profile Settings** window allows the user to add a profile to which multicast IPv4 address(es) reports are to be received on specified ports or VLANs 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 IPv4 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports or VLANs.

To view this window, click **Switch Configuration > IGMP Snooping > IPv4 Multicast Profile Settings** as shown below:

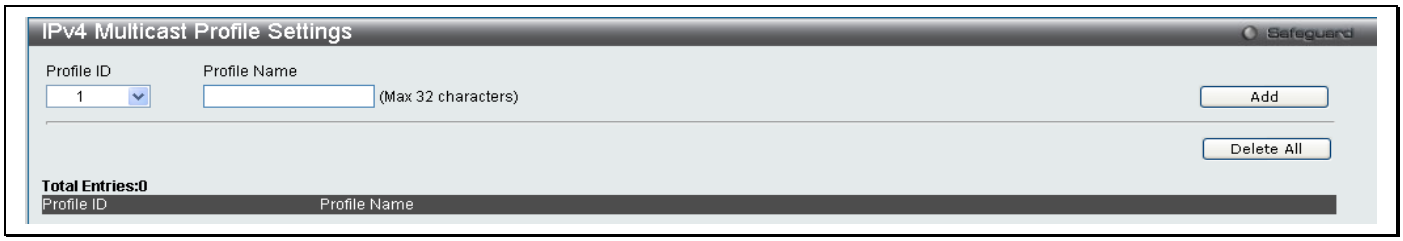


Figure 71. IPv4 Multicast Profile Settings menu

The following fields can be set

Parameter	Description
Profile ID	Use the drop-down menu to choose a Profile ID.
Profile Name	Enter a name for the IPv4 Multicast Profile.

To edit and entry click the corresponding **Edit** button and to delete an entry click the corresponding **Delete** button.

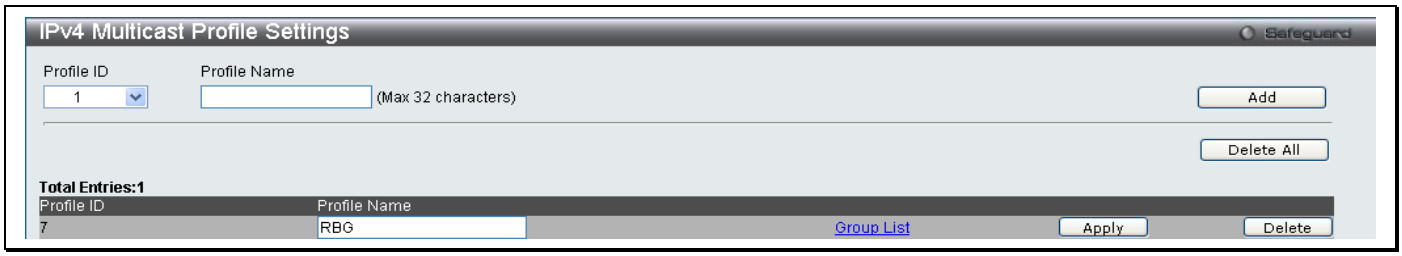


Figure 72. IPv4 Multicast Profile Settings – Edit menu

To configure the Group List Settings click the hyperlinked Group List.

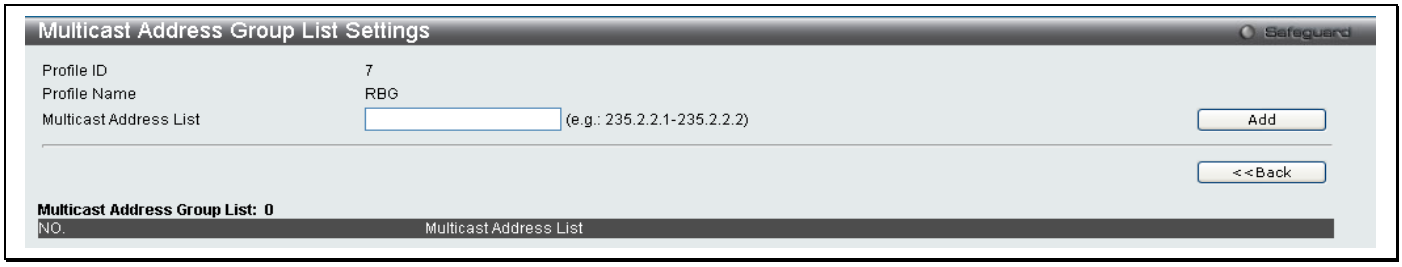


Figure 73. IP Multicast Address Group List Settings – Group List menu

Enter the multicast Address List starting with the lowest in the range, and click **Add**. To return to the IP Multicast Profile Settings window, click the **<<Back** button.

IPv4 Limited Multicast Range Settings

The **IPv4 Limited Multicast Range Settings** enables the user to configure the ports or VLANs on the switch that will be involved in the Limited IPv4 Multicast Range. The user can configure the range of IPv4 multicast addresses that will be accepted on the ports or VLANs.

To configure these settings, click **Switch Configuration > IGMP Snooping > IPv4 Limited Multicast Range Settings**.

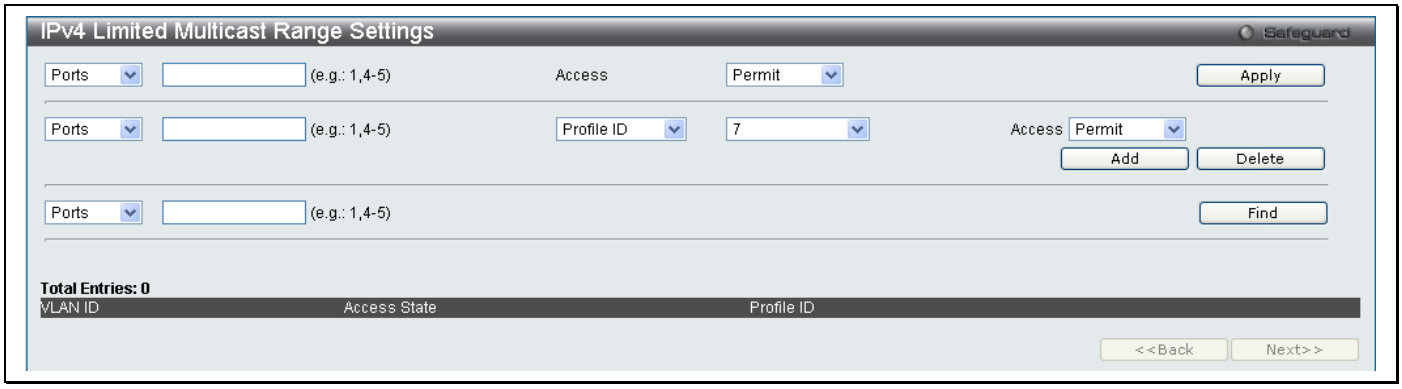


Figure 74. IPv4 Limited Multicast Range Settings menu

To add a new range enter the information and click **Add**, to delete an entry enter the information and click **Delete**.

IPv4 Max Multicast Group Settings

The **IPv4 Max Multicast Group Settings** allows users to configure the ports on the switch that will be apart of the max number of multicast groups that can be learned by data driven.

To view this window, click **Switch Configuration > IGMP Snooping > IPv4 Max Multicast Group Settings** as shown below:

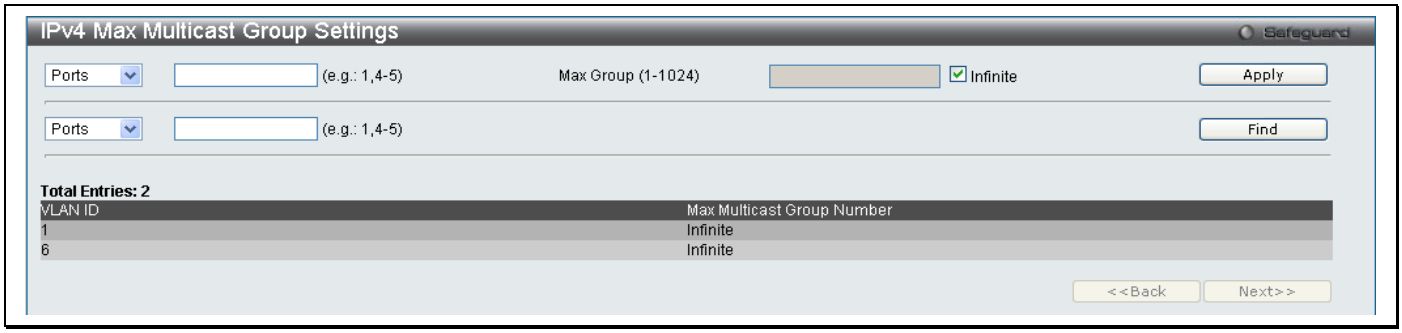


Figure 75. IPv4 Max Multicast Group Settings menu

To add a new IPv 4 Max Multicast Group, enter the information and click **Apply**, to search for an entry click **Find.**

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 a 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 three ICMPv6 packet headers, labeled 130, 131 and 132.

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 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** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening host 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 host 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 host.

MLD Snooping Settings

This table is used to enable MLD Snooping on the switch and to configure the settings for MLD snooping.

To view this window, click **Switch Configuration > MLD Snooping > MLD Snooping Settings**, as shown below:

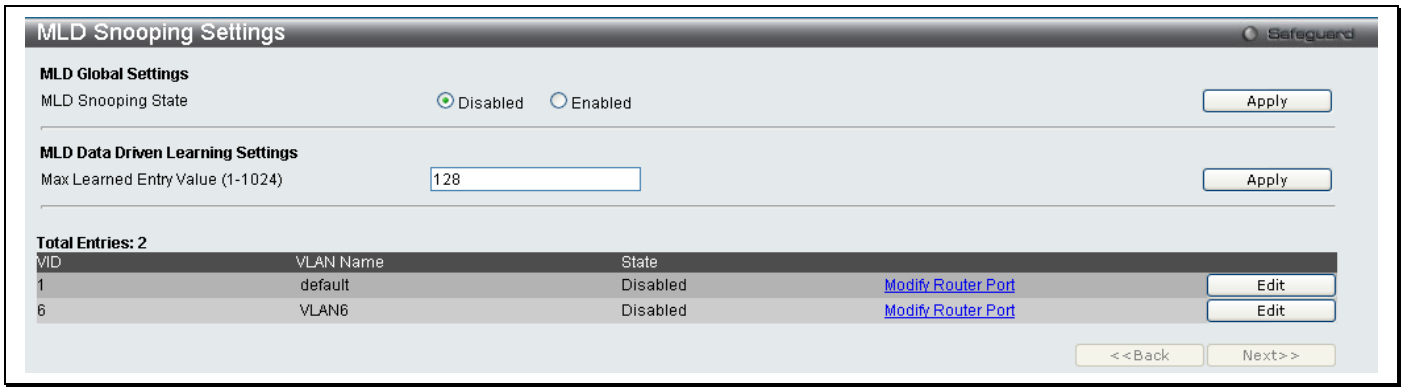


Figure 76. MLD Snooping Settings menu

To configure the settings for an existing entry click the corresponding **Edit** button which will display the following window.

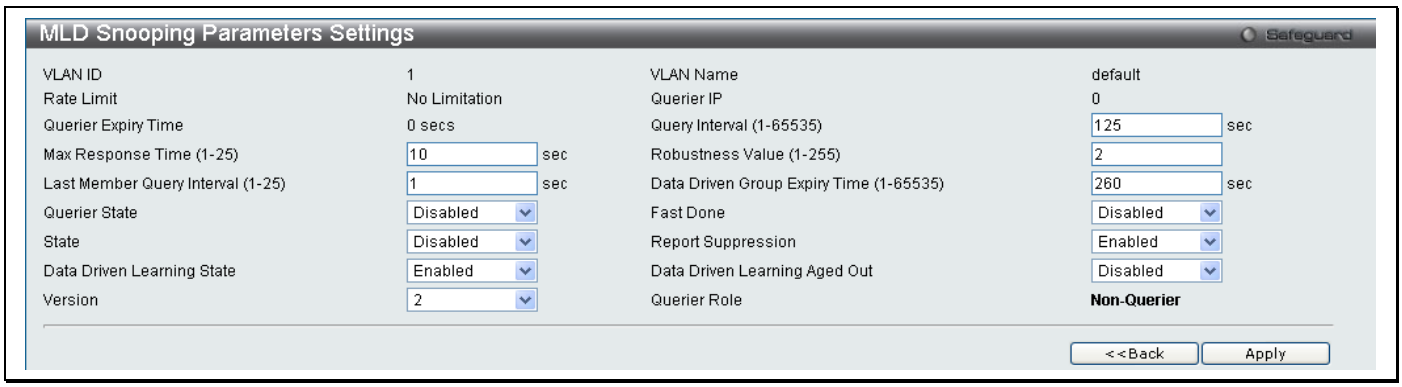


Figure 77. MLD Snooping Parameters Settings – Edit menu

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which to modify the MLD Snooping Settings.
Query Expiry Time	Displays the query expiry time in seconds.
Query Interval (1-65535 sec)	Allows the entry of a value between *1* and *65535* seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time (1-25 sec)	This determines the maximum amount of time in seconds allowed to wait for a response for MLD port listeners. The Max Response Time field allows an entry between *1* and *25* (seconds). Default = *10*.
Robustness Value (1-255)	Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval.
Last Listener Query Interval (1-25 sec)	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. A value between 1 and 25. The default is *1* second.
Data Driven Group Expiry Time (1-65535)	Specifies the data driven group expiry, in seconds. The user may specify a time between *1* and *65535* with a default setting of *260* seconds.
Querier State	The default is *Disabled*. If the field displays “Disabled”, it will always be in MLD-Snooping non-querier state.
Fast Done	Used to enable or disable the *fast done* state of the switch. This field is disabled by default.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
Report Suppression	Used to enable or disable MLD Snooping report suppression for the specified VLAN.
Data Driven Learning State	If the state is *Enabled*, it allows the switch to be selected as a MLD Querier (sends MLD query packets). It the state is *Disabled*, then the switch cannot play the role as a querier.
Data Driven Learning Aged Out	Used to *Enable* or *Disable* the aging out of MLD Snooping data driven learning for the specified VLAN.
Version	Used to configure the version of MLD used on switch. The default value is *2*.
Querier Role	This read-only field describes the current querier state of the switch, whether Querier, which will send out Multicast Listener Query Messages to links, or Non-Querier, which will not send out Multicast Listener Query Messages.

Click **Apply** to implement any changes made and **<<Back** to return to the MLD Snooping Settings window. To modify the router port settings click the hyperlinked Modify Router Port as shown below:

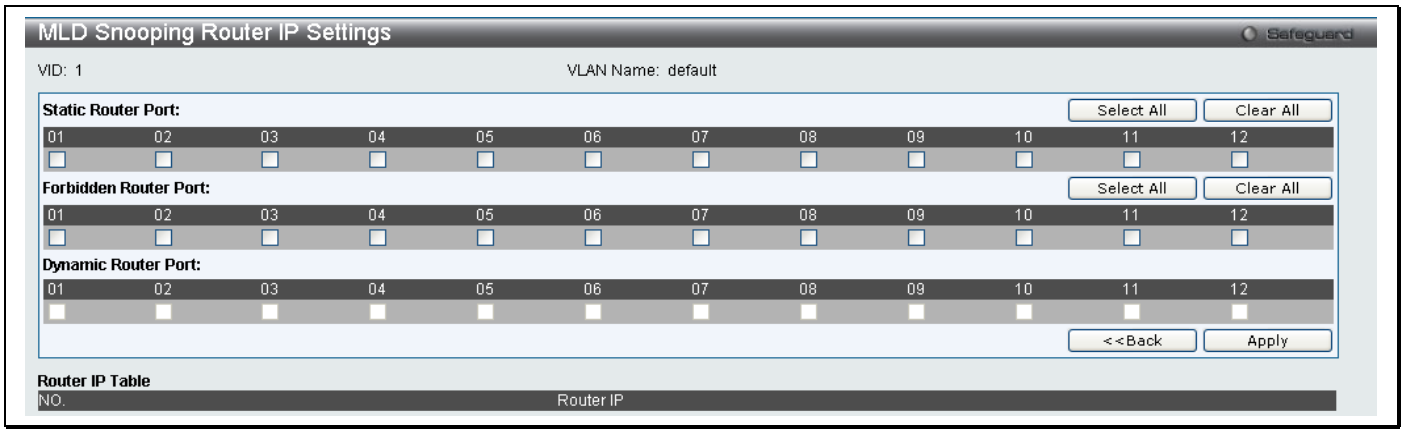


Figure 78. MLD Snooping Router IP Settings – Modify menu

MLD Snooping Rate Limit Settings

This window is used to configure the rate of MLD control packets that are allowed per port or per VLAN.

To view this window, click **Switch Configuration > MLD Snooping > MLD Snooping Rate Limit Settings**, as shown below:

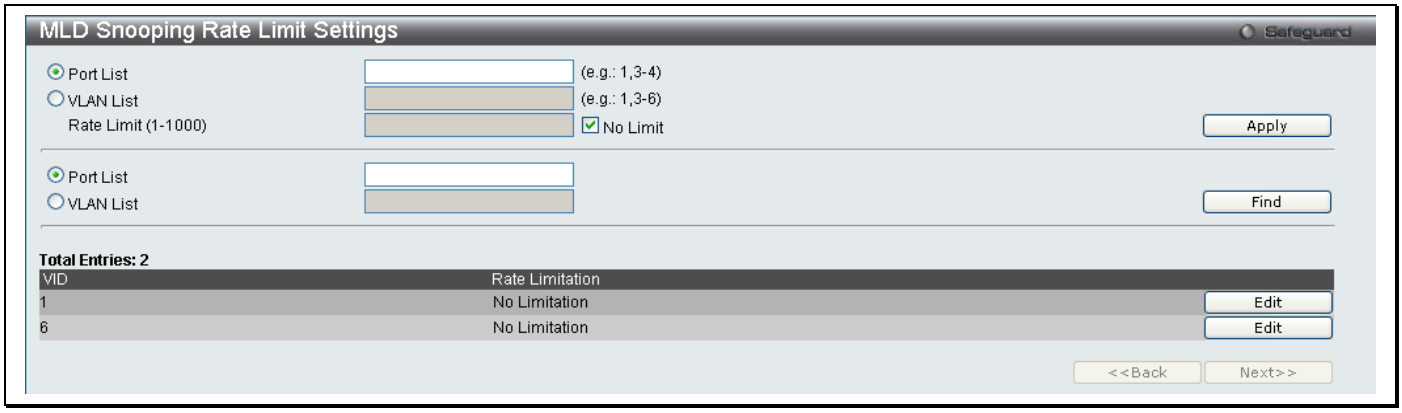


Figure 79. MLD Snooping Rate Limit Settings menu

The following parameters may be viewed or modified:

Parameter	Description
Port List	Specifies a port or range ports to configure or display.
VLAN List	Specifies a VLAN or range of VLANs to configure or display.
Rate Limit	Specifies the rate of MLD control packets that the switch can process on a specific port. The rate is specified in packets per second. The packet that exceeds the limited rate will be dropped. The default setting is No Limit.

Click **Apply** to implement new changes. To modify the rate limit click the corresponding **Edit** button.

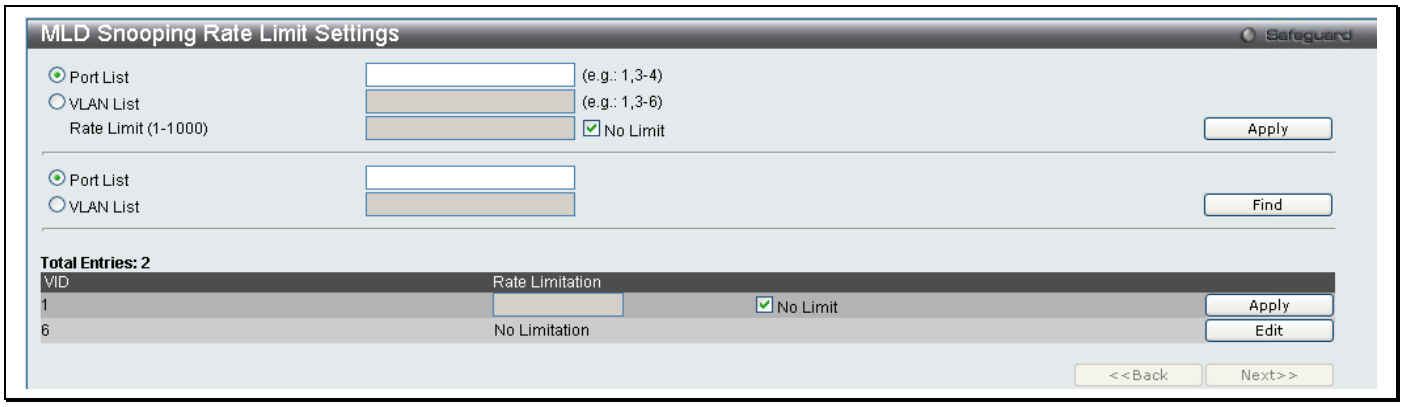


Figure 80. MLD Snooping Rate Limit Settings – Edit menu

Enter the new rate limit and click **Apply**.

MLD Snooping Static Group Settings

This window is used to configure the MLD Snooping static group information on the Swtich:

To view this window, click **Switch Configuration > MLD Snooping > MLD Snooping Static Group Settings**, as shown below

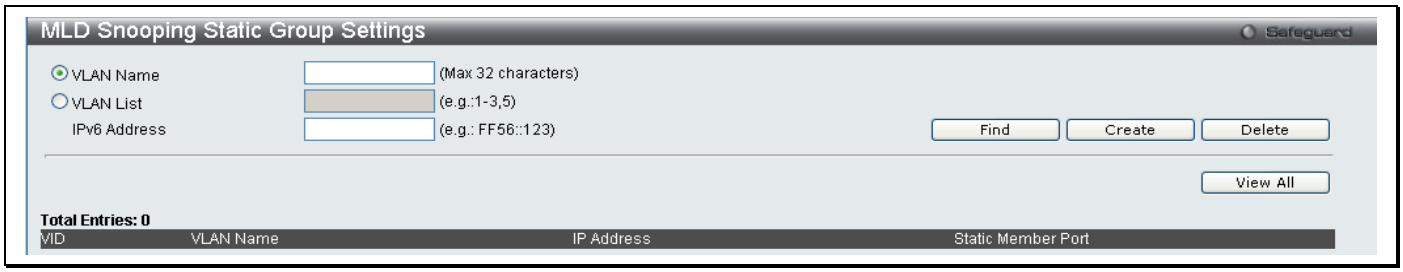


Figure 81. MLD Snooping Static Group Settings menu

The following parameters may be viewed or modified:

Parameter	Description
VLAN Name	Specifies the name of the VLAN for which to configure the MLD snooping static group information.
VLAN List	Specifies the list of the VLAN IDs for which to configure the MLD snooping static group information.
IPv6 Address	Specifies the static group IPv6 address for which to configure the MLD snooping static group information.

Click **Create** to create a new entry. To search for an entry enter the information and click **Find**. To view all previously configured entries click **View All**.

MLD Multicast Group Profile Settings

This table allows the user to create MLD multicast group profiles and specify multicast address lists on the switch.

To view this window, click **Switch Configuration > MLD Snooping > MLD Multicast Group Profile Settings** as shown below:

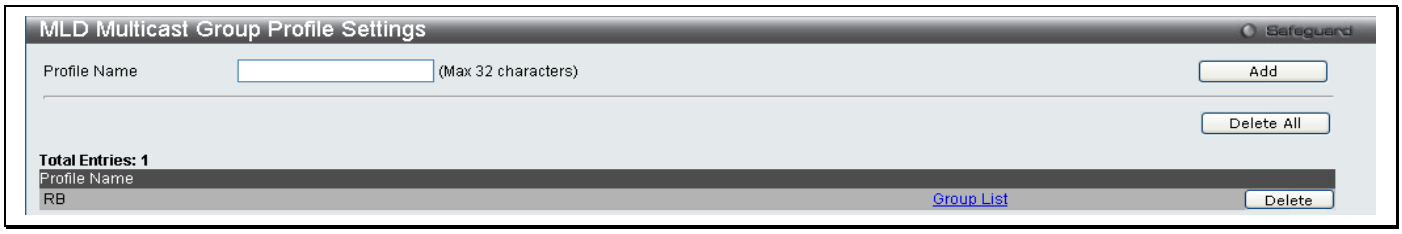


Figure 82. MLD Multicast Group Profile Settings menu

To configure the group list once a profile has been created, click on the hyperlinked Group List to reveal the following window:

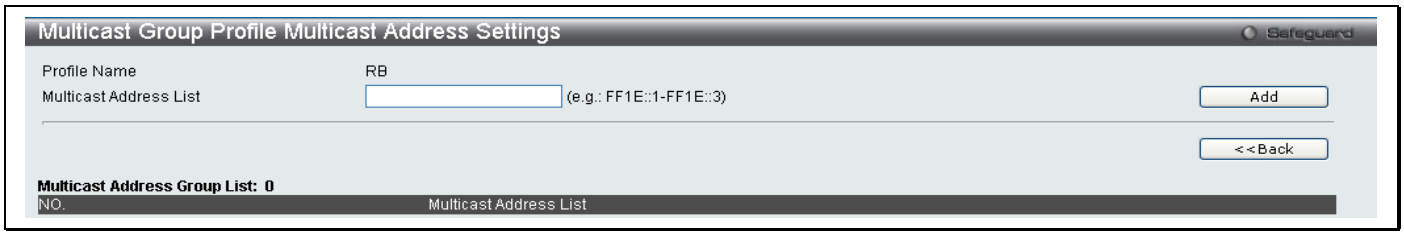


Figure 83. Multicast Group Profile Multicast Address Settings menu – Group List

Enter the Multicast Address List and click **Add** the new information will be displayed in the table. Click **<<Back** to return to the **IGMP Multicast Group Profile Settings** window and click **Delete** to remove an entry.

MLD Snooping Multicast VLAN Settings

This window is used to configure the MLD Snooping Multicast VLAN settings on the switch.

To view this window, click **Switch Configuration > MLD Snooping > MLD Snooping Multicast VLAN Settings** as shown below:

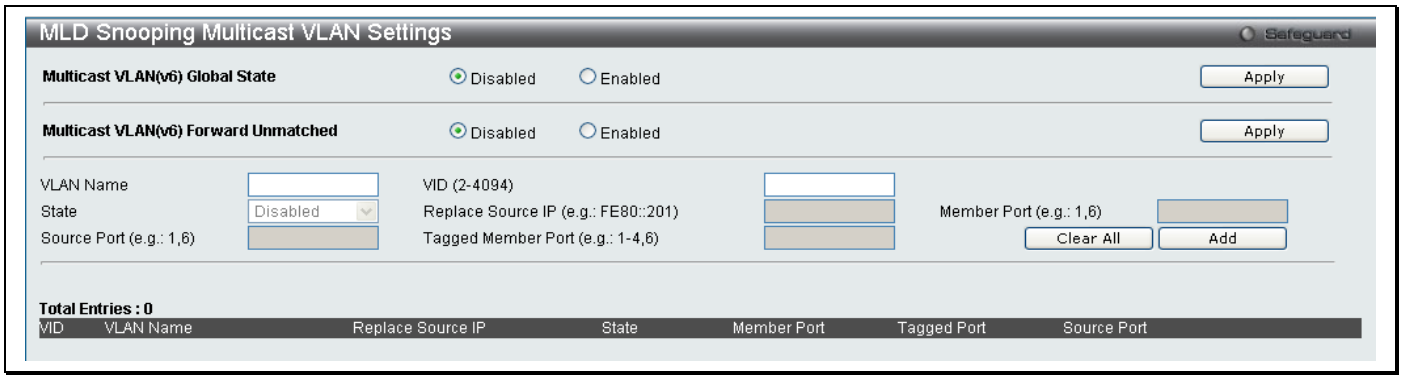


Figure 84. MLD Snooping Multicast VLAN Settings menu

The following fields can be set:

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the MLD Snooping Settings for.
VID (2-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the MLD Snooping Settings for.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*
Replace Source IP	Enter an IP address that new IP address to be used.
Member Port (e.g.:1,6)	Select the ports that will be members of the Multicast VLAN. (Eg. Ports 1 to 4 and port 6)
Source Port (e.g.:1,6)	Select the source Port for the Multicast VLAN.
Tagged Member Port (e.g.:1-4,6)	Select the ports that will be tagged as members of the VLAN.

To modify an entry click the corresponding **Modify** button. To remove an entry click the corresponding **Delete** button.

Multicast Forwarding

The following figure and table describe how to set up **Multicast Forwarding** on the switch.

To view this window, click **Switch Configuration > Forwarding & Filtering > Multicast Forwarding** as shown below:

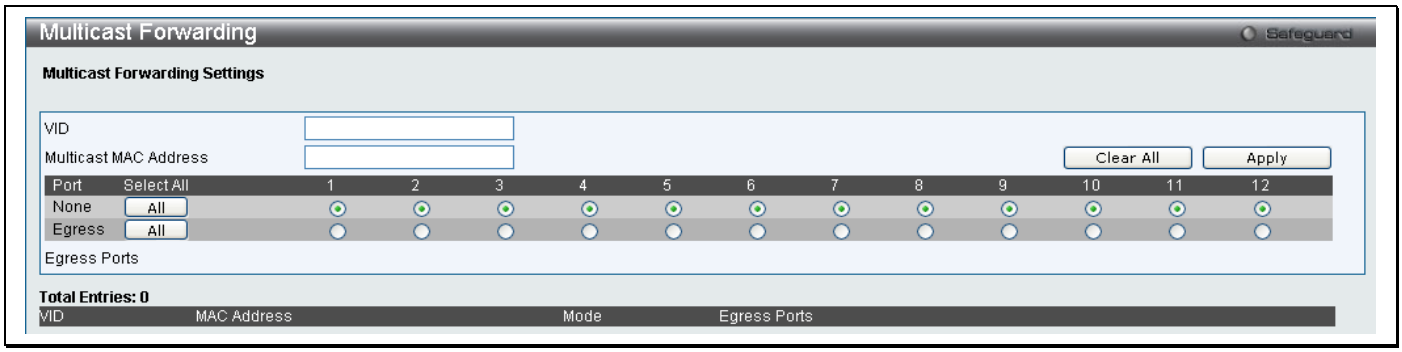


Figure 85. Multicast Forwarding menu

The following parameters can be set:

Parameter	Description
VID	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	Allows the selection of ports that will be members of the static multicast group and ports either that are 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. *Egress* – The port is a static member of the multicast group.

Click **Apply** to implement the changes made. To delete an entry in the Static Multicast Forwarding Table, click the corresponding **Delete** button. All the entries will be shown on the lower half of the **Multicast Forwarding Table** window.

Multicast Filtering Mode

This table is used to configure the Multicast Filtering settings on the switch. It allows users to configure the switch to forward or filter the Unregistered Groups per VLAN.

To view this window, click **Switch Configuration > Forwarding & Filtering > Multicast Filtering Mode** as shown below:

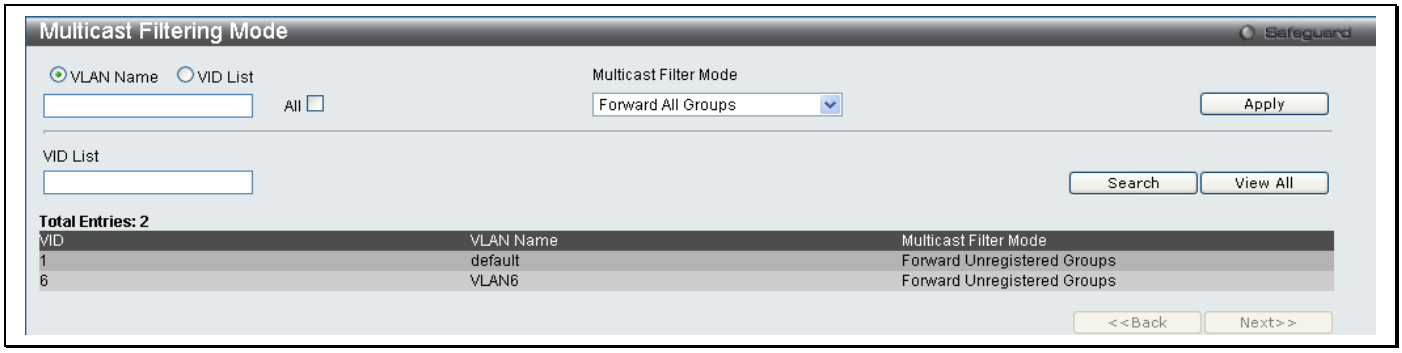


Figure 86. Multicast Filtering Mode menu

Section 6

Storm Control

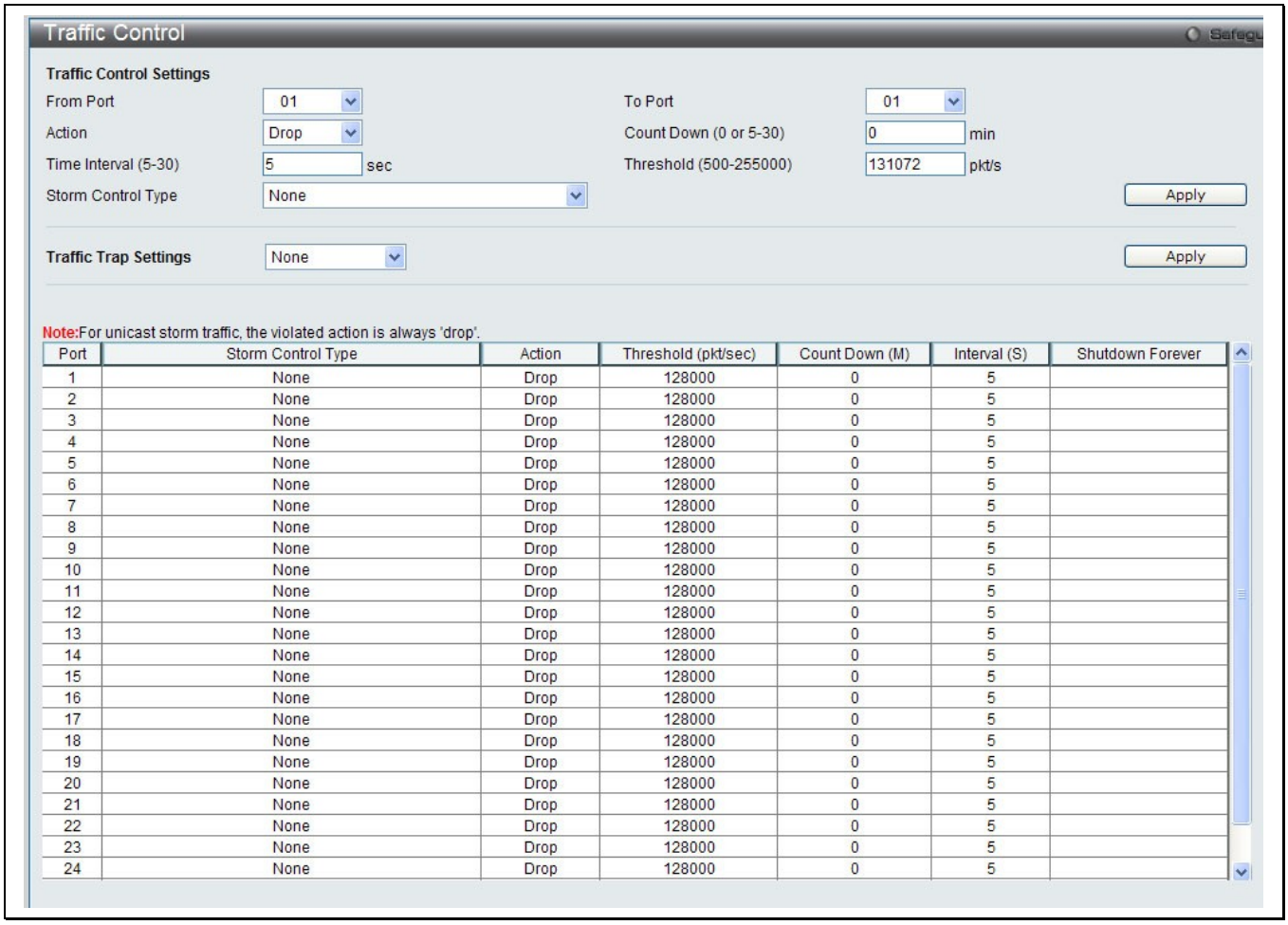
On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems 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.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level 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 field in the window below.

Traffic Control

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 shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field. If the packet storm discontinues before the Countdown timer expires, the port will again allow all incoming traffic. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recover it using the **Port Configuration** window in the **Configuration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the Shutdown option of the Action field in the window below.

To view this window click **Storm Control > Traffic Control** as shown below:



Port	Storm Control Type	Action	Threshold (pkt/sec)	Count Down (M)	Interval (S)	Shutdown Forever
1	None	Drop	128000	0	5	
2	None	Drop	128000	0	5	
3	None	Drop	128000	0	5	
4	None	Drop	128000	0	5	
5	None	Drop	128000	0	5	
6	None	Drop	128000	0	5	
7	None	Drop	128000	0	5	
8	None	Drop	128000	0	5	
9	None	Drop	128000	0	5	
10	None	Drop	128000	0	5	
11	None	Drop	128000	0	5	
12	None	Drop	128000	0	5	
13	None	Drop	128000	0	5	
14	None	Drop	128000	0	5	
15	None	Drop	128000	0	5	
16	None	Drop	128000	0	5	
17	None	Drop	128000	0	5	
18	None	Drop	128000	0	5	
19	None	Drop	128000	0	5	
20	None	Drop	128000	0	5	
21	None	Drop	128000	0	5	
22	None	Drop	128000	0	5	
23	None	Drop	128000	0	5	
24	None	Drop	128000	0	5	

Figure 87. Traffic Control menu

The following parameters can be configured:

Traffic Control Settings	
From Port / To Port	A consecutive group of ports may be configured starting with the selected port.
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 Countdown 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 user manually resets the port using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Time Interval (5-30)	The 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 Interval may be set between *5* and *30* seconds with the 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* to *255000* with a default setting of *131072*.
Storm Control Type	Select the type of Storm Type to detect, either Broadcast Multicast or Unicast. Once selected, use the pull-down menu to enable or disable this storm detection.
Traffic Trap Setting	
Traffice 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 not send any 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 in the Action field.

Click **Apply** to implement the settings made.

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.

Section 7

QoS

HOL Blocking Pevention

Bandwidth Control

Traffic Control

802.1p Default Priority

802.1p User Priority

QoS Scheduling Mechanism

QoS Scheduling

In Band Manage Settings

SRED

The following section discusses the implementation of 802.1p priority queuing as it is supported on the switch.

Advantages of QoS

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.

Understanding QoS

The Switch has eight priority queues. These priority queues are labeled from 0-7, with 7 being the highest priority and 0 the lowest priority queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags 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 queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues 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 8 CoS queues, A~H, with their respective weight value: 8~1. When each queue has 10 outbound packets, they 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,

A9, B8, C7, D6, E5, F4, G3, H2,

A10, B9, C8, D7, E6, F5, G4

B10, C9, D8, E7, F6,

C10, D9, E8,

D10,

E9, F7, G5, H3,

E10, F8, G6,

F9,

F10, G7, H4,

G8,

G9, H5,

G10, H6 ~ H10

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 DAS-3626 has eight priority queues (and eight Classes of Service) for each port on the switch.

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

To view this window, click **QoS > Bandwidth Control** as shown below:

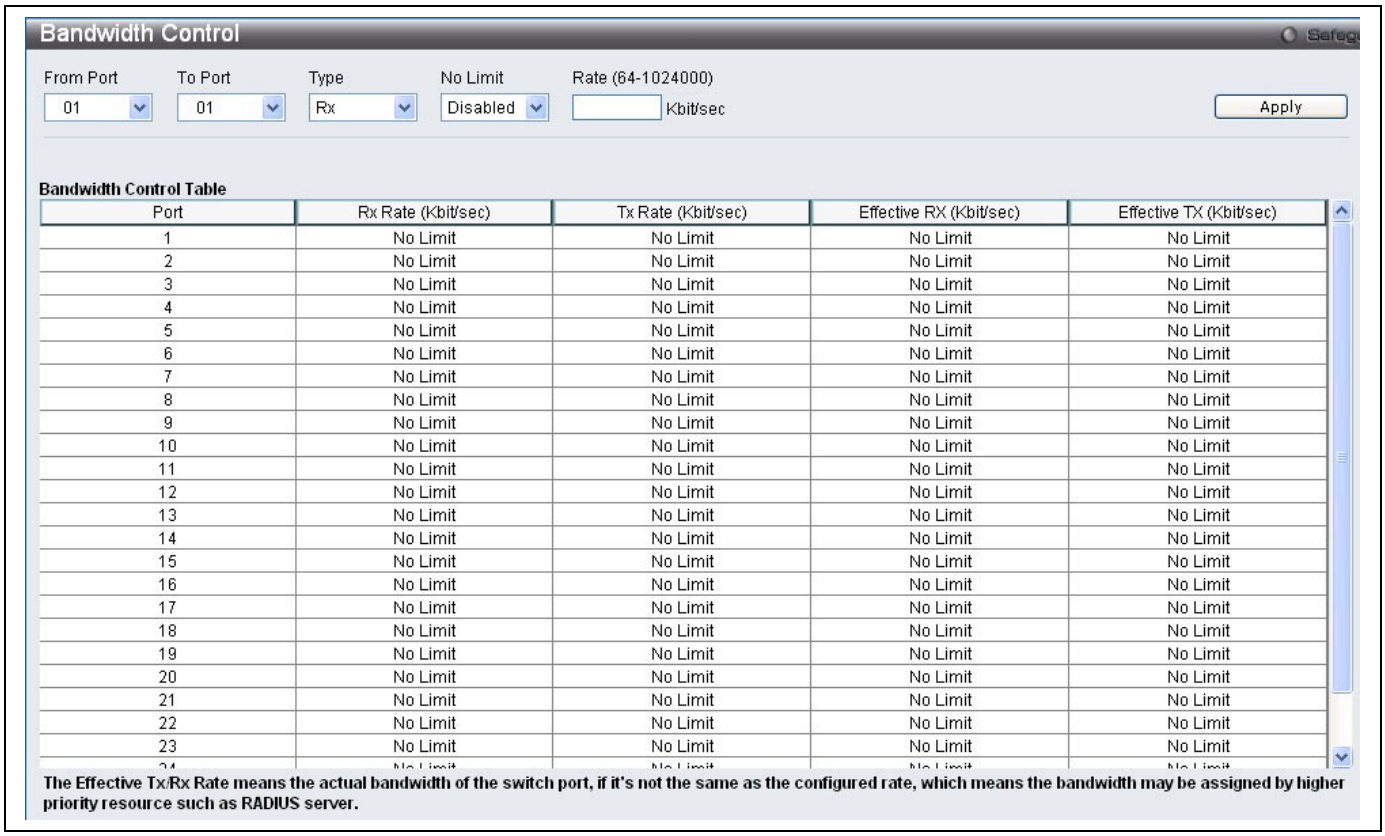


Figure 88. Bandwidth Control menu

The following parameters can be set or are displayed:

Parameter	Description
From port / To port	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select 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 you to select *Enabled* or *Disabled* to specify whether the selected port have unlimited bandwidth.
Rate (64-1024000)	This field allows you to enter the data rate, in Kbits per second, that will be the limit for the selected port. The value must be a multiple of 64, between 64 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured Bandwidth Settings will be displayed in the **Bandwidth Control Table** on the lower half of the window.

802.1p Default Priority

The switch allows the assignment of a default 802.1p priority to each port on the switch.

To view this window, click **QoS > 802.1p Default Priority** as shown below:

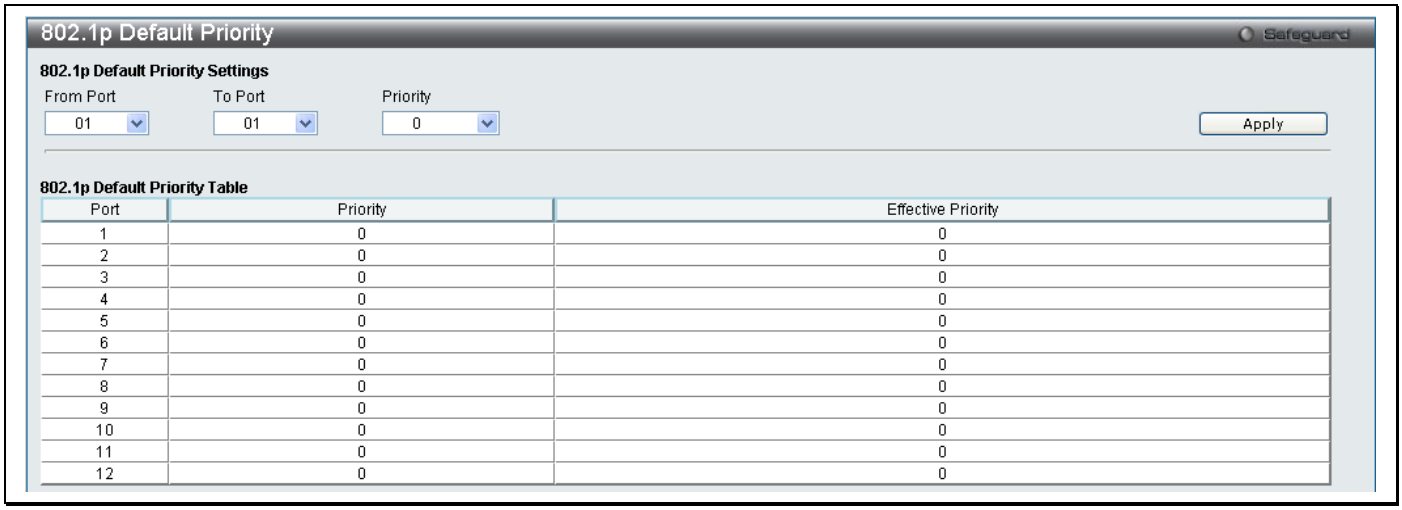


Figure 89. 802.1p Default Priority menu

This window allows you to assign a default 802.1p priority to any given port on the switch. The priority queues are numbered from 0, the lowest priority, to 7, the highest priority. Click **Apply** to implement your settings.

802.1p User Priority

The switch allows the assignment of a user priority to each of the 802.1p priorities.

To view this window, click **QoS > 802.1p User Priority** as shown below:

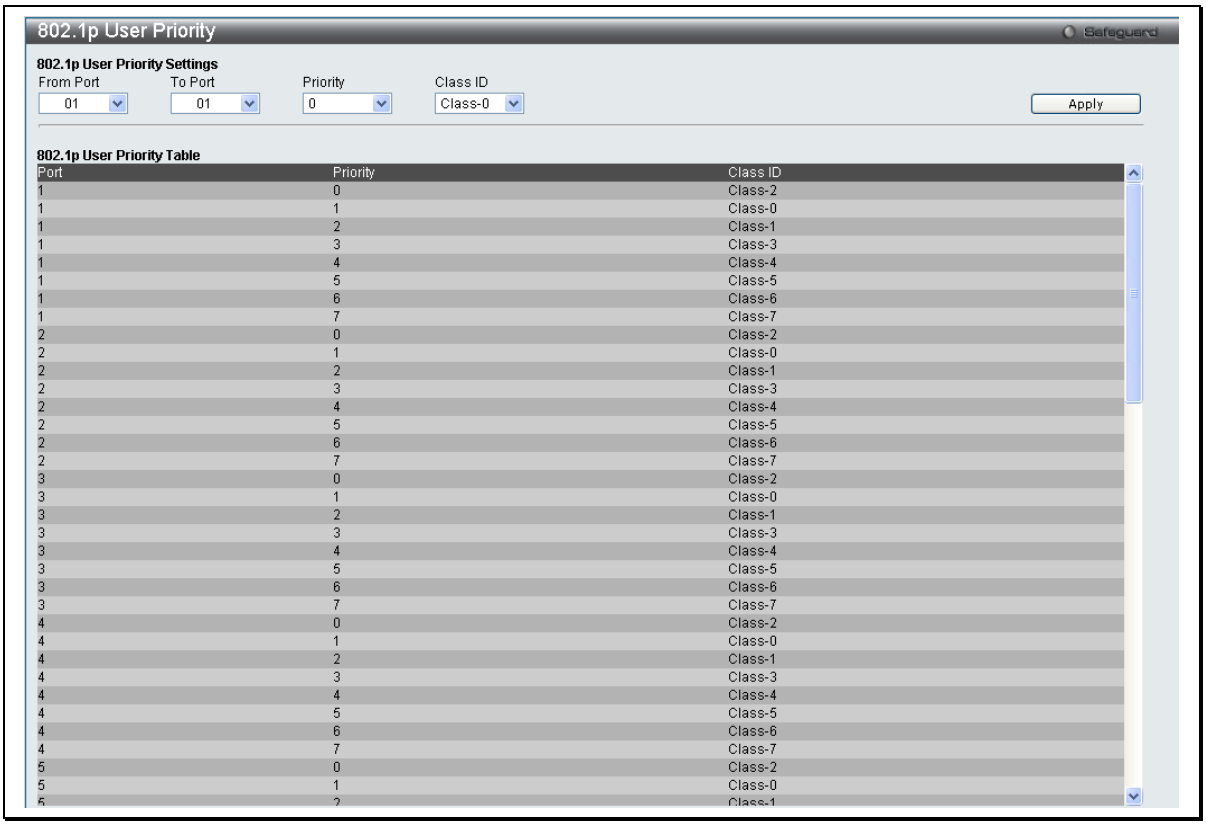


Figure 90. 802.1p User Priority menu

Once you have assigned a priority to the port groups on the switch, you can then assign this Class to each of the 7 levels of 802.1p priorities. Click **Apply** to set your changes.

QoS Scheduling Mechanism

Changing the output scheduling used for the hardware queues in the switch can customize QoS. As with any changes to 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 monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view this window, click **QoS > QoS Scheduling Mechanism** as shown below:

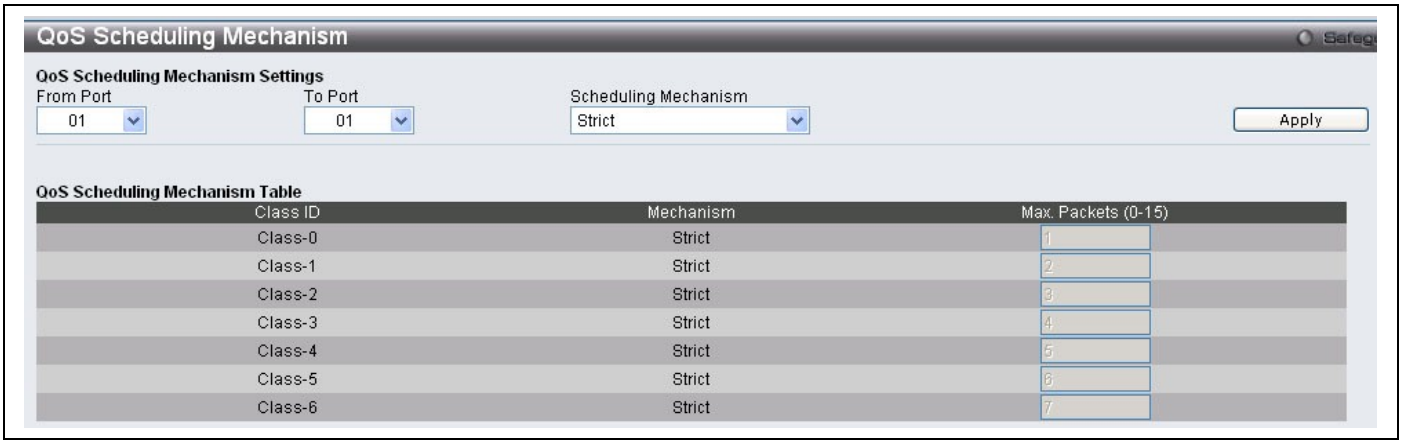


Figure 91. QoS Scheduling Mechanism

The following parameters can be configured.

Parameter	Description
From Port / To Port	Enter the port or port list you wish to configure.
Scheduling Mechanism	*Strict* – The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weighted Round Robin* – Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority classes of service. For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight.

Click **Apply** to implement changes made.

QoS Scheduling

This window allows the user to configure the way the switch will map an incoming packet per port based on its 802.1p user priority, to one of the eight available hardware priority queues available on the switch.

To view this window, click **QoS > QoS Scheduling** as shown below:

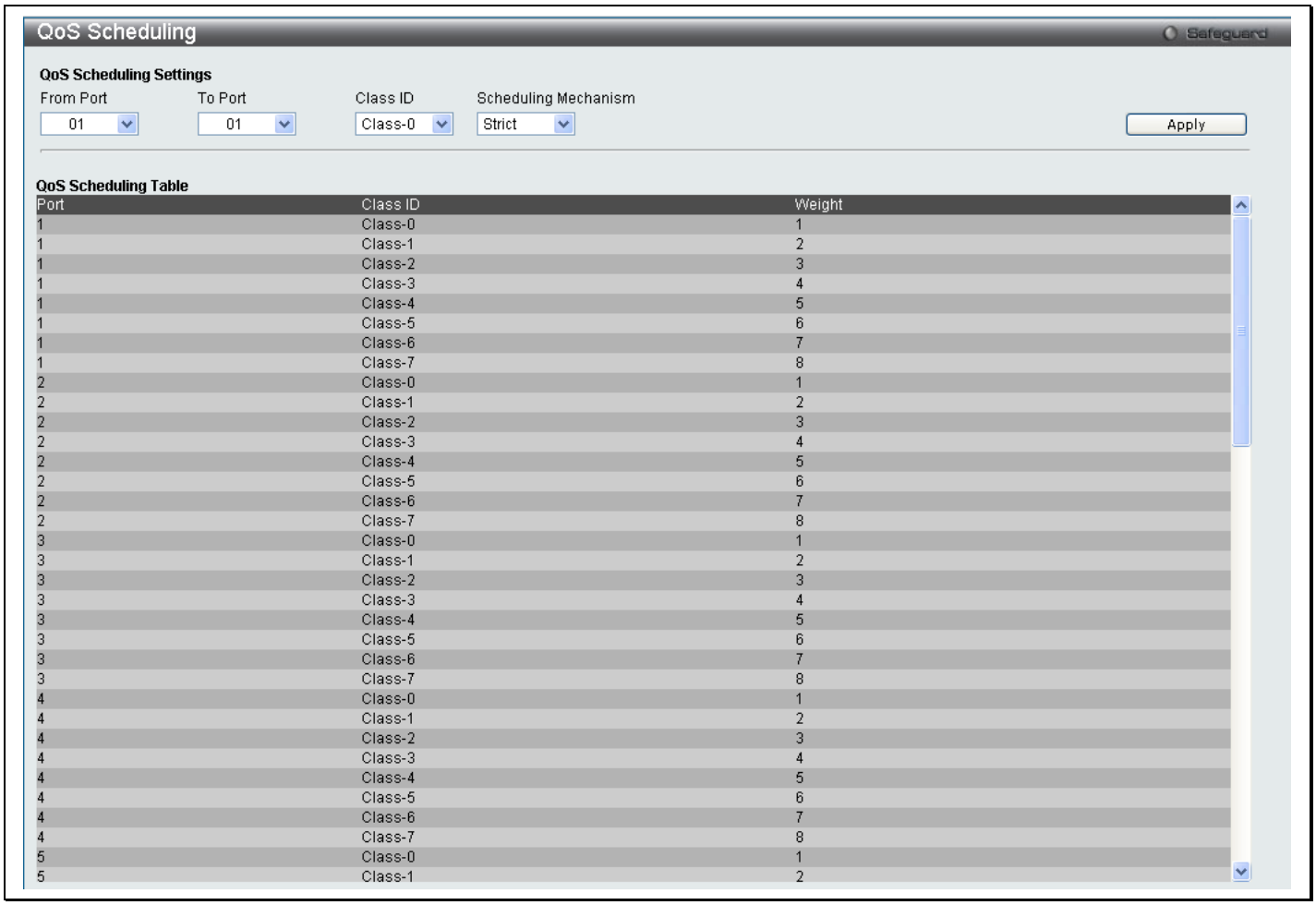


Figure 92. QoS Scheduling

The following parameters can be configured:

Parameter	Description
From Port / To Port	Enter the port or port list you wish to configure.
Class ID	Select the Class ID, from *0-7*, to configure for the QoS parameters.
Scheduling Mechanism	*Strict* – 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* – Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority classes of service. When *Weight* is selected, a field appears next to this field for the user to specify the maximium number of packets. The specified hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. The value is ranged from 1 to 127.

Click **Apply** to implement changes made.

In Band Manage Settings

This window allows the user to specify a priority handling of untagged in-band management packets received by the switch. The priority value entered in this window will be used to determine which of the eight hardware priority queues the packet is forwarded to.

To view this window, click **QoS > In Band Manage Settings** as shown below:

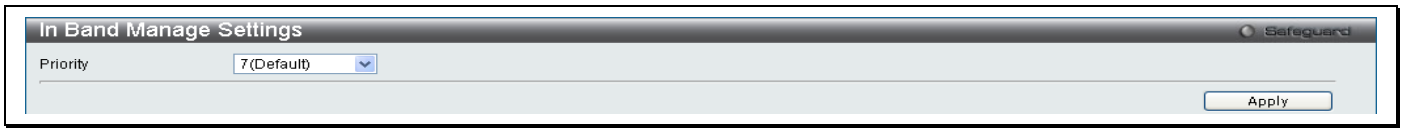


Figure 93. In Band Manage Settings

Select the priority and click **Apply**.

DSCP Trust Settings

This window is used to enable DSCP Trust Settings on the switch.

To view this window, click **QoS > SRED > DSCP Trust Settings** as shown below:

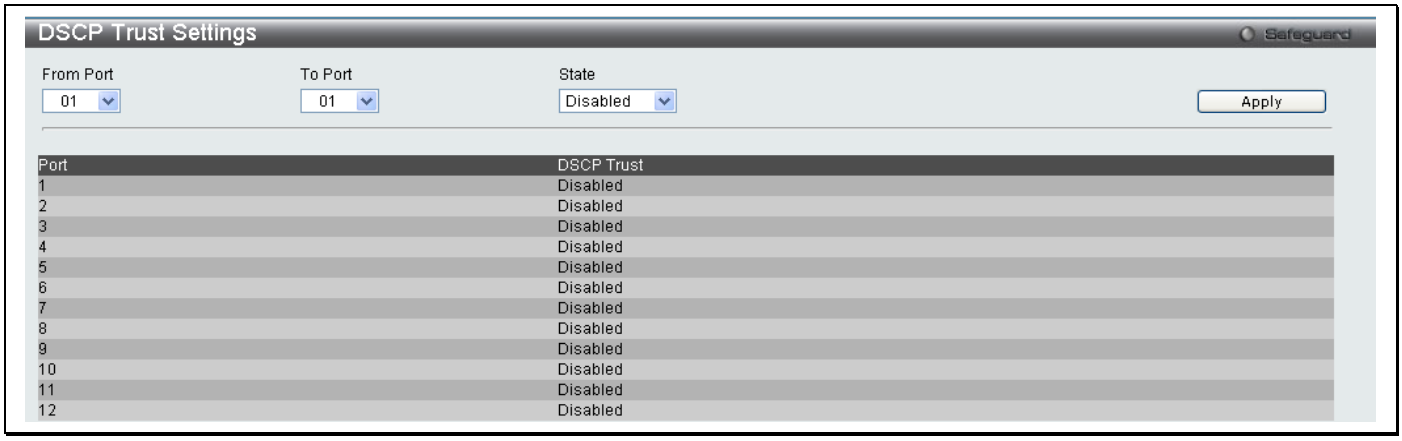


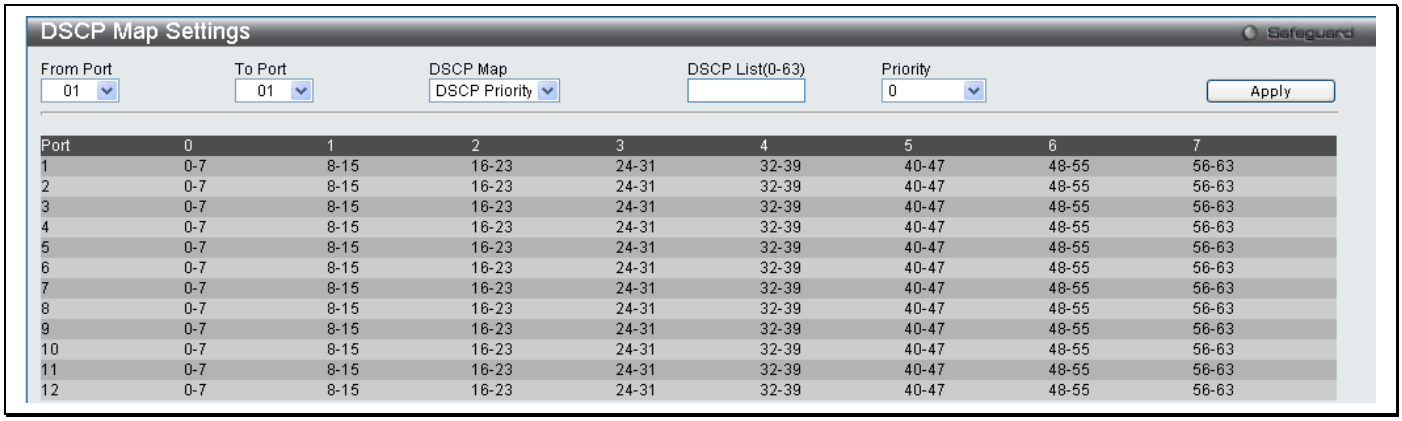
Figure 94. DSCP Trust Settings menu

Select the port or port range you wish to *Enable* or *Disable* and click **Apply**.

DSCP Map Settings

This window is used to enable DSCP Map Settings.

To view this window, click **QoS > SRED > DSCP Map Settings** as shown below:



Port	0	1	2	3	4	5	6	7
1	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
2	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
3	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
4	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
5	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
6	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
7	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
8	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
9	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
10	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
11	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
12	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Figure 95. DSCP Map Settings menu

The following parameters may be set:

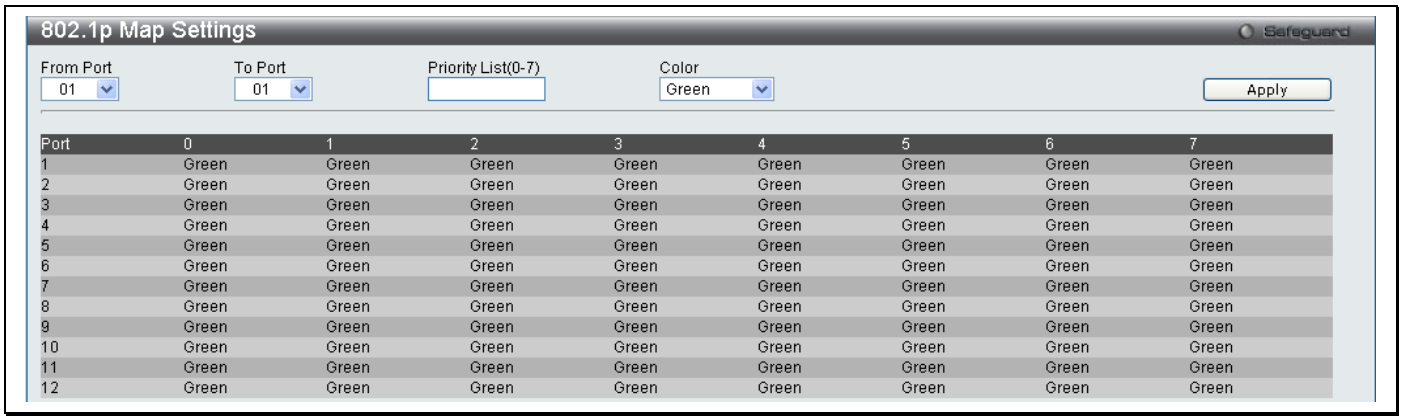
Parameter	Description
From port / To port	A consecutive group of ports may be configured starting with the selected port.
DSCP Map	Use the drop-down menu to choose a DSCP Map, you can choose between *DSCP Priority*, *DSCP DSCP* and *DSCP Color*.
DSCP List(0-63)	This field allows the user to enter a DSCP value in the space provided, which will instruct the switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between *0* and *63*.
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 **Apply** to implement changes.

802.1p Map Settings

This window is used to enable 802.1p Map Settings.

To view this window, click **QoS > SRED > 802.1p Map Settings** as shown below:



Port	0	1	2	3	4	5	6	7
1	Green	Green	Green	Green	Green	Green	Green	Green
2	Green	Green	Green	Green	Green	Green	Green	Green
3	Green	Green	Green	Green	Green	Green	Green	Green
4	Green	Green	Green	Green	Green	Green	Green	Green
5	Green	Green	Green	Green	Green	Green	Green	Green
6	Green	Green	Green	Green	Green	Green	Green	Green
7	Green	Green	Green	Green	Green	Green	Green	Green
8	Green	Green	Green	Green	Green	Green	Green	Green
9	Green	Green	Green	Green	Green	Green	Green	Green
10	Green	Green	Green	Green	Green	Green	Green	Green
11	Green	Green	Green	Green	Green	Green	Green	Green
12	Green	Green	Green	Green	Green	Green	Green	Green

Figure 96. DSCP Map Settings menu

The following parameters may be set:

Parameter	Description
From port / To port	A consecutive group of ports may be configured starting with the selected port.
Priority List(0-7)	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.
Color	Specify the color *Red*, *Yellow* or *Green*.

Click **Apply** to implement changes.

Section 8

ACL

ACL Configuration Wizard

Access Profile List

CPU Access Profile List

ACL Finder

ACL Flow Meter

Access profiles allow you to establish criteria to determine whether or not the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of Packet Content, MAC address, or IP address.

Due to a chipset limitation, the switch supports a maximum of 12 access profiles. The rules used to define the access profiles are limited to a total of 1536 rules for the switch.

ACL Configuration Wizard

The ACL Configuration Wizard will aid with the creation of access profiles and ACL rules. The ACL Wizard will create the access rule and profile automatically.

To view this window, click **ACL > ACL Configuration Wizard** as shown below:

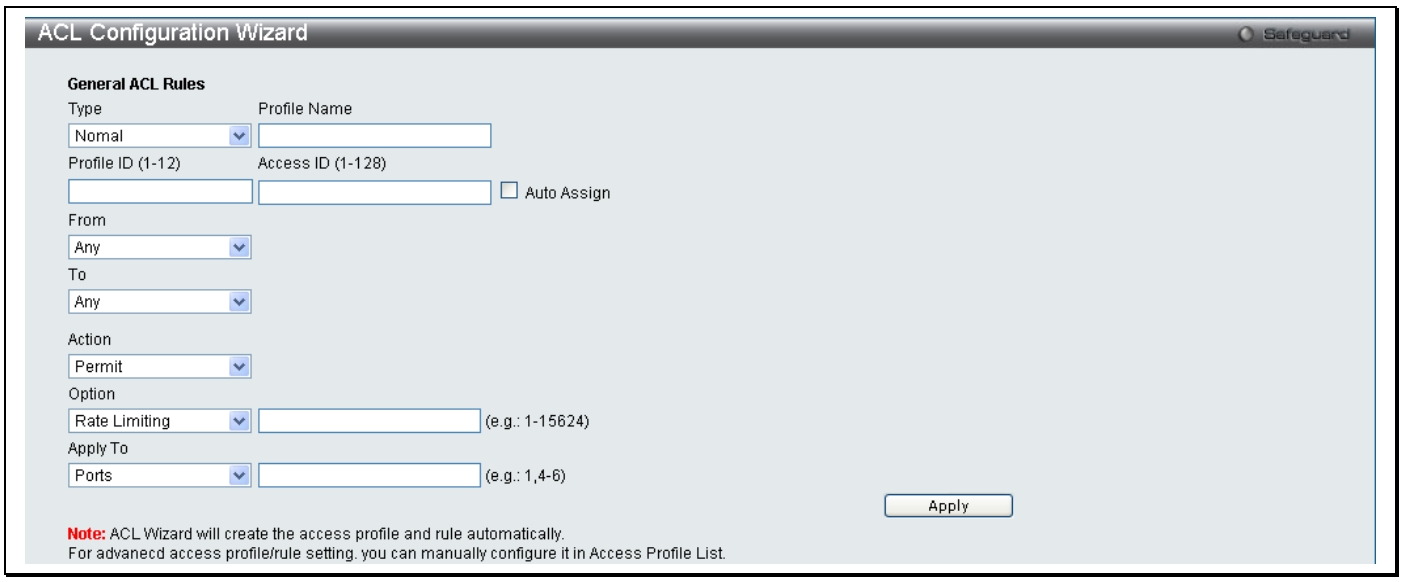


Figure 97. ACL Configuration Wizard menu

The following parameters can be configured.

Parameter	Description
Type	Select the type of ACL you wish to create, either normal or CPU.
Profile Name	Select a unique Profile Name for this profile set.
Profile ID (1-12)	Enter a unique identifier number for this profile set. This value can be set from *1* to *12*.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.
From	Use the drop-down menu to select from MAC Address, IPv4 Address or IPv6.
To	Use the drop-down menu to select from MAC Address, IPv4 Address or IPv6. When IPv6 is selected the user can only enter the IPv6 source address or the IPv6 destination address at any one time.
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 the packets that match the access profile to 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.
Option	Use the pull down menu to select an option, the user can choose between *Rate Limiting*, *Change 1P Priority*, *Replace DSCP* and *Replace ToS Precedence*.
Apply To	Use the pull down menu to select an option, the user can choose between *Ports*, *VLAN Name* or *VLAN ID* and enter the appropriate information.

Click **Apply** to implement changes made.

Access Profile List

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.

To view this window, click **ACL > Access Profile List** as shown below:

Figure 98. Access Profile Lists

To add an ACL Profile, click the **Add ACL Profile** button, which, will display the window below. There are four **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IPv4** address-based profile configuration, one for the **Packet Content** and one for **IPv6**. You can explore the four **Access Profile Configuration** options by entering a Profile ID and Profile Name and using the radio button to select an ACL Type and click **Select**. The user may remove all Access Profiles by clicking the **Delete All** button. The page shown below is the **Ethernet Access Profile Configuration** page.

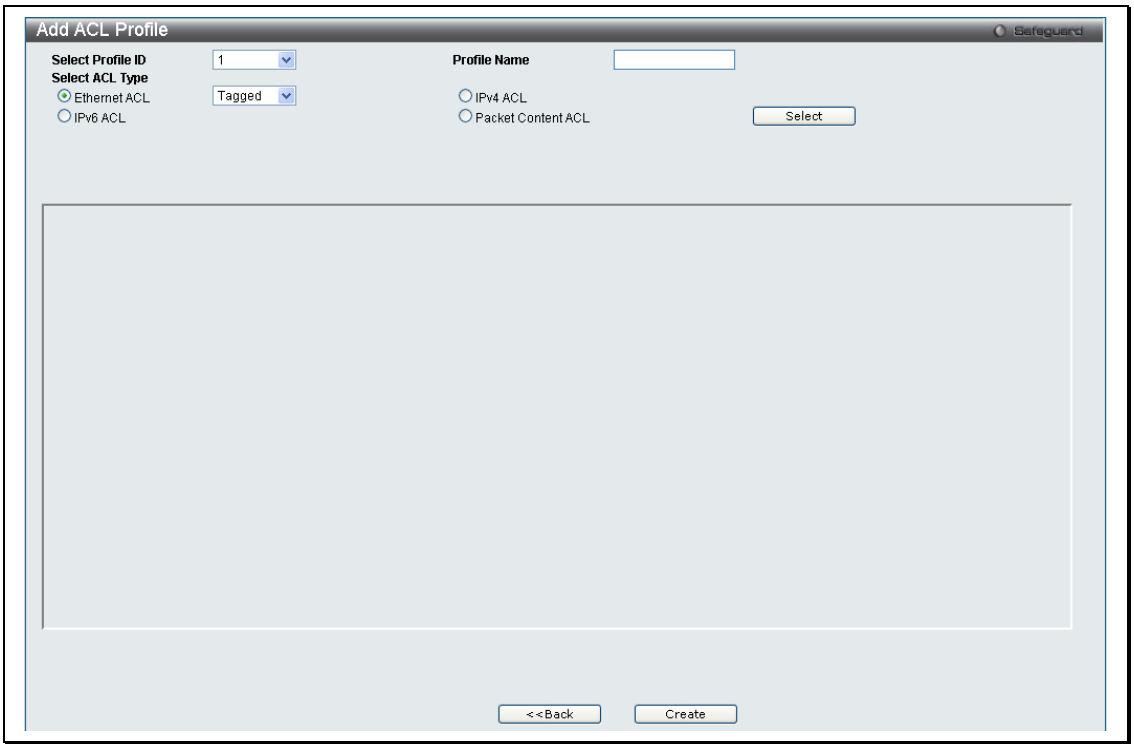


Figure 99. Add Access Profile (Ethernet)

If creating an **Ethernet ACL** enter the Profile ID and Profile Name and click **Select** the following window will appear.

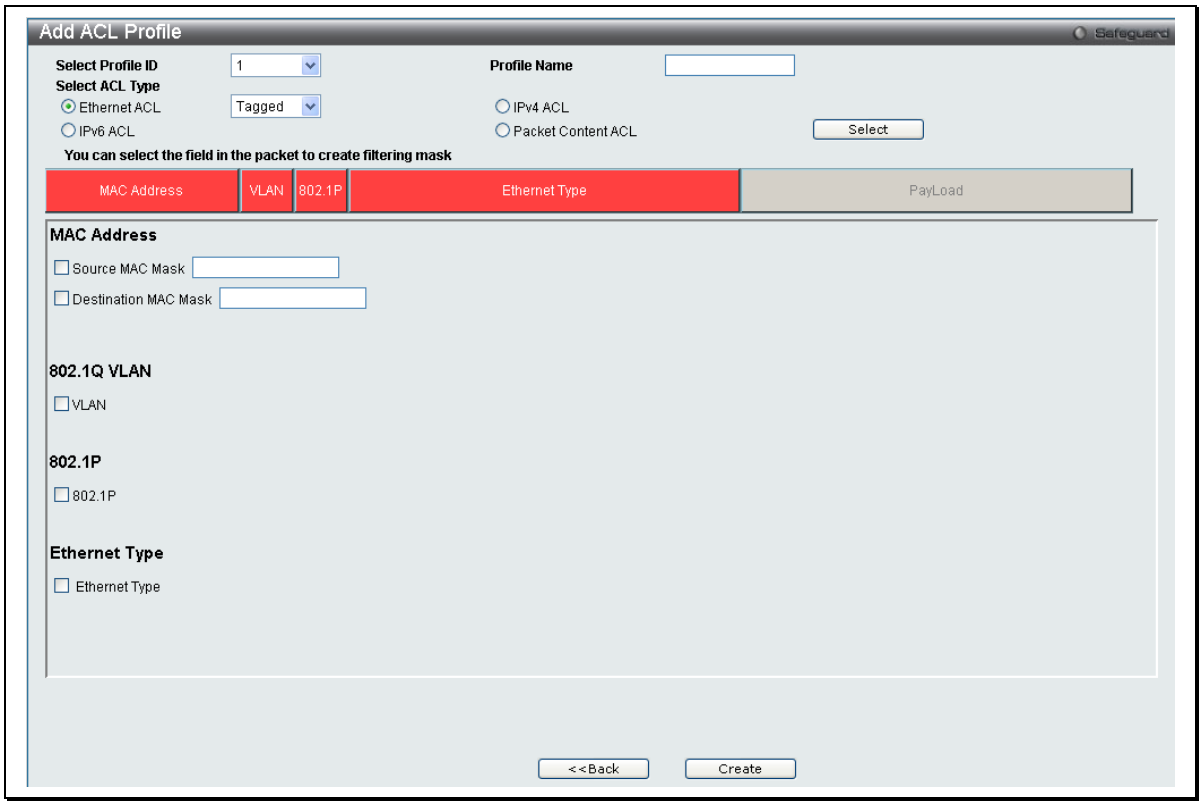


Figure 100. Add Ethernet ACL Profile menu

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the Access Profile List page click **Back**.

The following parameters can be configured.

Parameter	Description
Ethernet ACL	To configure this profile select the Ethernet ACL, and use the drop down menu to choose between *tagged* or *untagged*.
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.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 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 IPv4 address in each frame's header. Select *IPv6* to instruct the switch to examine the IPv6 address in each frame's header. Select *Packet Content Mask* to specify a mask to check the content of the packet header.
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 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 **Create** to view the new Access Profile List entry in the **Access Profile List** table shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

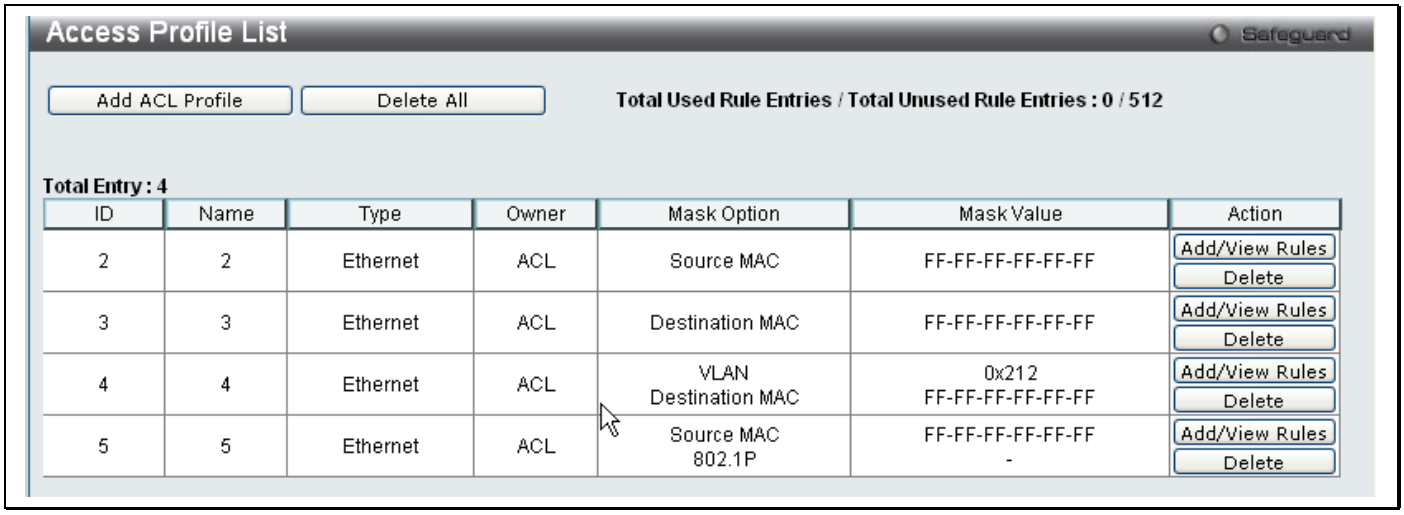


Figure 101. Access Profile List (Ethernet)

To view the configurations for previously configured entry click on the corresponding **Show Details** Button which will display the following window.

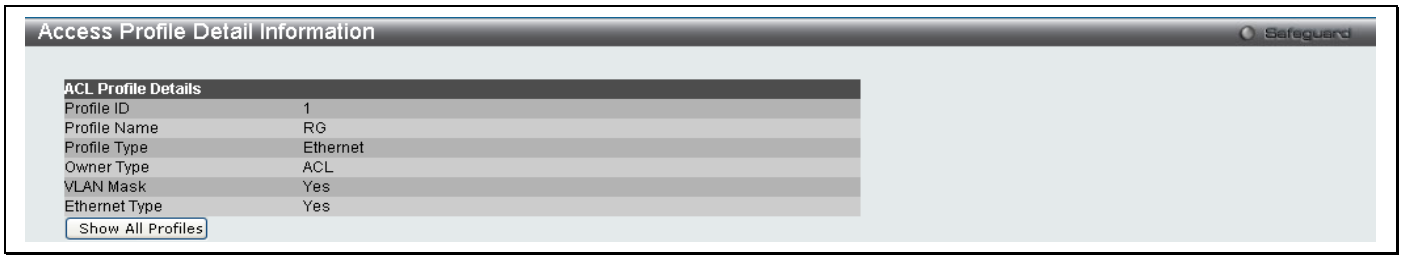


Figure 102. Access Profile Details (Ethernet)

To return to the Access Profile List click **Show All Profiles**, to add a rule to a previously configured entry click on the corresponding **Add/View Rules**, which will reveal the following window.

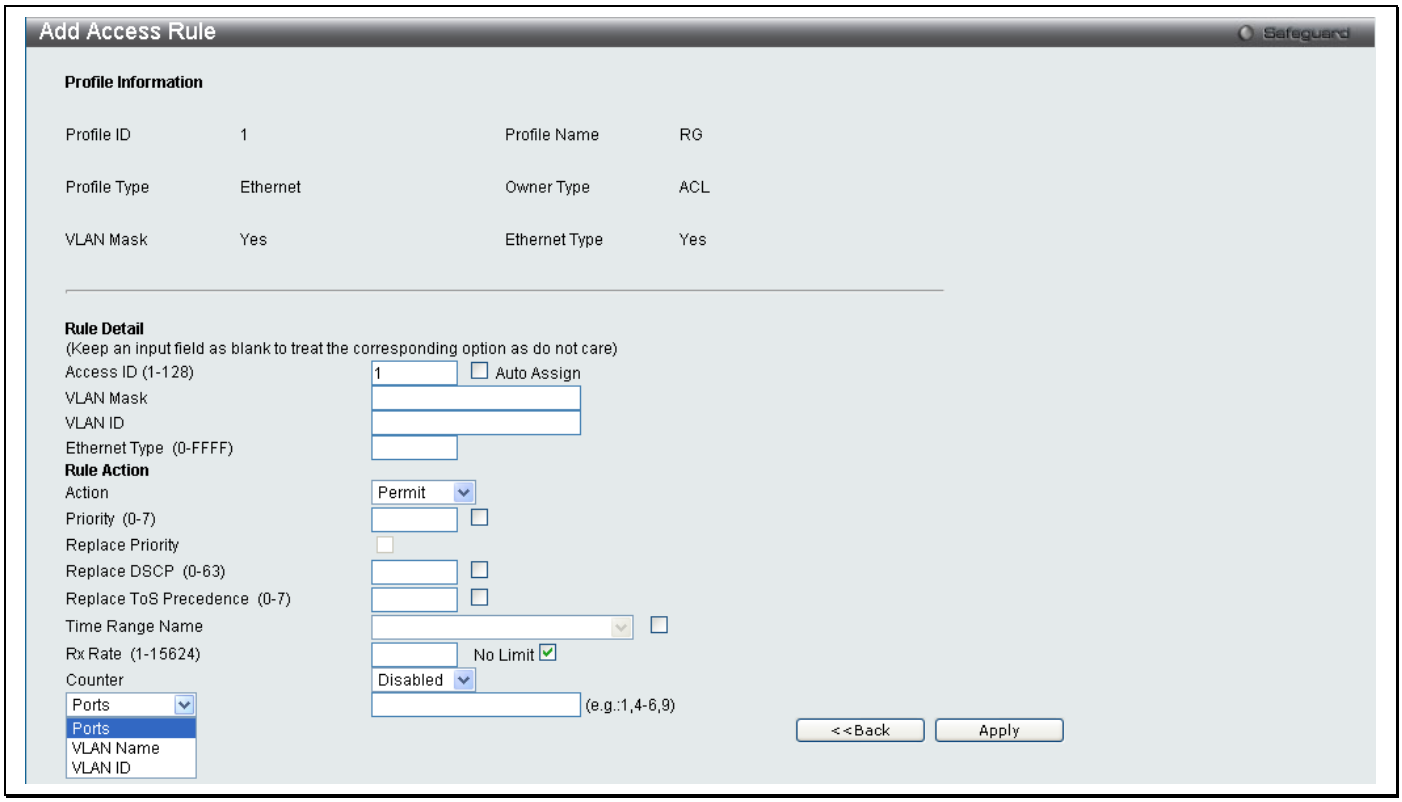


Figure 103. Access Profile Ethernet

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the switch to automatically assign an Access ID for the rule being created.
VLAN Mask	Allows the entry of a VLAN Mask for a previously configured VLAN.
VLAN ID	Allows the entry of a VLAN ID for a previously configured VLAN.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
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 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	Enter a priority value 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	Enter a replace priority manually 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.
Replace ToS Precedence	Select this option to instruct the switch to replace the Type of Service as part of the packet header.
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.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640Kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
Counter	Specifies whether counter feature will be enabled/disabled This is optional, the default is disabled. If the rule is not binded with flow_meter, then all packet matched will be countered. If the rule is binded with flow_meter, then “counter” here will be overrided.
Ports	Specifies the access rule will take effect on one port or a range of ports.
VLAN Name	Specifies the access rule will take effect on the VLAN Name specified.
VLAN ID	Specifies the access rule will take effect on the VLAN ID specified.

Click **Apply** to display the following **Access Rule List** window.

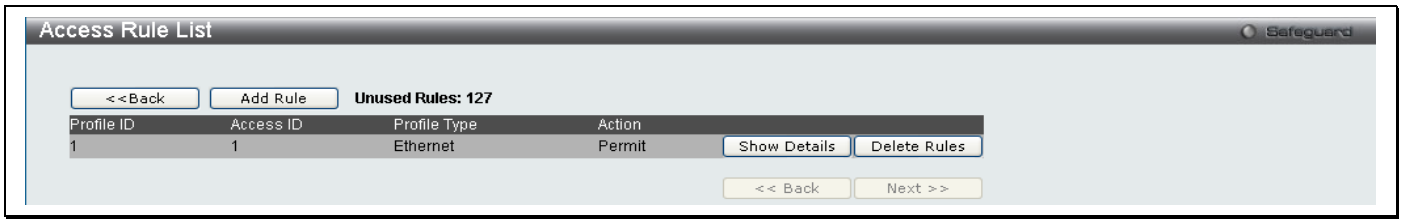


Figure 104. Access Rule List (Ethernet)

To view the configurations for previously configured rules click on the corresponding **Show Details** Button which will display the following **Access Rule Details** window.

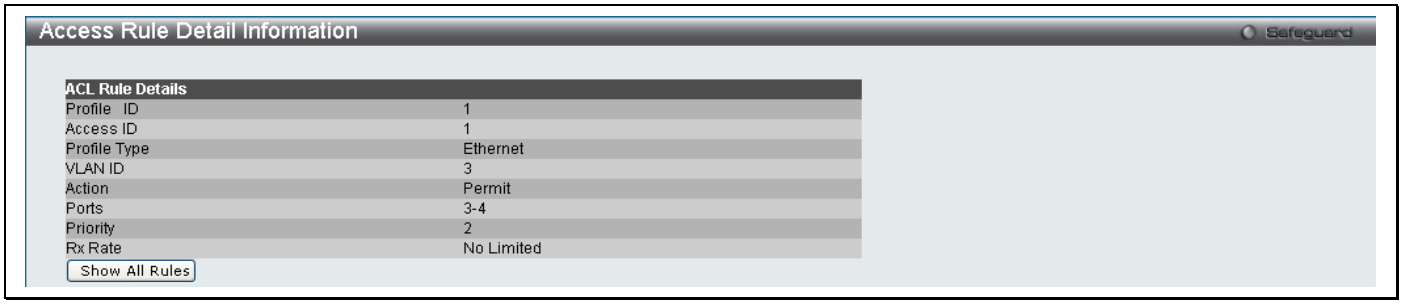


Figure 105. Access Rule Detail Information (Ethernet)

To create an **IPv4 ACL** select IPv4, enter the Profile ID and Profile Name into the top half of the screen in the **Add ACL Profile** window and click **Select** the following window will appear.

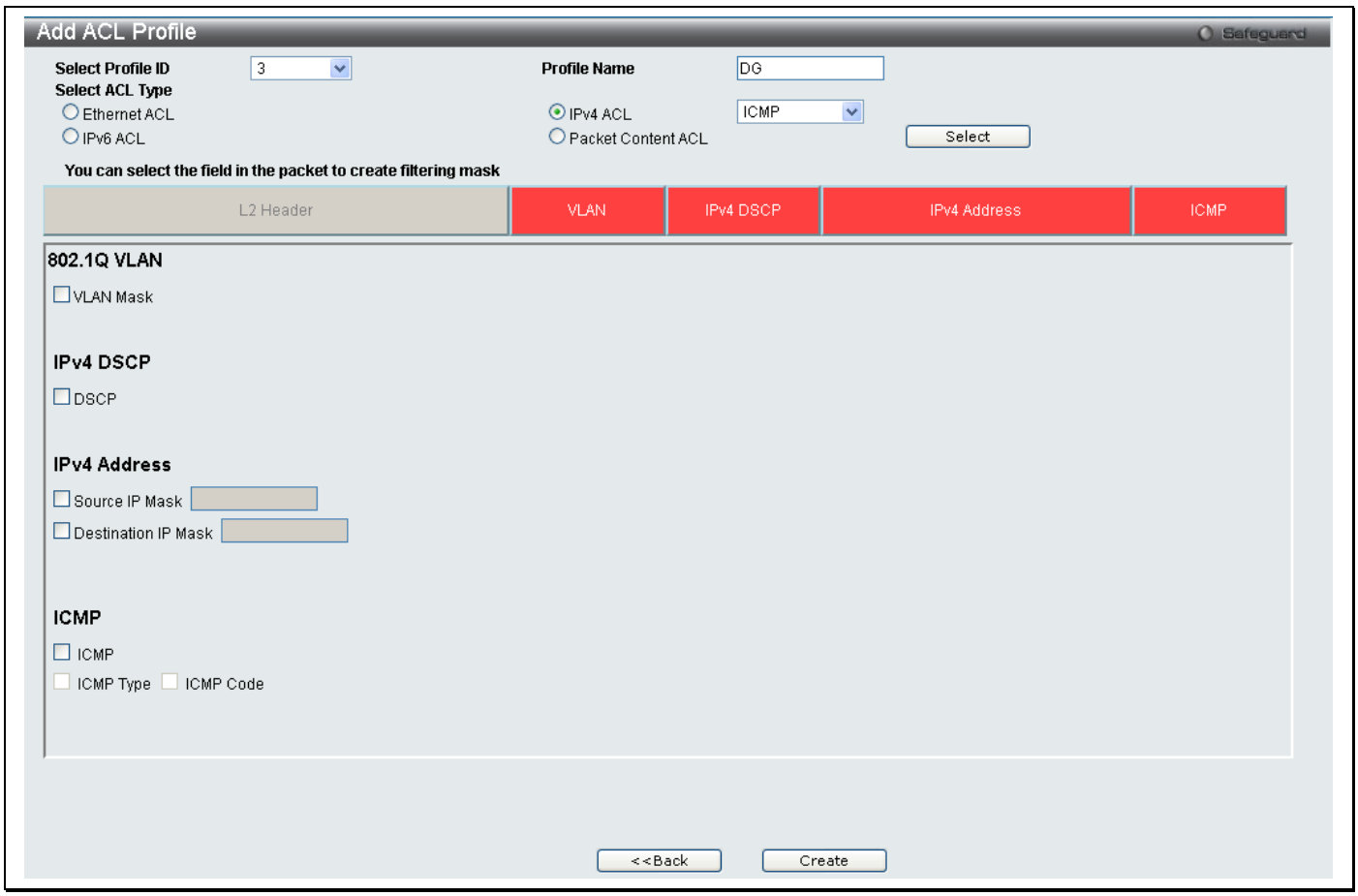


Figure 106. Add IPv4 ACL Profile

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the Access Profile List page click **Back**.

The following parameters can be set, for **IP**:

Parameter	Description
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.
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.
ICMP Type	• *icmp* – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field within each packet. • *type <value 0-255>* – Specifies that the switch will examine the type field within each packet. • *code <value 0-255>* – Specifies that the switch will examine the code field within each packet.
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 that you specify a source port mask and/or a destination port mask. 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 TCP port mask for the source port in hex form (hex 0x0-0xffff) to be filtered. **dst port mask** – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) to be filtered. ***Protocol_id <0x0-0xff>*** – Enter a value defining the protocol ID in the packet header to mask. ***user_define_mask <hex 0x0-0xffffffff>*** – Enter a value defining the mask options behind the IP header.

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** table shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

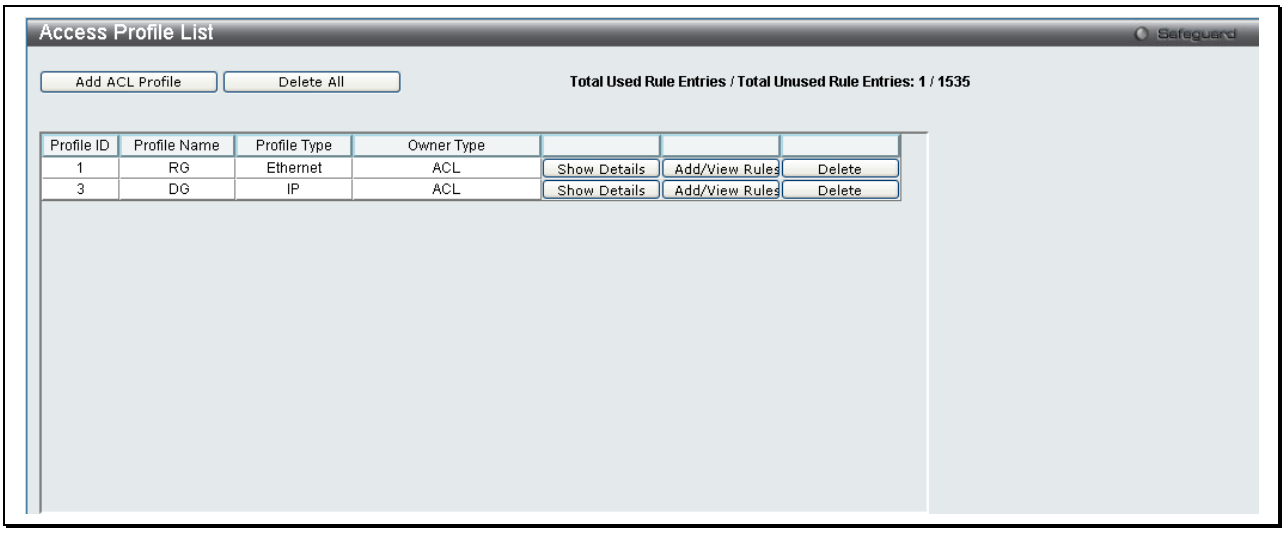


Figure 107. Access Profile List (IPv4)

To view the configurations for previously configured entry click on the corresponding **Show Details** Button which will display the following window.

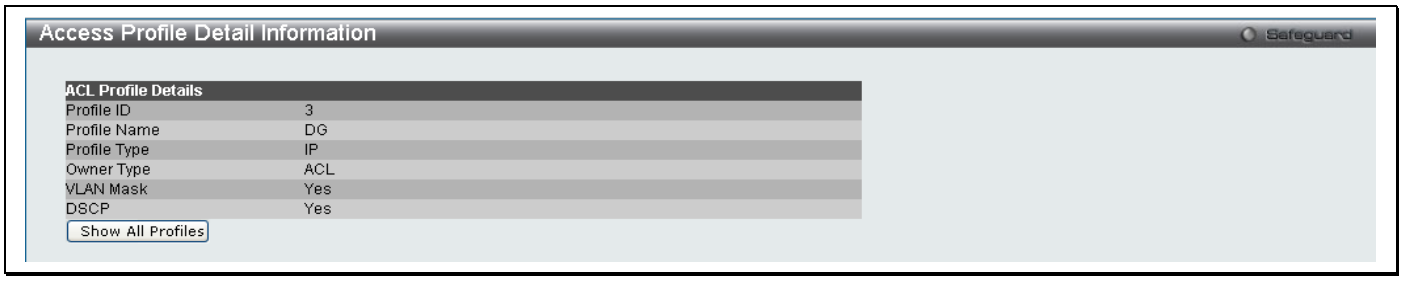


Figure 108. Access Profile Details (IPv4)

To return to the Access Profile List click **Show All Profiles**, to add a rule to a previously configured entry click on the corresponding **Add/View Rules**, which will reveal the following window;

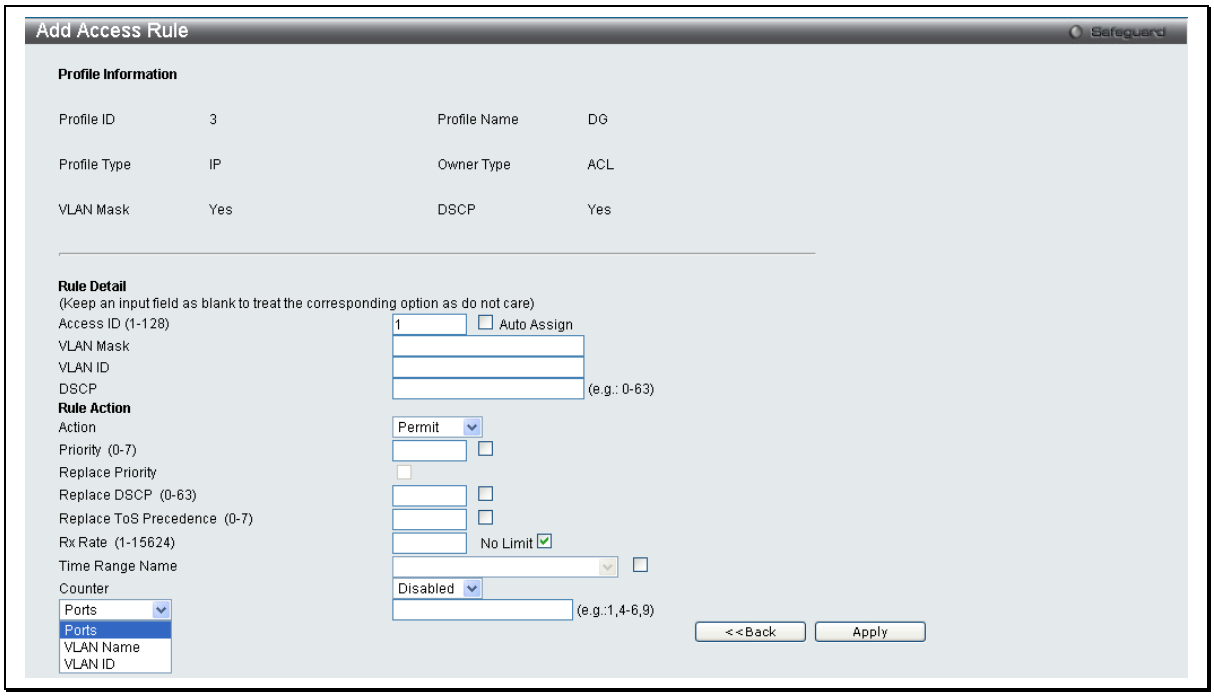


Figure 109. Access Profile (IPv4)

The following parameters may be configured for the IP (IPv4) filter.

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.
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 the packets that match the access profile to 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)	Enter a priority value 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	Enter a replace priority manually 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	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.
Replace ToS Precedence	Select this option to instruct the switch to replace the Type of Service as part of the packet header.
VLAN Mask	Allows the entry of a name for a previously configured VLAN.
VLAN ID	Allows the entry of a VLAN ID for a previously configured VLAN.
DSCP	Selecting this option instructs the switch to examine the DiffServ Code part of each packet header and use this as the criteria, or part of the criterion for forwarding.
ICMP	Select *ICMP* to instruct the switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640Kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
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	Enable or disable the counter settings.
Ports	Specifies that the access rule will take effect on one port or a range of ports.
VLAN Name	Specifies the access rule will take effect on the VLAN Name specified.
VLAN ID	Specifies the access rule will take effect on the VLAN ID specified.

Click **Apply** to display the following Access Rule List window.

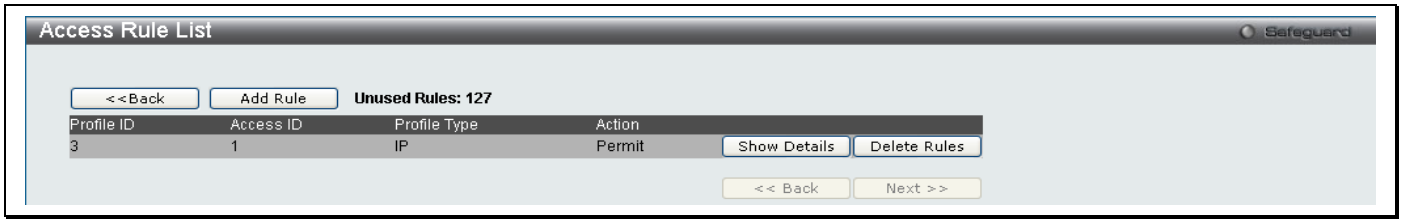


Figure 110. Access Rule List (IPv4)

To view the configurations for previously configured rule click on the corresponding **Show Details** Button which will display the following **Access Rule Details** window.

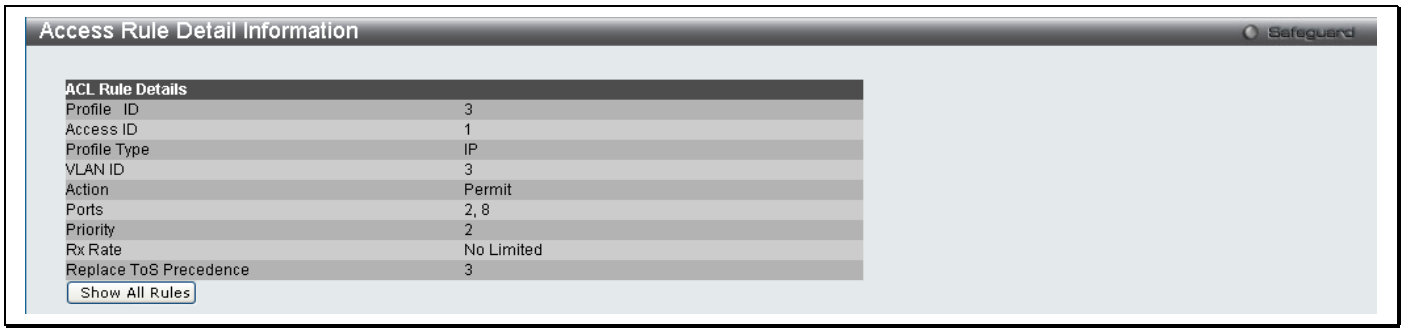


Figure 111. Access Rule Detail Information

To configure the **IPv6 ACL** select IPv6 in the Add ACL Profile window, enter the Profile ID and Profile Name into the top half of the screen in the **Add ACL Profile** window and click **Select,** the following window will appear.

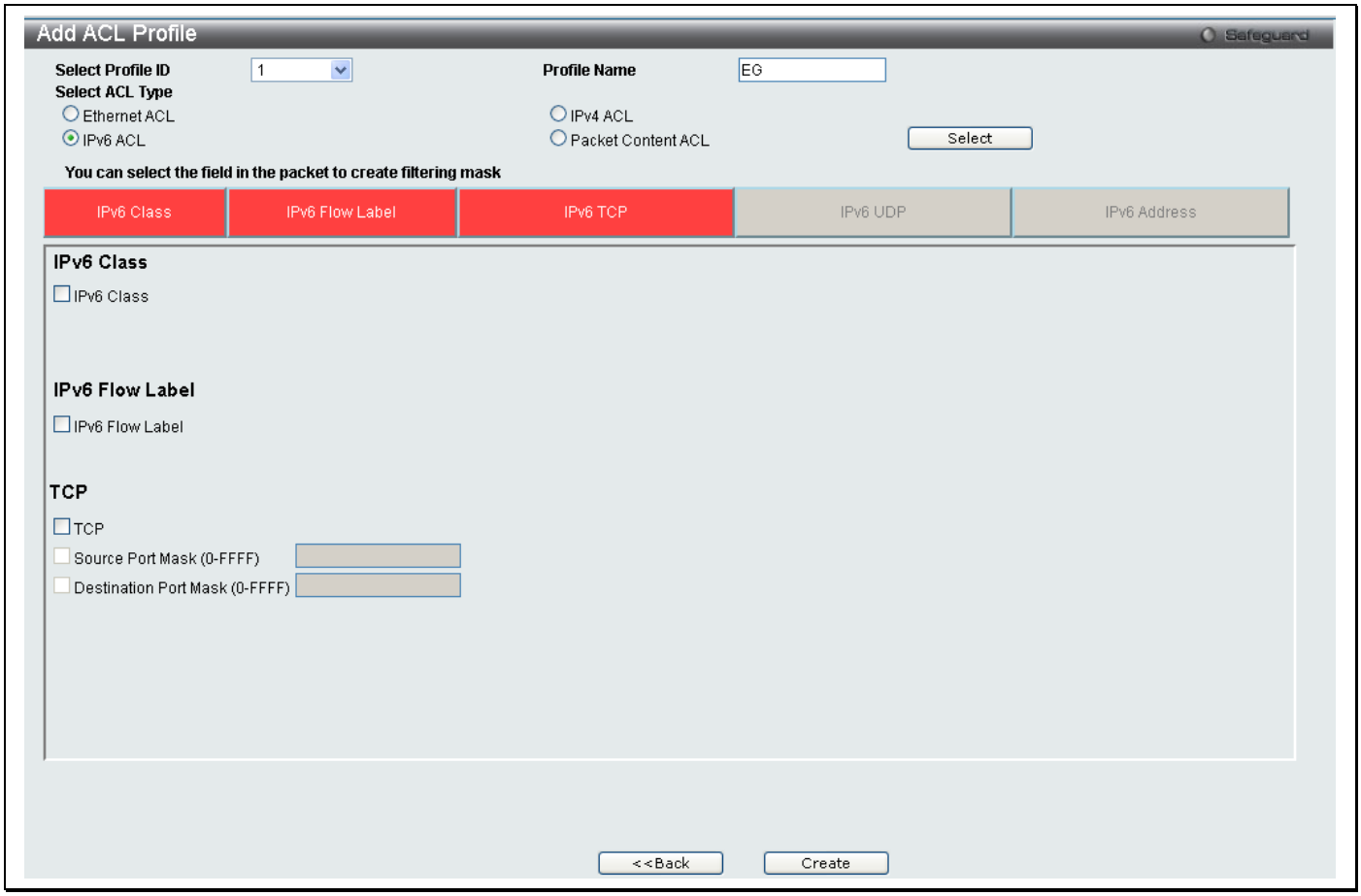


Figure 112. Add IPv6 ACL Profile

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the Access Profile List page click **Back**.

The following parameters can be set, for **IPv6**:

Parameter	Description
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	Ticking this check box will specify that the rule applies to TCP traffic. The user can enter a specific TCP Source Port Mask or TCP Destination Port Mask.
IPv6 UDP	Ticking this check box will specify that the rule applies to UDP traffic. The user can enter a specific UDP Source Port Mask or UDP Destination Port Mask.
IPv6 Address	*IPv6 Source Address* – Enter an IPv6 address to be used as the source address mask. *IPv6 Destination Address* – Enter an IPv6 address that will be used as the destination address mask. **NOTE:** At any one time the user can only choose IPv6 class and IPv6 Flow Label together or IPv6 Address by itself.

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** table shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

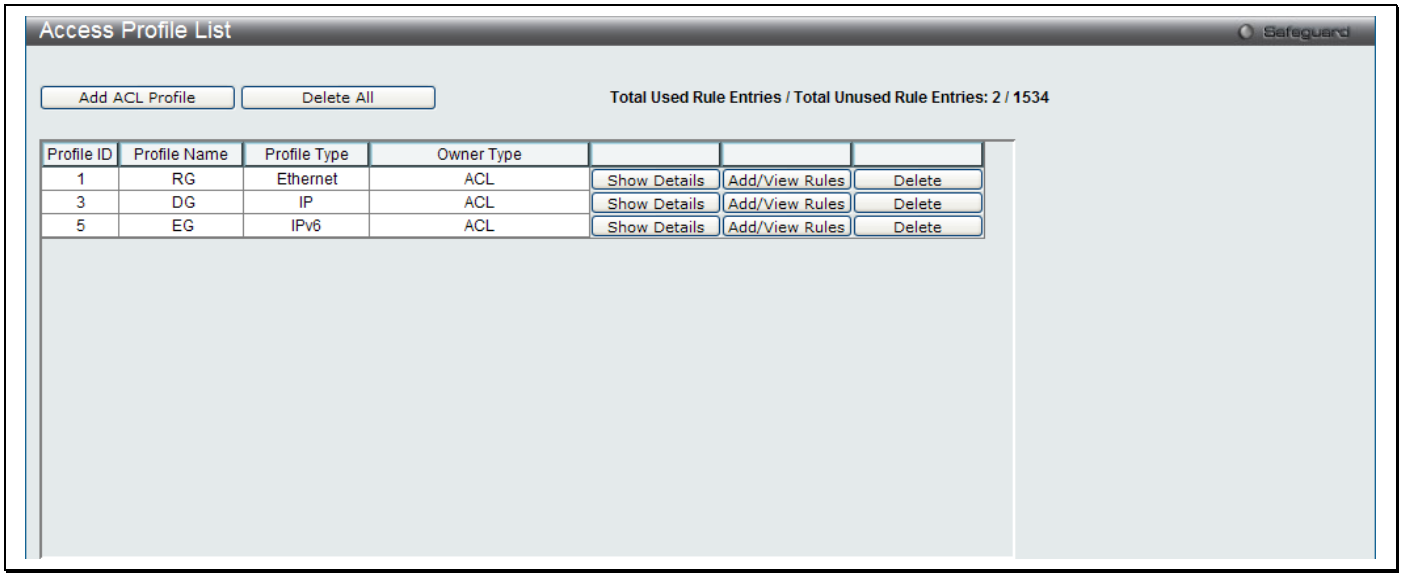


Figure 113. Access Profile List (IPv6)

To view the configurations for previously configured entry click on the corresponding **Show Details** Button which will display the following window.

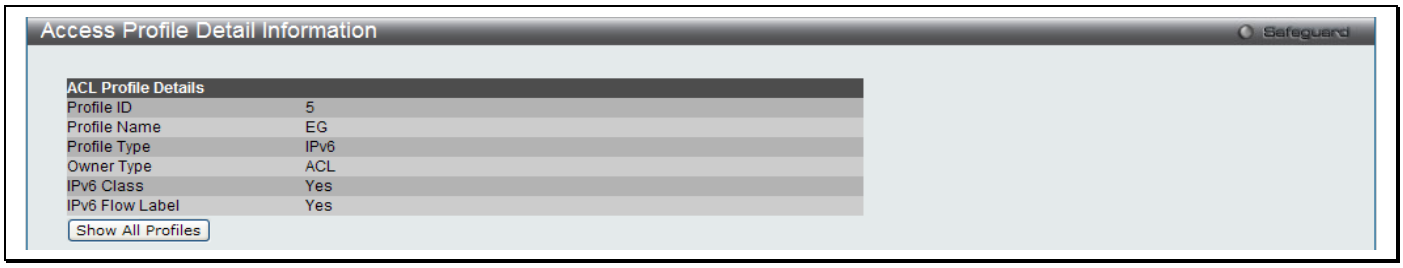


Figure 114. Access Profile Details (IPv6)

To return to the CPU Access Profile List click **Show All Profiles**, to add a rule to a previously configured entry click on the corresponding **Add/View Rules**, which will reveal the following window.

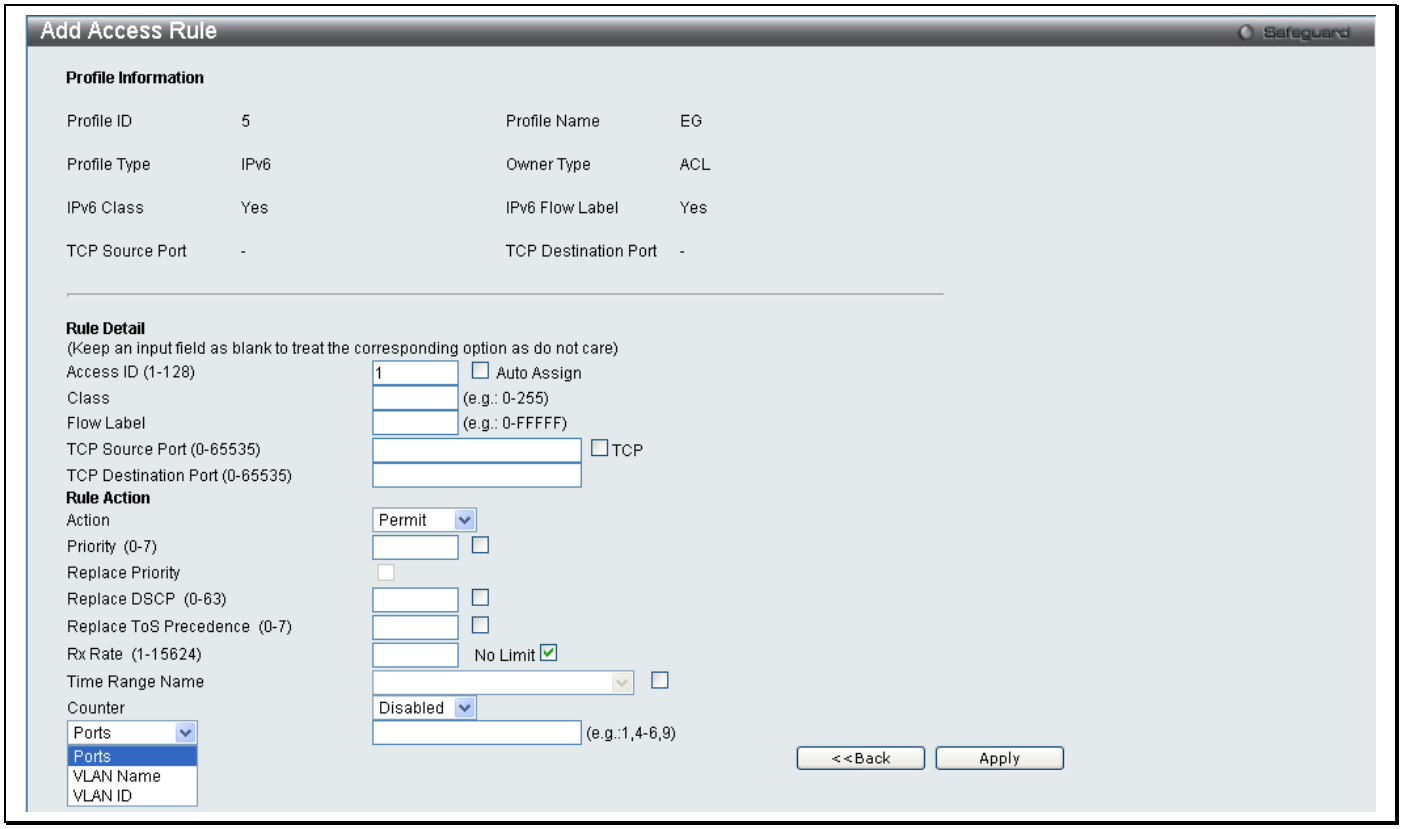


Figure 115. Access Profile (IPv6)

The following parameters may be configured for the IP (IPv6) filter.

Parameter	Description
Access ID (1-128)	Enter a unique identifier number for this access. This value can be set from *1* to *128*.
Class	Specifies the IPv6 Class. Enter a value between *0 – 255*.
Flow Label	Specifies the IPv6 Flow Label. Enter a value between *0 – FFFFF*.
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 the packets that match the access profile to 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)	Enter a priority value 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	Enter a replace priority manually 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	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.
Replace ToS Precedence	Select this option to instruct the switch to replace the Type of Service as part of the packet header.
Class	Entering a class 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.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640Kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
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	Enable or disable the counter settings.
Ports	Specifies that the access rule will take effect on one port or a range of ports.
VLAN Name	Specifies the access rule will take effect on the VLAN Name specified.
VLAN ID	Specifies the access rule will take effect on the VLAN ID specified.

Click **Apply** to display the following **Access Rule List** window.

Figure 116. Access Rule List (IPv6)

To view the configurations for previously configured rule click on the corresponding **Show Details** Button which will display the following **Access Rule Details** window.

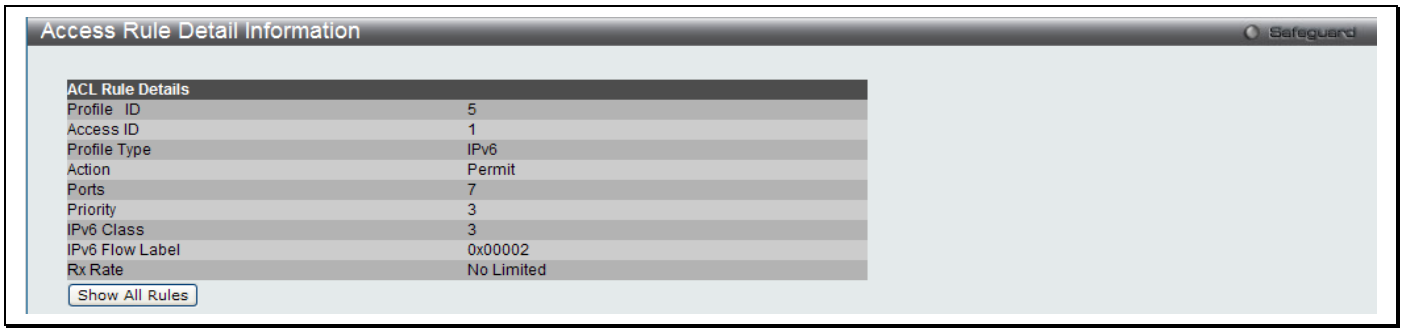


Figure 117. Access Rule Detail Inforamtion (IPv6)

To configure the **Packet Content ACL** select Packet Content in the Add ACL Profile window, enter the Profile ID and Profile Name into the top half of the screen in the **Add ACL Profile** window and click **Select,** the following window will appear.

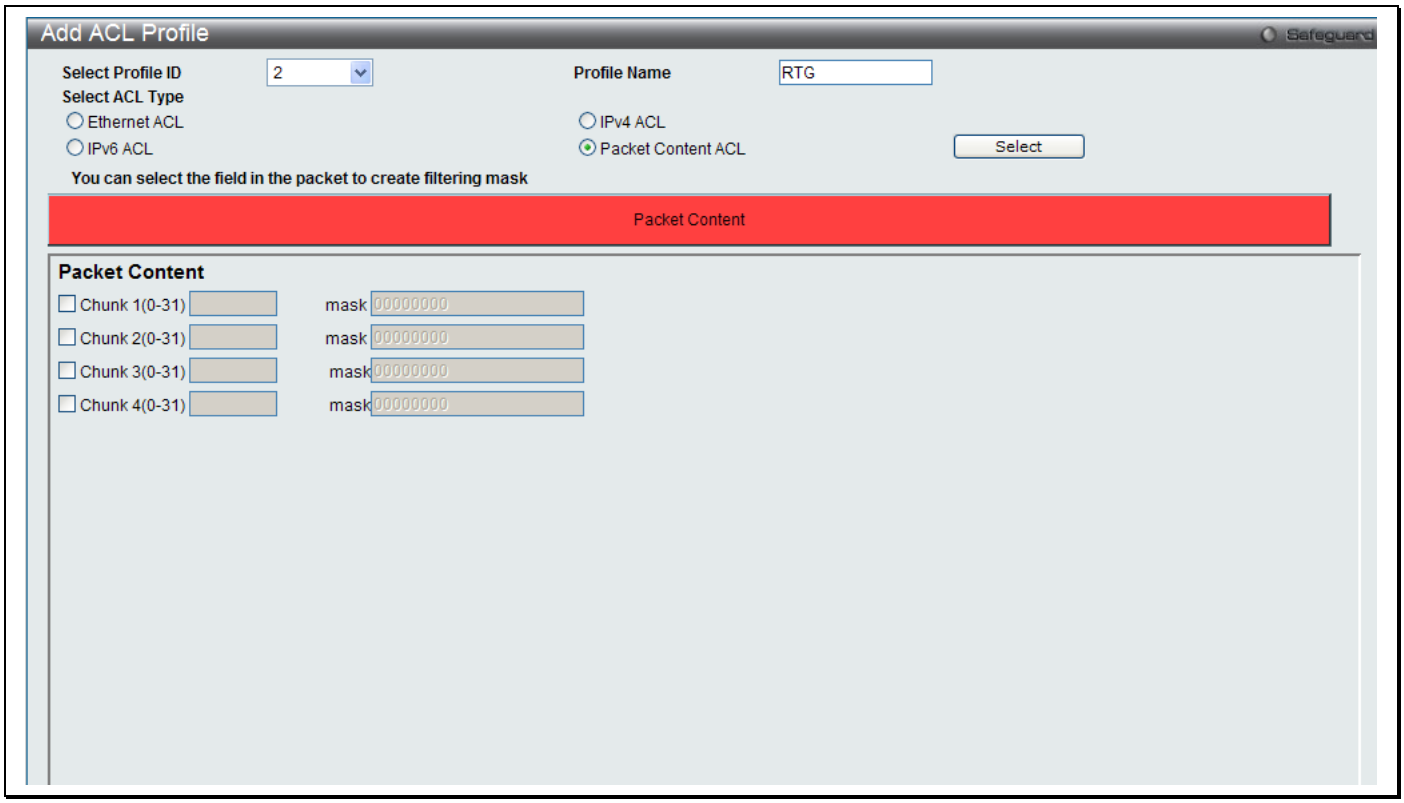


Figure 118. Add Packet Content ACL Profile

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the Access Profile List page click **Previous Page**.

The following parameters can be set, for **Packet Content**:

Parameter	Description
Chunk	Allows users to examine up to 4 specified offset_chunks within a packet at one time and specifies the frame content offset and mask. There are 4 chunk offsets and masks that can be configured. A chunk mask presents 4 bytes. 4 offset_chunks can be selected from a possible 32 predefined offset_chunks as described below: offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4. chunk0: B126, B127, B0, B1 chunk1: B2, B3, B4, B5 chunk2: B6, B7, B8, B9 …… chunk29: B114, B115, B116, B117 chunk30: B118, B119, B120, B121 chunk31: B122, B123, B124, B125 Example: offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1 offset_chunk_1 0 0xffff will match packet byte offset,0,1 Note: Only one packet_content_mask profile can be created. With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click **Apply** to implement changes made.

Click Create to view the new Access Profile List entry in the **Access Profile List** table shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

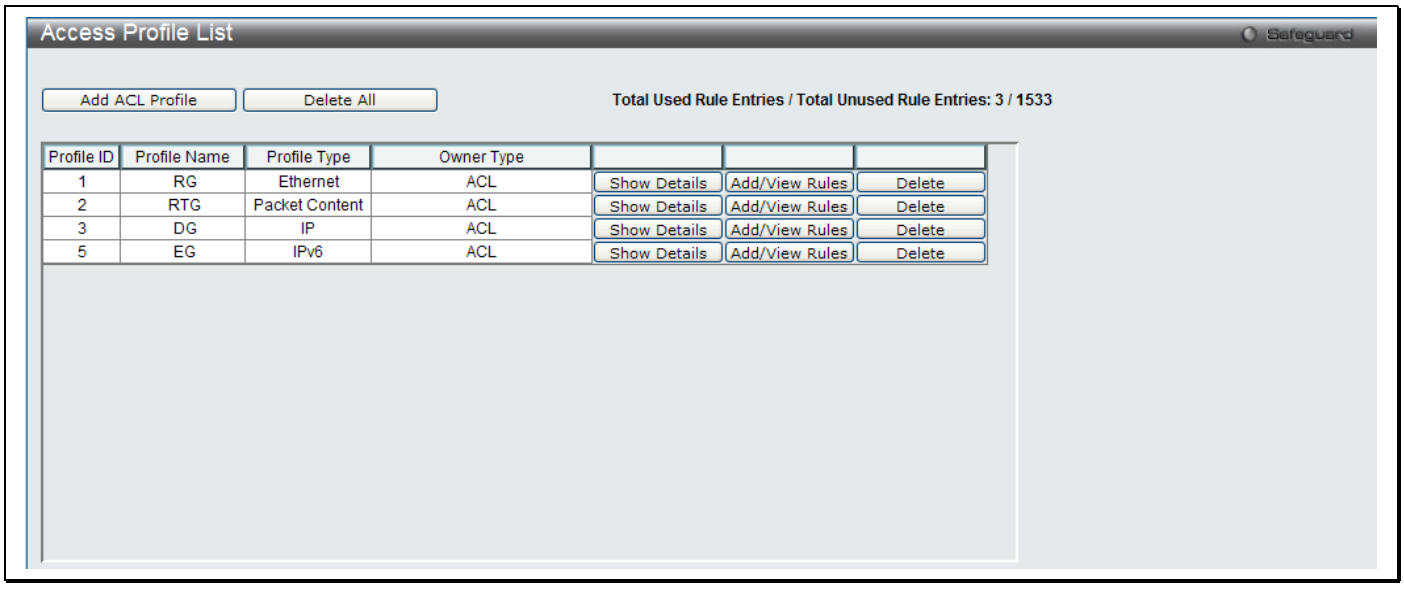


Figure 119. Access Profile List (Packet Content)

To view the configurations for previously configured entry click on the corresponding **Show Details** Button which will display the following window.

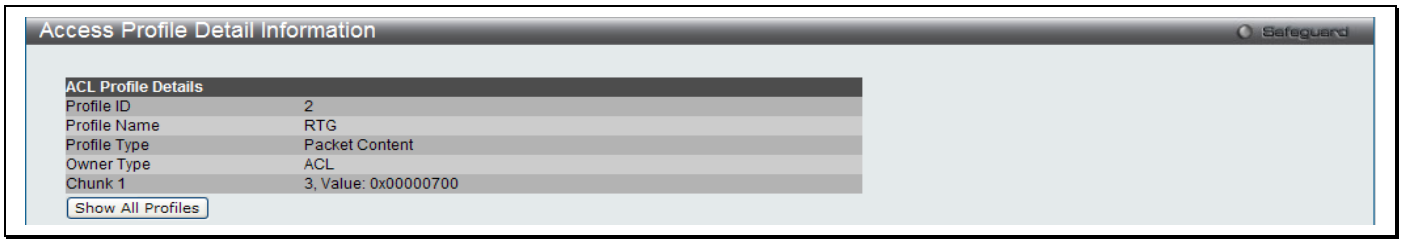


Figure 120. Access Profile Details (Packet Content)

To return to the CPU Access Profile List click **Show All Profiles**, to add a rule to a previously configured entry click on the corresponding **Add/View Rules**, which will reveal the following window:

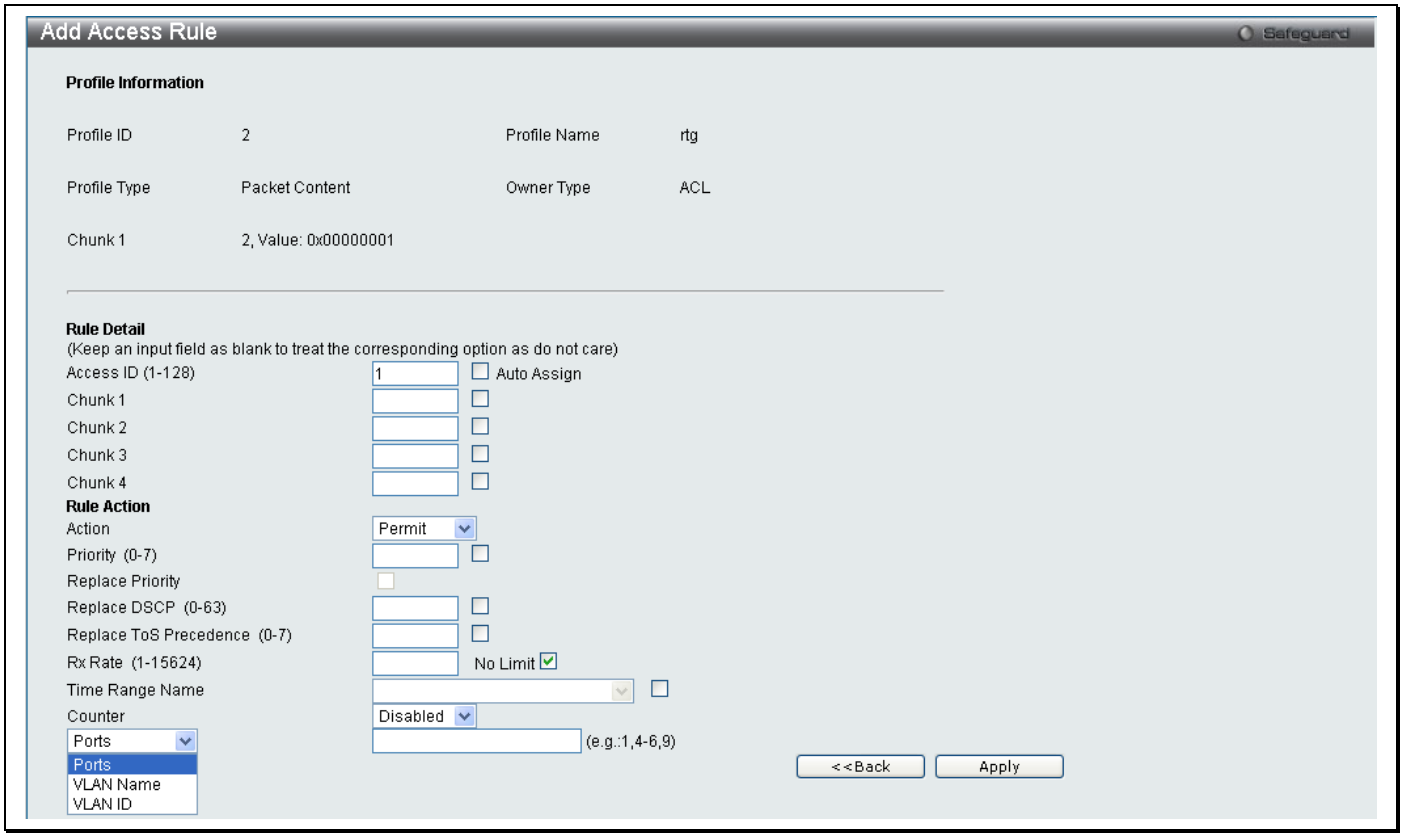


Figure 121. Access Profile (Packet Content)

The following parameters may be configured for the Packet Content filter.

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.
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 the packets that match the access profile to 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)	Enter a priority value 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	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.
Replace ToS Precedence	Select this option to instruct the switch to replace the Type of Service as part of the packet header.
Chunk	This field will instruct the switch to mask the packet header beginning with the offset value specified.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640Kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
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	Enable or disable the counter settings.
Ports	Specifies that the access rule will take effect on one port or a range of ports.
VLAN Name	Specifies the access rule will take effect on the VLAN Name specified.
VLAN ID	Specifies the access rule will take effect on the VLAN ID specified.

Click **Apply** to display the following **Access Rule List** window.

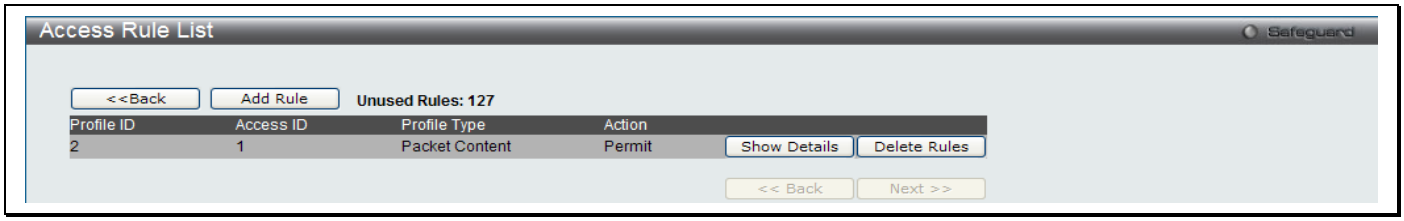


Figure 122. Access Rule List (Packet Content)

To view the configurations for previously configured rule click on the corresponding **Show Details** Button which will display the following **Access Rule Details** window.

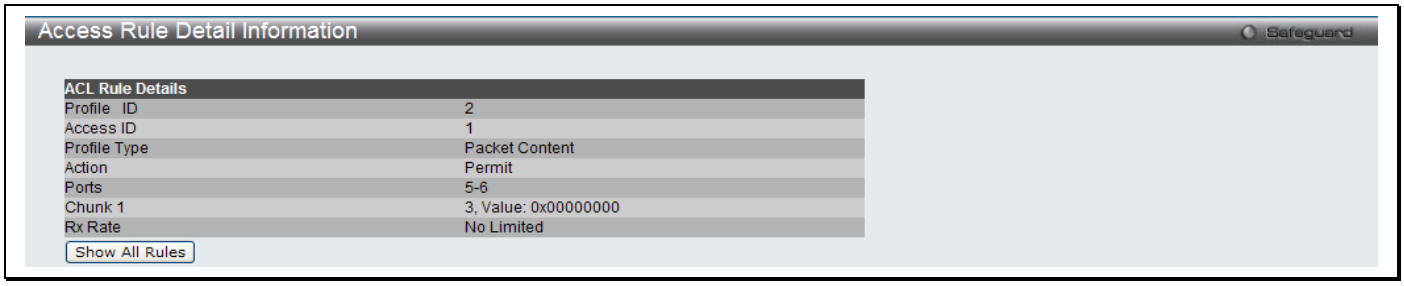


Figure 123. Access Rule Detail Information (Packet Content)

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. For a more detailed explanation on how ARP works and how to employ D-Link's advanced unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix B, at the end of this manual.

ACL Finder

This window is used to help find a previously configured ACL entry. To search for an entry, enter the profile ID from the drop down menu, select a port that you wish to view, define the state and click **Find,** the table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

To view this window, click **ACL > ACL Finder** as shown below:

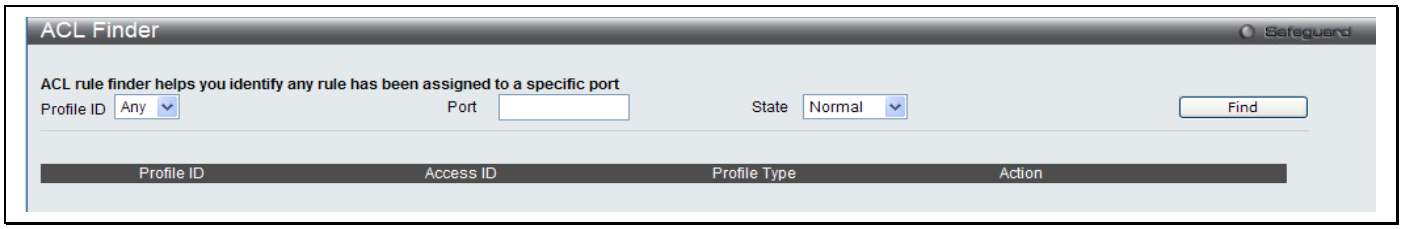


Figure 124. ACL Finder menu

Section 9

VLAN

Management VLAN

The **802.1Q VLAN** window lists all previously configured VLANs by VLAN ID and VLAN Name.

To view this window, click **Switch Configuration > Management VLAN** as shown below:

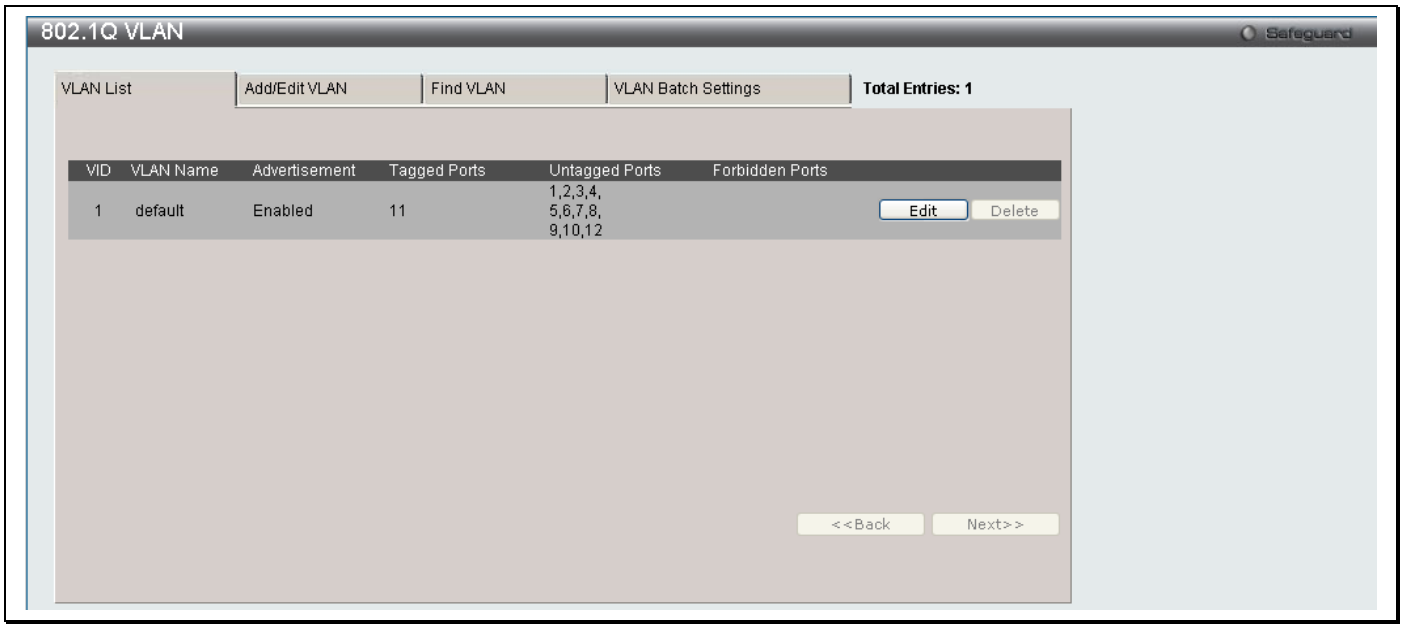


Figure 125. Current 802.1Q Static VLANs Entries menu

To create a new 802.1Q VLAN entry or edit an existing one, click the **Add/Edit VLAN** tab at the top of the **802.1Q VLAN** window. A new window will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.

NOTE: After all IP interfaces are set for your configurations, VLANs on the switch can be routed without any additional steps.

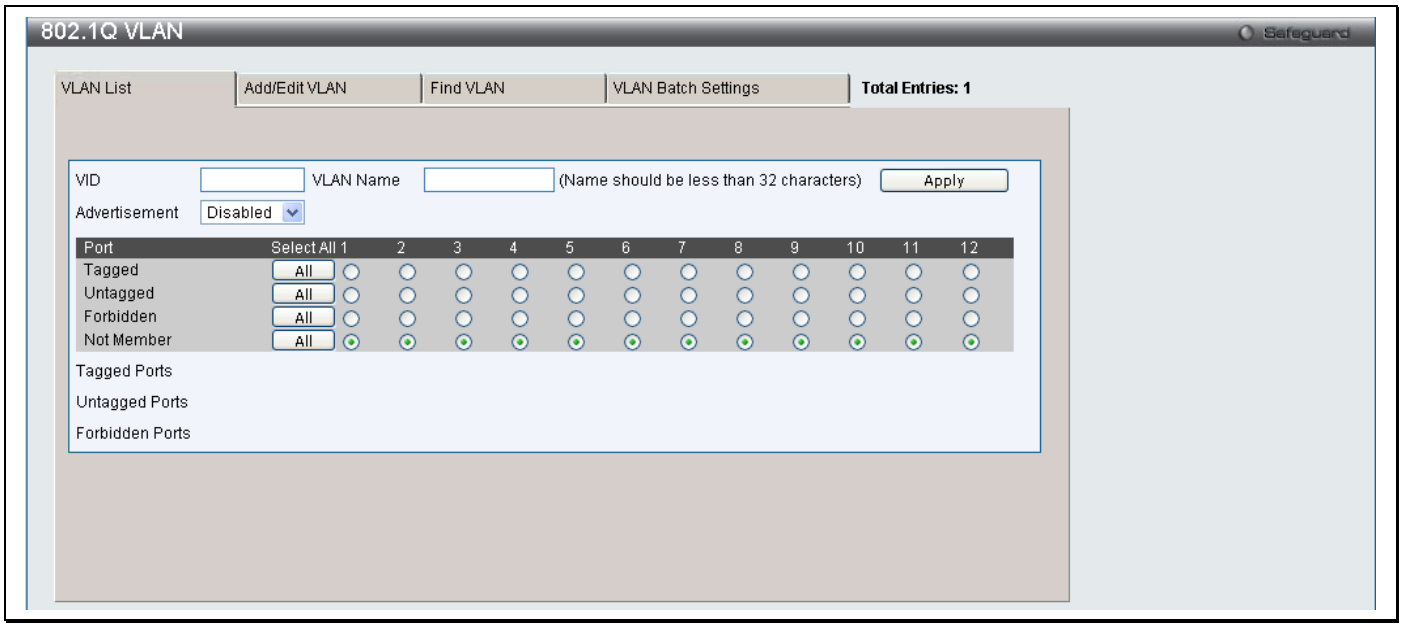


Figure 126. 802.1Q VLAN menu – Add/Edit VLAN Tab

To return to the **802.1Q VLAN** window, click the **VLAN List** Tab at the top of the window. To change an existing 802.1Q VLAN entry, click the corresponding **Edit** button. A new window will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

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

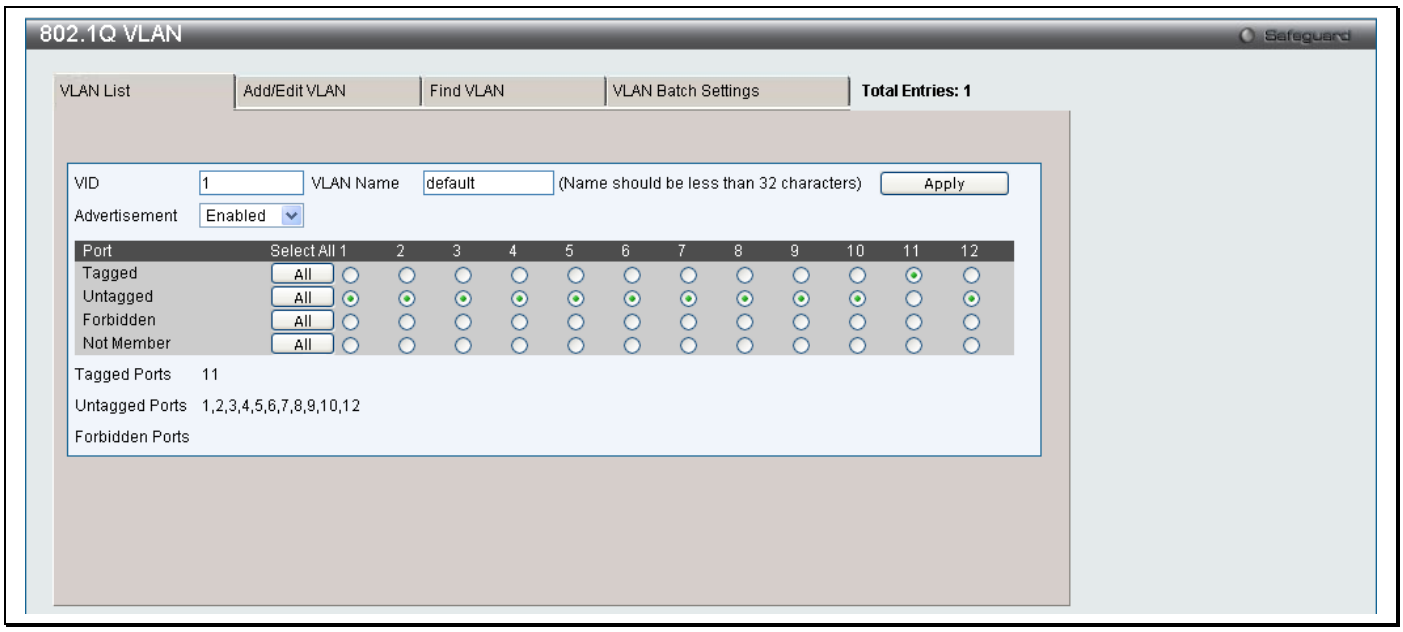


Figure 127. 802.1Q VLAN menu – Edit menu

The following fields can then be set in either the **Add/Edit VLAN** or **Edit** 802.1Q VLAN windows:

Parameter	Description
VID	Allows the entry of a VLAN ID, or displays the VLAN ID of an existing VLAN in the **Edit** window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for a new VLAN, or modifying the VLAN name in the **Edit** window. VLAN Name should be no more than 32 characters in length.
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 Settings	Allows an individual port to be specified as member of a VLAN.
Tagged	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this 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.
Not Member	Allows an individual port to be specified as a non-VLAN member.

Click **Apply** to implement changes made.

To search for a VLAN click the **Find VLAN** tab at the top of the screen which will display the following window, enter a VLAN ID and click **Find** to display the settings for a previously configured VLAN.

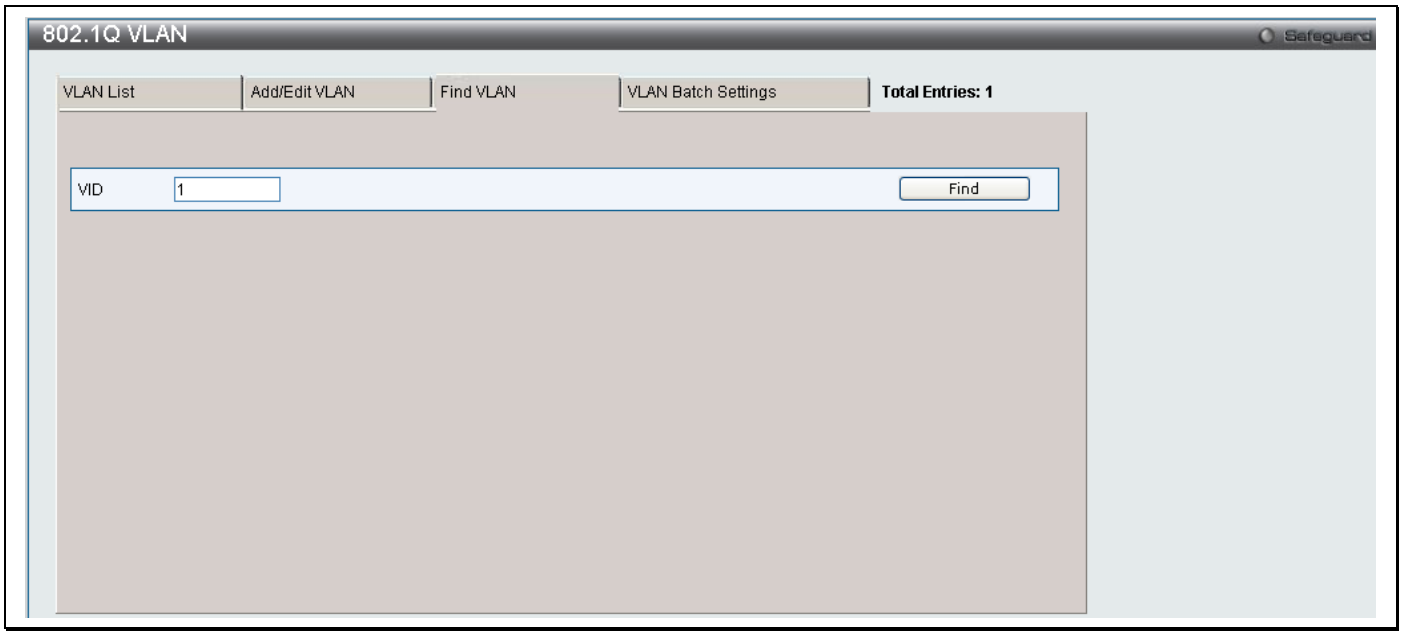


Figure 128. 802.1Q VLAN menu – Find VLAN menu

To create a VLAN Batch entry click the **VLAN Batch Settings** tab at the top of the screen which will display the following window.

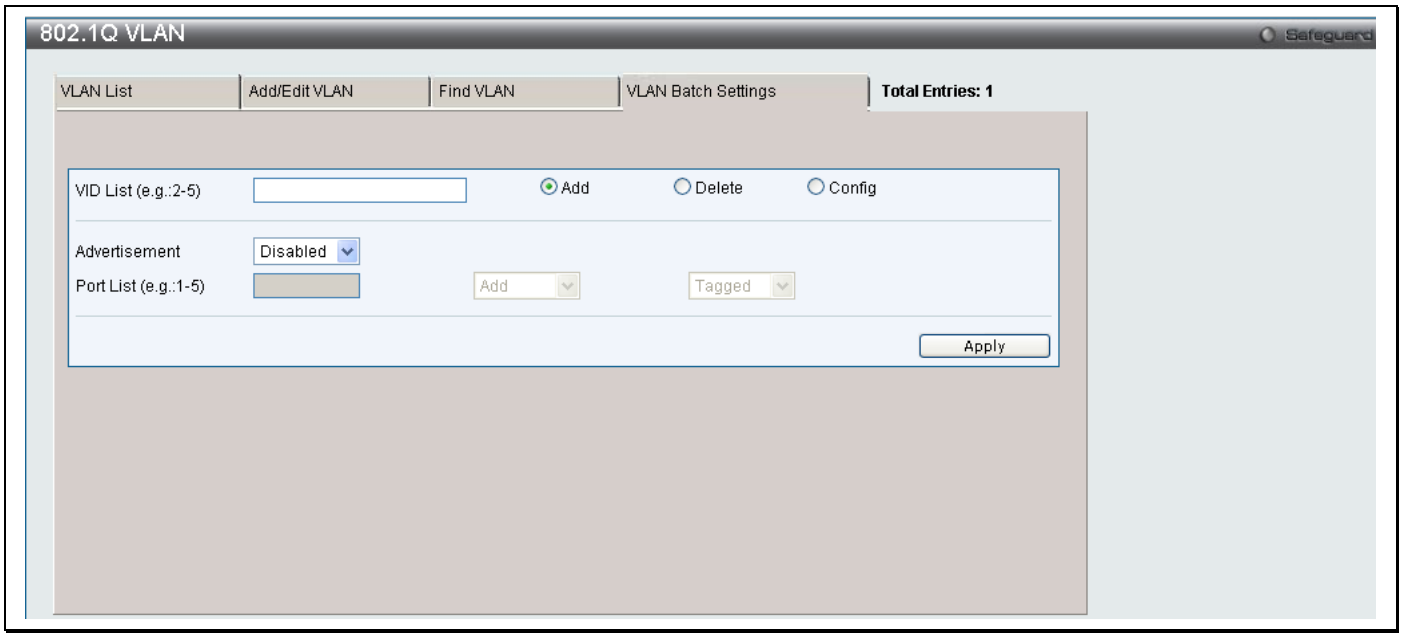


Figure 129. 802.1Q VLAN menu – VLAN Batch Settings menu

The following fields can be set in the **VLAN Batch Settings** windows:

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. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this 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 **Apply** to implement changes made.

802.1v Protocol VLAN

802.1v Protocol Group Settings

The table allows the user to create Protocol VLAN groups and add protocols to that group. The 802.1v Protocol VLAN Group Settings supports 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 this window, click **Switch Configuration > 802.1v Protocol VLAN > 802.1v Protocol Group Settings** as shown below:

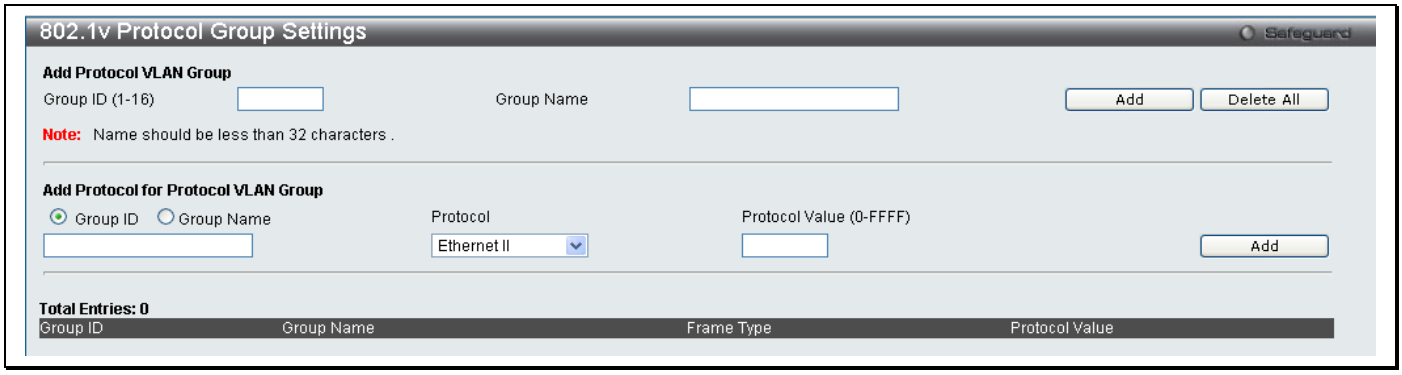


Figure 130. 802.1v Protocol Group Settings menu

The following fields can be set:

Parameter	Description
Group ID	Select an ID number for the group, between *1* and *16.*
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 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.

Click **Add** to make a new entry and **Delete All** to remove an entry.

802.1v Protocol VLAN Settings

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

To view this window, click **Switch Configuration > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings** as shown below:

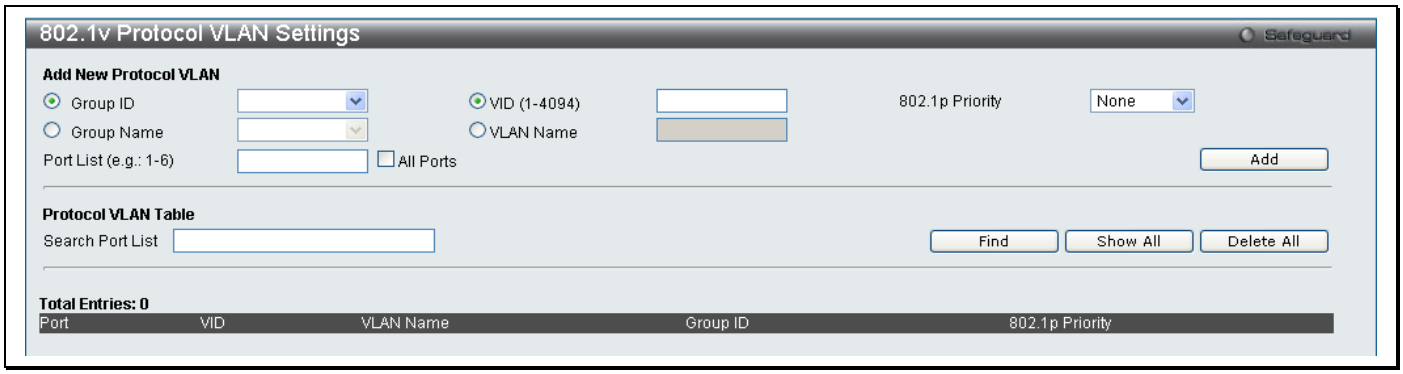


Figure 131. Protocol VLAN Settings menu

The following fields can be set:

Parameter	Description
Group ID	Click the corresponding radio button to select a previously configured Group ID from the drop-down menu.
Group Name	Click the corresponding radio button to select a previously configured Group Name from the drop-down menu.
VID (1-4094)	Click the radio button to enter the VID. This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to create.
VLAN Name	Click the radio button to enter a 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 (e.g.: 1-6)	Select the specified ports you wish to configure by entering the port number in this field, or check the **Select All Ports** 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. To search for a port list enter the port number you wish to view and click **Find**. To display all previously configured port lists on the bottom half of the screen click the **Show All** button, to clear all previously configured lists click the **Delete All** button.

Section 10

Security

Safeguard Engine

Trusted Host

Port Security

MAC Spoofing Access

Authentication Control

Safeguard Engine

Periodically, malicious hosts on the network will attack the switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the Safeguard Engine 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. When the switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an *Exhausted* mode. When in this mode, the switch only receives a small amount of ARP or IP broadcast packets for a calculated time interval. Every five seconds, the switch will check to see if there are too many packets flooding the switch. If the threshold has been crossed, the switch will do a rate limit and only allow a small amount of ARP and IP broadcast packets 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 still only accept a small amount of ARP and IP broadcast packets for double the time of the previous stop period. This doubling of time for stopping ingress ARP and IP broadcast 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, examine the following example of the Safeguard Engine.

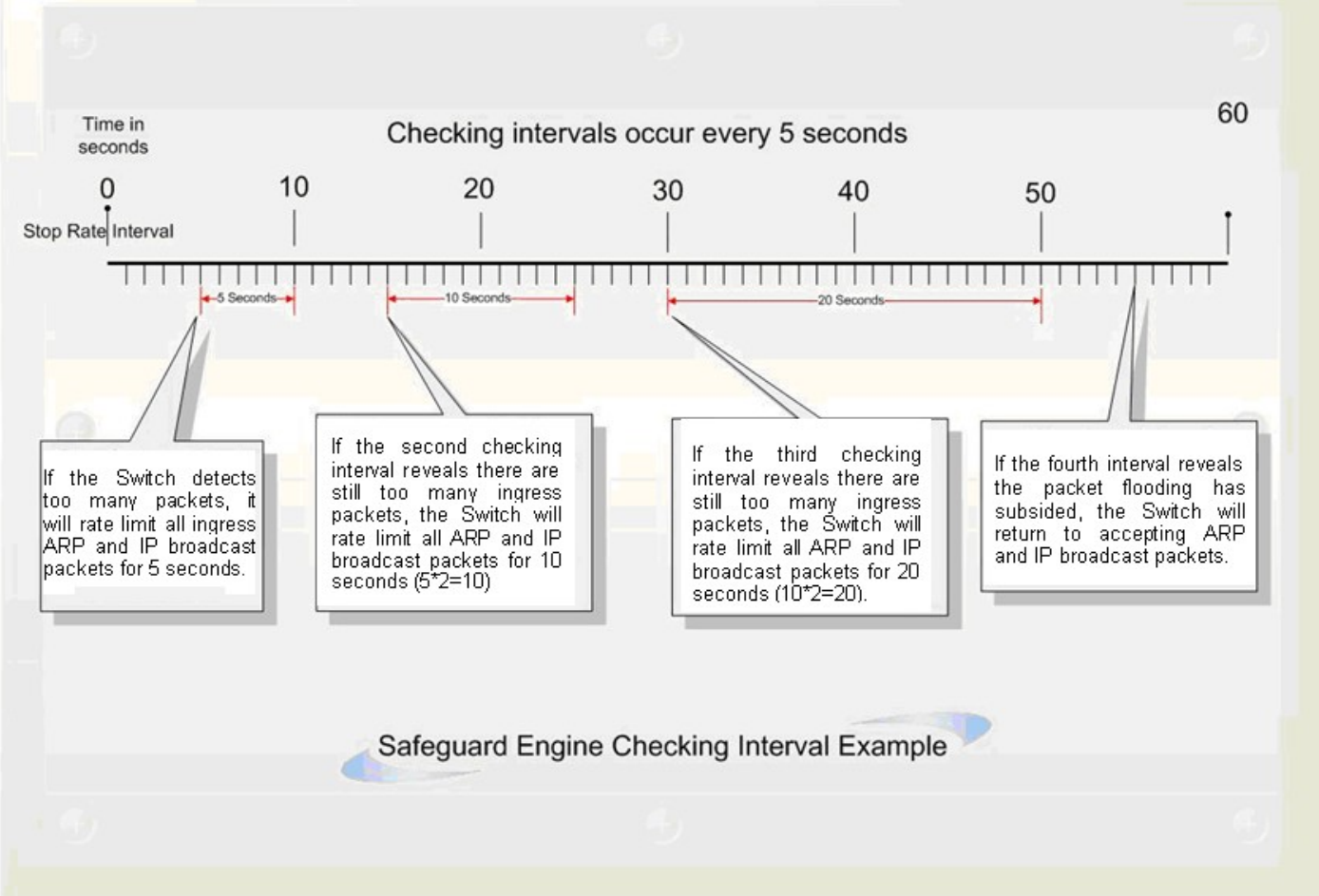


Figure 132. Mapping QoS on the Switch

For every consecutive checking interval that reveals a packet flooding issue, the switch will double the time it will accept a few ingress ARP and IP broadcast packets. 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 limiting ARP and IP broadcast packets will return to 5 seconds and the process will resume.

Once in Exhausted mode, the packet flow will decrease by half of the level that caused the switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.

To view this window, click **Security > Safeguard Engine** as shown below:

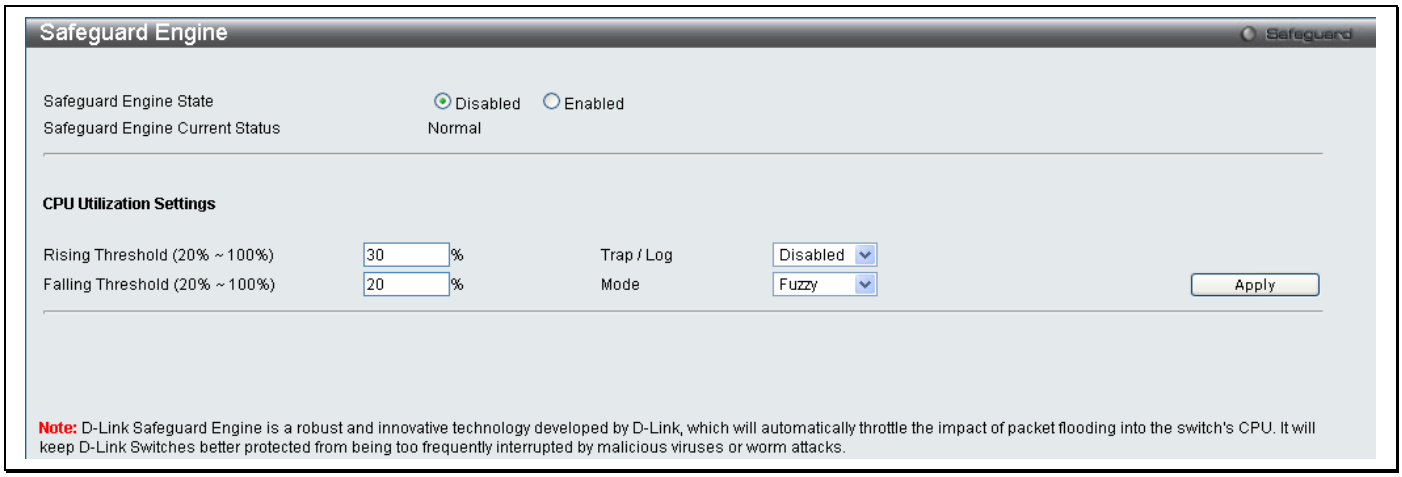


Figure 133. Safeguard Engine menu

To configure the switch's Safeguard Engine, change the State to *Enabled* when the Safeguard Engine is enabled a green light will show on the gray bar at the top of this window, next to Safeguard. To set the Safeguard Engine for the switch, complete the following fields:

Parameter	Description
Rising Threshold	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 the Exhausted state.
Falling Threshold	Used to configure the acceptable level of CPU utilization as a percentage, where the switch leaves the Exhausted 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	Toggle the State field to either *Strict* or *Fuzzy* for the Safeguard Engine of the switch.

Click **Apply** to implement the settings made.

Trusted Host

Use the Security IP Management to permit remote stations to manage the switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address with a proper subnet mask and click the **Add** button.

To view this window, click **Security > Trusted Host** as shown below:

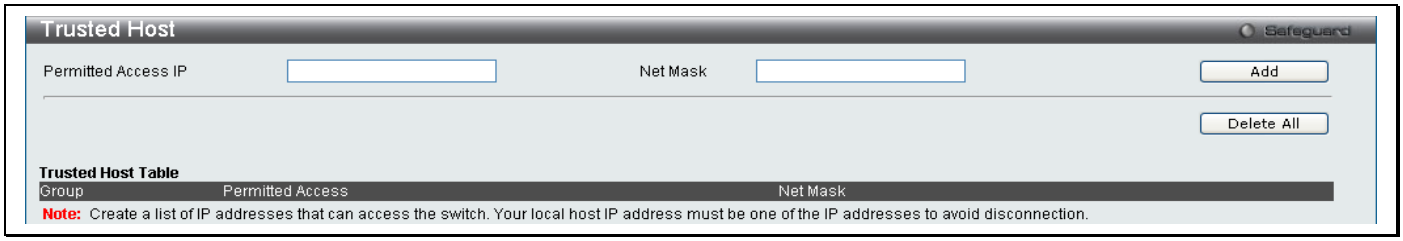


Figure 134. Trusted Host menu

To delete an entry click the corresponding **Delete** button.

Port Security

Port Security Port Settings

A given ports' (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. Setting the **Admin State** pull-down menu to *Enabled*, and clicking **Apply** can lock the port.

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 this window, click **Security > Port Security > Port Security Port Settings** as shown below:

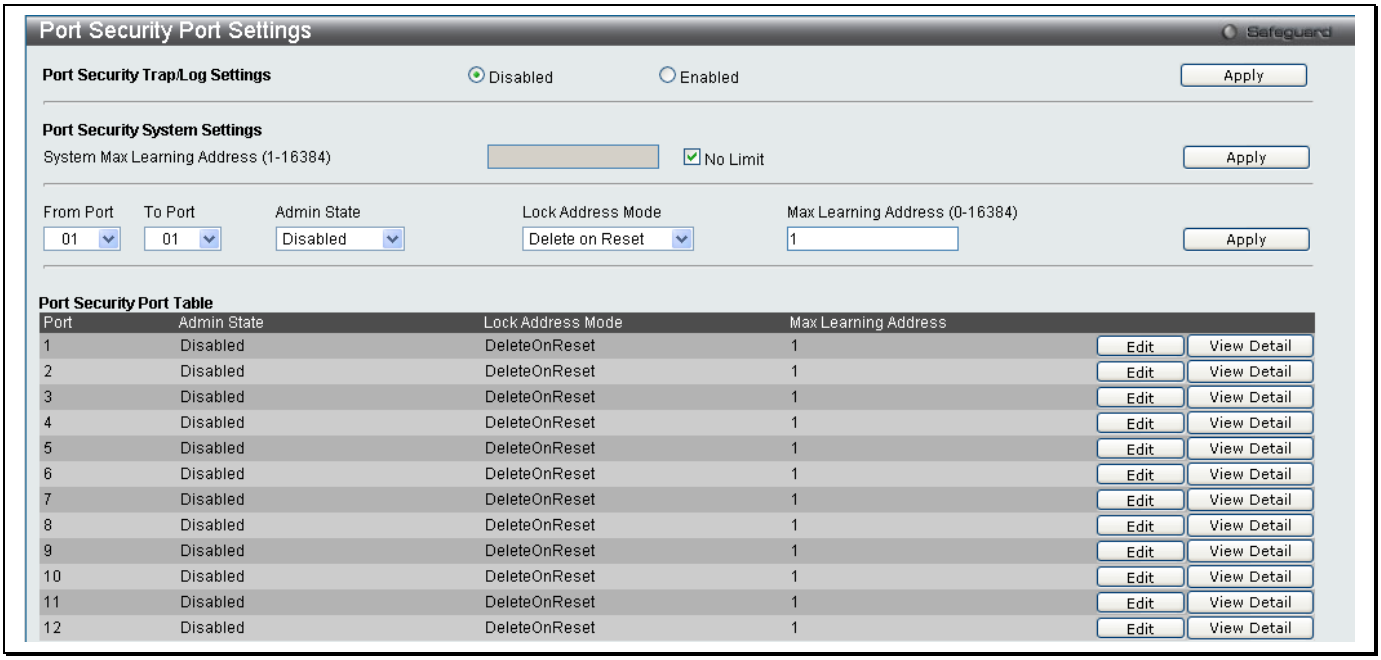


Figure 135. Port Security Port Settings menu

The following parameters can be set:

Parameter	Description
From Port / To Port	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Lock Address Mode	This pull-down menu allows you to select 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 not age out after the aging timer expires. *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.
Max. Learning Address (0-16384)	The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.

Click **Apply** to implement changes made.

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.

Please note that when the user logins to the device successfully through TACACS/XTACACS/TACACS+server or none method, the “user” priviledge level is the only level assigned. If the user wants to get the administration privilege level, the user must use the “enable admin” command to promote his privilege level. However when the user logins to the device successfully through the RADIUS server or through the local method, 3 kinds of privilege levels can be assigned to the user and the user cannot use the “enable admin” command to promote to the admin privilege level.

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.)

Authentication Policy Settings

This command will 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 this window, click **Security > Access Authentication Control > Authentication Policy Settings** as shown below:

Figure 136. Authentication Policy Settings menu

The following parameters can be set:

Parameters	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 **Apply** to implement changes made.

Application Authentication Settings

This window is used to 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 this window, click **Security > Access Authentication Control > Application Authentication Settings** as shown below:

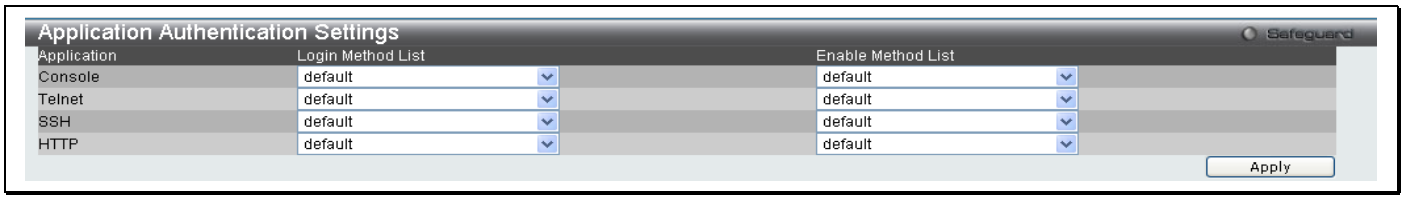


Figure 137. Application's Authentication Settings menu

The following parameters can be set:

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 pull-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** window, in this section, for more information.
Enable Method List	Using the pull-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 **Enable Method Lists** window, in this section, for more information

Click **Apply** to implement changes made.

Authentication Server Group

This window will allow users to 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 three 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 this window, click **Security > Access Authentication Control > Authentication Server Group** as shown below:

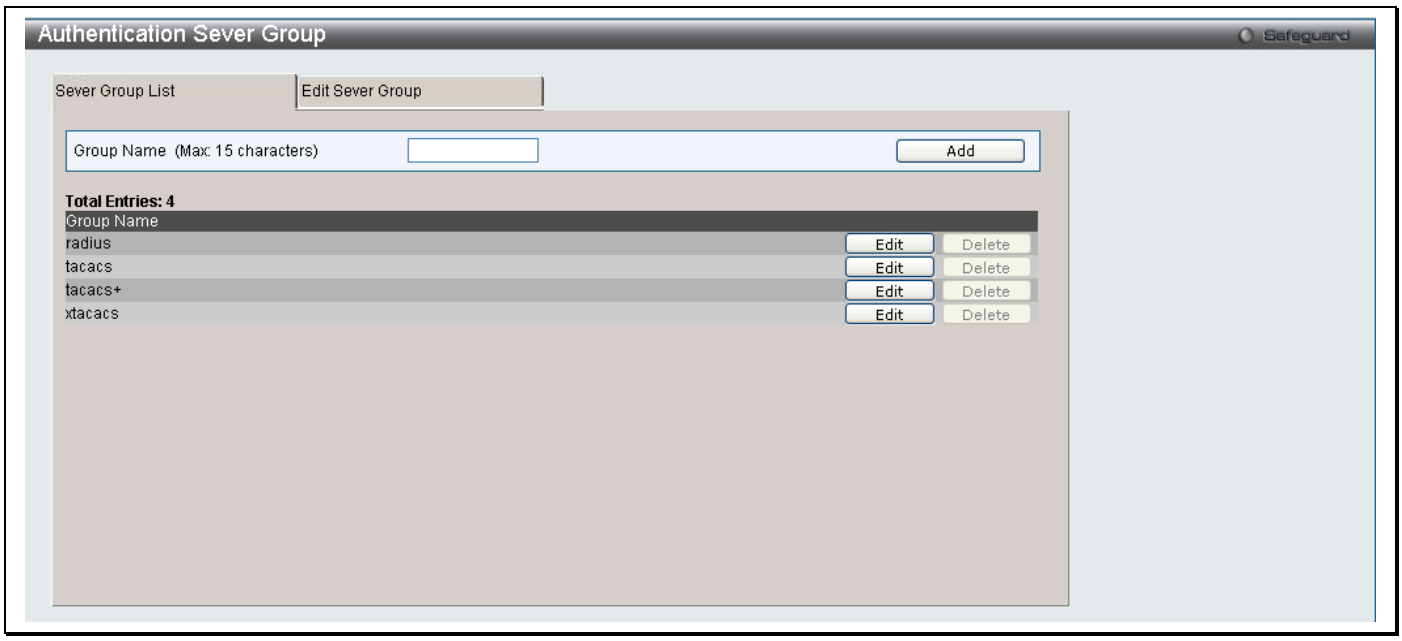


Figure 138. Authentication Server Group Settings menu

The switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click on its corresponding **Edit** button or click the **Edit Server Group** tab at the top of this window, the following screen will be displayed.

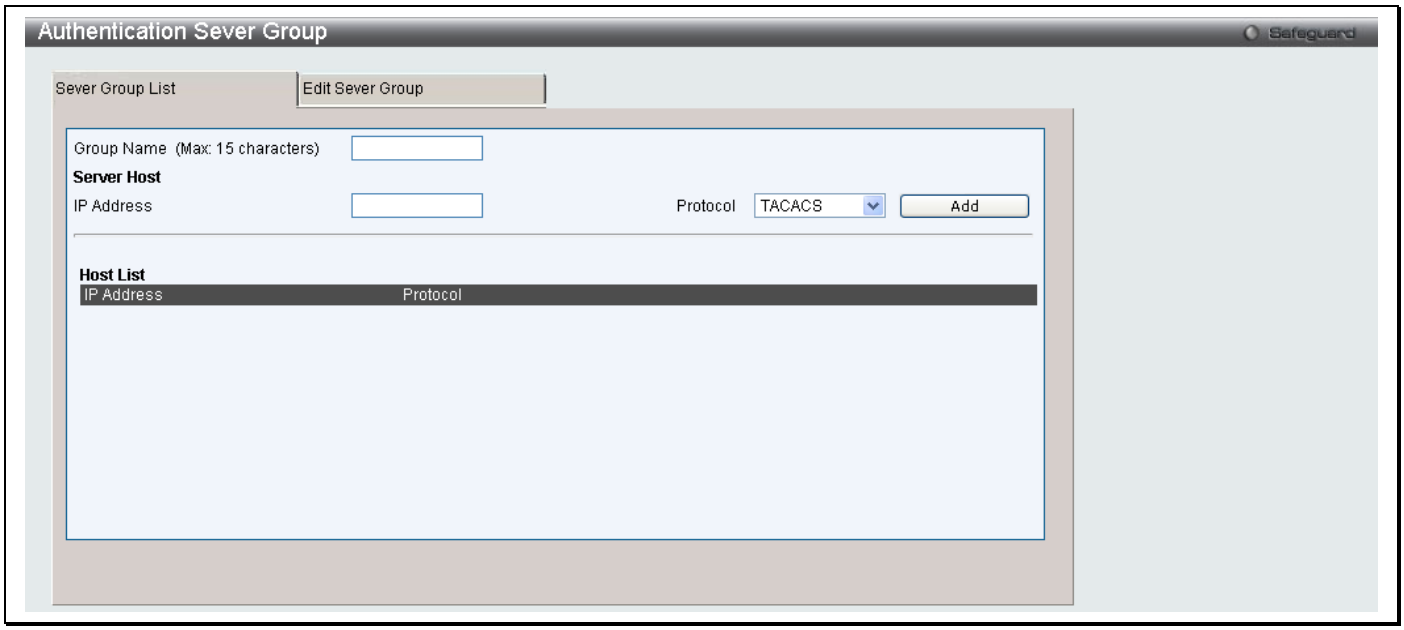


Figure 139. Authentication Server Group Settings Edit menu

To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host and click **Add** to add this Authentication Server Host to the group.

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 four 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

This window will set user-defined Authentication Server Hosts for the TACACS/XTACACS/TACACS+/RADIUS security protocols 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 this window, click **Security > Access Authentication Control > Authentication Server** as shown below:

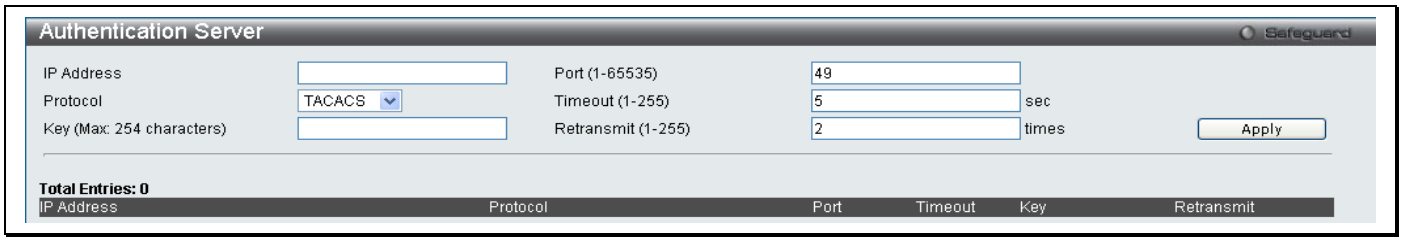


Figure 140. Authentication Server Settings menu

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host the user wishes to add.
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.
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.
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.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.

Click **Apply** to add the server host. Entries will be displayed in the table on the lower half of this window.

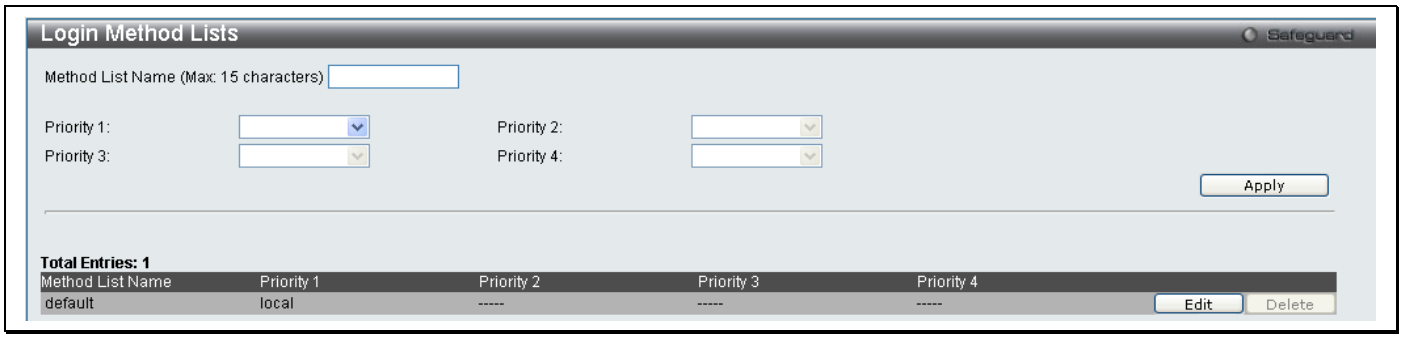
NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other

Login Method Lists

This command will configure a user-defined or default Login Method List of authentication techniques 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 dependant on the local account privilege configured on the switch.

When the user logins to the device successfully through TACACS/XTACACS/TACACS+server or none method, the “user” privilege level is assigned only. If the user wants to get admin privilege level, the user must use the **Enable Admin** window to promote his privilege level. (See the Enable Admin part of this section for more detailed information.) But when the user logins to the device successfully through RADIUS server or local method, 3 kinds of privilege levels can be assigned to the user and the user cannot use the **Enable Admin** window to promote to admin privilege level.

To view this window, click **Security > Access Authentication Control > Login Method Lists** as shown below:



5 - Login Method Lists menu

The switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the corressponding **Delete** button. To modify a Login Method List, click on its corresponding **Edit** button.

To define a Login Method List, set the following parameters and click **Apply**:

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. *server_group* – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch. *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 to access the switch.

Enable Method Lists

The **Enable Method List Settings** window is used to 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 table, click **Security > Access Authentication Control > Enable Method Lists** as shown below:

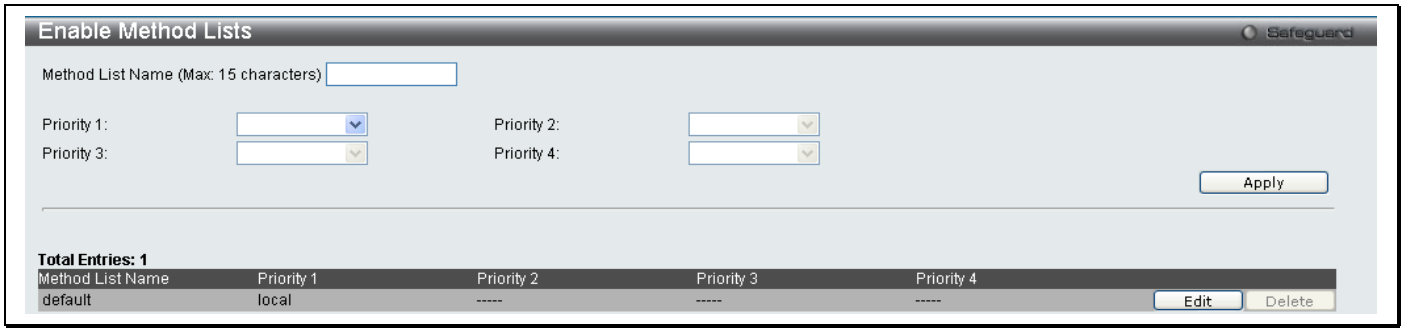


Figure 141. Enable Method List menu

To delete an Enable Method List defined by the user, click the correspoinding **Delete** button. To modify an Enable Method List, click its corresponding **Edit** button.

To define an Enable Login Method List, set the following parameters and click **Apply**:

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 user in the next section entitled Local Enable Password must set the local enable password. *none* – Adding this parameter will require no authentication 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. server_group – Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the switch.

Local Enable Password Settings

This window will configure the locally enabled password for the Enable Admin command. 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 this window, click **Security > Access Authentication Control > Local Enable Password Settings** as shown below:

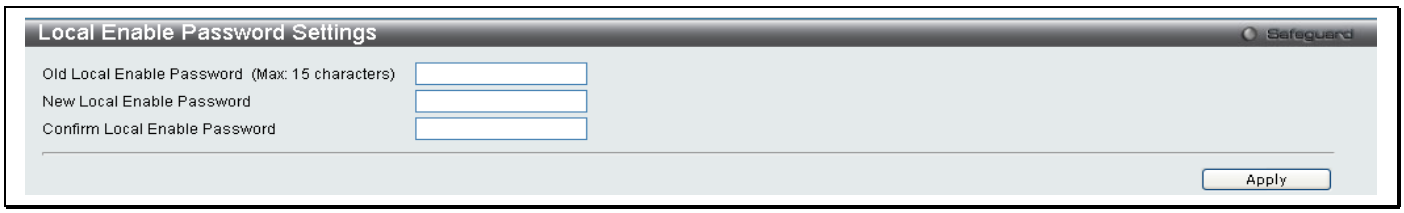


Figure 142. Local Enable Password menu

To set the Local Enable Password, set the following parameters and click **Apply**.

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.

If the user has configured the user privilege attribute of the RADIUS server (for example, User A has “Admin” privilege) and the login is successful, the device will assign the correct privilege level (according to the RADIUS server) to the user. However, if the user does not configure the user privilege attribute and logs in successfully, the device will assign “User” privilege to this user.

RADIUS Accounting Settings

The **Accounting** feature of the switch uses a remote RADIUS server to collect information regarding events occurring on the switch. The following is a list of information that will be sent to the RADIUS server when an event triggers the switch to send these informational packets.

- Account Session ID
- Account Status Type
- Account Terminate Cause
- Account Authentication
- Account Delay Time
- Account Session Time
- Username
- Service Type
- NAS IP Address
- NAS Identifier
- Calling Station ID

There are three types of Accounting that can be enabled on the switch.

Network – When enabled, the switch will send informational packets to a remote RADIUS server when network 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.

Remember, this feature will not work properly unless a RADIUS Server has first been configured. This RADIUS server will format, store and manage the information collected here.

To view this window, click **Security > Access Authentication Control > RADIUS Accounting Settings** as shown below:

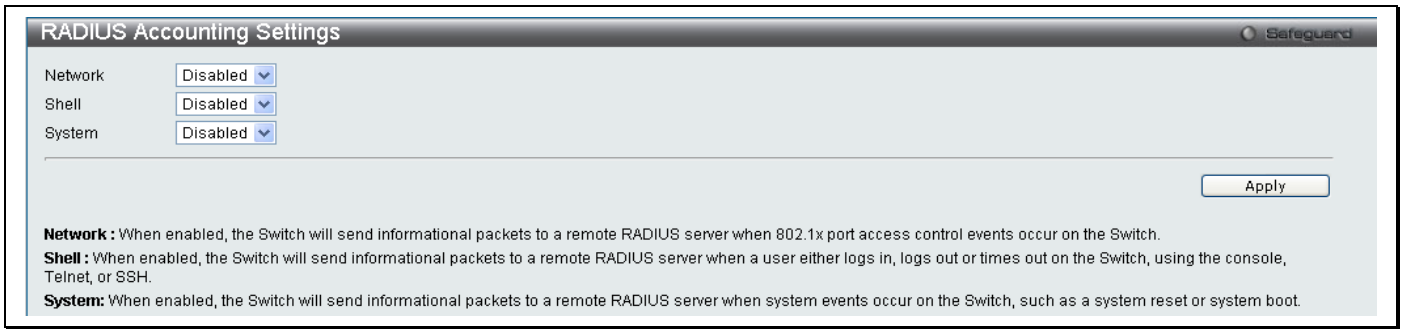


Figure 143. RADIUS Accounting Settings menu

Section 11

CPE Management

The following menus are used for configuration of features for CPE (Customer Premises Equipment) devices connected to VDSL lines of the switch. Each CPE is equipped with four Ethernet ports that can be configured individually here for VLAN settings, QoS and Speed.

CPE Basic Information

To view the CPE Basic Information menu, click **CPE Management > CPE Basic Information**.

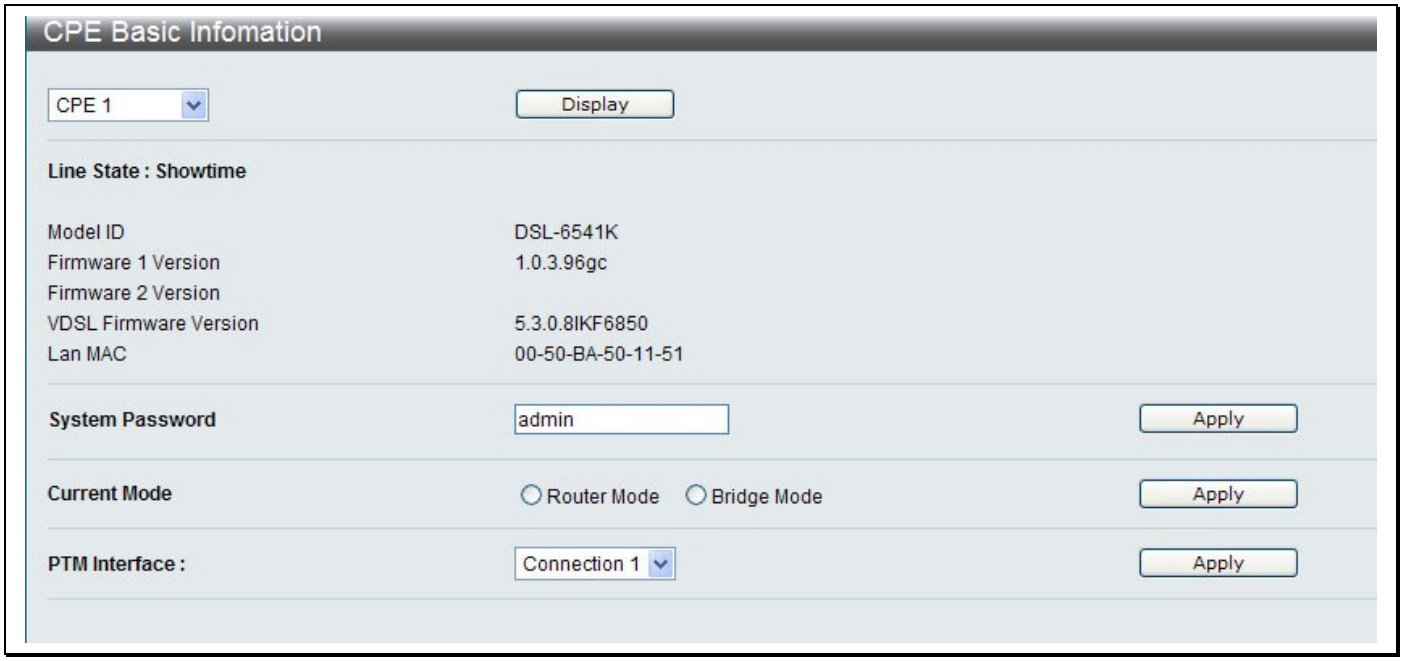


Figure 144. CPE Basic Information menu

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The status of the line is displayed along with basic device information including the model, firmware version, MAC address and VDSL firmware version. The following parameters are configured in the **CPE Basic Information** menu:

Parameter	Description
System Password	Enter a password used for the CPE administrator and click on the **Apply** button.
Current Mode	Choose to operate CPE in **Router** or **Bridge Mode**, click on **Apply**.
PTM Interface	Select the PTM connection (if applicable) on which to apply the settings and click on **Apply**.

Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

Where are these settings stored?

CPE Advanced Information

To view the CPE Advanced Information menu, click **CPE Management > CPE Advanced Information**.

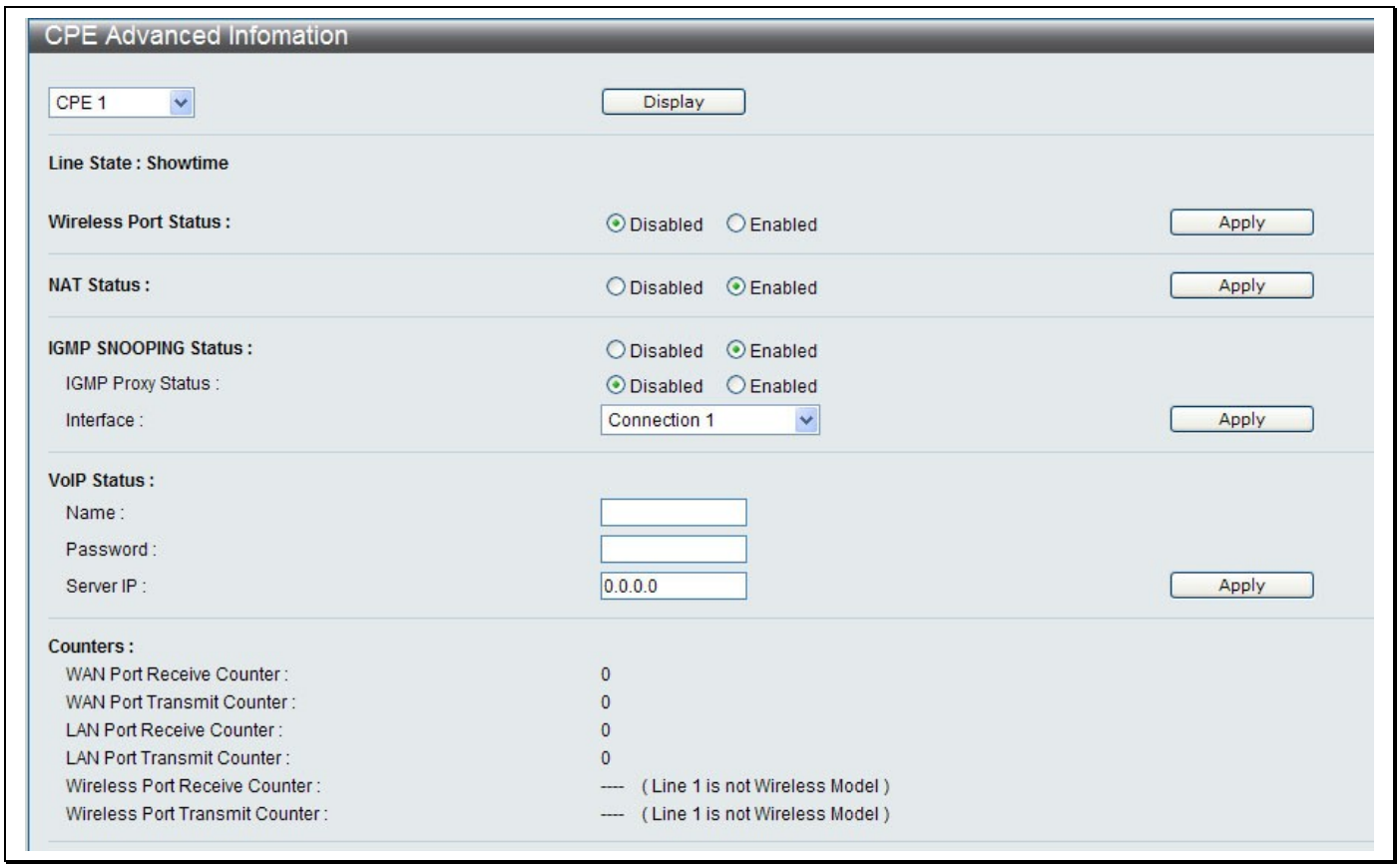


Figure 145. CPE Advanced Information menu

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The status of the line is displayed along with packet counters for the WAN, LAN and Wireless interfaces. The following parameters are configured in the **CPE Advanced Information** menu:

Parameter	Description
Wireless Port Status	Choose to enable or disable the wireless interface (if applicable) and click on the **Apply** button. Default = **Disabled**
NAT Status	Choose to enable or disable NAT for the CPE and click on **Apply**. Default = **Enabled**
IGMP Snooping Status	Choose the Connection to which the IGMP Snooping settings are applied, then choose enable or disable IGMP Snooping (default = **Enabled**). Additionally an IGMP Proxy can be enabled or disabled (default = **Disabled**).
VoIP Status	Enter VoIP account settings including **Name** and **Password**. Enter the VoIP **Sever IP** address and click on **Apply**.

Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

CPE WAN Settings

To view the CPE WAN Settings menu, click **CPE Management > CPE WAN Settings**.

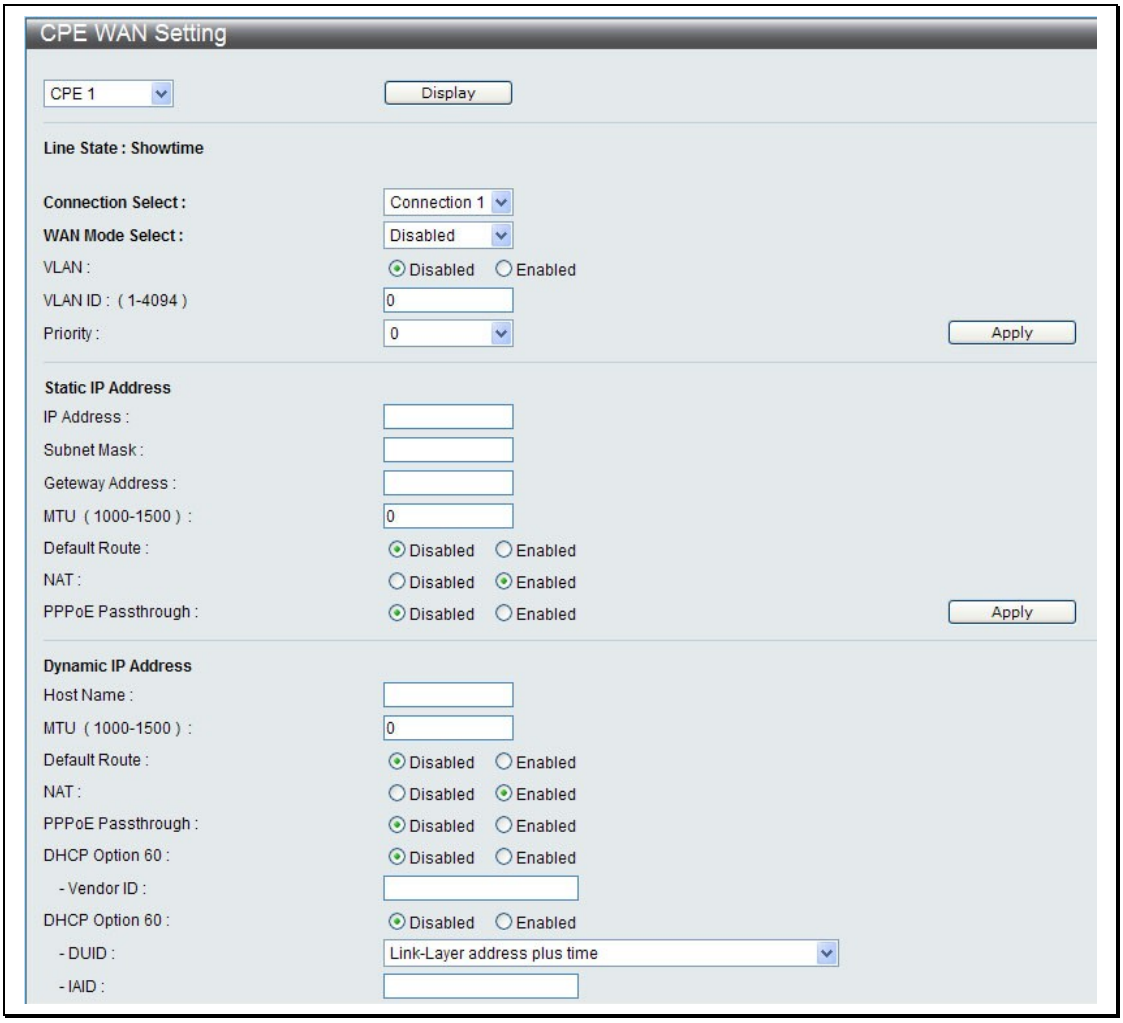


Figure 146. CPE WAN Settings

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The status of the line is displayed. The settings are dvided into three sections for configuring **Connection / WAN Mode / VLAN / Priority** settings, **Static IP** settings and **Dynamic IP** settings. Use the **WAN Mode Select** pull-down menu to choose the WAN settings for the selected CPE connection. Enter an MTU value and click on the **Apply** button. **Static** or **Dynamic** WAN connections require further configuration in the menus provided.

The following parameters are configured in the **CPE WAN Settings** menu:

Parameter	Description
Connection / WAN Mode / VLAN / Priority settings	Use the Connection Select menu to choose the CPE connection to which the settings are applied. Use the **WAN Mode Select** pull-down menu to choose the WAN settings for the selected CPE connection. Enter an MTU value and click on the **Apply** button. For Static connections, continue to configure **Static IP Address** settings in the menu below.
Static IP settings	Configure Static IP Address settings including **Static IP Address**, **Subent Mask** and **Gateway IP Address**. Enter an MTU value from 1000 to 1500. Other options include to enable or disable **NAT**, **Default Route** and **PPPoE Passthrough**. Click **Apply** to set the configuration.
Dynamic IP settings	Configure Dynamic IP Address settings including **Host Name** (optional) and enter an MTU value from 1000 to 1500. Other options include to enable or disable **NAT**, **Default Route** and **PPPoE Passthrough**. Click **Apply** to set the configuration. This menu is also used to configure **DHCP Option 60** settings if applicable.

Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

CPE PPPoE Settings

To view the CPE PPPoE Settings menu, click **CPE Management > CPE Advanced Information**.

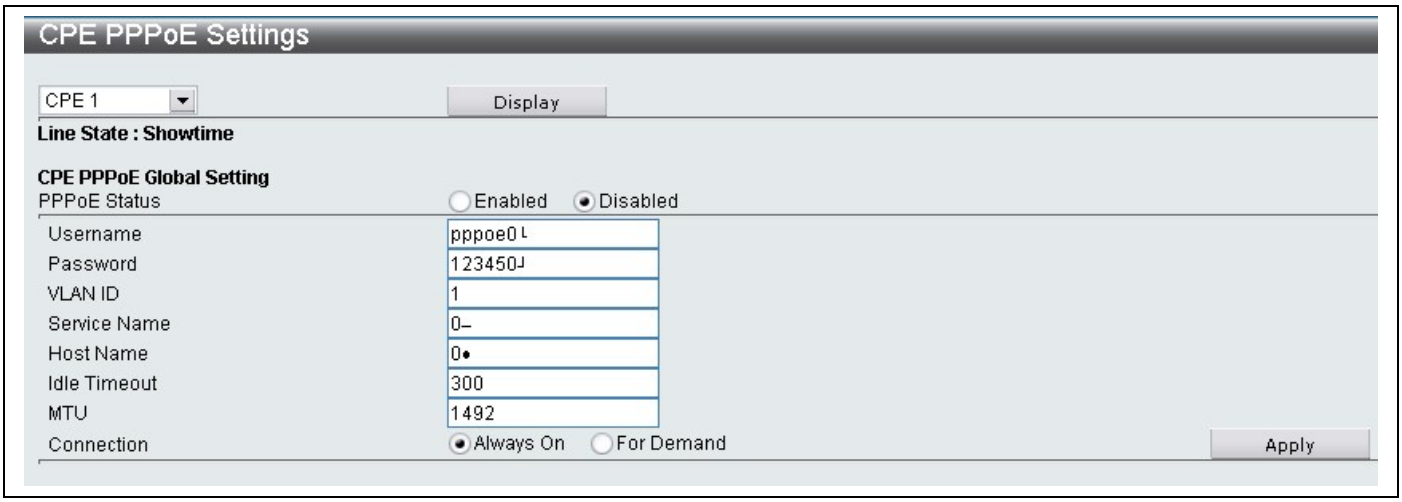


Figure 147. CPE PPPoE Settings menu

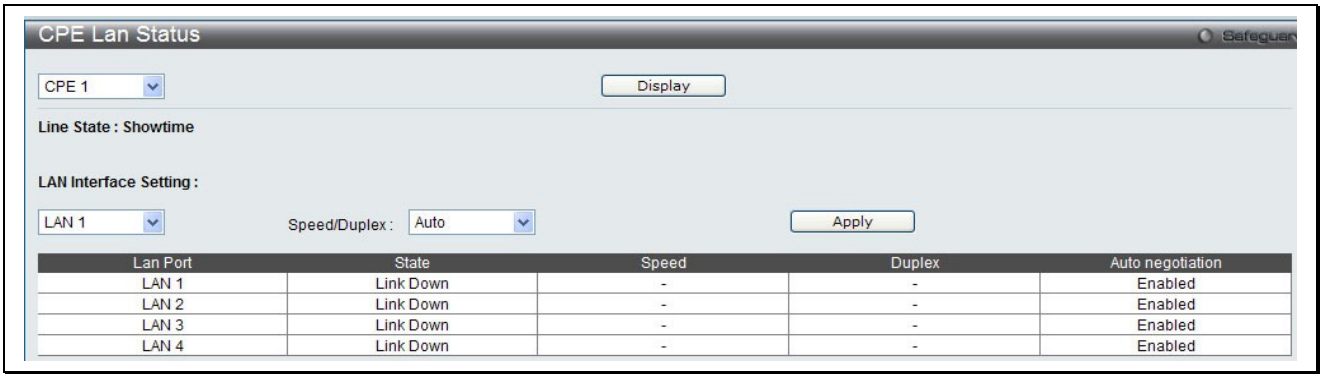
Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The status of the line is displayed. The following parameters are configured in the **CPE PPPoE Settings** menu:

Parameter	Description
Username	Type in the account user name used to establish the PPPoE connection.
Password	Type in the account password used to establish the PPPoE connection.
VLAN ID	Enter the VLAN ID used for the CPE.
Service Name	Enter the Service Name for the PPPoE connection (optional).
Host Name	Enter the Host Name for the PPPoE connection (optional).
Idle Timeout	Enter the amount of time in minutes allowed for the connection to be idle for before disconnecting the PPPoE connection.
MTU	Enter an MTU value (default = 1492).
Connection	Choose **Always On** or **On Demand** connection for PPPoE.

Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

CPE LAN Settings

To view the CPE LAN Settings menu, click **CPE Management > CPE LAN Settings**.



Lan Port	State	Speed	Duplex	Auto negotiation
LAN 1	Link Down	-	-	Enabled
LAN 2	Link Down	-	-	Enabled
LAN 3	Link Down	-	-	Enabled
LAN 4	Link Down	-	-	Enabled

Figure 148. CPE LAN Port Settings

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The status of the line is displayed. Use the menu to change the **Speed** and **Duplex** settings for the Ethernet LAN ports. Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

CPE Server Status

To view the CPE Basic Information menu, click **CPE Management > CPE Server Status**.

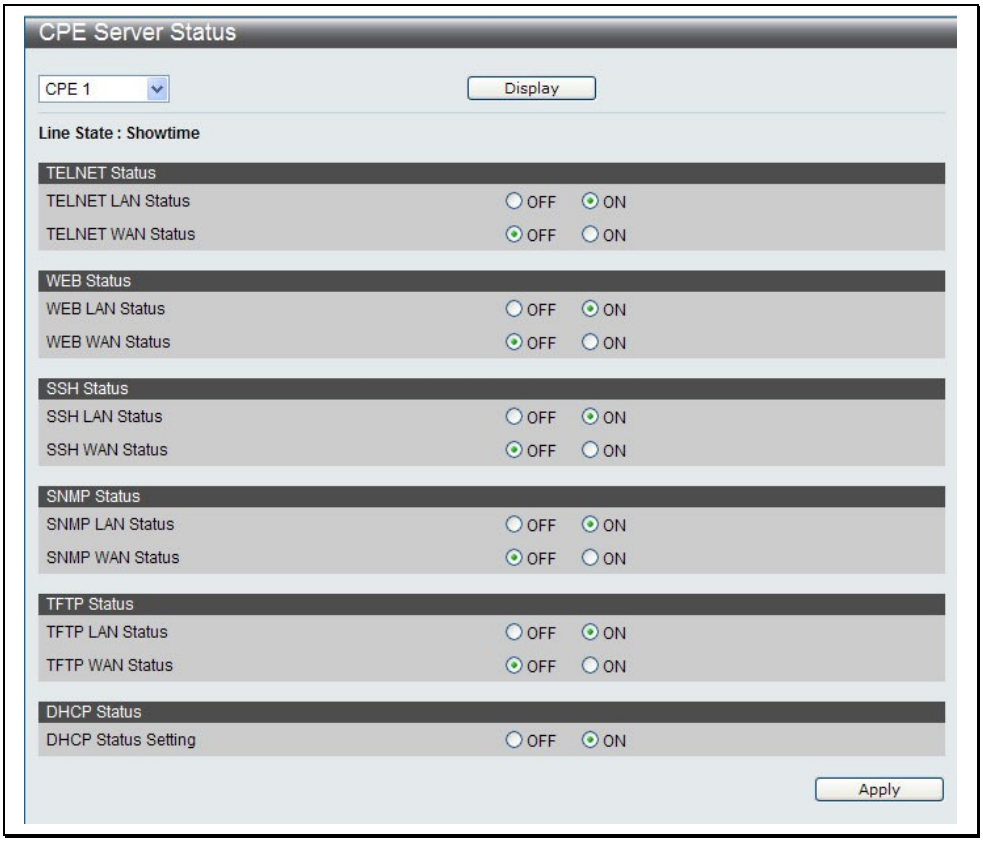


Figure 149. CPE Server Status

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The status of the line is displayed. Use the menu to enable or disable various standard network serices on the LAN and WAN interfaces of the CPE. Services that can be enabled or diabled include Telnet, HTTP Web (UDP/TCP port 80), SSH, SNMP, tftp and DHCP. Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

CPE VLAN Settings

To view the CPE VLAN Settings menu, click **CPE Management > CPE VLAN Settings**.

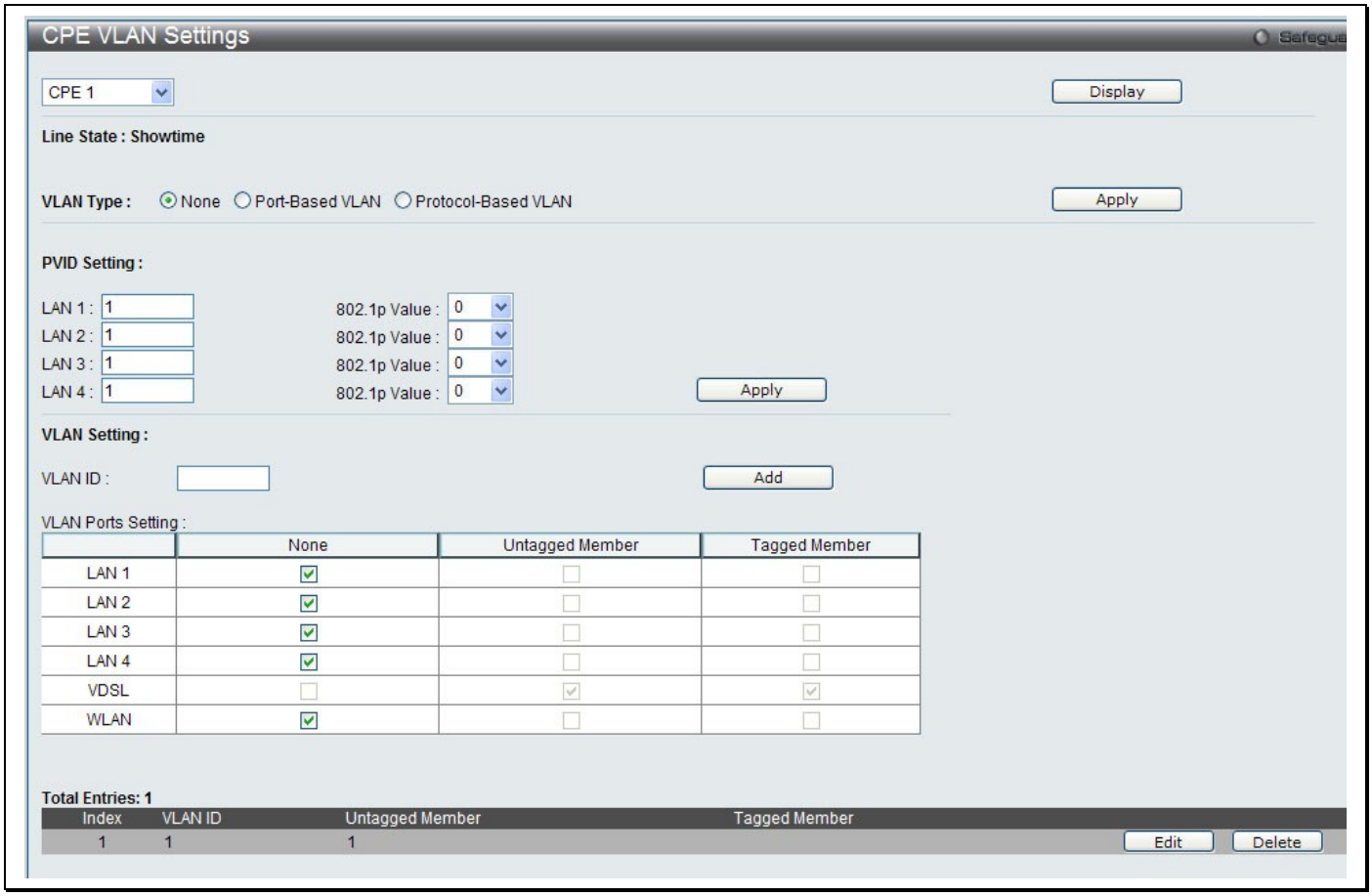


Figure 150. CPE VLAN Settings menu

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The current VLAN configuration, if any, is didplayed in table form at the bottom of the menu. Use the configuration menu on this page to configure port-based VLANs. To configure protocol-based based VLANs click to select the Protocol-Based radio button and click on **Apply**. A new menu appears. See the next section for details about the Protocol-Based VLAN Settings menu. To configure port-based VLAN settings, select the **Port-Based VLAN** radio button, click on **Apply**. and configure the settings visble in this menu. The following parameters are configured in the **CPE VLAN Settings** (port-based VLAN) menu:

Parameter	Description
PVID Setting	Configure the LAN ports for PVID and 802.1p values. Click on **Apply** to save the settings.
VLAN ID	Choose the tagging options for the CPE interfaces, enter the VLAN ID applied and click on the **Add** button. The new entry appears listed in the table below. To change tagging configuration for CPE interfaces that have been configured in the list, click on the **Edit** button, choose Tagged or Untagged options for the interfaces and click the **Apply** button for the configuration.

Click on the **Apply** button to set these configurations in the memory of the switch.

CPE ProtoVLAN Settings

To view the **CPE Protocol VLAN Settings** menu, click **CPE Management > CPE ProtoVLAN Settings**. Any previous configuration for the CPE is listed in the table. To edit an existing configuration, click on the **Edit** button; to remove an existing configuration. Click on the **Delete** buttone.

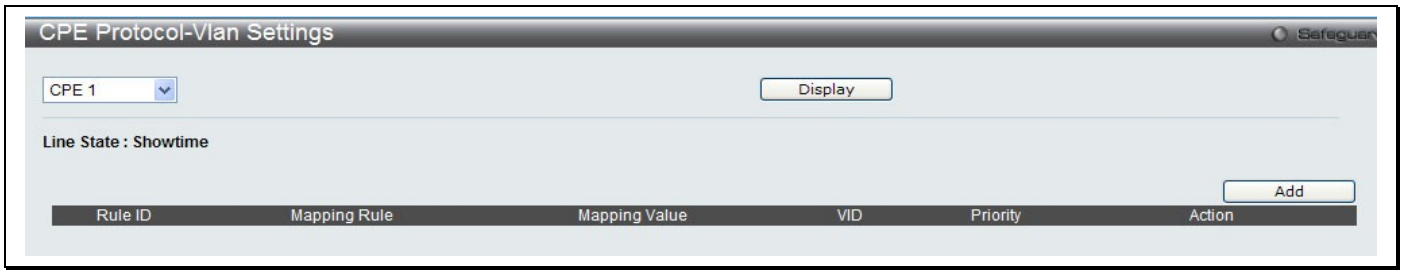


Figure 151. CPE Protocol VLAN Settings table

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. Click the **Add** button to configure settings in a new menu.

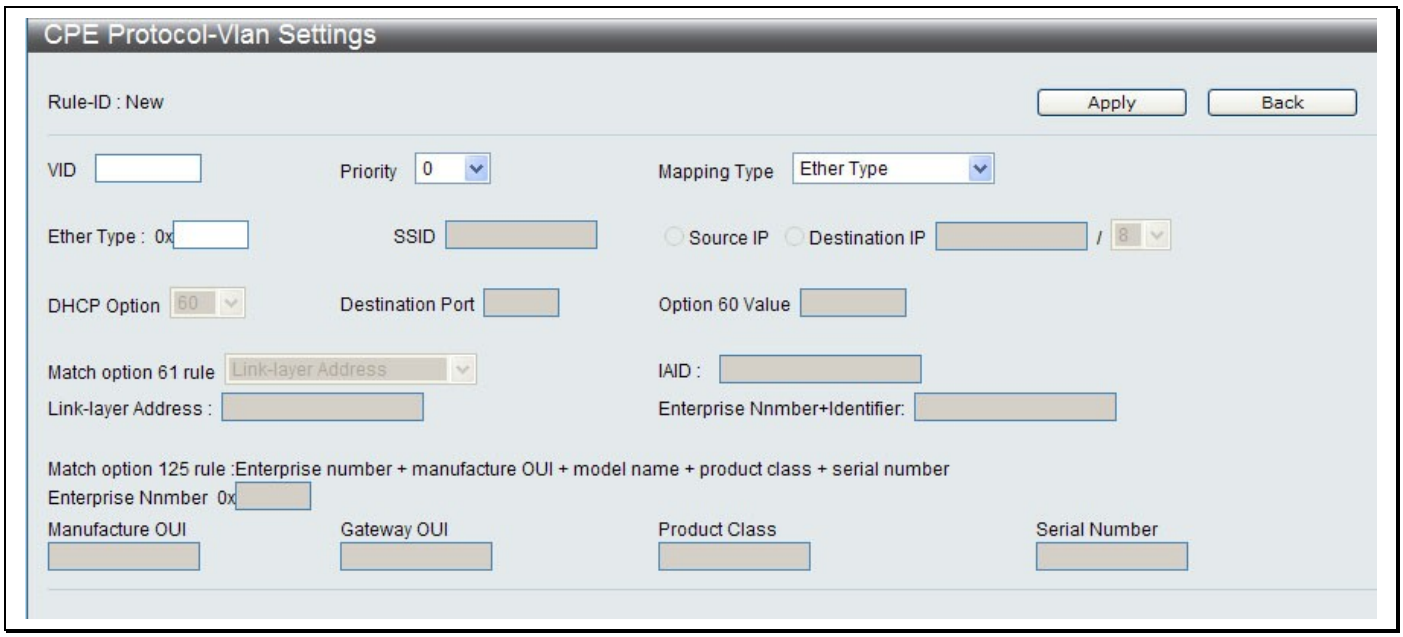


Figure 152. CPE Protocol VLAN configuration menu

Select the Mapping Type used for the Protocol VLAN, the menu options allowed change according to what type of mapping is used. Configure the settings appropriate for the mapping. Click on the **Apply** button for the menu parameter being set to set these configurations in the memory of the switch.

CPE QoS Settings

The following window will allow the user to configure the QoS settings for individual CPE devices attached to the VDSL switch. To view the CPE QoS Settings menu, click **CPE Management > CPE QoS Settings**.

Figure 153. CPE QoS Settings menu

Choose the QoS classification used and click on the **Apply** button.

The **User Define** option requires additional configuration in a new menu.

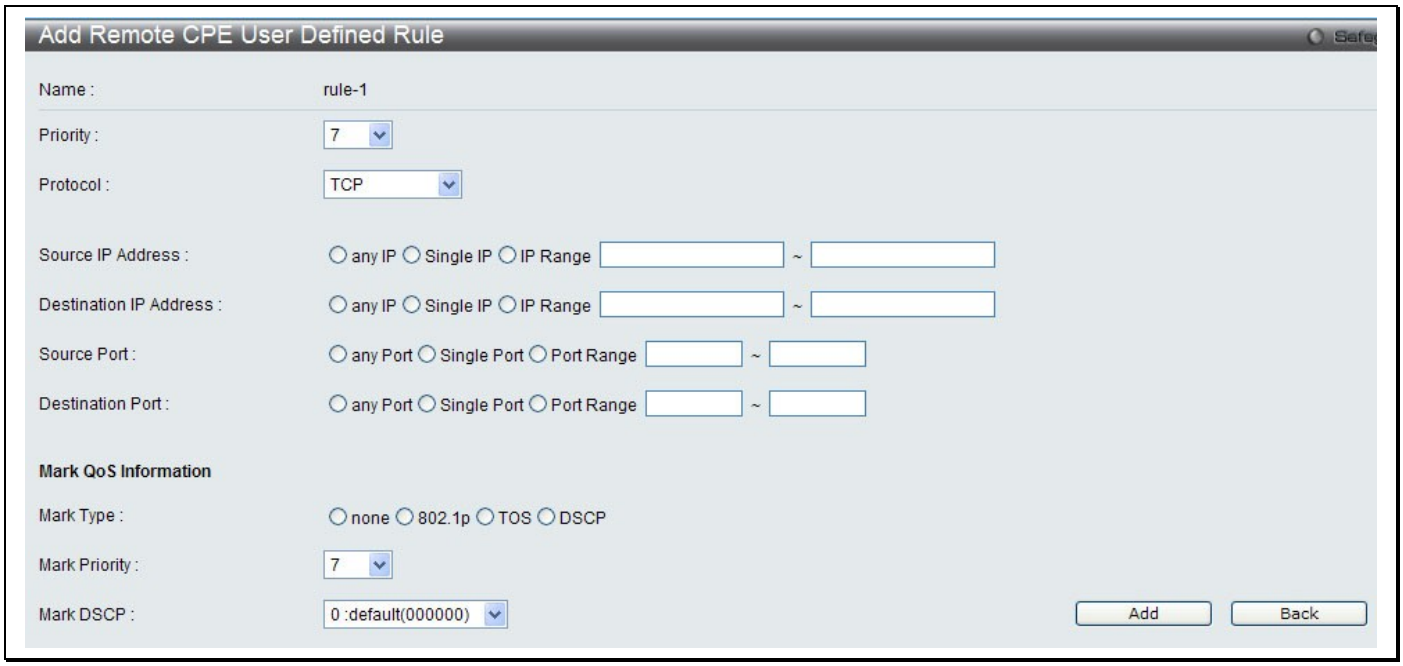


Figure 154. User Define rule configuration for CPE

Configure the **Priority**, **Protocol** and IP source and destination settings. In addition, the **Mark QoS Information** settings can be configured to use **802**.1p, **ToS** or **DSCP**. Click on **Apply** to save the new settings. An new entry appears in the QoS Settings table for the line.

CPE Filter

To view the CPE Filter menu, click **CPE Management > CPE Filter**.

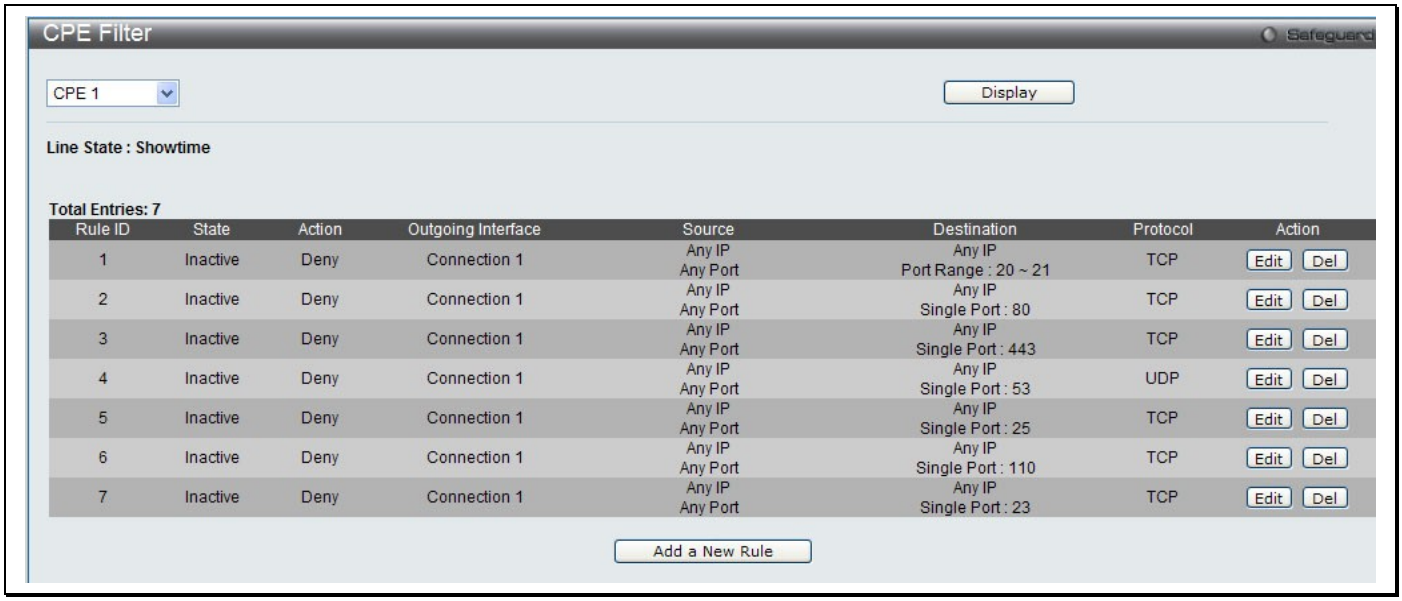


Figure 155. CPE Filter settings menu

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The filter rule table lists existing filter rules. To change a rule, click on the **Edit** button for the rule to change. To remove a filter rule, click on the **Delete** button for that rule. To crate a new filter rule, click on the **Add aNew Rule** button, a new menu appears.

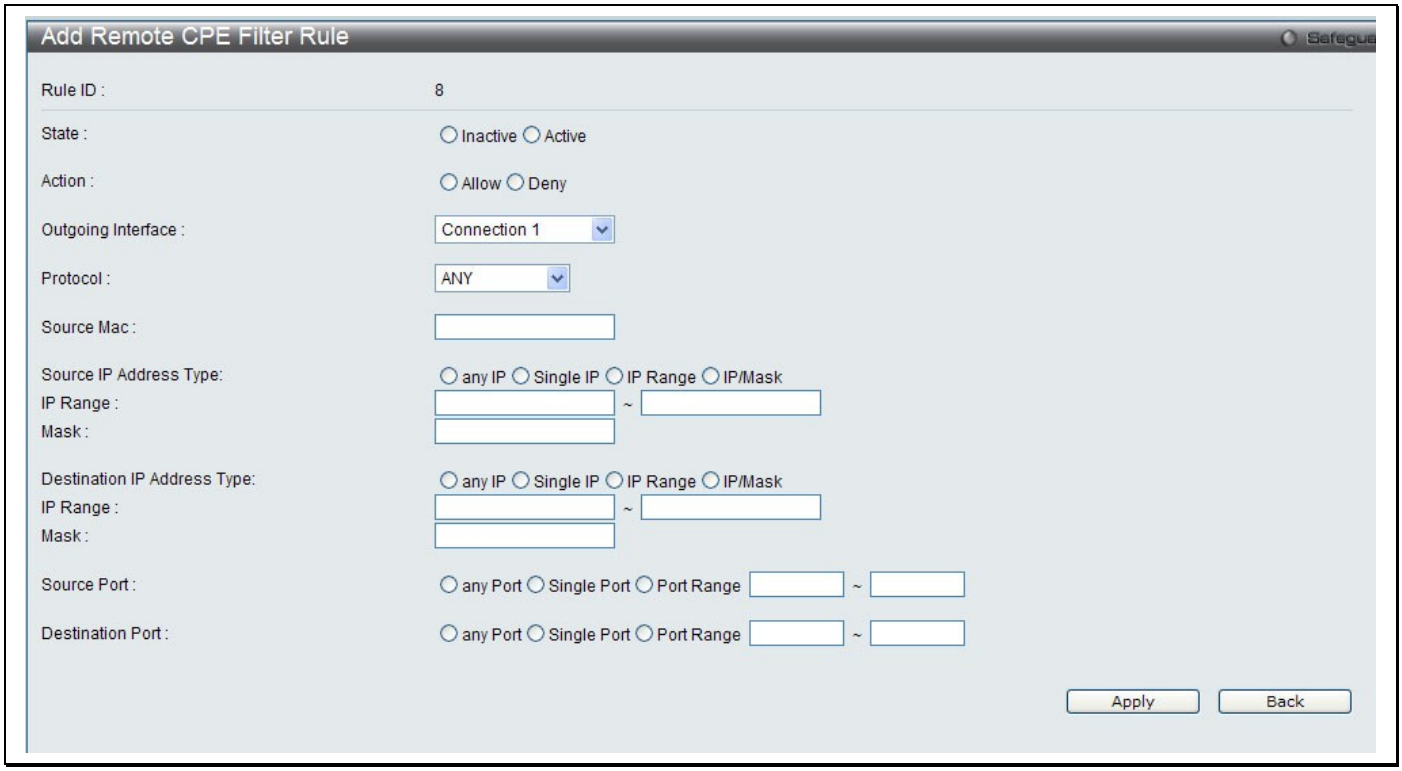
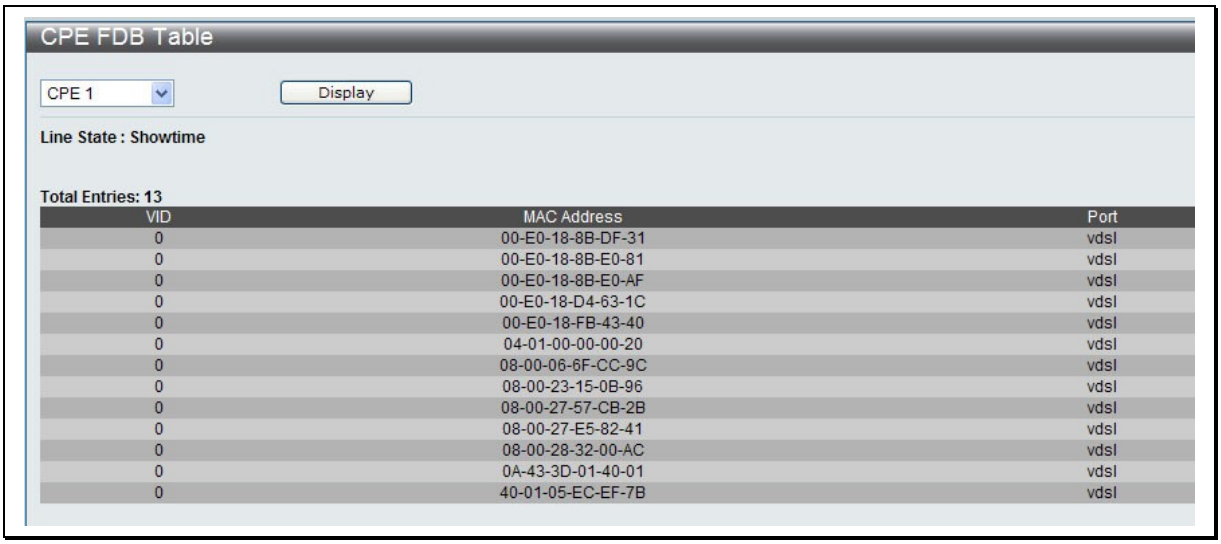


Figure 156. Add Filter Rule for CPE

Use the **State** radio button to make the new rule **Active** or **Inactive**. Choose to **Allow** or **Deny** forwarding according to the rule being created, and configure the conditions used for the filter rule. Click on the **Apply** button to create the new rule, it appears listed in the filter rule table.

CPE FDB

To view the CPE FDB Table, click **CPE Management > CPE FDB**.



VID	MAC Address	Port
0	00-E0-18-8B-DF-31	vdsl
0	00-E0-18-8B-E0-81	vdsl
0	00-E0-18-8B-E0-AF	vdsl
0	00-E0-18-D4-63-1C	vdsl
0	00-E0-18-FB-43-40	vdsl
0	04-01-00-00-00-20	vdsl
0	08-00-06-6F-CC-9C	vdsl
0	08-00-23-15-0B-96	vdsl
0	08-00-27-57-CB-2B	vdsl
0	08-00-27-E5-82-41	vdsl
0	08-00-28-32-00-AC	vdsl
0	0A-43-3D-01-40-01	vdsl
0	40-01-05-EC-EF-7B	vdsl

Figure 157. CPE FDB Table

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. The read-only table lists all dynamic MAC address entries in the CPE forwarding database with the VID and Port information.

CPE CFM

To view the CPE CFM Setting menu, click **CPE Management > CPE CFM**.

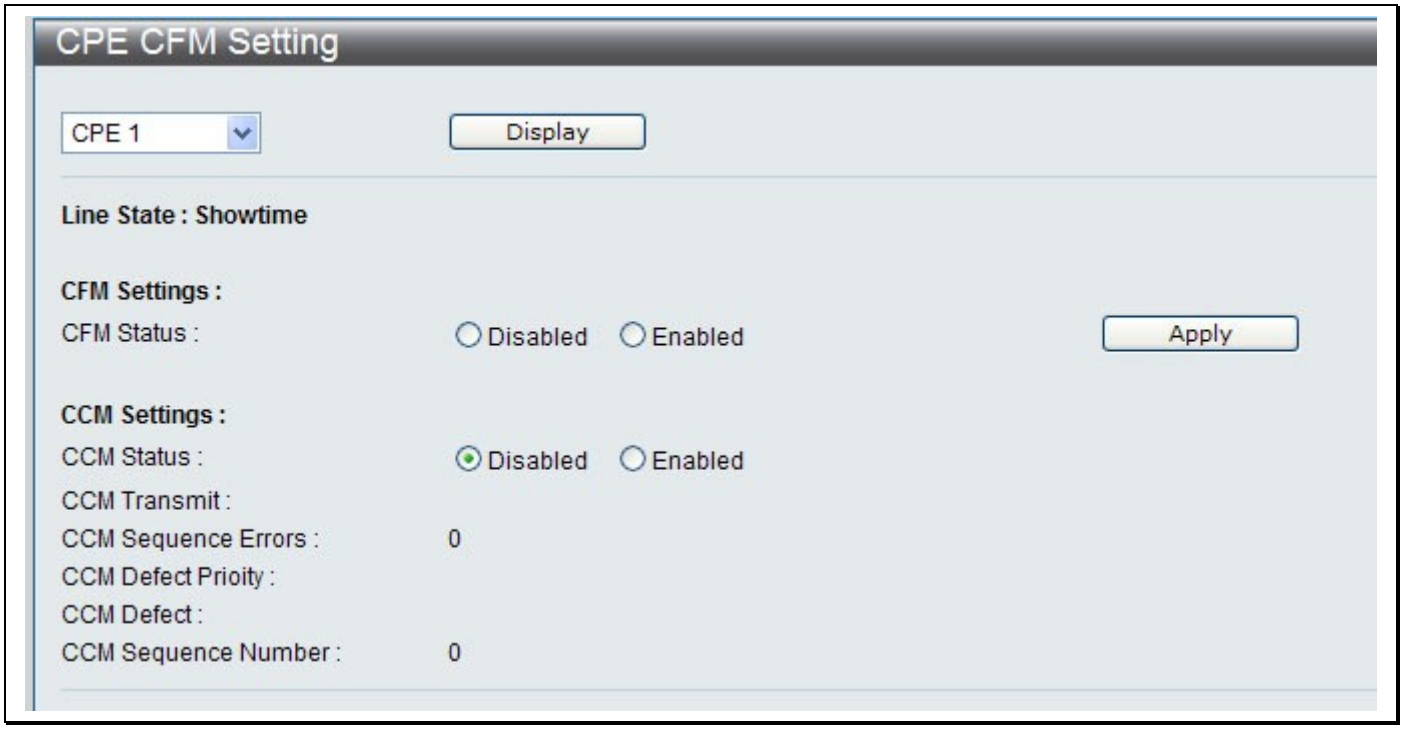
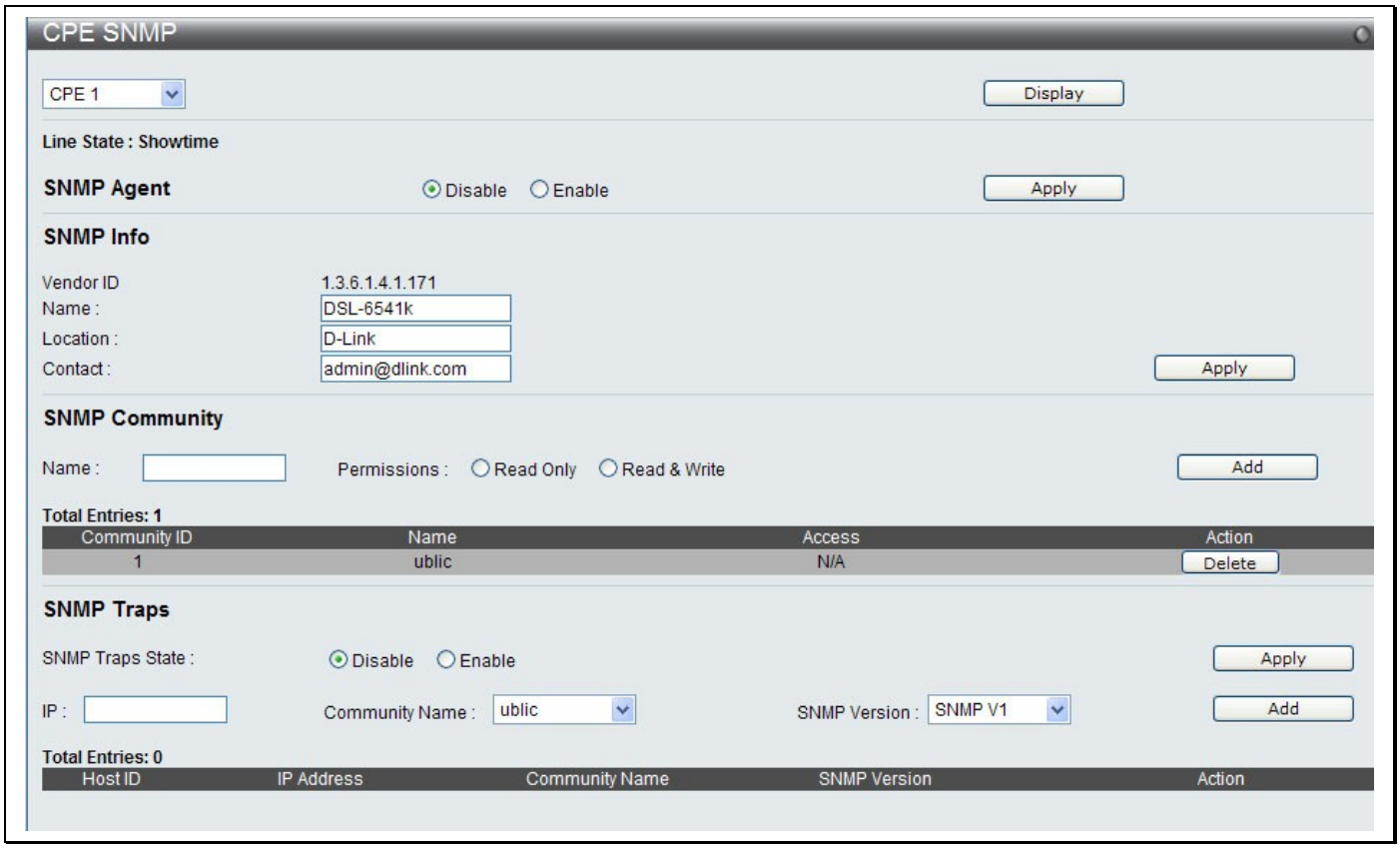


Figure 158. CPE CFM Setting menu

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. Use the menu to enable or disable CFM and CCM on the CPE. Click on the **Apply** button to set these configurations in the memory of the switch.

CPE SNMP

To view the CPE SNMP menu, click **CPE Management > CPE SNMP**.



Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. Use the menu to enable or disable an **SNMP Agent** on the CPE and click on **Apply** for the agent status. Configure administrator contact information, **SNMP Community** and **Traps** settings in separate menus.

CPE Firmware

To upgrade CPE firmware, choose the line of the CPE being upgraded, enter the IP address of the server where the firmware is located together with the complete file name and path of and click the **Upgrade** button. To view the menu, click **CPE Management > CPE Firmware**

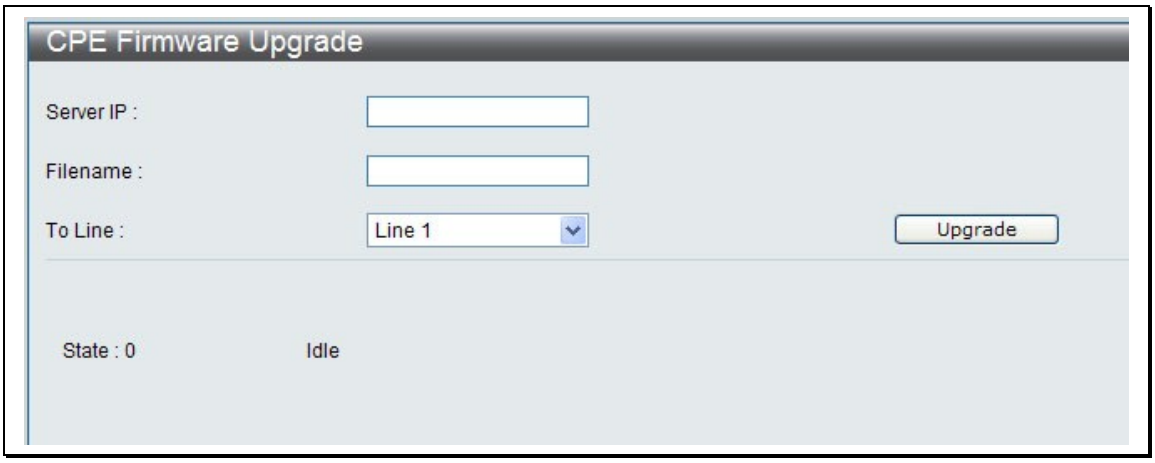


Figure 159. CPE Firmware Upgrade menu

CPE Loopback

The CPE Loopback menu is used to perform a CPE loopback test. To view the CPE Basic Information menu, click **CPE Management > CPE Loopback**.

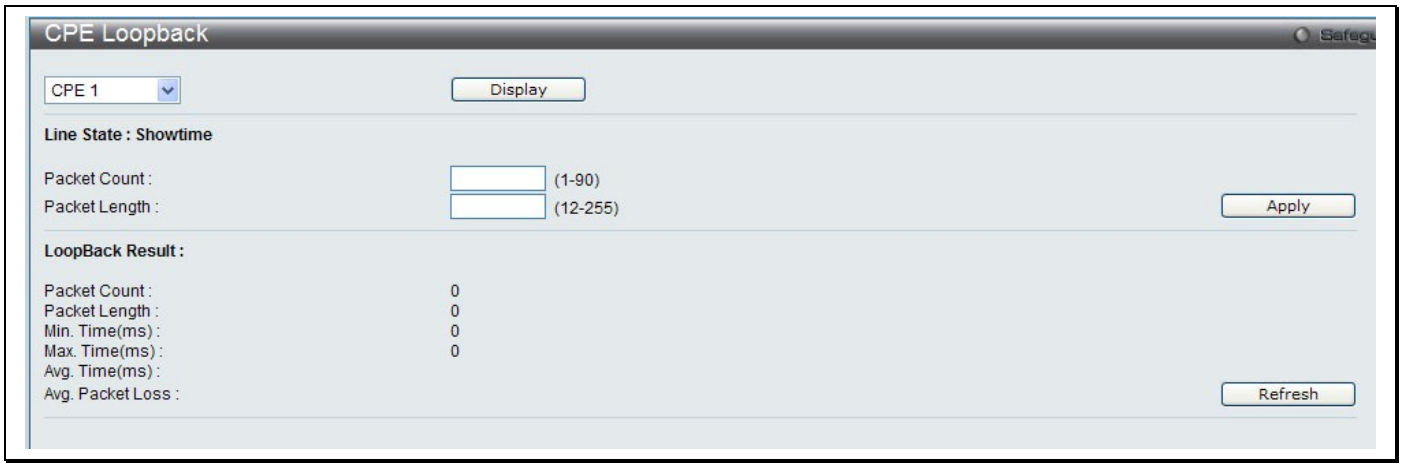


Figure 160. CPE Loopback menu

Select the CPE unit to be configured with the pull-down line menu and click on the **Display** button. Choose the **Packet Count** and **Packet Length** used for the test and click **Apply**. The test results appear in the bottom half of the menu.

CPE Maintenance

To view the CPE Maintenance menu, click **CPE Management > CPE Maintenance**.

Figure 161. CPE Maintenance menu

Use the CPE Maintenance menu to perform a simple reboot, save configuration settings, to reset the configuration settings without changing IP settings or to perform a factory reset (including IP settings). Click on the **Apply** button for the function being performed.

Section 12

Status

Status menus are used for monitoring switch and network funtion status.

VDSL Status

Alarm

View alarm status for each line.

VDSL Alarms

VDSL Line	CRC_I	RS	ESs	Status
1	0/0	0/0	0/0	Showtime
2	0/0	0/0	0/0	Training
3	0/0	0/0	0/0	Training
4	0/0	0/0	0/0	Training
5	0/0	0/0	0/0	Training
6	0/0	0/0	0/0	Training
7	0/0	0/0	0/0	Training
8	0/0	0/0	0/0	Training
9	0/0	0/0	0/0	Training
10	0/0	0/0	0/0	Training
11	0/0	0/0	0/0	Training
12	0/0	0/0	0/0	Training
13	0/0	0/0	0/0	Training
14	0/0	0/0	0/0	Training
15	0/0	0/0	0/0	Training
16	0/0	0/0	0/0	Training
17	0/0	0/0	0/0	Training
18	0/0	0/0	0/0	Training
19	0/0	0/0	0/0	Training
20	0/0	0/0	0/0	Training
21	0/0	0/0	0/0	Training
22	0/0	0/0	0/0	Training
23	0/0	0/0	0/0	Training
24	0/0	0/0	0/0	Training

Figure 162. VDSL Alarms

15 Min ES/SES/UAS

This status window allows you to display Downstream/Upstream information for either Error Second (ES), Severely Errored Second (SES), or Unavailable Second (UAS). View ES/SES/UAS statistics for 15 minute interval.

15 Min ES/SES/UAS

Line 1 Display

Line State : Showtime

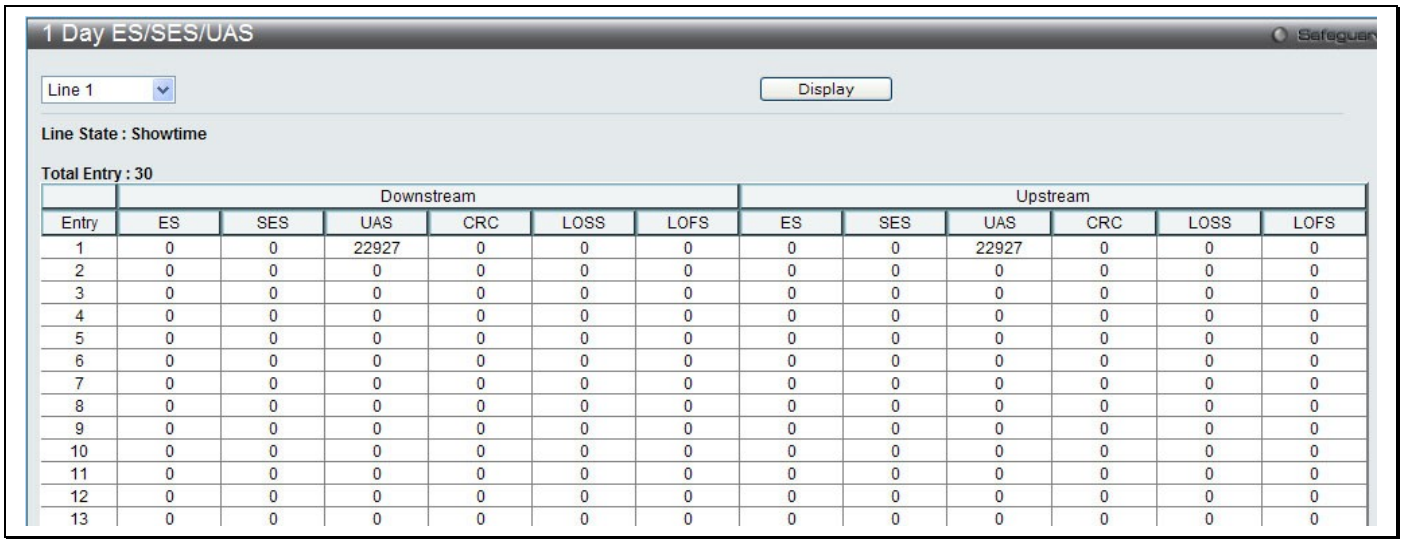
Total Entry : 96

	Downstream						Upstream					
Entry	ES	SES	UAS	CRC	LOSS	LOFS	ES	SES	UAS	CRC	LOSS	LOFS
1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	589	0	0	0	0	0	589	0	0	0
5	0	0	898	0	0	0	0	0	898	0	0	0
6	0	0	898	0	0	0	0	0	898	0	0	0
7	0	0	898	0	0	0	0	0	898	0	0	0
8	0	0	898	0	0	0	0	0	898	0	0	0
9	0	0	898	0	0	0	0	0	898	0	0	0
10	0	0	897	0	0	0	0	0	897	0	0	0
11	0	0	898	0	0	0	0	0	898	0	0	0
12	0	0	898	0	0	0	0	0	898	0	0	0

Figure 163. 15 Min ES/SES/UAS

1 Day ES/SES/UAS

This status window allows you to display Downstream/Upstream information for either Error Second (ES), Severely Errored Second (SES), or Unavailable Second (UAS). View ES/SES/UAS statistics for 1 Day interval.



	Downstream						Upstream					
Entry	ES	SES	UAS	CRC	LOSS	LOFS	ES	SES	UAS	CRC	LOSS	LOFS
1	0	0	22927	0	0	0	0	0	22927	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0

Figure 164. 1 Day ES/SES/UAS

VDSL PM Threshold

Use this to set the near end and far end PM threshold.

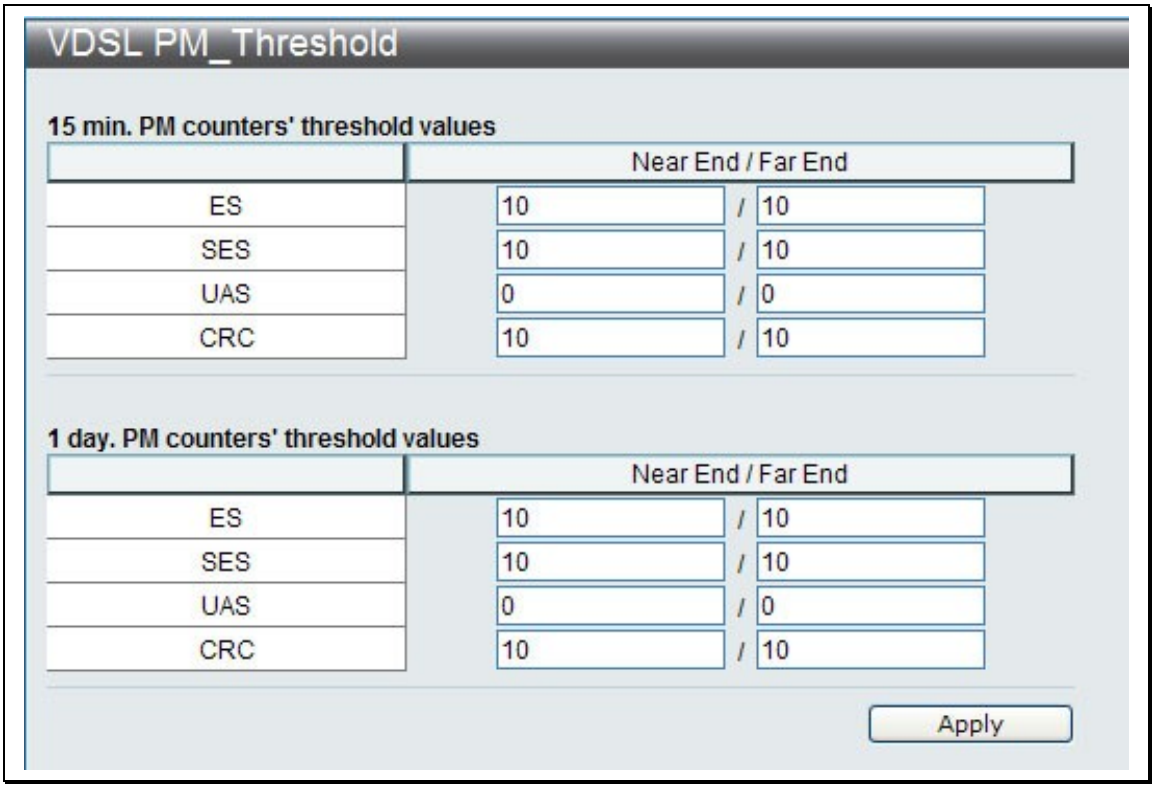


Figure 165. VDSL PM Threshold

Click **Apply** to set the threshold settings.

CPU Utilization

The **CPU Utilization** window displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

To view this window, click **Status > CPU Utilization** as shown below:

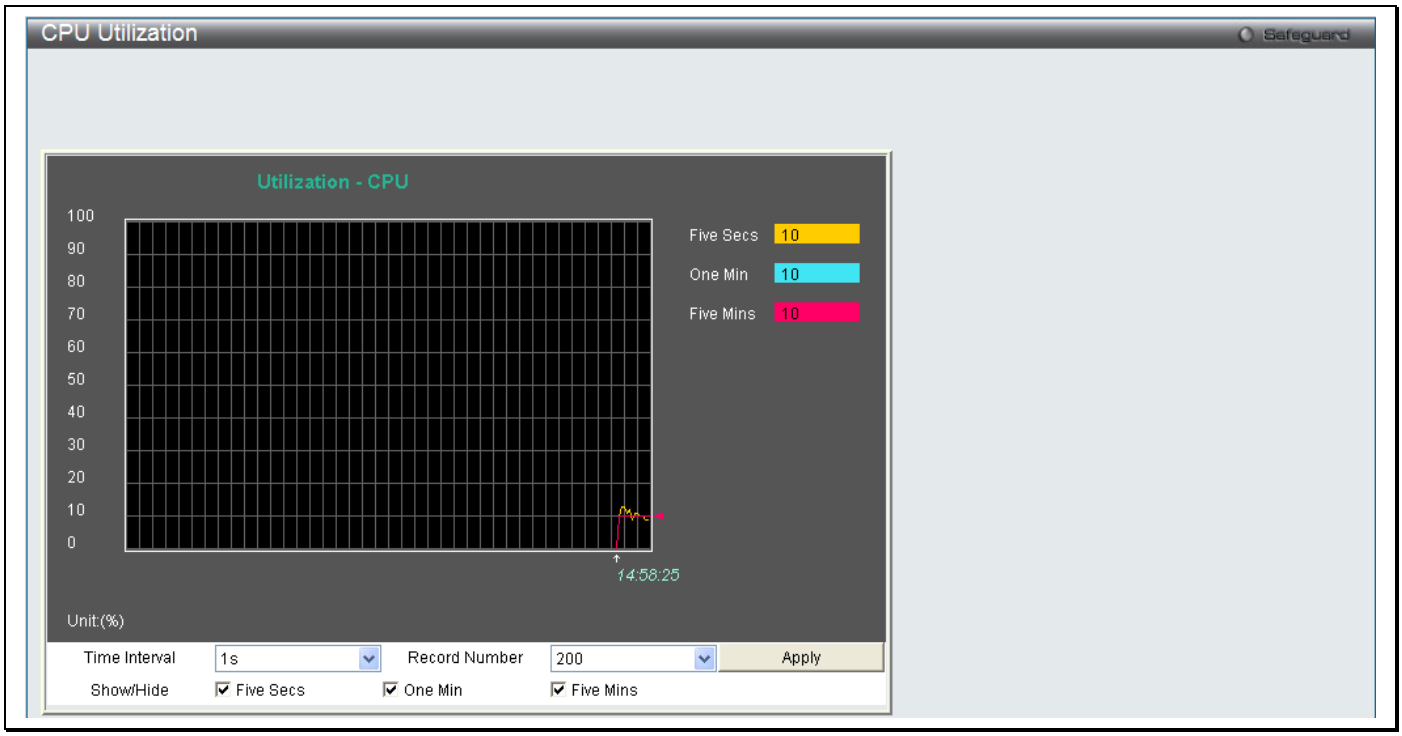


Figure 166. CPU Utilization menu

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.

Change the view parameters as follows:

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 Secs, One Min, and Five Mins.

Port Utilization

The **Port Utilization** window displays the percentage of the total available bandwidth being used on the port.

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

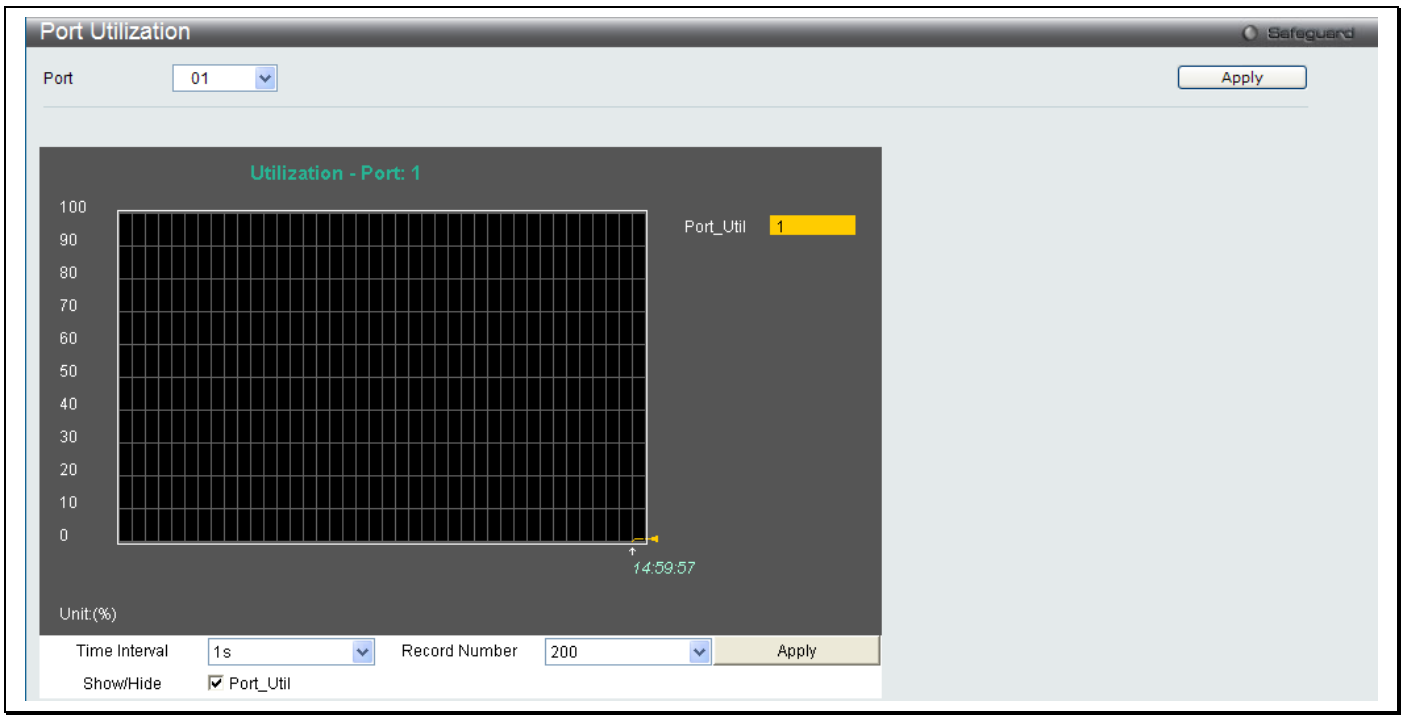


Figure 167. Port Utilization menu

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.

Change the view parameters as follows:

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 Util.

Packet Ports

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Three windows are offered in the **Packets** folder to view and configure these settings.

Packet Size

The Web Manager allows packets received by the switch, arranged in six groups and classed by size, to be viewed 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 this window, click **Status > Packet Ports > Packet Size** as shown below:

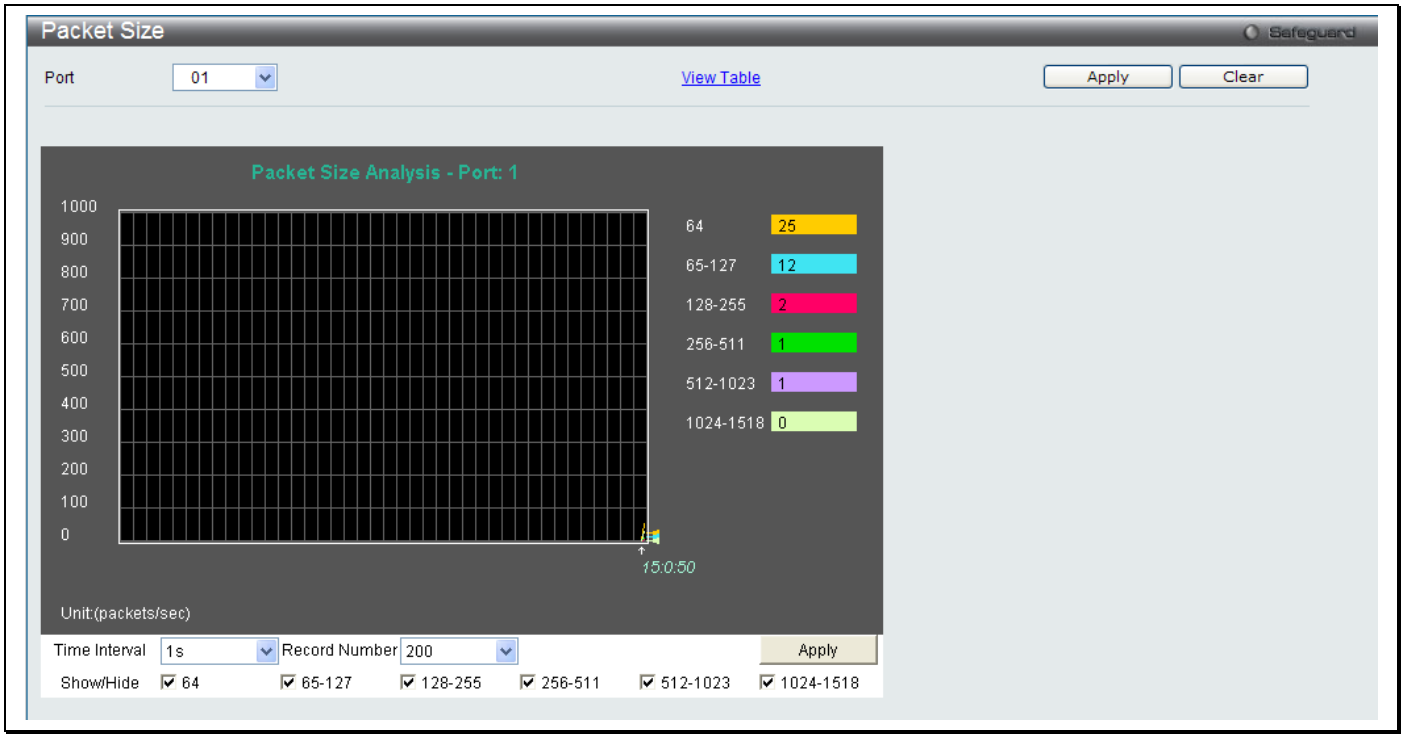
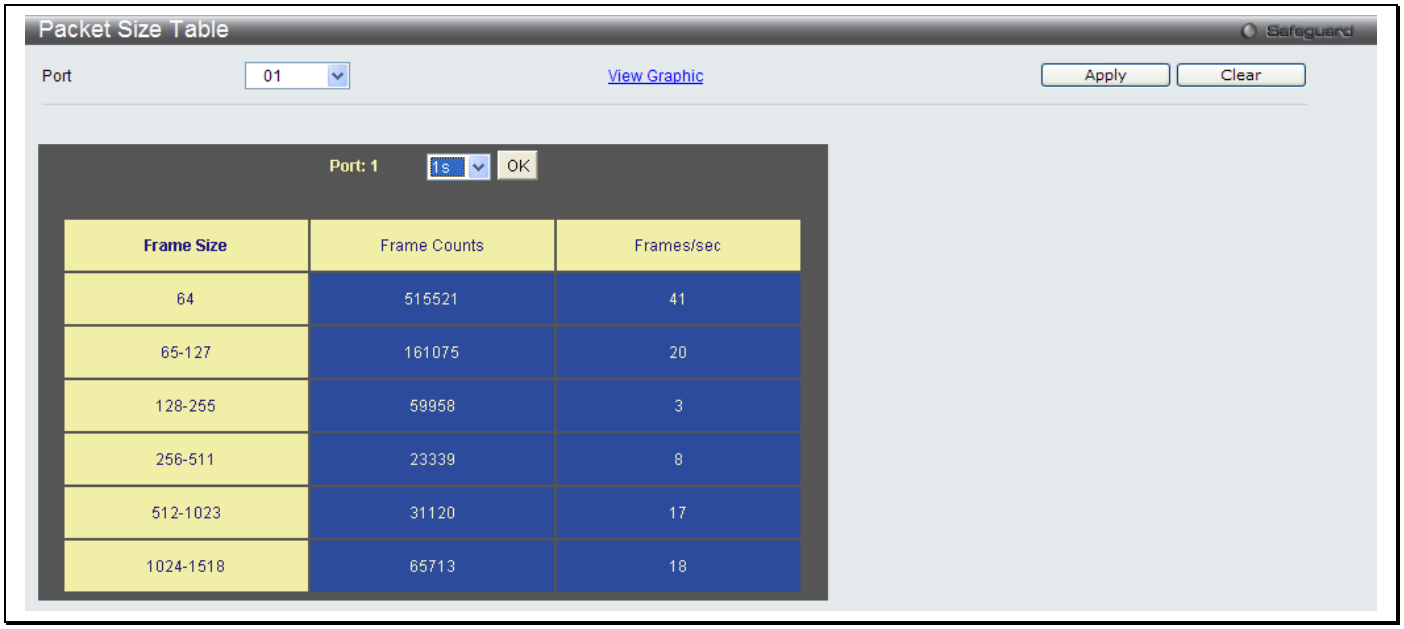


Figure 168. Packet Size menu

To view the **Packet Size Table** window, click the link View Table, which will show the following table:



Frame Size	Frame Counts	Frames/sec
64	515521	41
65-127	161075	20
128-255	59958	3
256-511	23339	8
512-1023	31120	17
1024-1518	65713	18

Figure 169. Packet Size Table menu

The following fields can be set or viewed:

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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the switch to display a line graph rather than a table.

Received (RX)

This table displays the RX packets on the switch. 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 this window, click **Status > Packet Ports > Received (RX)** as shown below:

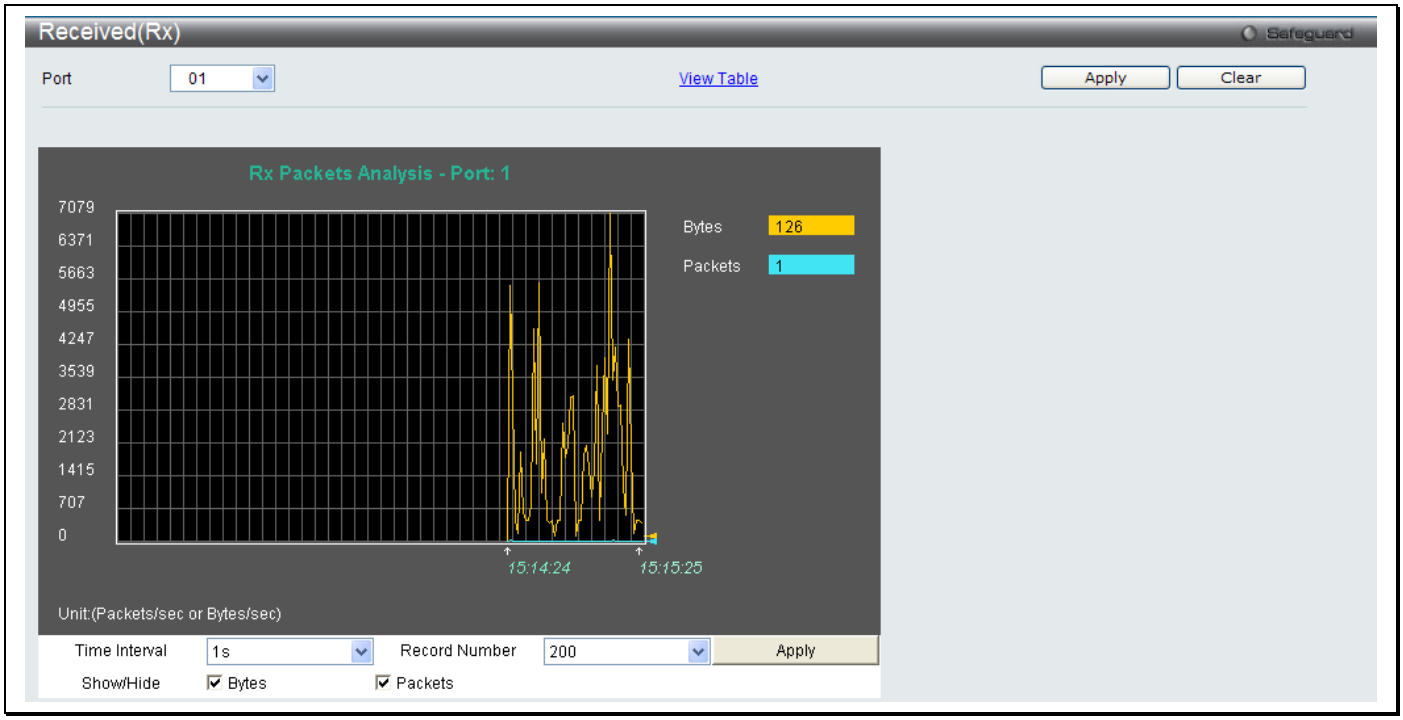


Figure 170. Received (RX) menu (for Bytes and Packets)

To view the **Received (RX) Table** window, click View Table.

Figure 171. Received (RX) Table menu (for Bytes and Packets)

The following fields may be set or viewed:

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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the switch to display a line graph rather than a table.

UMB_cast (RX)

This table displays the UMB_cast RX Packets on the switch. 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 this window, click **Monitoring > Packets > UMB_cast (RX)** as shown below:

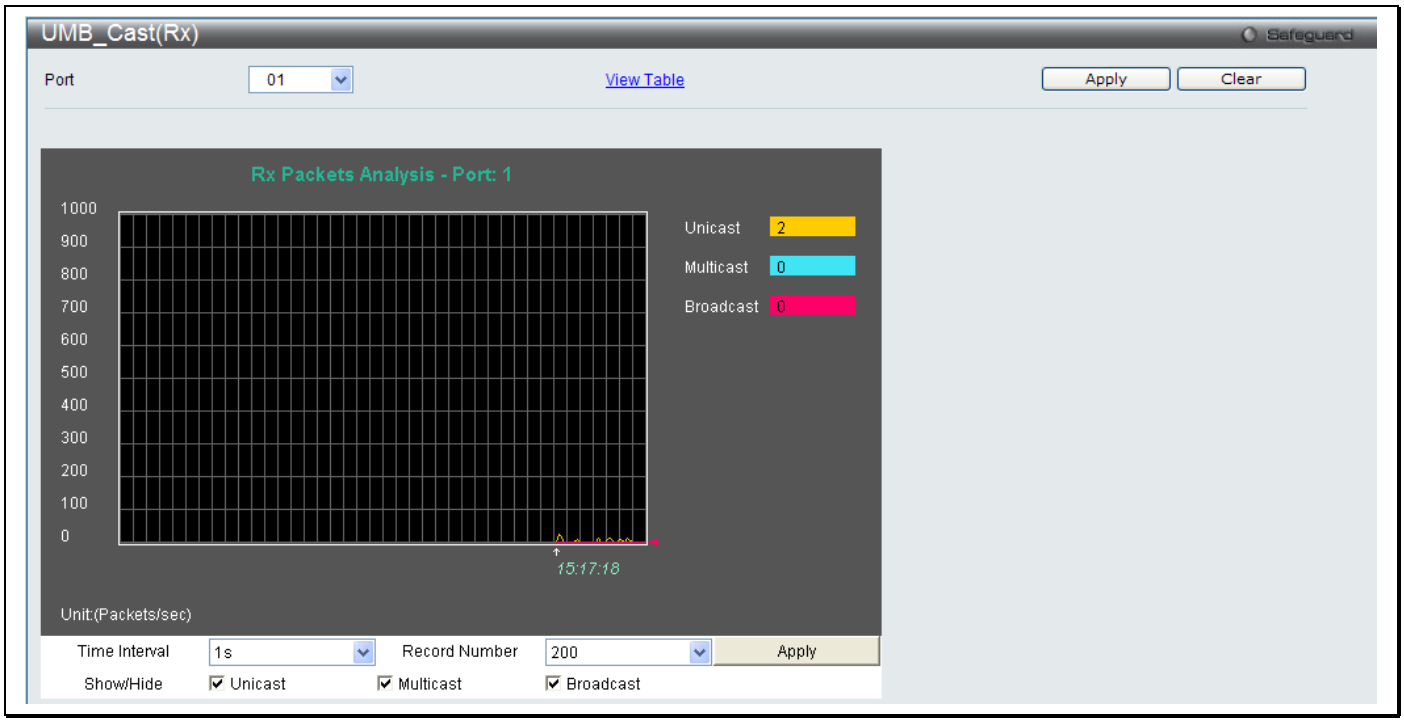


Figure 172. UMB_cast (RX) menu (for Unicast, Multicast, and Broadcast Packets)

To view the **UMB_cast (RX) Table** window, click the View Table link.

Figure 173. UMB_cast (RX) Table menu (for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

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 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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the switch to display 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 this window, click **Status > Packet Ports > > Transmitted (TX)** as shown below:

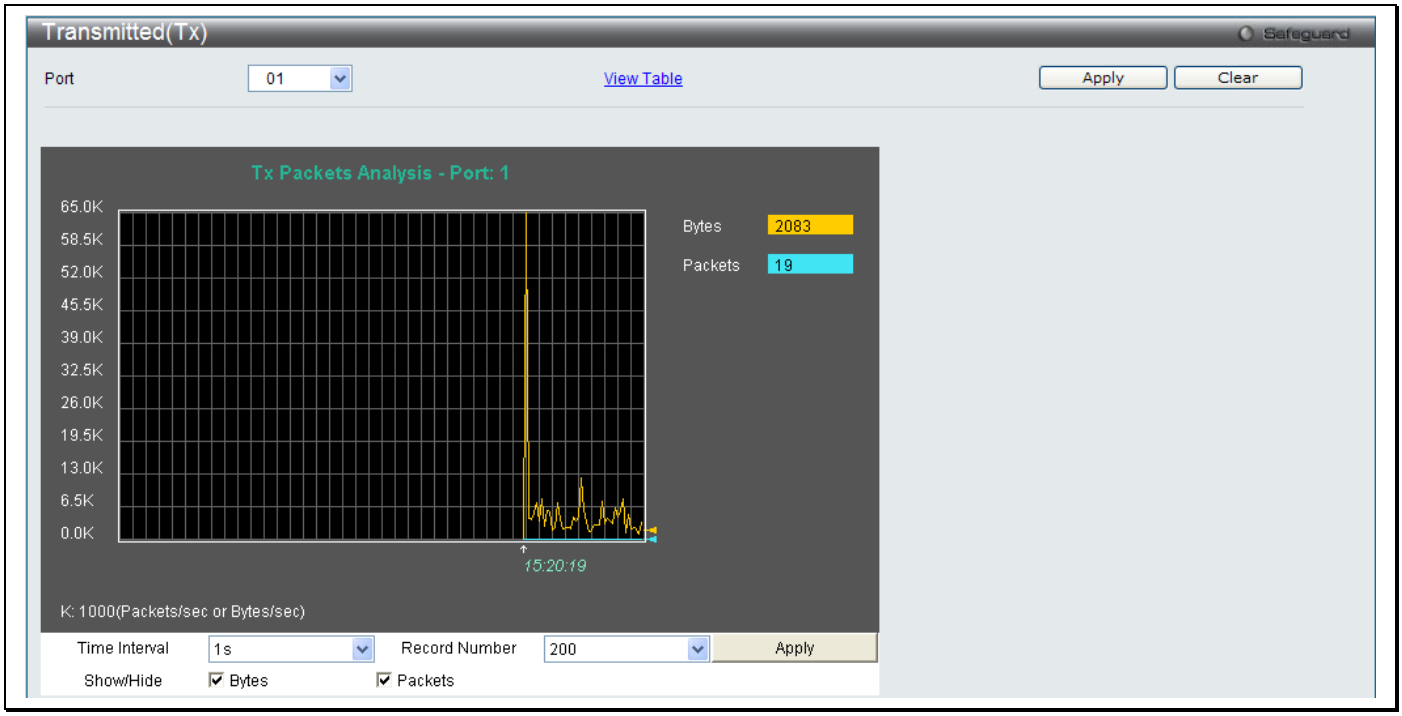


Figure 174. Transmitted (TX) menu (for Bytes and Packets)

To view the **Transmitted (TX) Table** window, click the link View Table.

Figure 175. Transmitted (TX) Table menu (for Bytes and Packets)

The following fields may be set or viewed:

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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the switch to display a line graph rather than a table.

Error Ports

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 this window, click **Status > Error Ports > Received (RX)** as shown below:

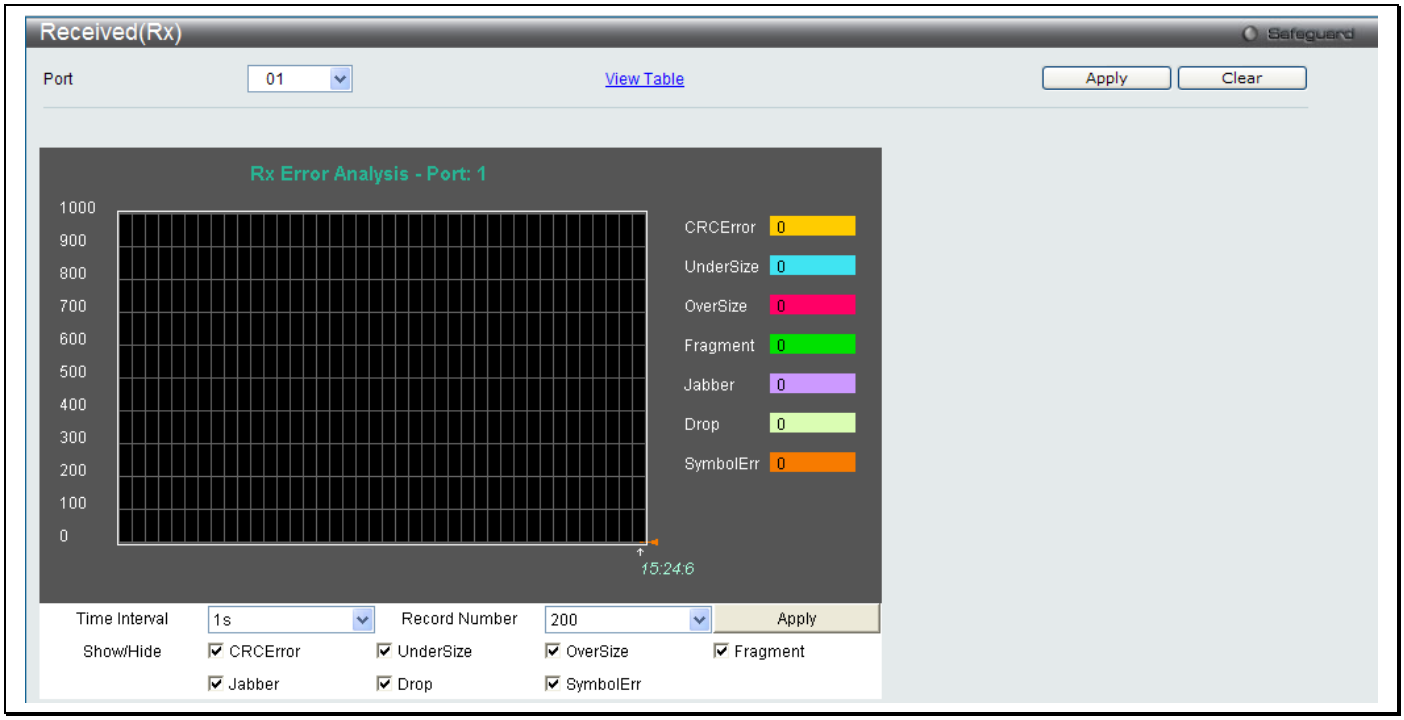


Figure 176. Received (RX) menu (for errors)

To view the **Received (RX) Table** window for errors, click the link View Table, which will show the following table:

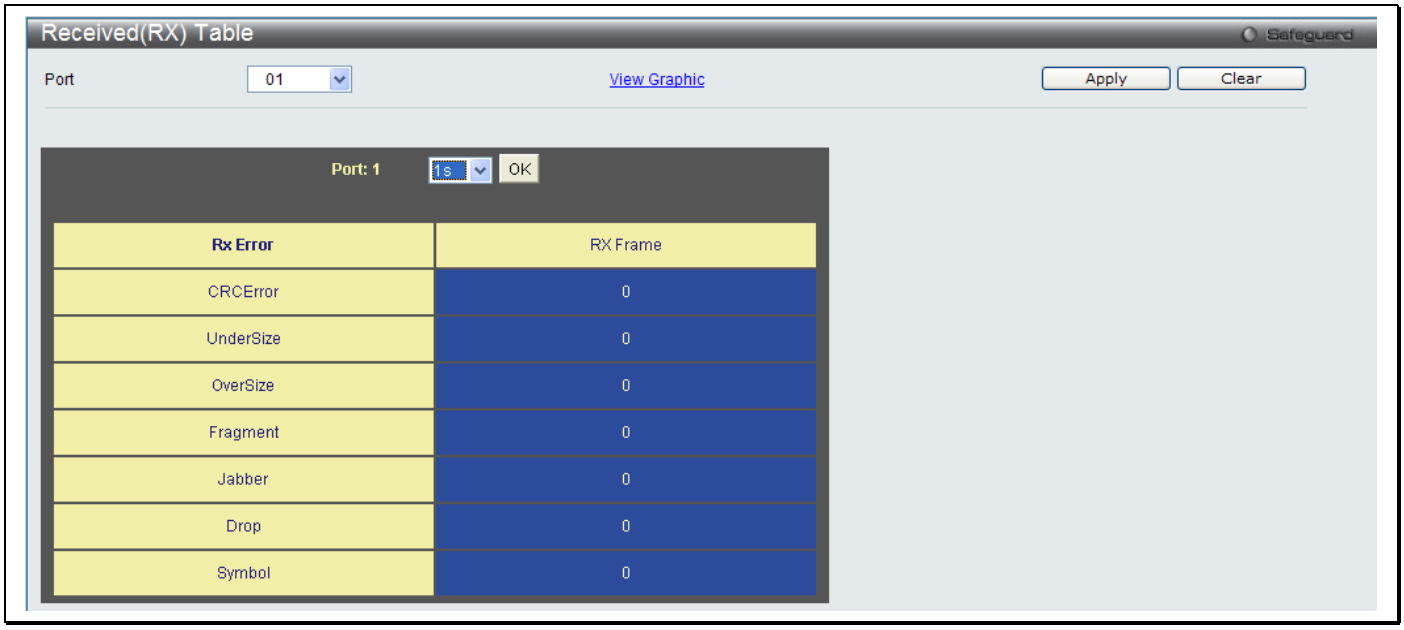


Figure 177. Received (RX) Table menu (for errors)

The following fields can be set:

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.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the switch to display 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 this window, click **Status > Error Ports > Transmitted (TX)** as shown below:

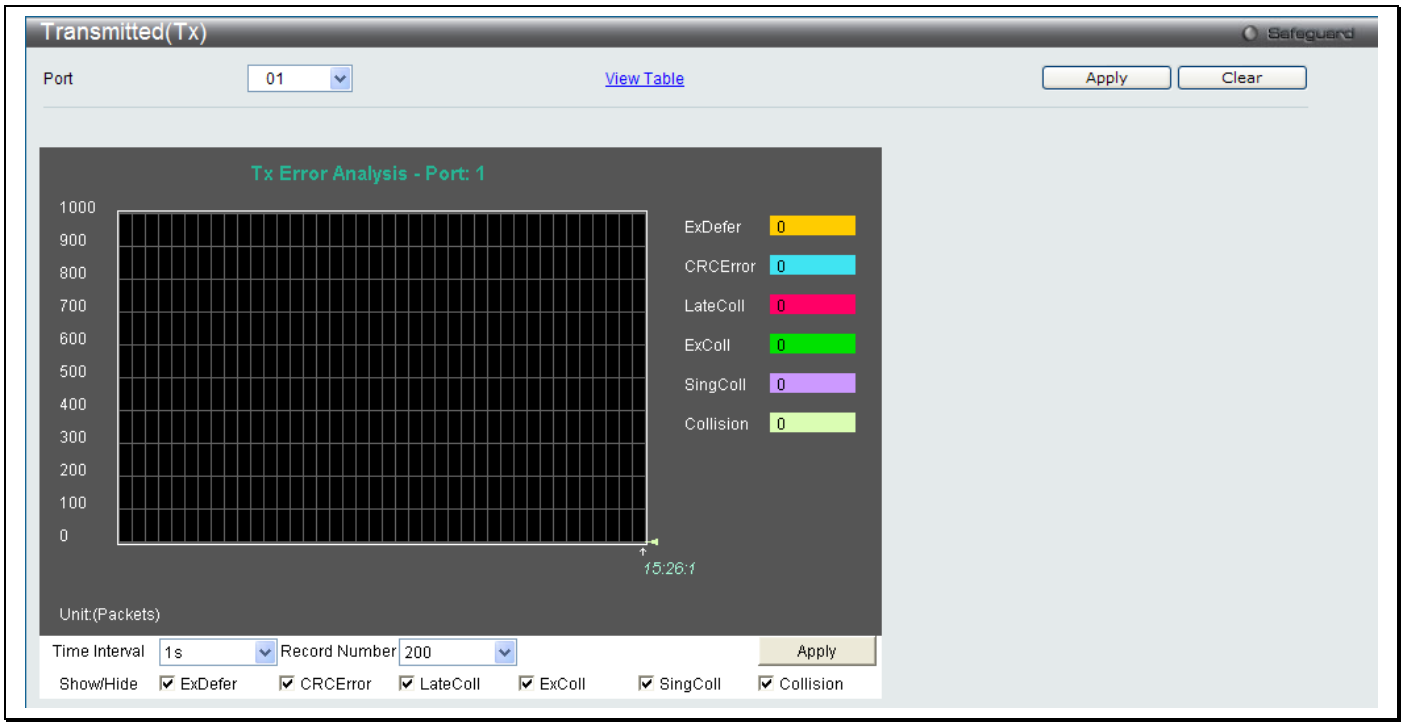


Figure 178. Transmitted (TX) menu (for errors)

To view the **Transmitted (TX) Table** window, click the link View Table, which will show the following table:

Figure 179. Transmitted (TX) Table menu (for errors)

The following fields may be set or viewed:

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*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
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.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the switch to display a line graph rather than a table.

Utilization

Memory Utilization

This window is used to display the utilization of the CPU and memory on the switch.

To view this window, click **Status > Utilization > Memory Utilization** as shown below:

Figure 180. Packet Size Table menu

Click **Refresh** to reload the display.

Ping Test

Ping is a small program that sends ICMP Echo packets to the IPv6 or IPv4 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 this window, click **Status > Ping Test** as shown below:

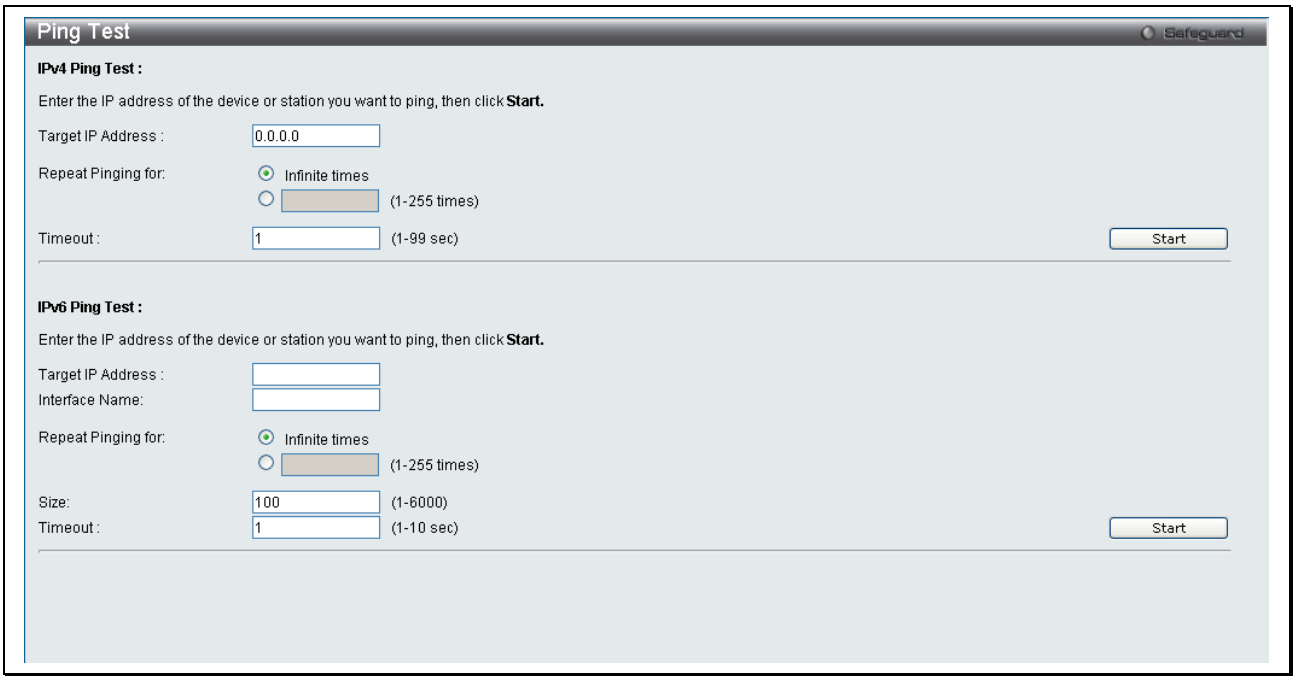


Figure 181. Ping Test menu

IPv4 Ping Test	
Target IP Address	Enter the Target IPv4 Address of the host.
Repeat Pinging for	Check the Infinite times radio button, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. Or the user may opt to choose a specific number of times to ping the **Target IP Address** by entering a number between *1* and *255*.
Timeout	Select a timeout period between *1* and *10* seconds for this Ping message to reach its destination. If the packet fails to find the IPv4 address in this specified time, the Ping packet will be dropped.
IPv6 Ping Test	
Target IP Address	Enter the Target IPv6 Address of the host.
Interface Name	Enter the Target Interface Name of the host.
Repeat Pinging for	Check the Infinite times radio button, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. Or the user may opt to choose a specific number of times to ping the **Target IP Address** by entering a number between *1* and *255*.
Size	Use this parameter to set the datagram size of the packet, or the number of bytes in each ping packet. Users may set a size between *1* and *6000* bytes with a default setting of 100 bytes.
Timeout	Select a timeout period between *1* and *10* seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.

Click **Start** to initiate the Ping program

Firmware Information

The following screen allows the user to view information about current firmware images stored on the switch.

To view this menu, click the **Firmware Information** link in the Quick Configuration menu as shown below:

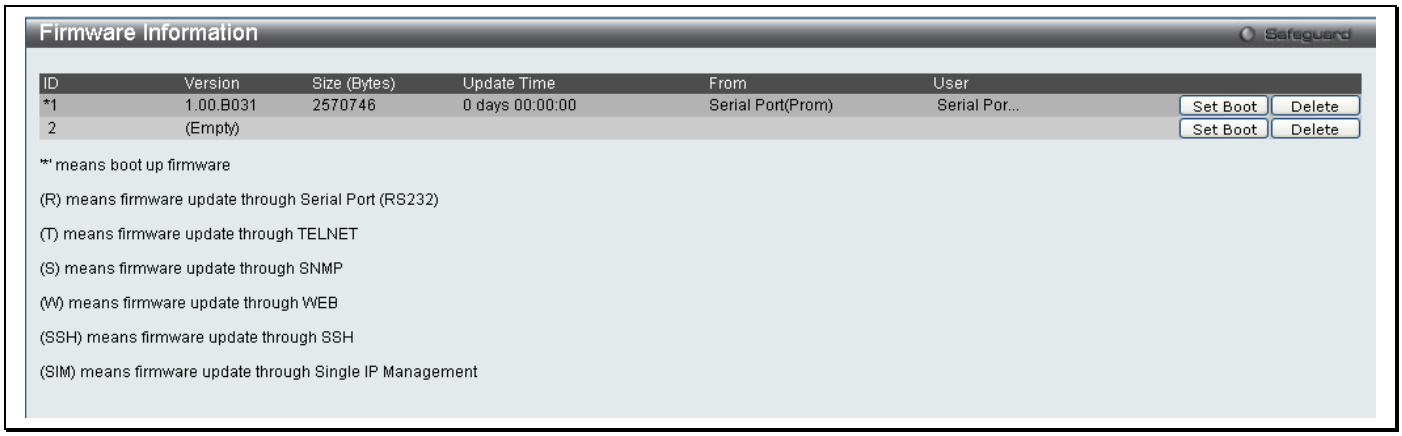


Figure 182. Firmware Information menu

This window holds the following information:

Parameter	Description
ID	States the image ID number of the firmware in the switch's memory. The switch can store two firmware images for use. Image ID 1 will be the default boot up firmware for the switch unless otherwise configured by the user.
Version	States the firmware version.
Size (Bytes)	States the size of the corresponding firmware, in bytes.
Update Time	States the specific time the firmware version was downloaded to the switch.
From	States the IP address of the origin of the firmware. There are five ways firmware may be downloaded to the switch. **R** – If the IP address has this letter attached, it denotes a firmware upgrade through the serial port RS232. **T** – If the IP address has this letter attached to it, it denotes a firmware upgrade through Telnet. **S** – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Simple Network Management Protocol (SNMP). **W** – If the IP address has this letter attached to it, it denotes a firmware upgrade through the web-based management interface. **SSH** – If the IP address has these three letters attached, it denotes a firmware update through SSH. **SIM** – If the IP address has these letters attached, it denotes a firmware upgrade through the Single IP Management feature.
User	States the user who downloaded the firmware. This field may read "Anonymous" or "Unknown" for users that are unidentified.

Section 13

Maintenance

Firmware Upgrade

Configuration File Backup & Restore

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 this window, click **Maintenance > Firmware Upgrade** as shown below:

Figure 183. Firmware Upgrade menu

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 this window, click **Maintenance > Configuration File Backup/Restore** as shown below:

Figure 184. Configuration File Backup/Restore menu

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 DAS-3626 supports the SNMP versions 1, 2c, and 3. The default SNMP setting is disabled. You must enable SNMP. Once SNMP is enabled you can choose which version you want to use 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.

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 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 DAS-3626 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** window.

SNMP Global State Settings

The SNMP Global State Settings is used to globally enable or disable the SNMP Settings on the switch.

To view this window, click **Configuration > SNMP Settings > SNMP Global State Settings** as shown below:

Figure 185. SNMP Global State Settings menu

SNMP View Table

This window is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager.

To view this window, click **Configuration > SNMP Settings > SNMP View Table** as shown below:

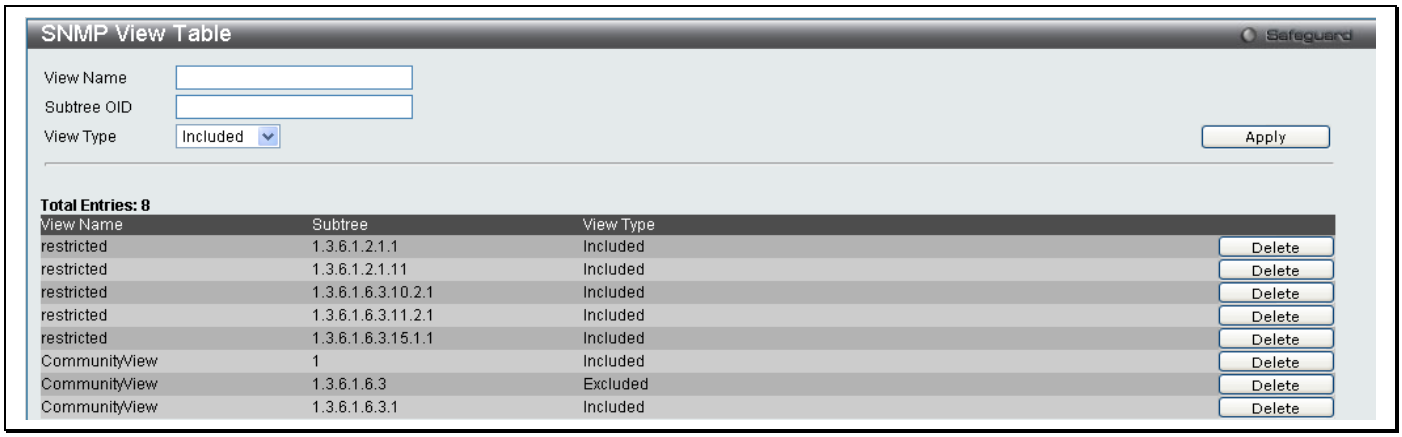


Figure 186. SNMP View Table menu

The following parameters can be set:

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.

To implement the new settings, click **Apply**. To delete an entry click the corresponding **Delete** button.

SNMP Group Table

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

To view this window, click **Configuration > SNMP Settings > SNMP Group Table** as shown below:

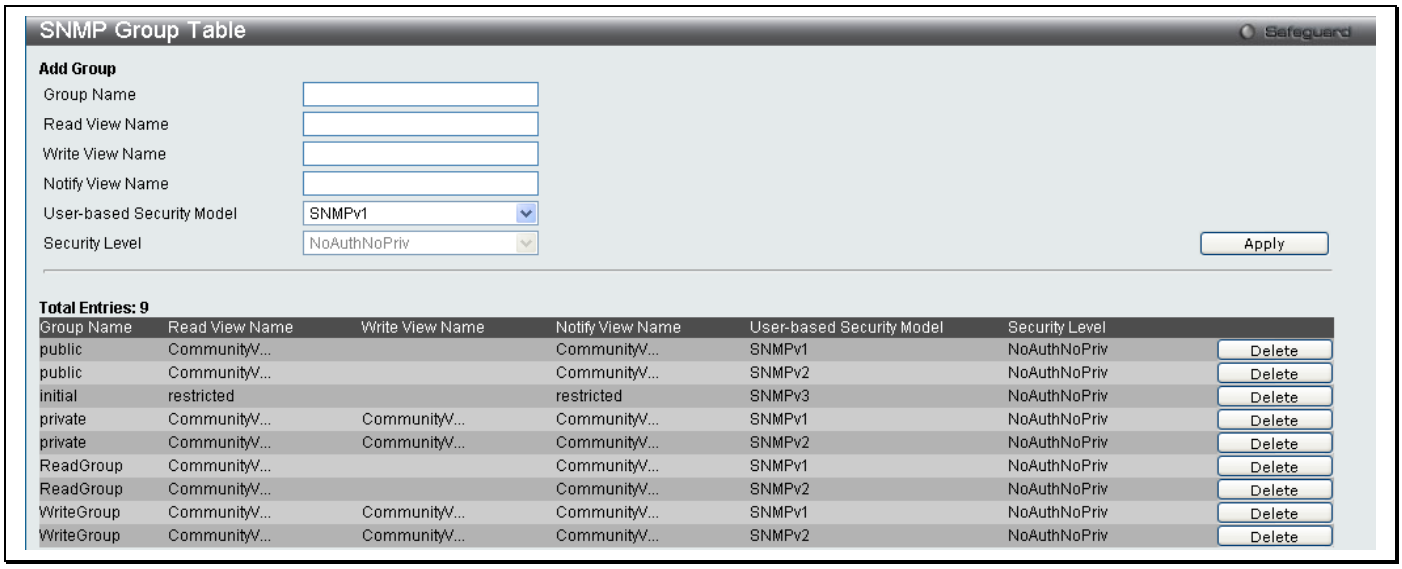


Figure 187. SNMP Group Table menu

To delete an existing SNMP Group Table entry, click the corresponding **Delete** button.

The following parameters can be set:

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.

To implement the new settings, click **Apply**.

SNMP User Table

This window displays all of the SNMP User's currently configured on the switch and also allows you to add new users.

To view this window, click **Maintenance > SNMP Settings > SNMP User Table** as shown below:

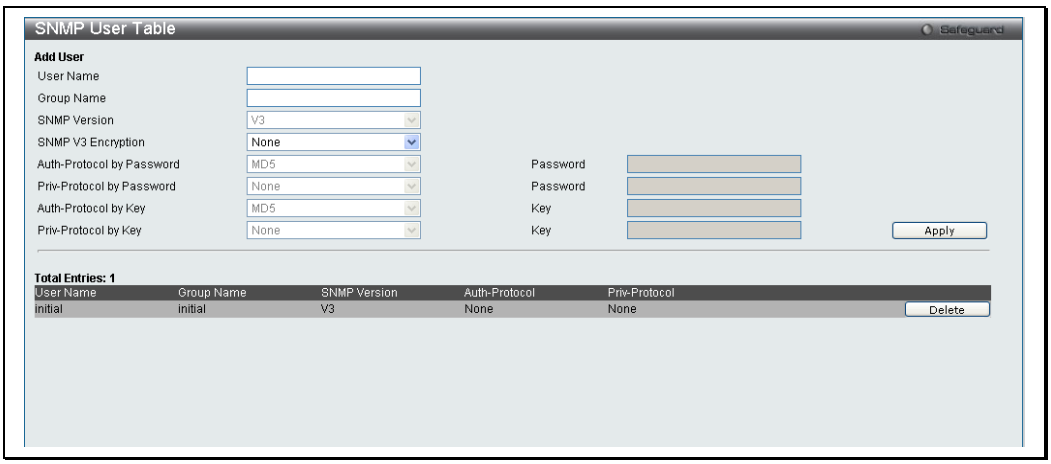


Figure 188. SNMP User Table menu

The following parameters may be set:

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	*V1* – Indicates that SNMP version 1 is in use. *V2* – Indicates that SNMP version 2 is in use. *V3* – Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	*None* – Indicates that there is no SNMP V3 Encryption *Password* – Indicates that there is SNMP V3 Encryption through a password *Key* – Indicates that there is SNMP V3 Encryption through a key.
Auth-Protocol by Password	*MD5* – Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* – Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by Password	*None* – Indicates that no authorization protocol is in use. *DES* – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Auth-Protocol by Key	*MD5* – Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* – Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by password	*None* – Indicates that no authorization protocol is in use. *DES* – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Password	Enter a Password when SNMP V3 Encryption is enabled for Password mode.
Key	Enter a Key when SNMP V3 Encryption is enabled for Key mode.

To implement changes made, click **Apply**. To delete an existing **SNMP User Table** entry, click the corresponding **Delete** button.

SNMP Community Table

Use this table to view existing SNMP Community Table configurations and to create a 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 this window, click **Maintenance > SNMP Settings > SNMP Community Table** as shown below:

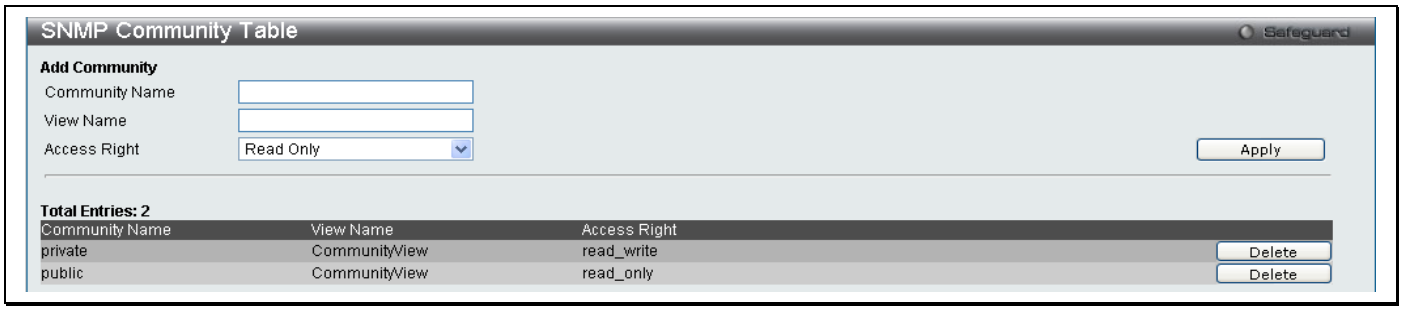


Figure 189. SNMP Community Table menu

The following parameters can set:

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.

To implement the new settings, click **Apply**. To delete an entry from the **SNMP Community Table**, click the corresponding **Delete** button.

SNMP Host Table

The **SNMP Host Table** window is used to set up SNMP trap recipients.

To view this window, click **Maintenance > SNMP Settings > SNMP Host Table** as shown below:

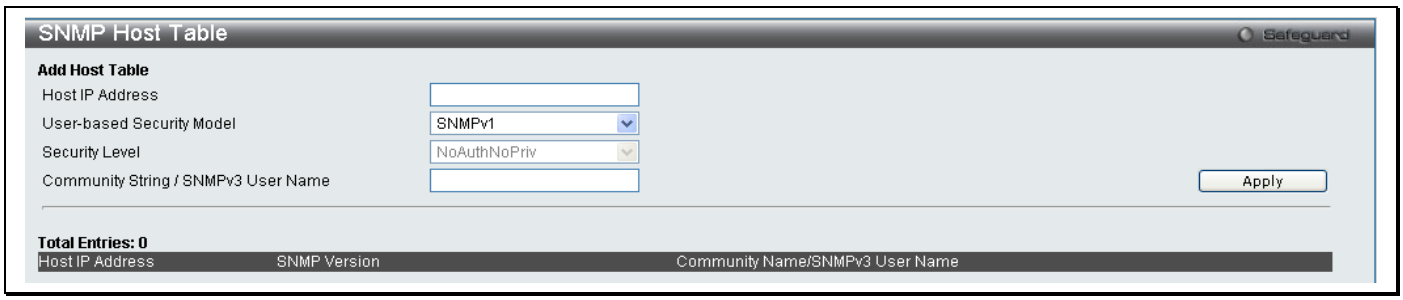


Figure 190. SNMP Host Table menu

The following parameters can set:

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. *SNMPV2c* – Specifies that SNMP version 2 will be used. *SNMPV3* – To specify that the SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify a NoAuthNoPriv security level. *AuthNoPriv* – To specify an AuthNoPriv security level. *AuthPriv* – To specify an AuthPriv security level.
Community String/ SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To implement your new settings, click **Apply**.

SNMP v6Host Table

This window is used to specify the IPv6 host IP address to which the trap packets will be sent.

To view this window, click **Maintenance > SNMP Settings > SNMP v6Host Table** as shown below:

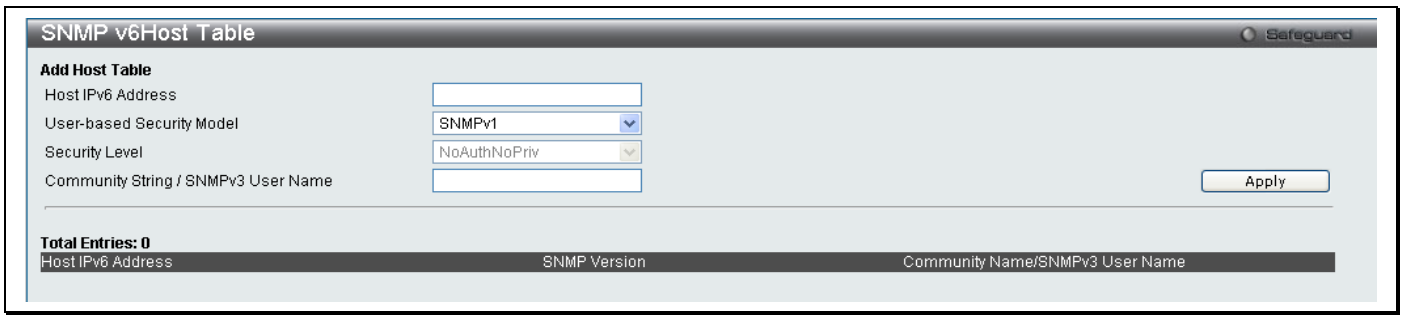


Figure 191. SNMP V6Host Table menu

The following parameters can be configured:

Parameter	Description
Host Ipv6 Address	Enter the IPv6 host IP address to which the trap packet will be sent.
User-based Security Model	Used the drop down menu to select the user-based security model. *SNMPv1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP) version 1, is a network management protocol that provides a means to monitor and control network devices. *SNMPv2* – Specifies that SNMP version 2 will be used. The SNMP v2 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 SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.
Security Level	When SNMPv3 is in use, it is necessary to choose the security level. Use the drop down menu to select from the following: *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.
Community String/SNMPv3 User Name	Enter an alphanumeric string that will be used to authorize a remote SNMP manager to access the switch's SNMP agent. Alternatively enter the SNMPv3 user name.

Click **Apply** to implement changes made.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the switch.

To view this window, click **Maintenance > SNMP Settings > SNMP Engine ID** as shown below:

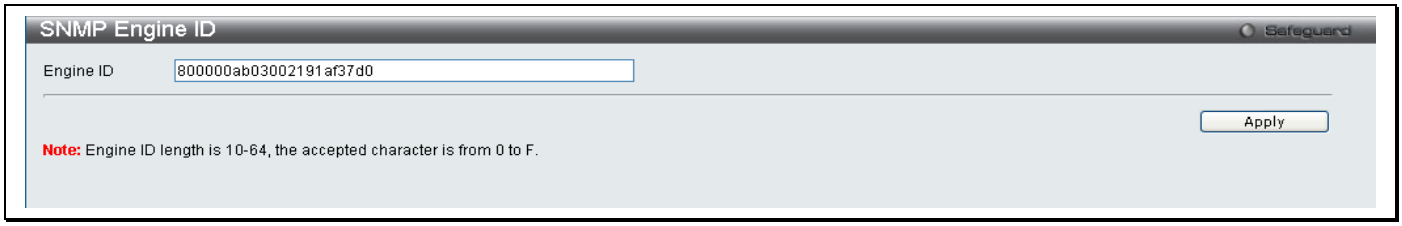


Figure 192. SNMP Engine ID menu

To change the Engine ID, enter the new Engine ID in the space provided and click the **Apply** button.

SNMP Trap Configuration

The following window is used to enable and disable trap settings for the SNMP function on the switch.

To view this window, click **Maintenance > SNMP Settings > SNMP Trap Configuration** as shown below:

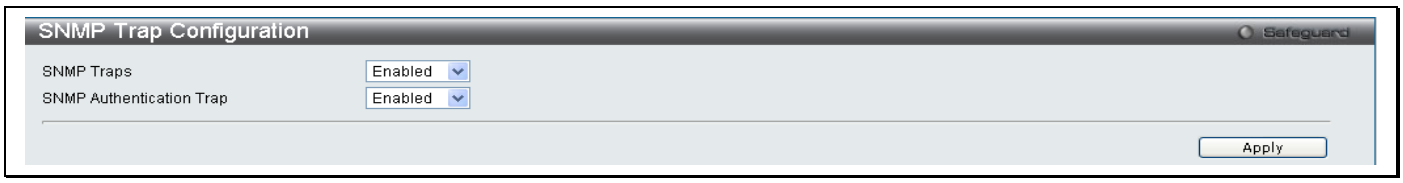


Figure 193. SNMP Trap Configuration menu

To enable or disable the Traps State and/or the Authenticate Traps State, use the corresponding pull-down menu to change and click **Apply**.

Appendix A

System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this switch.

Category	Event Description	Log Information	Severity
System	System started up	System started up	Critical
	Configuration saved to flash	Configuration saved to flash (Username: <username>)	Informational
	System log saved to flash	System log saved to flash (Username: <username>)	Informational
	Configuration and log saved to flash	Configuration and log saved to flash(Username: <username>)	Informational
	Internal Power failed	Internal Power failed	Critical
	Internal Power is recovered	Internal Power is recovered	Critical
	Redundant Power failed	Redundant Power failed	Critical
	Redundant Power is working	Redundant Power is working	Critical
	Side Fan failed	Side Fan failed	Critical
	Side Fan recovered	Side Fan recovered	Critical
Upload/ Download	Firmware upgraded successfully	Firmware upgraded by <console | telnet | WEB | SSH | SNMP | SIM> successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful	Firmware upgrade by <console | telnet | WEB | SSH | SNMP | SIM> was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded by <console | telnet | WEB | SSH | SNMP | SIM> (Username: <username>)	Informational
	Configuration download was unsuccessful	Configuration download by <console | telnet | WEB | SSH | SNMP | SIM> was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded by <console | telnet | WEB | SSH | SNMP | SIM> (Username: <username>)	Informational
	Configuration upload was unsuccessful	Configuration upload by <console | telnet | WEB | SSH | SNMP | SIM> was unsuccessful! (Username: <username>)	Warning
	Log message successfully uploaded	Log message successfully uploaded by <console | telnet | WEB | SSH | SNMP | SIM> (Username: <username>)	Informational
	Log message upload was unsuccessful	Log message upload by <console | telnet | WEB | SSH | SNMP | SIM> was unsuccessful! (Username:	Warning

		<username>)	
Interface	Port link up	Port <portNum> link up, <link state>	Informational
	Port link down	Port <portNum> link down	Informational
Console	Successful login through Console	Successful login through Console (Username: <username>)	Informational
	Login failed through Console	Login failed through Console (Username: <username>)	Warning
	Logout through Console	Logout through Console (Username: <username>)	Informational
	Console session timed out	Console session timed out (Username: <username>)	Informational
Web	Successful login through Web	Successful login through Web (Username: <username>)	Informational
	Login failed through Web	Login failed through Web (Username: <username>)	Warning
	Logout through Web	Logout through Web (Username: <username>)	Informational
SSL	Successful login through Web(SSL)	Successful login through Web(SSL) (Username: <username>)	Informational
	Login failed through Web(SSL)	Login failed through Web(SSL) (Username: <username>)	Warning
	Logout through Web(SSL)	Logout through Web(SSL) (Username: <username>)	Informational
	Web(SSL) session timed out	Web(SSL) session timed out (Username: <username>)	Informational
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational
STP	Topology changed	Topology changed (Instance:%d, Port:%d)	Informational
	New Root selected	CIST New Root bridge selected (MAC:%s, Priority:%d)	Informational
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational

SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
	SSH server is enabled	SSH server is enabled	Informational
	SSH server is disabled	SSH server is disabled	Informational
	SSH authentication successful	SSH authentication successful (Username: <username>)	Informational
	SSH authentication failed	SSH authentication failed (Username: <username>)	Informational
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning

	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational
	Successful login through Web(SSL) authenticated by AAA none method	Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Warning
	Successful login through Web(SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Web(SSL) authenticated by AAA server	Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Warning
	Login failed through Web(SSL) due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)	Warning
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username:	Warning

		<username>, MAC: <macaddr>)	
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Warning
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Informational
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Informational
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Warning
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Informational
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Warning
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational

	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Warning
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Informational
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)	Warning
	Login failed through Console due to AAA server timeout or improper configuration.	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Enable Admin failed through Console due to AAA server timeout or improper configuration.	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Login failed through Web from user due to AAA server timeout or improper configuration.	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>,MAC:<mac>)	Warning
	Enable Admin failed through Web from user due to AAA server timeout or improper configuration.	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>,MAC:<mac>)	Warning
	Login failed through Web(SSL) from user due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <mac>)	Warning
	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration.	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>,MAC: <mac>)	Warning

	Login failed through Telnet from user due to AAA server timeout or improper configuration.	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>,MAC: <mac>)	Warning
	Enable Admin failed through Telnet from user due to AAA server timeout or improper configuration.	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>,MAC: <mac>)	Warning
	Login failed through SSH from user due to AAA server timeout or improper configuration.	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>,MAC: <mac>)	Warning
	Enable Admin failed through SSH from user due to AAA server timeout or improper configuration.	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <mac>)	Warning
	Successful Enable from user (Module: AAA)	Successful Enable from <userIP> (Module: AAA)	Informational
	Enable failed from user (Module: AAA)	Enable failed from <userIP> (Module: AAA)	Warning
	AAA server response is wrong	AAA server <serverIP> (Protocol: <protocol>) response is wrong	Warning
	AAA doesn't support this functionality	AAA doesn't support this functionality	Informational
Port Security	Port security has exceeded its maximum learning size and will not learn any new addresses	Port security violation mac addrss <macaddr> on locking address full port <unitID:portNum>	Warning
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational
	Safeguard Engine is in filtering packet mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast strom occurrence	Port <portNum> Broadcast storm is occurring	Warning
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shut down due to a packet storm	Port <portNum> is currently shut down due to a packet storm	Warning
IP-MAC-PORT Binding	Unauthenticated IP address and discard by IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IP-MAC port binding (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Unauthenticated IP address encountered and discarded by IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IP-MAC port binding (IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Warning

Loop-back Detection	LBD loop occurred	Port <portNum> LBD loop occurred. Port blocked	Critical
	LBD port recovered. Loop detection restarted	Port <portNum> LBD port recovered. Loop detection restarted	Informational
	LBD loop occurred. Packet discard begun	Port <portNum> VID <vid> LBD loop occurred. Packet discard begun	Critical
	LBD recovered. Loop detection restarted	Port <portNum> VID <vid> LBD recovered. Loop detection restarted	Informational
	Loop VLAN number overflow,	Loop VLAN number overflow	Informational
DOS	Spoofing attack	Possible spoofing attack from <mac> Port <portNum>	Critical
JWAC	Login OK	JWAC login successful (Username: %s, IP: %s, MAC: %s, Port: %s)	Informational
	Login fail	JWAC login rejected (Username: %s, IP: %s, MAC: %s, Port: %s)	Warning
	Logout normal	JWAC host logout normally (Username: %s, IP: %s, MAC: %s, Port: %s)	Informational
	Logout forcibly	JWAC host logout forcibly (Username: %s, IP: %s, MAC: %s, Port: %s)	Warning
CFM	Cross-connect is detected	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Critical
	Error CFM CCM packet is detected	CFM remote setting error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Warning
	Can not receive remote MEP's CCM packet	CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)	Warning
	Remote MEP's MAC reports an error status	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)	Warning
	Remote MEP detects CFM defects	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)	Informational
External Alarm	External Alarm	External Alarm Channel <channel_id> : <alarm_message>	Critical
MBAC		MAC-AC login successful (MAC: %s, port: %s, VID: %d)	Informational
		MAC-AC login rejected (MAC: %s, port: %s, VID: %d)	Informational
		MAC-AC host aged out (MAC: %s, port: %s, VID: %d)	Informational
DDM		Port %d SFP %s exceeded the %s alarm threshold	Critical

		Port %d SFP %s exceeded the %s warning threshold	Warning
IP and Password Changed	IP Address change activity	Management IP address was changed by (Username: <username>)	Informational
	Password change activity	Password was changed by (Username: <username>)	Informational
Dual Configuration	Excution error encountered druring system boot-up	Configuration had <int> syntax error and <int> execute error	Warning
802.1X	VID assigned from RADIUS server after RADIUS client authenticated by RADIUS server successfully. This VID will assign to the port and this port will be the VLAN untagged port member.	Radius server <ipaddr> assigned vid :<vlanID> to port <portNum> (account :<username>)	Informational
	Ingress bandwidth assigned from RADIUS server after RADIUS client authenticated by RADIUS server successfully. This Ingress bandwidth will assign to the port.	Radius server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <portNum> (account : <username>)	Informational
	Egress bandwidth assigned from RADIUS server after RADIUS client authenticated by RADIUS server successfully. This egress bandwidth will assign to the port.	Radius server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <portNum> (account: <username>)	Informational
	802.1p default priority assigned from RADIUS server after RADIUS client authenticated by RADIUS server successfully. This 802.1p default priority will assign to the port.	Radius server <ipaddr> assigned 802.1p deafult priority:<priority> to port <portNum> (account : <username>)	Informational
	802.1X Authentication failure	802.1x Authentication failure [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Warning
	802.1X Authentication success	802.1x Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Informational
DHCP	Detect untrusted DHCP server IP address	Detected untrusted DHCP server(IP: <ipaddr>, Port: <portNum>)	Informational
MBAC	Login OK	MAC-AC login successful (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Informational
	Login Fail	MAC-AC login rejected (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Warning

	Aged out	MAC-AC host aged out (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Informational

DAS-3626 Trap List

Trap Name/OID	Variable Bind	Format	MIB Name	Severity
coldStart 1.3.6.1.6.3.1.1.5.1	None	V2	RFC1907 (SNMPv2-MIB)	Critical
WarmStart 1.3.6.1.6.3.1.1.5.2	None	V2	RFC1907 (SNMPv2-MIB)	Critical
authenticationFailure 1.3.6.1.6.3.1.1.5.5	None	V2	RFC1907 (SNMPv2-MIB)	Informational
linkDown 1.3.6.1.6.3.1.1.5.3	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)	Informational
linkup 1.3.6.1.6.3.1.1.5.4	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)	Informational
newRoot	None	V2	RFC1493 (BRIDGE-MIB)	Informational
topologyChange	None	V2	RFC1493 (BRIDGE-MIB)	Informational

Proprietary Trap List

Trap Name/OID	Variable Bind	Format	MIB Name	Severity
swL2macNotification 1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.1	swL2macNotifyInfo	V2	L2Mgmt-MIB	Warning
SwIpMacBindingViolationTrap 1.3.6.1.4.1.171.12.23.5.0.1	swIpMacBindingPortIndex swIpMacBindingViolationIP swIpMacBindingViolationMac	V2	IPMacBind-MIB	Warning
swPktStormOccurred 1.3.6.1.4.1.171.12.25.5.0.1	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB	Warning
swPktStormCleared 1.3.6.1.4.1.171.12.25.5.0.2	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB	Warning
swSafeGuardChgToExhausted 1.3.6.1.4.1.171.12.19.4.1.0.1	swSafeGuardCurrentStatus	V2	SAFEGUARD-ENGINE-MIB	Warning
swSafeGuardChgToNormal 1.3.6.1.4.1.171.12.19.4.1.0.2	swSafeGuardCurrentStatus	V2	SAFEGUARD-ENGINE-MIB	Warning
swPowerStatusChg 1.3.6.1.4.1.171.12.11.2.2.2.0.1	swPowerStatusChgSeverity	V2	EQUIPMENT-MIB	Warning
swFanFailure	swFanFailureSeverity	V2	EQUIPMENT-	Warning

1.3.6.1.4.1.171.12.11.2.2.3.0.1			MIB	
swFanRecover 1.3.6.1.4.1.171.12.11.2.2.3.0.2	swFanRecoverSeverity	V2	EQUIPMENT-MIB	Warning
swMacBasedAuthLoggedSuccess 1.3.6.1.4.1.171.12.35.11.1.0.1	swMacBasedAuthLoggedSuccess	V2	MBA-MIB	Warning
SwMacBasedAuthLoggedFail 1.3.6.1.4.1.171.12.35.11.1.0.2	SwMacBasedAuthLoggedFail	V2	MBA-MIB	Warning
SwMacBasedAuthAgesOut 1.3.6.1.4.1.171.12.35.11.1.0.3	SwMacBasedAuthAgesOut	V2	MBA-MIB	Warning
SwExternalAlarm 1.3.6.1.4.1.171.12.11.2.2.5.0.1	swExternalAlarm	V2	EQUIPMENT-MIB	Warning
SwDdmAlarmTrap 1.3.6.1.4.1.171.12.72.4.0.1	swDdmAlarmTrap	V2	DDM-MIB	Warning
SwDdmWarningTrap 1.3.6.1.4.1.171.12.72.4.0.2	swDdmWarningTrap	V2	DDM-MIB	Warning
swL2PortLoopOccurred 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.3	swL2PortLoopOccurred	V2	L2Mgmt-MIB	Warning
swL2PortLoopRestart 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.4	swL2PortLoopRestart	V2	L2Mgmt-MIB	Warning
swL2VlanLoopOccurred 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.5	swL2VlanLoopOccurred	V2	L2Mgmt-MIB	Warning
swL2VlanLoopRestart 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.6	swL2VlanLoopRestart	V2	L2Mgmt-MIB	Warning

Glossary

1000BASE-SX: A short laser wavelength on multimode fiber optic cable for a maximum length of 500 meters

1000BASE-LX: A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers

1000BASE-T: 1000Mbps Ethernet implementation over Category 5E cable.

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

aging: The automatic removal of dynamic entries from the switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation: A feature on a port, which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The switching speed of a line. Also known as line speed between network segments.

BOOTP: The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher-level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching: The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet: A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the Ethernet/CMSA/CD network access method.

Flow Control: (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN - Local Area Network: A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI - Medium Dependent Interface: An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X - Medium Dependent Interface Cross-over: An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB - Management Information Base: Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link: A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS - Redundant Power System: A device that provides a backup source of power when connected to the switch.

server farm: A cluster of servers in a centralized location serving a large user population.

SLIP - Serial Line Internet Protocol: A protocol, which allows IP to run over a serial line connection.

SNMP - Simple Network Management Protocol: A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

stack: A group of network devices that are integrated to form a single logical device.

standby port: The port in a resilient link that will take over data transmission if the main port in the link fails.

switch: A device, which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP - Trivial File Transfer Protocol: Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

UDP - User Datagram Protocol: An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN - Virtual LAN: A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT - Virtual LAN Trunk: A switch-to-switch link which carries traffic for all the VLANs on each switch.

VT100: A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.

Password Recovery Procedure

This section 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 section will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on 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 runtime image 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.B06
-----------------------------------------------------------------------------

  Power On Self Test ......................................  100%

  MAC Address    : 00-19-5B-EC-32-15
  H/W Version    : A1

  Please wait, loading V1.00.B031 Runtime image.............  00 %

The switch is now entering Password Recovery Mode:_


The switch is currently in 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 will be back to the default value
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 password of all users will be reset.

Command	Parameters
show account	The show account command displays all previously created accounts.