



XSTACK[®]

Web UI Reference Guide

Product Model: **xStack**[®] DES-3200 Series
Layer 2 Managed Fast Ethernet Switch
Release 1.28



Information in this document is subject to change without notice.

© 2011 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

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

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

March 2011 P/N 651ES3200045G

Table of Contents

Intended Readers	viii
Typographical Conventions	viii
Notes, Notices, and Cautions	viii
Web-based Switch Configuration	9
Introduction	9
Login to Web Manager	9
Web-based User Interface	10
Web Pages	11
Configuration	12
Device Information	13
System Information	13
Serial Port Settings	14
IP Address Settings	15
IPv6 Address Settings	17
IPv6 Route Settings	18
IPv6 Neighbor Settings	18
Port Configuration	19
Port Settings	19
Port Description Settings	21
Port Error Disabled	21
Static ARP Settings	22
User Accounts	23
System Log Configuration	24
System Log Settings	24
System Log Server	24
DHCP Relay	26
DHCP Relay Global Settings	26
DHCP Relay Interface Settings	29
DHCP Local Relay Settings	29
DHCP Auto Configuration Settings	30
MAC Address Aging Time	30
Web Settings	31
Telnet Settings	31
Password Encryption	31
CLI Paging Settings	32
Firmware Information	33
SNTP Settings	34
Time Settings	34
Time Zone Settings	35
SMTP Settings	37

SMTP Service Settings	37
SMTP Service	38
MAC Notification Settings	38
MAC Notification Global Settings	38
MAC Notification Port Settings	38
SNMP Settings	39
SNMP View Table	40
SNMP Group Table	41
SNMP User Table	42
SNMP Community Table	43
SNMP Host Table	44
SNMP Trap Configuration	45
RMON	45
Time Range Settings	46
Single IP Management	46
Single IP Settings	48
Topology	49
Tool Tips	51
Right-Click	52
Menu Bar	54
Firmware Upgrade	55
Configuration File Backup/Restore	55
Upload Log File	56
Gratuitous ARP	56
Gratuitous ARP Global Settings	56
Gratuitous ARP Settings	57
ARP Spoofing Prevention Settings	58
PPPoE Circuit ID Insertion Settings	59
L2 Features	60
Jumbo Frame	60
VLANs	61
Understanding IEEE 802.1p Priority	61
VLAN Description	61
IEEE 802.1Q VLANs	62
Q-in-Q VLANs	65
802.1Q Static VLAN	67
Q-in-Q	70
Q-in-Q Settings	71
VLAN Translation Settings	72
802.1v Protocol VLAN	72
802.1v Protocol Group Settings	72
802.1v Protocol VLAN Settings	74
VLAN Trunk Settings	75

GVRP Settings.....	76
Asymmetric VLAN Settings.....	77
MAC-based VLAN Settings	77
PVID Auto Assign Settings	78
Port Trunking	78
LACP Port Settings.....	80
Traffic Segmentation.....	81
Layer 2 Protocol Tunneling Settings.....	82
BPDU Attack Protection Settings	83
IGMP Snooping	84
IGMP Snooping Settings.....	84
IGMP Access Control Settings.....	86
IGMP Snooping Multicast VLAN Settings	87
IP Multicast Profile Settings	88
Limited Multicast Range Settings.....	90
Max Multicast Group Settings	90
MLD Snooping Settings	91
Port Mirror	94
Loopback Detection Settings.....	94
Spanning Tree	96
STP Bridge Global Settings	98
STP Port Settings	99
MST Configuration Identification.....	101
STP Instance Settings	102
MSTP Port Information	103
Forwarding & Filtering.....	103
Unicast Forwarding Settings	103
Multicast Forwarding Settings.....	104
Multicast Filtering Mode	105
NLB Settings.....	106
LLDP	106
LLDP Global Settings.....	107
LLDP Port Settings	108
LLDP Basic TLVs Settings.....	109
LLDP Dot1 TLVs Settings	110
LLDP Dot3 TLVs Settings	111
Ethernet OAM	112
Ethernet OAM Port Settings.....	112
Ethernet OAM Event Configuration.....	113
Connectivity Fault Management (CFM).....	114
CFM Settings	116
CFM MA Settings.....	117
CFM MEP Settings	118

CFM Port Settings.....	120
CFM Loopback Settings.....	121
CFM Linktrace Settings.....	122
ERPS Settings	123
QoS	125
Advantages of QoS.....	125
Understanding QoS	126
Bandwidth Control	127
Traffic Control	128
Queue Bandwidth Control Settings	130
802.1p Default Priority	131
802.1p User Priority	131
QoS Scheduling Settings.....	132
Priority Mapping	133
TOS Mapping.....	134
DSCP Mapping	135
Security.....	136
Safeguard Engine	136
Trusted Host	138
IP-MAC-Port Binding	138
IMP Binding Global Settings	139
IMP Binding Port Settings	140
IMP Binding Entry Settings	141
DHCP Snooping Entries	142
MAC Block List.....	142
Port Security	142
Port Security Port Settings.....	142
Port Security FDB Entries	144
802.1X.....	144
Understanding 802.1X Port-based and Host-based Network Access Control.....	147
Port-based Network Access Control	147
Host-based Network Access Control	148
802.1X Settings.....	149
802.1X User	150
Authentication RADIUS Server	151
Guest VLAN Configuration.....	152
Guest VLAN	153
Initialize Port(s)	153
Reauthenticate Port(s)	154
SSL Settings	155
Download Certificate.....	156
Ciphersuite.....	156
SSH.....	157

SSH Settings.....	158
SSH Authmode and Algorithm Settings	158
SSH User Authentication Lists	160
Access Authentication Control.....	161
Authentication Policy Settings.....	162
Application Authentication Settings.....	162
Authentication Server Group.....	163
Authentication Server.....	164
Login Method Lists.....	165
Enable Method Lists	166
Local Enable Password Settings.....	167
MAC-based Access Control.....	168
MAC-based Access Control Settings	168
MAC-based Access Control Local Settings.....	170
DoS Prevention Settings.....	171
DHCP Server Screening Settings.....	172
DHCP Server Screening Port Settings.....	172
DHCP Offer Permit Entry Setting	174
ACL	175
ACL Configuration Wizard	175
Access Profile List	176
CPU Interface Filtering	193
CPU Access Profile List.....	193
ACL Finder.....	207
ACL Flow Meter	207
Monitoring	209
Cable Diagnostics.....	209
CPU Utilization.....	210
Port Utilization.....	211
Packet Size.....	212
Memory Utilization	213
Packets	214
Received (Rx)	214
UMB_cast (Rx).....	216
Transmitted (Tx).....	217
Errors	219
Received (RX).....	219
Transmitted (TX)	221
Port Access Control	223
RADIUS Authentication.....	223
RADIUS Account Client	225
Authenticator State	227
Authenticator Statistics	228

Authenticator Diagnostics	232
Browse ARP Table	234
Browse VLAN	234
IGMP Snooping	234
Browse IGMP Router Port.....	234
IGMP Snooping Group.....	235
IGMP Snooping Host	236
MLD Snooping	236
Browse MLD Router Port.....	236
MLD Snooping Group	237
LLDP	237
LLDP Statistics System.....	237
LLDP Local Port Information.....	238
LLDP Remote Port Information.....	238
Ethernet OAM	239
Browse Ethernet OAM Event Log	239
Browse Ethernet OAM Statistics	239
Connectivity Fault Management	240
CFM Fault Table	240
CFM MP Table.....	240
CFM Packet Counter	241
CFM MIPCCM Table.....	241
MAC-based Access Control Authentication State	242
Browse Session Table	242
MAC Address Table.....	243
System Log.....	244
Save and Tools.....	245
Save Configuration	245
Save Log.....	246
Save All.....	246
Configuration File Upload & Download.....	246
Upload Log File.....	247
Reset.....	247
Ping Test.....	248
Download Firmware.....	249
Reboot System	249
Appendix A Password Recovery Procedure	250
Appendix B System Log Entries.....	252
Appendix C Trap List.....	263
Appendix D RADIUS Attributes Assignment	268

Intended Readers

The *DES-3200 Series Web UI Reference Guide* contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel . Used for emphasis. May also indicate system messages or prompts appearing on 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

Login to Web Manager

Web-based User Interface

Web Pages

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 Firefox, Microsoft Internet Explorer, Mozilla, or Netscape. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

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

Login to Web Manager

To begin managing the Switch, simply 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.



NOTE: The Factory default IP address for the Switch is 10.90.90.90.

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

Connect to 10.90.90.90

User name: admin

Password:

Remember my password

OK Cancel

Figure 1 - 1 Enter Network Password dialog

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

Web-based User Interface

The user interface provides access to various Switch configuration and management 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.

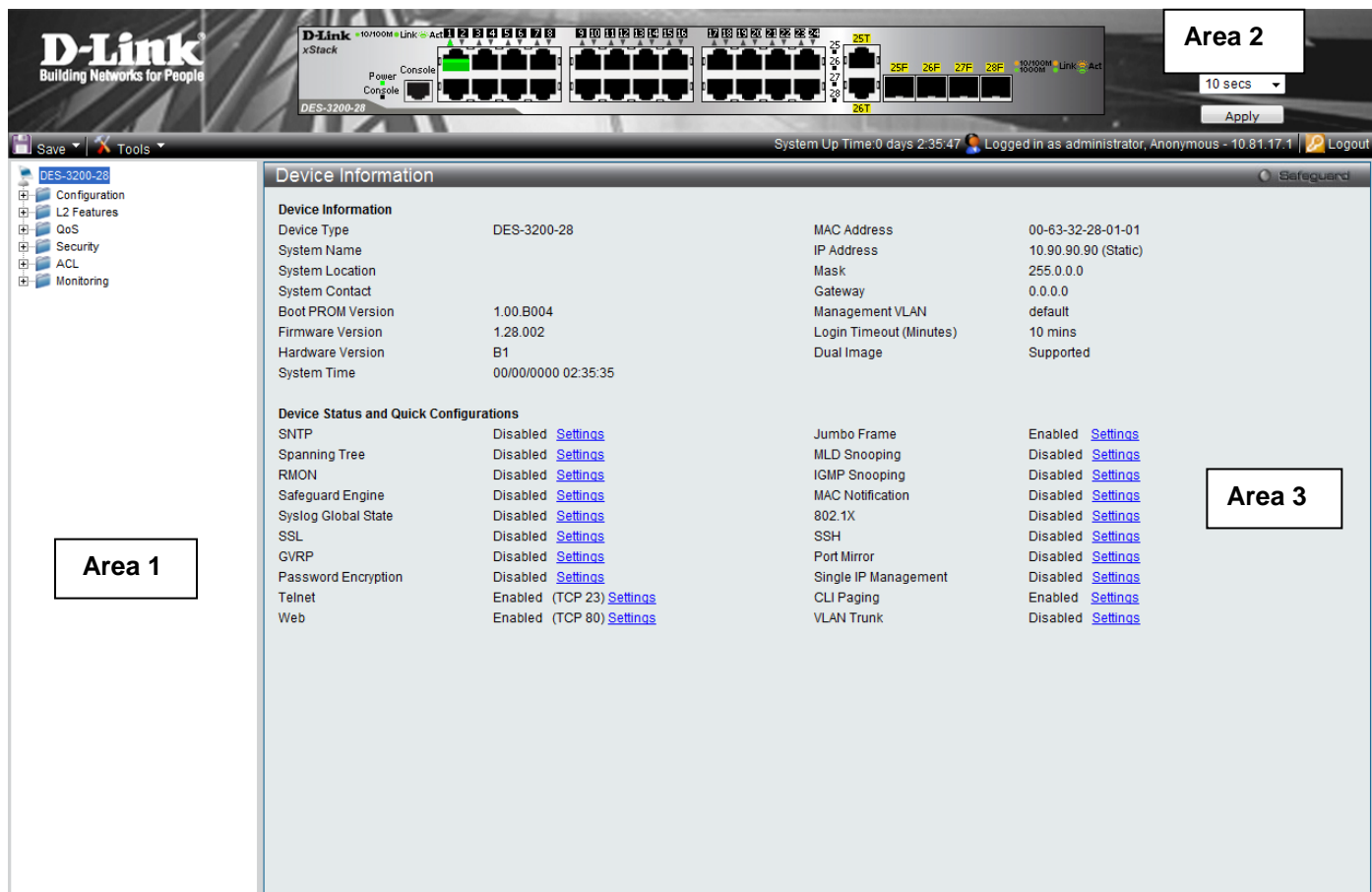


Figure 1 - 2 Main Web-Manager page

Area	Function
Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyperlinked 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, duplex mode, or flow control, depending on the specified mode. 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.



NOTICE: Any changes made to the Switch configuration during the current session must be saved in the **Save Configuration** window (**Save > Save Configuration**) or use the command line interface (CLI) command **save config**.

Web Pages

When you connect to the management mode of the Switch with a Web browser, a login window is displayed. Enter a user name and password to access the Switch's management mode.

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

Configuration – Contains main windows concerning Device Information, System Information, Serial Port Settings, IP Address, IPv6 Interface Settings, IPv6 Route Settings, IPv6 Neighbor Settings, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, DHCP Relay, DHCP Auto Configuration Settings, MAC Address Aging Time, Web Settings, Telnet Settings, Password Encryption, CLI Paging Settings, Firmware Information, SNTP Settings, SMTP Settings, MAC Notification Settings, SNMP Settings, Time Range Settings, Single IP Management, Gratuitous ARP, ARP Spoofing Prevention Settings and PPPoE Circuit ID Insertion Settings.

L2 Features – Contains main windows concerning Jumbo Frame, 802.1Q Static VLAN, Q-in-Q, 802.1v Protocol VLAN, VLAN Trunk Settings, GVRP Settings, Asymmetric VLAN Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, L2PT Settings, IGMP Snooping, MLD Snooping Settings, Port Mirror, Loopback Detection Settings, Spanning Tree, Forwarding & Filtering, NLB Settings, LLDP, Ethernet OAM, Connectivity Failure Management, and ERPS Settings.

QoS – Contains main windows concerning Bandwidth Control, Queue Bandwidth Control Settings, Traffic Control, Queue Bandwidth Control Settings, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Settings, Priority Mapping, TOS Mapping, and DSCP Mapping.

Security – Contains main windows concerning Safeguard Engine, Trusted Host, IP-MAC-Port Binding, Port Security, 802.1X, SSL Settings, SSH, Access Authentication Control, MAC-based Access Control, DoS Prevention Settings and DHCP Server Screening.

ACL – Contains main windows concerning ACL Configuration Wizard, Access Profile List, CPU Access Profile List, ACL Finder, and ACL Flow Meter.

Monitoring – Contains main windows concerning Cable Diagnostics, CPU Utilization, Port Utilization, Packet Size, Memory Utilization, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, IGMP Snooping, MLD Snooping, LLDP, Connectivity Failure Management, MAC-based Access Control Authentication State, Browse Session Table, MAC Address Table, and System Log.

Save & Tools – Contains main windows concerning Save Configuration, Save Log, Save All, Configuration File Upload & Download, Upload Log File, Reset, Ping Test, Download Firmware, and Reboot System.



NOTE: Be sure to configure the user name and password in the **User Accounts** window (**Configuration > User Accounts**) before connecting the Switch to the greater network.

Section 2

Configuration

Device Information

System Information

Serial Port Settings

IP Address Settings

IPv6 Interface Settings

IPv6 Route Settings

IPv6 Neighbor Settings

Port Configuration

Static ARP Settings

User Accounts

System Log Configuration

DHCP Relay

DHCP Auto Configuration Settings

MAC Address Aging Time

Web Settings

Telnet Settings

Password Encryption

CLI Paging Settings

Firmware Information

SNTP Settings

SMTP Settings

MAC Notification Settings

SNMP Settings

Time Range Settings

Single IP Management

Gratuitous ARP

ARP Spoofing Prevention Settings

PPPoE Circuit ID Insertion Settings

Device Information

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** window, click the **DES-3200 Series** folder. The **Device Information** window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version, the Hardware Version, and 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.

The screenshot shows the 'Device Information' window with a 'Safeguard' indicator in the top right. It is divided into two main sections: 'Device Information' and 'Device Status and Quick Configurations'.

Device Information			
Device Type	DES-3200-28	MAC Address	00-63-32-28-01-01
System Name		IP Address	10.90.90.90 (Static)
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	1.00.B004	Management VLAN	default
Firmware Version	1.28.002	Login Timeout (Minutes)	10 mins
Hardware Version	B1	Dual Image	Supported
System Time	00/00/0000 02:35:35		

Device Status and Quick Configurations			
SNTP	Disabled	Jumbo Frame	Enabled
Spanning Tree	Disabled	MLD Snooping	Disabled
RMON	Disabled	IGMP Snooping	Disabled
Safeguard Engine	Disabled	MAC Notification	Disabled
Syslog Global State	Disabled	802.1X	Disabled
SSL	Disabled	SSH	Disabled
GVRP	Disabled	Port Mirror	Disabled
Password Encryption	Disabled	Single IP Management	Disabled
Telnet	Enabled (TCP 23)	CLI Paging	Enabled
Web	Enabled (TCP 80)	VLAN Trunk	Disabled

Figure 2 - 1. Device Information window

System Information

This window contains the System Information details. The user may enter a System Name, System Location and System Contact to aid in defining the Switch, to the user's preference. This window displays the MAC Address, Firmware Version and Hardware Version.

Click **Configuration > System Information** to display the following window:

The screenshot shows the 'System Information' window with a 'Safeguard' indicator in the top right. It displays read-only information and three input fields.

MAC Address	00-63-32-28-01-01
Firmware Version	1.28.002
Hardware Version	B1
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

Figure 2 - 2. System Information window

The fields that can be configured are described below:

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.

Click **Apply** to implement changes made.

Serial Port Settings

The following window allows the Baud Rate and the Auto Logout to be changed as well as containing information about the Serial Port Settings.

Click **Configuration > Serial Port Settings** to display this window:

Parameter	Value
Baud Rate	9600
Auto Logout	10 minutes
Data Bits	8
Parity Bits	None
Stop Bits	1

Figure 2 - 3. Serial Port Settings window

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

Click **Apply** to implement changes made.



NOTE: If a user configures the serial port's baud rate, the baud rate will take effect and save immediately.

IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the introduction of the *DES-3200 Series CLI Reference Manual* for more information.

Click **Configuration > IP Address Settings** to display the following window:

Figure 2 - 4. IP Address Settings window

To manually assign the Switch's IP address, subnet mask, and default gateway address:

1. Click *Static* at the top of the window.
2. Enter the appropriate IPv4 Address and Subnet Mask.
3. To access the Switch from a different subnet from the one it is installed on, enter the IP address of the Gateway. If the Switch will be managed from the subnet on which it is installed, leave the default address (0.0.0.0) in this field.
4. If no VLANs have been previously configured on the Switch, you can use the *default* Management VLAN Name. The *default* VLAN contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, the Management VLAN Name of the VLAN that contains the port connected to the management station will have to be entered to access the Switch.
5. Use the drop-down Interface Admin State menu to select *Enabled* if it has not already been done.



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

To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address, select either *BOOTP* or *DHCP*.

The IP Address Settings options are:

Parameter	Description
Static	Allows the entry of an IPv4 address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
IP Interface	The current IP Interface being assigned an IP address on this window.
Management VLAN Name	This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management window. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned.
Interface Admin State	Toggle between <i>Enabled</i> and <i>Disabled</i> . This must be set to <i>Enabled</i> when setting an IP address on this window.
IPv4 Address	Enter the desired IPv4 address to be set. The default address is <i>10.90.90.90</i> .
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
DHCP Option 12 State	Use to enable or disable DHCP Option 12.
DHCP Option 12 Host Name	Type the name of the host used for Option 12. Up to 63 characters are allowed.

Click **Apply** to allow changes to take effect.

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands **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.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the x's represent the IP address to be assigned to the IP interface named System and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

IPv6 Address Settings

Users can display the Switch's current IPv6 interface settings.

To view the following window, click **Configuration > IPv6 Interface Settings**:

Interface Name	System
VLAN Name	default
Admin. State	Disabled
IPv6 Address	<input type="text"/>
Automatic Link Local Address	Disabled
NS Retransmit Time (0-4294967295)	<input type="text"/> ms

IPv6 Type	IPv6 Address

Figure 2 - 5. IPv6 Interface Settings window

To configure IPv6 interface settings, enter an IPv6 Address and click **Apply**. The new entry will appear in the table at the bottom of the window.

After making the desired changes, click the **Apply** button.

The following parameters may be configured or viewed:

Parameter	Description
Interface Name	The name of the IPv6 interface being displayed or modified.
VLAN Name	Display the VLAN name of the IPv6 interface.
Admin. State	Display the current administrator state.
IPv6 Address	Enter the IPv6 address of the interface to be modified.
Automatic Link Local Address	Toggle between <i>Enabled</i> and <i>Disabled</i> . Enabling this is helpful when no external source of network addressing information is available.
NS Retransmit Time (0-4294967295)	Enter a value between 0 and 4294967295. This is the neighbor solicitation's retransmit timer in milliseconds. The default is zero.

IPv6 Route Settings

The user can configure the Switch's IPv6 Route Table.

To view the following window, click **Configuration > IPv6 Route Settings**:

Figure 2 - 6. IPv6 Route Settings window

Enter an IP Interface, an IPv6 address in the Default Gateway field and then click the **Create** button. In addition, the Metric can be entered between 1 and 65535. The new IPv6 route will be displayed in the table at the bottom of the window.

IPv6 Neighbor Settings

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

To view the following window, click **Configuration > IPv6 Neighbor Settings**:

Figure 2 - 7. IPv6 Neighbor Settings window

Enter the Interface Name, Neighbor IPv6 Address, and the Link Layer MAC Address and then click the **Add** button.

To look for an IPv6 Neighbor Settings table entry, enter the Interface Name, select the desired State (*All*, *Address*, *Static*, or *Dynamic*) in the middle section of this window, and then click the **Find** button.

To delete all the entries being displayed on the table at the bottom of this window, click the **Clear** button.

The following parameters may be configured or viewed:

Parameter	Description
Interface Name	Enter the name of the IPv6 neighbor. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window, tick the All check box, and then click the Find button.
Neighbor IPv6 Address	Enter the neighbor IPv6 address.
Link Layer MAC Address	Enter the link layer MAC address.
State	Use the drop-down menu to select <i>All</i> , <i>Address</i> , <i>Static</i> , or <i>Dynamic</i> .

Port Configuration

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control.

Port Settings

Various port settings, including State, Speed/Duplex, Flow Control, Address Learning, Medium Type, and MDIX can be configured on the Switch.

To view the following window, click **Configuration > Port Configuration > Port Settings**:

Port	State	Speed/Duplex	Flow Control	Connection	Address Learning	MDIX
01	Enabled	Auto	Disabled	100M/Full/None	Enabled	Auto
02	Enabled	Auto	Disabled	Link Down	Enabled	Auto
03	Enabled	Auto	Disabled	Link Down	Enabled	Auto
04	Enabled	Auto	Disabled	Link Down	Enabled	Auto
05	Enabled	Auto	Disabled	Link Down	Enabled	Auto
06	Enabled	Auto	Disabled	Link Down	Enabled	Auto
07	Enabled	Auto	Disabled	Link Down	Enabled	Auto
08	Enabled	Auto	Disabled	Link Down	Enabled	Auto
09	Enabled	Auto	Disabled	Link Down	Enabled	Auto
10	Enabled	Auto	Disabled	Link Down	Enabled	Auto
11	Enabled	Auto	Disabled	Link Down	Enabled	Auto
12	Enabled	Auto	Disabled	Link Down	Enabled	Auto
13	Enabled	Auto	Disabled	Link Down	Enabled	Auto
14	Enabled	Auto	Disabled	Link Down	Enabled	Auto
15	Enabled	Auto	Disabled	Link Down	Enabled	Auto
16	Enabled	Auto	Disabled	Link Down	Enabled	Auto
17	Enabled	Auto	Disabled	Link Down	Enabled	Auto
18	Enabled	Auto	Disabled	Link Down	Enabled	Auto
19	Enabled	Auto	Disabled	Link Down	Enabled	Auto
20	Enabled	Auto	Disabled	Link Down	Enabled	Auto
21	Enabled	Auto	Disabled	Link Down	Enabled	Auto
22	Enabled	Auto	Disabled	Link Down	Enabled	Auto
23	Enabled	Auto	Disabled	Link Down	Enabled	Auto
24	Enabled	Auto	Disabled	Link Down	Enabled	Auto
25 (C)	Enabled	Auto	Disabled	Link Down	Enabled	Auto
25 (F)	Enabled	Auto	Disabled	Link Down	Enabled	Auto
26 (C)	Enabled	Auto	Disabled	Link Down	Enabled	Auto

Figure 2 - 8. Port Settings window

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

Parameter	Description
From Port/To Port	Use the pull-down menus to select the port or range of ports to be configured.
State	Toggle this field to either enable or disable a given port or group of ports.
Speed/Duplex	<p>Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. <i>Auto</i> denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The <i>Auto</i> setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are <i>Auto</i>, <i>10M Half</i>, <i>10M Full</i>, <i>100M Half</i> and <i>100M Full</i>, <i>1000M Full_Master</i>, <i>1000M Full_Slave</i> and <i>1000M Full</i>. There is no automatic adjustment of port settings with any option other than <i>Auto</i>.</p> <p>The Switch allows the user to configure two types of gigabit connections; <i>1000M/Full_M</i> and <i>1000M/Full_S</i>. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed.</p> <p>The <i>1000M Full_Master</i> and <i>1000M Full_Slave</i> parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (<i>1000M Full_Master</i>) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (<i>1000M Full_Slave</i>) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for <i>1000M Full_Master</i>, the other side of the connection must be set for <i>1000M Full_Slave</i>. Any other configuration will result in a link down status for both ports.</p>
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and <i>Auto</i> ports use an automatic selection of the two. The default is <i>Disabled</i> .
Address Learning	When <i>Enabled</i> , destination and source MAC addresses are automatically listed in the forwarding table. The default setting is <i>Enabled</i> .
Medium Type	This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be set at <i>Fiber</i> and the Combo 1000BASE-T ports should be set at <i>Copper</i> .
MDIX	This can be specified as <i>Auto</i> , <i>Normal</i> , or <i>Cross</i> . In <i>Normal</i> state, the port is in MDIX mode and can be connected to a PC NIC using a straight cable. If it is in <i>Cross</i> state, the port is in MDI mode, and can be connected to a port (in MDIX mode) on another switch through a straight cable.

Click **Apply** to implement the new settings on the Switch.

Port Description Settings

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

To view the following window, click **Configuration > Port Configuration > Port Description Settings**:

Figure 2 - 9. Port Description Settings window

Use the From Port and To Port pull-down menus to choose a port or range of ports to describe, and then enter a description of the port(s).

The Medium Type applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be nominated *Fiber* and the Combo 1000BASE-T ports should be nominated *Copper*. The result will be displayed in the appropriate switch port number slot (C for copper ports and F for fiber ports).

The following parameters can be configured:

Parameter	Description
From Port/To Port	Use the pull-down menus to select the port or range of ports to be configured.
Medium Type	This only applies to the Combo ports. If configuring the Combo ports, this defines the type of transport medium used. SFP ports should be set at <i>Fiber</i> and the Combo 1000BASE-T ports should be set at <i>Copper</i> .
Description	The description of the the ports.

Click **Apply** to implement the new settings on the Switch.

Port Error Disabled

The following window will display information about ports that have had their connection status disabled for reasons such as STP loopback detection or link down status.

To view this window, click **Configuration > Port Configuration > Port Error Disabled**:

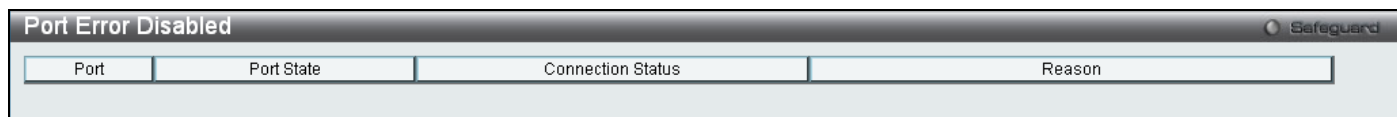


Figure 2 - 10. Port Error Disabled window

The following parameters are displayed:

Parameter	Description
Port	Displays the port that has been error disabled.
Port State	Describes the current running state of the port, whether Enabled or Disabled.
Connection Status	This field will read the uplink status of the individual ports, whether Enabled or Disabled.
Reason	Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

Static ARP Settings

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

To view this window, click **Configuration > Static ARP Settings**

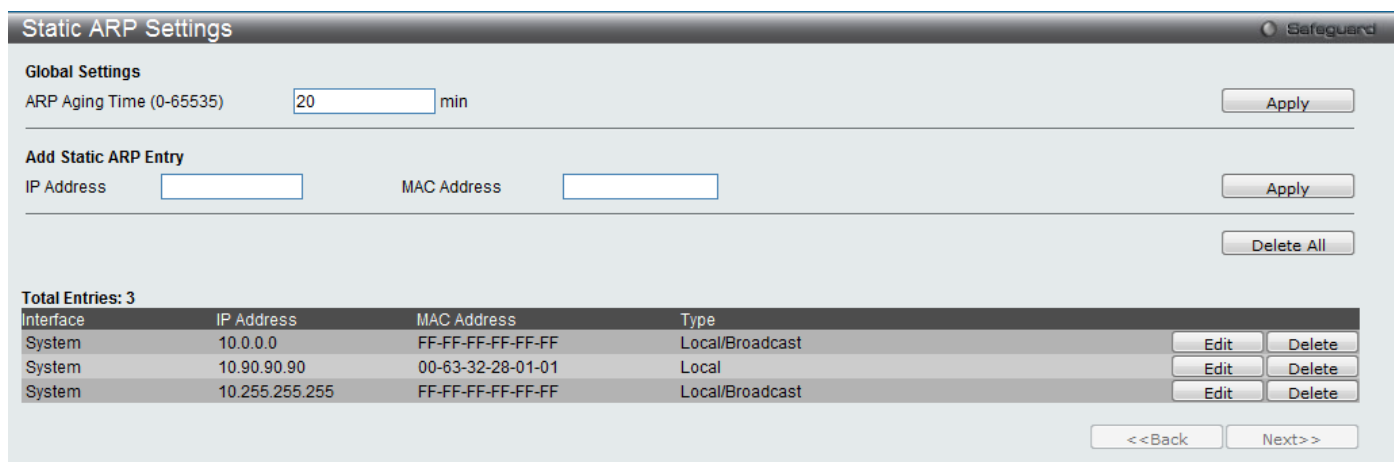


Figure 2 - 11. Static ARP Settings window

The following fields can be set:

Parameter	Description
ARP Aging Time (0-65535)	The user may globally set the maximum amount of time, in seconds, that an Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table. The value may be set in the range of 0 to 65535 seconds, with a default setting of 20 seconds.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To completely clear the Static ARP Settings, click the **Delete All** button. To modify a static ARP entry, click the corresponding **Edit** button in the table. To delete a static ARP entry, click the corresponding **Delete** button in the table.



NOTE: The Switch supports up to 255 static ARP entries.

User Accounts

Use this window to control user privileges, create new users, and view existing User Accounts.

To view this window, click **Configuration > User Accounts**:

Figure 2 - 12. User Accounts window

The following fields can be set:

Parameter	Description
User Name	The name of the user, an alphanumeric string of up to 15 characters.
Password	Enter a password for the new user.
Access Right	There are two levels of user privileges, <i>Admin</i> and <i>User</i> . Some features and selections available to users with <i>Admin</i> privileges may not be available to those with <i>User</i> level privileges. (Table 2 - 1 below summarizes Admin and User level privileges)
Confirm Password	Retype the new password.

To add a new user, enter the appropriate information and click **Apply**. To modify or delete an existing user, click on the **Edit** button for that user.



NOTICE: In case of lost passwords or password corruption, please refer to the “Password Recovery Procedure” Appendix in the **DES-3200 Series CLI Reference Manual** which will guide you through the steps necessary to resolve this issue.

Admin and User Privileges

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

The following table summarizes the Admin and User privileges:

Management	Admin	User
Configuration	Yes	Read-only
Network Monitoring	Yes	Read-only
Community Strings and Trap Stations	Yes	Read-only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	No
Factory Reset	Yes	No

User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Table 2 - 1. Admin 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 configure the system log settings, click **Configuration > System Log Configuration > System Log Settings**

Figure 2 - 13. System Log Settings window

The following parameters can be set:

Parameter	Description
System Log	Use the radio buttons to either enable or disable the system log feature.
Save Mode	Use this drop-down menu to choose the method that will trigger a log entry. Choose among <i>On Demand</i> , <i>Time Interval</i> , and <i>Log Trigger</i> .
min (1-65535)	Enter a time interval, in minutes, for which a log entry is to be made.

To modify the system log settings on this window, 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 configure the system log settings, click **Configuration > System Log Configuration > System Log Server**:

Figure 2 - 14. System Log Server window

The following parameters can be set:

Parameter	Description																																																				
Server ID	Syslog server settings index (1-4).																																																				
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are <i>Warning</i> , <i>Informational</i> , and <i>All</i> .																																																				
Server IP Address	The IP address of the Syslog server.																																																				
Facility	<p>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.</p> <table border="1"> <thead> <tr> <th>Numerical</th> <th>Facility Code</th> <th>Numerical</th> <th>Facility Code</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>kernel messages</td> <td>12</td> <td>NTP subsystem</td> </tr> <tr> <td>1</td> <td>user-level messages</td> <td>13</td> <td>log audit</td> </tr> <tr> <td>2</td> <td>mail system</td> <td>14</td> <td>log alert</td> </tr> <tr> <td>3</td> <td>system daemons</td> <td>15</td> <td>clock daemon</td> </tr> <tr> <td>4</td> <td>security/authorization messages</td> <td>16</td> <td>local use 0 (local0)</td> </tr> <tr> <td>5</td> <td>messages generated internally by syslog line printer subsystem</td> <td>17</td> <td>local use 1 (local1)</td> </tr> <tr> <td></td> <td></td> <td>18</td> <td>local use 2 (local2)</td> </tr> <tr> <td>7</td> <td>network news subsystem</td> <td>19</td> <td>local use 3 (local3)</td> </tr> <tr> <td>8</td> <td>UUCP subsystem</td> <td>20</td> <td>local use 4 (local4)</td> </tr> <tr> <td>9</td> <td>clock daemon</td> <td>21</td> <td>local use 5 (local5)</td> </tr> <tr> <td>10</td> <td>security/authorization messages</td> <td>22</td> <td>local use 6 (local6)</td> </tr> <tr> <td>11</td> <td>FTP daemon</td> <td>23</td> <td>local use 7 (local7)</td> </tr> </tbody> </table>	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)
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)																																																		
UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is 514.																																																				
Status	Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate.																																																				

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

DHCP Relay

The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is equal to or 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 BOOTREQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 0 and 65,535 seconds, with a default value of 0 seconds.

DHCP Relay Global Settings

To enable and configure DHCP Relay Global Settings on the Switch, click **Configuration > DHCP Relay > DHCP Relay Global Settings**:

Figure 2 - 15. DHCP Relay Global Settings window

The following fields can be set:

Parameter	Description
DHCP Relay State	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP Relay service on the Switch. The default is <i>Disabled</i>
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 BOOTP or 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 BOOTP or DHCP packet.
DHCP Relay Agent Information Option 82 State	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is <i>Disabled</i>.</p> <p><i>Enabled</i> – When this field is toggled to <i>Enabled</i> 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.</p> <p><i>Disabled</i> - If the field is toggled to <i>Disabled</i> the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the</p>

	check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field.</p> <p><i>Enabled</i> – When the field is toggled to <i>Enable</i>, 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.</p> <p><i>Disabled</i> - When the field is toggled to <i>Disabled</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
DHCP Relay Agent Information Option 82 Policy	<p>This field can be toggled between <i>Replace</i>, <i>Drop</i>, and <i>Keep</i> by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Agent Information Option 82 Check is set to <i>Disabled</i>. The default is <i>Replace</i>.</p> <p><i>Replace</i> - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>Drop</i> - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>Keep</i> -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.</p>
DHCP Relay Agent Information Option 82 Remote ID	<p>This field is for you to enter the remote ID. Tick Default to use the Switch's system MAC address as the remote ID.</p>

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.

The Implementation of DHCP Information Option 82 on the Switch

The `config dhcp_relay option_82` command configures the DHCP relay agent information option 82 setting of the switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:



NOTE: For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

a.	b.	c.	d.	e.	f.	g.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

- a. Sub-option type
- b. Length
- c. Circuit ID type
- d. Length
- e. VLAN: the incoming VLAN ID of DHCP client packet.
- f. Module: For a standalone switch, the Module is always 0; for a stackable switch, the Module is the Unit ID.
- g. Port: The incoming port number of DHCP client packet, port number starts from 1.

Remote ID sub-option format: (default)

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 byte	1 byte	1 byte	1 byte	6 bytes

- 1. Sub-option type
- 2. Length
- 3. Remote ID type
- 4. Length
- 5. MAC address: The Switch's system MAC address.

Remote ID sub-option format :(for user-configured string)

1.	2.	3.	4.	5.
2	N+2	1	N	ASCII Remote ID String (up to 127 characters)
1 byte	1 byte	1 byte	1 byte	N bytes

- 1. Sub-option type
- 2. Length
- 3. Remote ID type
- 4. Length
- 5. User configured Remote-ID

Figure 2 - 16. Circuit ID and Remote ID Sub-option Format

DHCP Relay Interface Settings

This window allows the user to set up a server, by IP address, for relaying DHCP/ BOOTP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP 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 enable and configure DHCP Relay Global Settings on the Switch, click **Configuration > DHCP Relay > DHCP Relay Interface Settings**:

Figure 2 - 17. DHCP Relay Interface Settings window

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

DHCP Local Relay Settings

This function on the Switch allows configuration of the DHCP local relay for VLAN.

To view this window, click Configuration > DHCP Local Relay> DHCP Local Relay Settings:

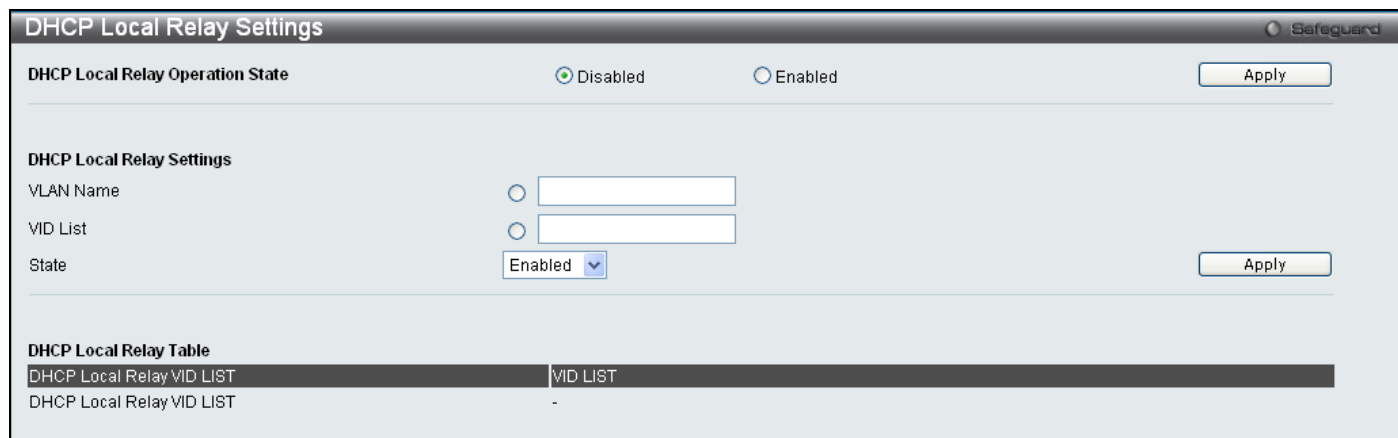


Figure 2 - 18. DHCP Local Relay Settings window

The following parameters may be configured.

Parameter	Description
DHCP Local Relay Operation State	This is used to enable or disable DHCP Local Relay service on the Switch. The default is Disabled.
VLAN Name	Enter a name of the VLAN to be enabled by DHCP local relay.
VID List	Enter a VLAN ID to be enabled by DHCP local relay.
State	This is used to enable or disable the DHCP local relay for the specified VLAN.

DHCP Auto Configuration Settings

The DHCP automatic configuration function on the Switch will load a previously saved configuration file for current use. When DHCP auto configuration is Enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply.

To view this window, click **Configuration > DHCP Auto Configuration Settings**:

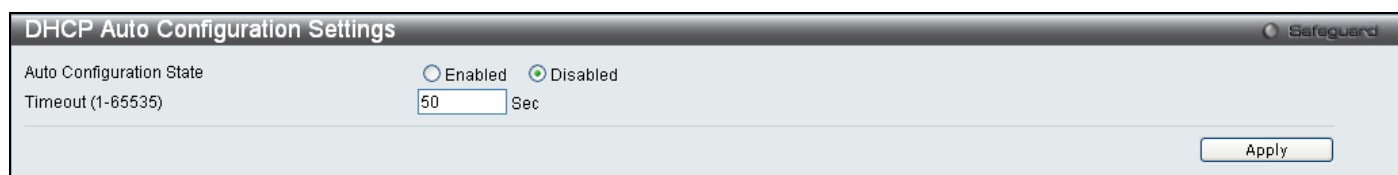


Figure 2 - 19. DHCP Auto Configuration Settings window

When DHCP automatic configuration is Enabled, the Switch becomes a DHCP client automatically after rebooting. The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a configuration file.

If the Switch is unable to complete the automatic configuration process, the previously saved local configuration file present in Switch memory will be loaded.

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 access this window, click **Configuration > MAC Address Aging Time**:

Figure 2 - 20. MAC Address Aging Time window

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. The TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Web protocol is 80.

To access this window, click **Configuration > Web Settings**:

Figure 2 - 21. Web Settings window

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 access this window, click **Configuration > Telnet Settings**:

Figure 2 - 22. Telnet Settings window

Password Encryption

Password Encryption can be Enabled or Disabled in this window. It is Disabled by default. Password encryption allows the user to encrypt a password for additional security. Select Enabled to change the password into encrypted form. When password encryption is Disabled, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last **enable password encryption** command, the password will still be in encrypted form and cannot be reverted back to plain text form.

To access this window, click **Configuration > Password Encryption**:

Figure 2 - 23. Password Encryption window

CLI Paging Settings

CLI paging can be Enabled or Disabled in this window. It is Enabled by default. CLI paging 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 access this window, click **Configuration > CLI Paging Settings**:

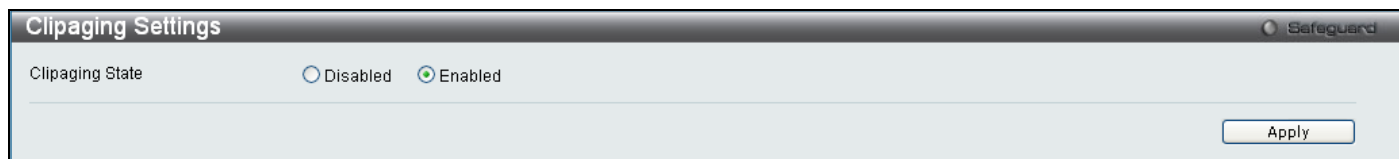


Figure 2 - 24. CLI Paging Settings window

Firmware Information

Information about current firmware images stored on the Switch can be viewed.

To access this window, click **Configuration > Firmware Information**:

ID	Version	Size (B)	Update Time	From	User		
*1	1.28.002	3970944	0000/00/00 21:49:49	10.63.54.1	Anonymous(CONSO...	Boot UP	Delete
2	1.28.001	3798872	0000/00/00 01:32:32	10.63.54.1	Anonymous(CONSO...	Boot UP	Delete

** : Boot up firmware

(SSH) : Firmware update through SSH

(Web) : Firmware update through Web

(SIM) : Firmware update through Single IP Management

(SNMP) : Firmware update through SNMP

(Telnet) : Firmware update through Telnet

(CONSOLE) : Firmware update through CONSOLE

Figure 2 - 25. Firmware Information window

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.
User	States the user who downloaded the firmware. This field may read "Anonymous" or "Unknown" for users that are unidentified.

SNTP Settings

The SNTP Settings folder offers two windows: **Time Settings** and **Time Zone Settings**.

Time Settings

To configure the time settings for the Switch, click **Configuration > SNTP Settings > Time Settings**:

Figure 2 - 26. Time Settings window

The following parameters can be set or are displayed:

Parameter	Description
Status	
SNTP State	Use the radio 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 (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 SNMP.

To configure the time zone settings for the Switch, click **Configuration > SNMP Settings > Time Zone Settings**:

Figure 2 - 27. Time Zone Settings window

The following parameters can be set:

Parameter	Description
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 on.

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

Click **Apply** to implement changes made in this window.

SMTP Settings

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered in the window below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events, and enhancing security by recording questionable events occurring on the Switch.

Users can set up the SMTP server for the Switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

SMTP Service Settings

To view the following window, click **Configuration > SMTP Service Settings**:

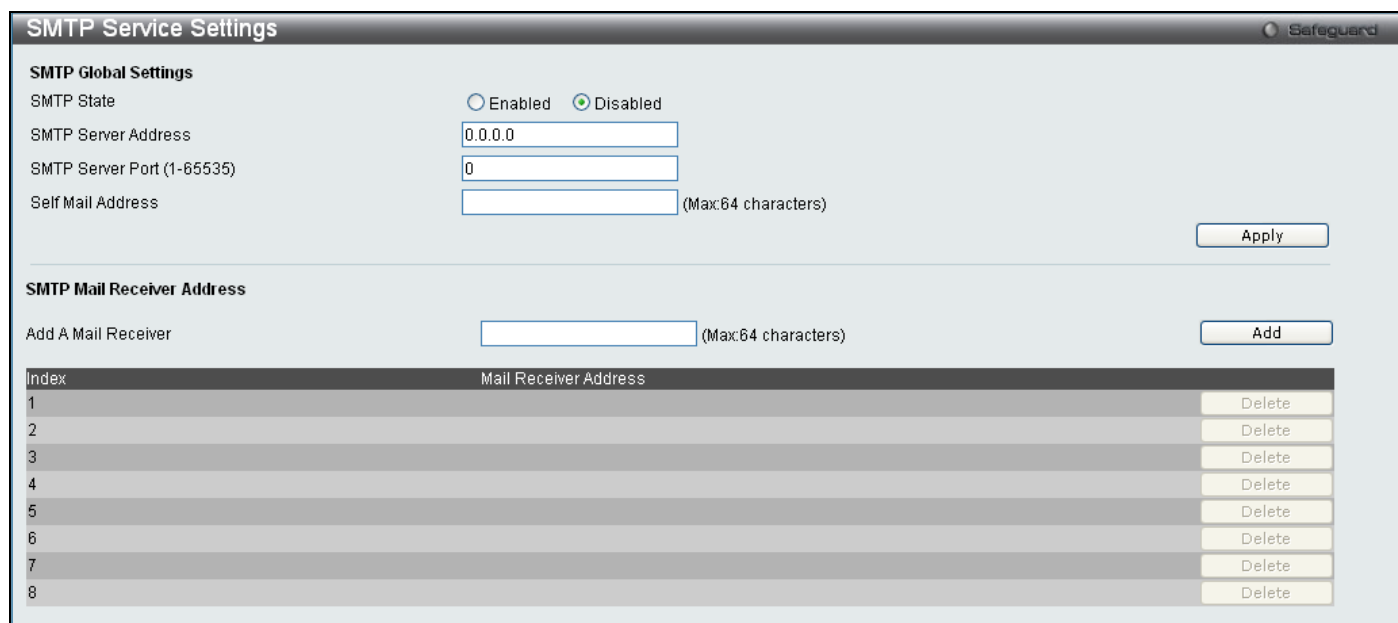


Figure 2 - 28. SMTP Service Settings window

The following parameters may be configured or viewed:

Parameter	Description
SMTP State	Use the radio button to enable or disable the SMTP service on this device.
SMTP Server Address	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port (1-65535)	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25, yet a value between 1 and 65535 can be chosen.
Self Mail Address	Enter the e-mail address from which mail messages will be sent. This address will be the “from” address on the e-mail message sent to a recipient. Only one self-mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters.
Add A Mail Receiver	Enter an e-mail address and click the Add button. Up to eight e-mail addresses can be added per Switch. To delete these addresses from the Switch, click the corresponding Delete button in the SMTP Mail Receiver Address table at the bottom of the window.

SMTP Service

This window is used to test the SMTP Service Settings configured in the previous window.

To view the following window, click **Configuration > SMTP Service**:

Figure 2 - 29. SMTP Service window

To test to see if the SMTP settings are working properly, enter a Subject, Content, and then click the **Send** button.

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, open the following window by opening the **MAC Notification Settings** in the Configuration folder.

MAC Notification Global Settings

To configure the MAC Notification Global Settings for the Switch, click **Configuration > MAC Notification Settings > MAC Notification Global Settings**

Figure 2 - 30. MAC Notification Global Settings window

The following parameters may be viewed and modified:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch.
Interval (1-2147483647 sec)	The time in seconds between notifications.
History Size (1-500)	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

Click **Apply** to implement changes.

MAC Notification Port Settings

To configure the MAC Notification Port Settings for the Switch, click **Configuration > MAC Notification Settings > MAC Notification Port Settings**:

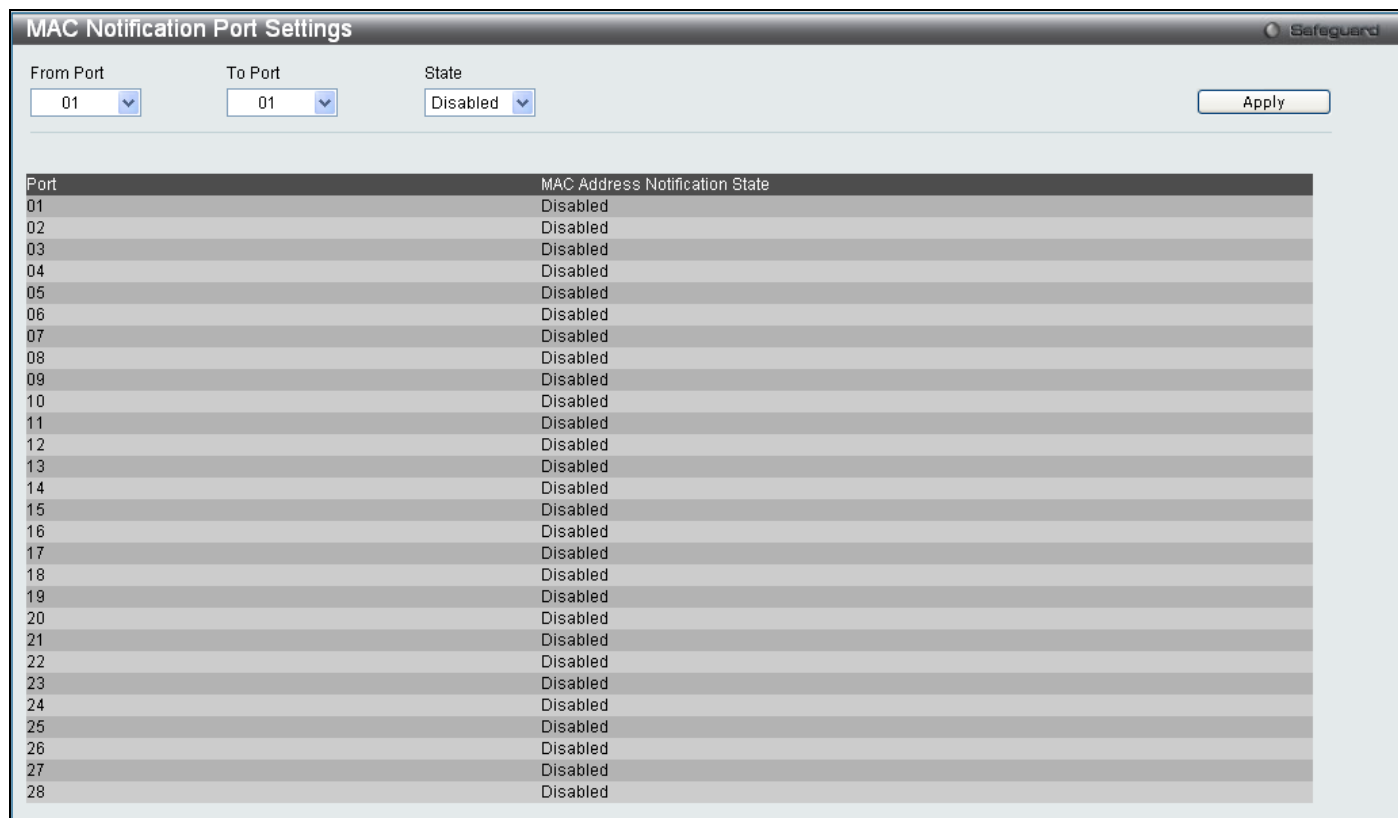


Figure 2 - 31. MAC Notification Port Settings window

The following parameters may be modified:

Parameter	Description
From Port/To Port	Select a port or group of ports to enable for MAC notification using the pull-down menus.
State	Enable MAC Notification for the ports selected using the pull-down menu.

Click **Apply** to implement changes.

SNMP Settings

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

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

The Switch supports the SNMP versions 1, 2c, and 3. Choose which version 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 Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator.

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

SNMP View Table

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

To configure SNMP View Settings for the Switch, click **Configuration > SNMP Settings > SNMP View Table**:

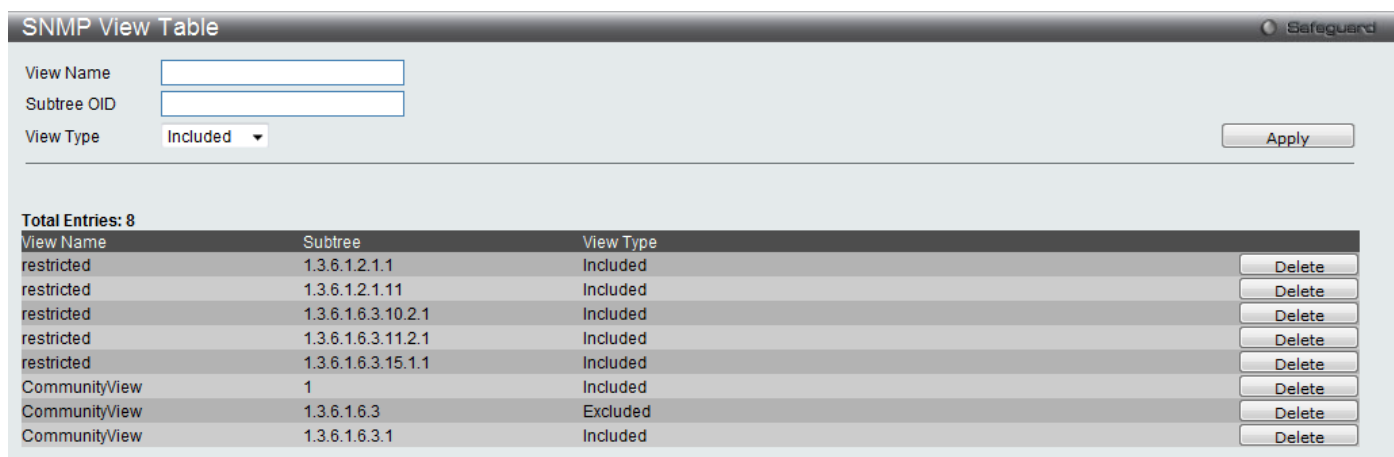


Figure 2 - 32. SNMP View Table window

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

To implement your 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** window) or community strings to the views created in the previous window.

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

Group Name	Read View Name	Write View Name	Notify View Name	User-based Security Model	Security Level	
public	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	Delete
public	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	Delete
initial	restricted		restricted	SNMPv3	NoAuthNoPriv	Delete
private	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv	Delete
private	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv	Delete
ReadGroup	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	Delete
ReadGroup	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	Delete
WriteGroup	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv	Delete
WriteGroup	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv	Delete

Figure 2 - 33. SNMP Group Table window

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	Specify an SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.
Write View Name	Specify an SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify an SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model	<i>SNMPv1</i> - Specifies that SNMP version 1 will be used. <i>SNMPv2</i> - 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. <i>SNMPv3</i> - 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. <i>NoAuthNoPriv</i> - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. <i>AuthNoPriv</i> - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. <i>AuthPriv</i> - 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 **Configuration > SNMP Settings > SNMP User Table**:

Figure 2 - 34. SNMP User Table window

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

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	<i>None</i> – Indicates that there is no SNMP V3 Encryption <i>Password</i> – Indicates that there is SNMP V3 Encryption through a password <i>Key</i> – Indicates that there is SNMP V3 Encryption through a key.
Auth-Protocol by Password	<i>MD5</i> - Indicates that the HMAC-MD5-96 authentication level will be used. <i>SHA</i> - Indicates that the HMAC-SHA authentication protocol will be used.

Priv-Protocol by Password	<i>None</i> - Indicates that no authorization protocol is in use. <i>DES</i> - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Auth-Protocol by Key	<i>MD5</i> - Indicates that the HMAC-MD5-96 authentication level will be used. <i>SHA</i> - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by Key	<i>None</i> - Indicates that no authorization protocol is in use. <i>DES</i> - 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**.

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:

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 configure SNMP Community entries, click **Configuration > SNMP Settings > SNMP Community Table**:

Figure 2 - 35. SNMP Community Table window

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	<i>Read Only</i> - Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. <i>Read Write</i> - 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

Use the **SNMP Host Table** window to set up SNMP trap recipients. To configure SNMP Host Table entries, click **Configuration > SNMP Settings > SNMP Host Table**

Figure 2 - 36. SNMP Host Table window

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	<i>SNMPv1</i> - Specifies that SNMP version 1 will be used. <i>SNMPV2c</i> - Specifies that SNMP version 2 will be used. <i>SNMPV3</i> - To specify that the SNMP version 3 will be used.
Security Level	<i>NoAuthNoPriv</i> – To specify a NoAuthNoPriv security level. <i>AuthNoPriv</i> - To specify an AuthNoPriv security level. <i>AuthPriv</i> - To specify an AuthPriv security level.
Community String/ SNMPv3 User Name	Type in the community string or SNMPv3 user name as appropriate.

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

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 display the Switch's SNMP Engine ID, click **Configuration > SNMP Settings > SNMP Engine ID**:

Figure 2 - 37. SNMP Engine ID window

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 for configuration, click **Configuration > SNMP Settings > SNMP Trap Configuration**:

The window is titled "SNMP Trap Configuration" and includes a "Safeguard" icon in the top right corner. It contains the following sections:

- SNMP Trap:** A dropdown menu set to "Enabled".
- SNMP Authentication Traps:** A dropdown menu set to "Enabled".
- SNMP Link Change Traps:** A dropdown menu set to "Enabled".
- Apply:** A button to save the changes.
- SNMP LinkChange Traps Port Settings:**
 - From Port:** A dropdown menu set to "01".
 - To Port:** A dropdown menu set to "01".
 - State:** A dropdown menu set to "Enabled".
 - Apply:** A button to save the changes.
- Table:** A table with two columns: "Port" and "State". The "Port" column lists ports from 1 to 21, followed by "--". The "State" column lists "Enabled" for each port.

Figure 2 - 38. SNMP Trap Configuration window

To enable or disable the SNMP Trap State, SNMP Authentication Traps, SNMP Link Change Traps, and configure SNMP Link Change Trap Port Settings, use the corresponding pull-down menus. Click **Apply** to let the changes take effect.

RMON

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch.

To view this window for configuration, click **Configuration > SNMP Settings > RMON**:

The window is titled "RMON" and includes a "Safeguard" icon in the top right corner. It contains the following section:

- RMON Status:** Two radio buttons: "Enabled" (unselected) and "Disabled" (selected).
- Apply:** A button to save the changes.

Figure 2 - 39. RMON window

To enable or disable RMON for SNMP, use the radio button. Click **Apply** when finished.

Time Range Settings

This window is used in conjunction with the Access Profile feature to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time range settings are to be applied to an access profile rule using the Access Profile table. The user may enter up to 64 time range entries on the Switch.

To open this window, click **Configuration > Time Range Settings**:

Figure 2 - 40. Time Range Settings window

Single IP Management

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

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

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

SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for SIM. The Commander Switch (CS), which is the master switch of the group, Member Switch (MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch (CaS), which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch (CS).

All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

A SIM group accepts up to 33 switches (numbered 0-32); including the Commander Switch (numbered 0).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain); however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the system VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

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

1. **Commander Switch (CS)** - This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
 - It has an IP Address.
 - It is not a commander switch or member switch of another Single IP group.
 - It is connected to the member switches through its management VLAN.
2. **Member Switch (MS)** - This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
 - It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN.

3. **Candidate Switch (CaS)** - This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of a switch by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN

After configuring one switch to operate as the CS of a SIM group, additional switches may join the group through a direct connection to the Commander switch. Only the Commander switch will allow entry to the candidate switch enabled for SIM. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

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

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

The Upgrade to v1.6

To better improve SIM management, the Switch has been upgraded to version 1.6 in this release. Many improvements have been made, including:

1. The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintain packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

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

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

3. This version will support multiple switch upload and downloads for firmware, configuration files and log files, as follows:

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

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

Single IP Settings

All switches are set as Candidate (CaS) switches as their factory default configuration and Single IP Management will be disabled.

To enable SIM for the Switch using the Web interface, click **Configuration > Single IP Management > Single IP Settings** which will reveal the following window:

The screenshot shows the 'Single IP Settings' window. The 'SIM State' dropdown is set to 'Disabled'. The 'Role State' dropdown is set to 'Candidate'. The 'Group Name' field is empty. The 'Discovery Interval (30 - 90)' is set to '30' seconds. The 'Hold Time Count (100-255)' is set to '100' seconds. An 'Apply' button is located at the bottom right.

Figure 2 - 41. Single IP Settings window (disabled)

Use the drop-down menus to change the SIM State to *Enabled*, the Role State to *Commander*, and then fill in the Group Name field. Click **Apply** to let the changes take effect.

The screenshot shows the 'Single IP Settings' window. The 'SIM State' dropdown is set to 'Enabled'. The 'Role State' dropdown is set to 'Commander'. The 'Group Name' field is empty. The 'Discovery Interval (30 - 90)' is set to '30' seconds. The 'Hold Time Count (100-255)' is set to '100' seconds. An 'Apply' button is located at the bottom right.

Figure 2 - 42. Single IP Settings window (enabled)

The following parameters can be set:

Parameters	Description
SIM State	Use the pull-down menu to either enable or disable the SIM state on the Switch. <i>Disabled</i> will render all SIM functions on the Switch inoperable.
Role State	Use the pull-down menu to change the SIM role of the Switch. The two choices are: <i>Candidate</i> - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role. <i>Commander</i> - Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	The user may enter a name for the group.
Discovery Interval (30-90)	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from 30 to 90 seconds.
Hold Time Count (100-255)	This parameter may be set for the time, in seconds the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from 100 to 255 seconds.

Click **Apply** to implement the settings.

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

Topology

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

The Java Runtime Environment on your server should initiate and lead you to the **Topology** window:

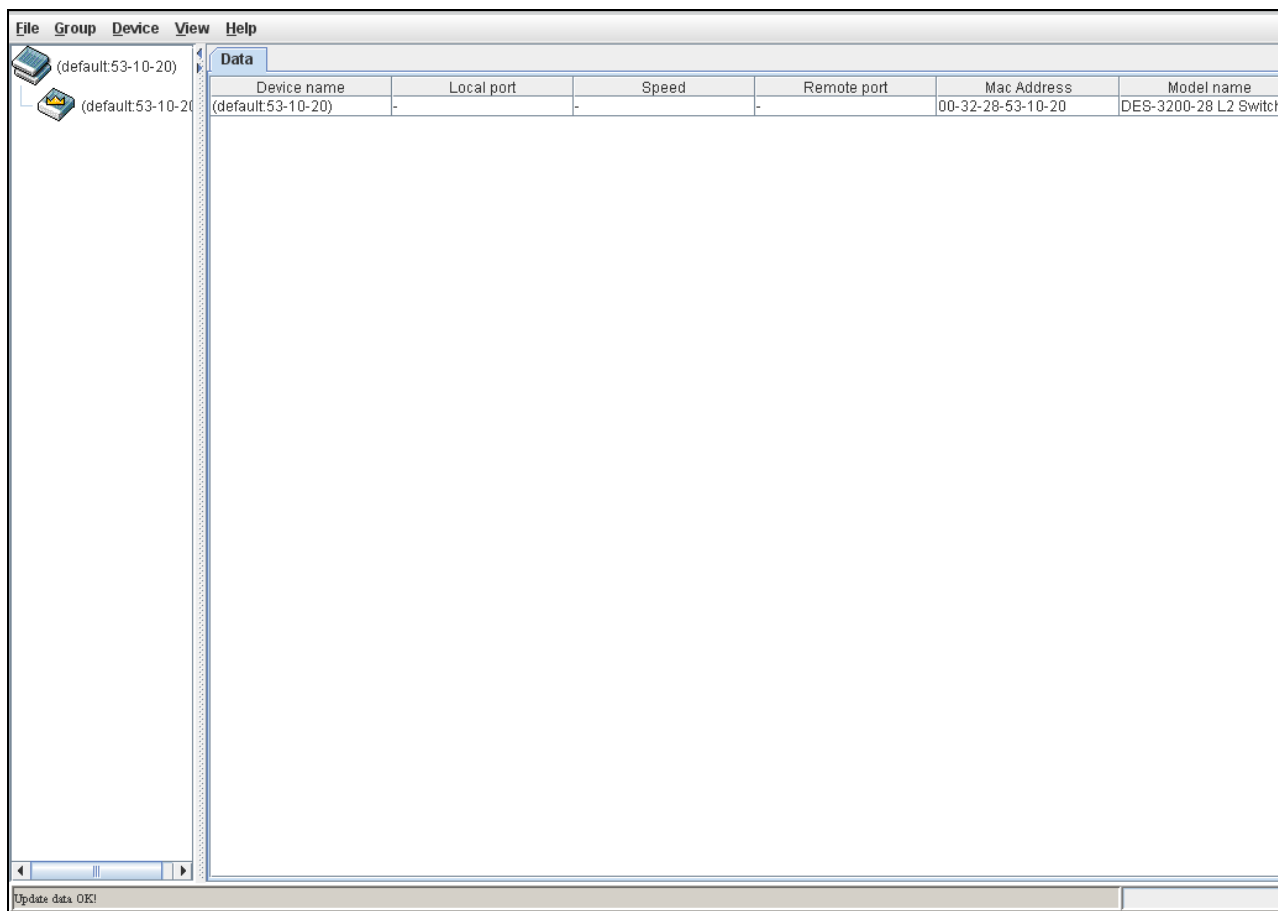


Figure 2 - 43. Topology window

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

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Speed	Displays the connection speed between the CS and the MS or CaS.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
MAC Address	Displays the MAC address of the corresponding Switch.
Model Name	Displays the full model name of the corresponding Switch.

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

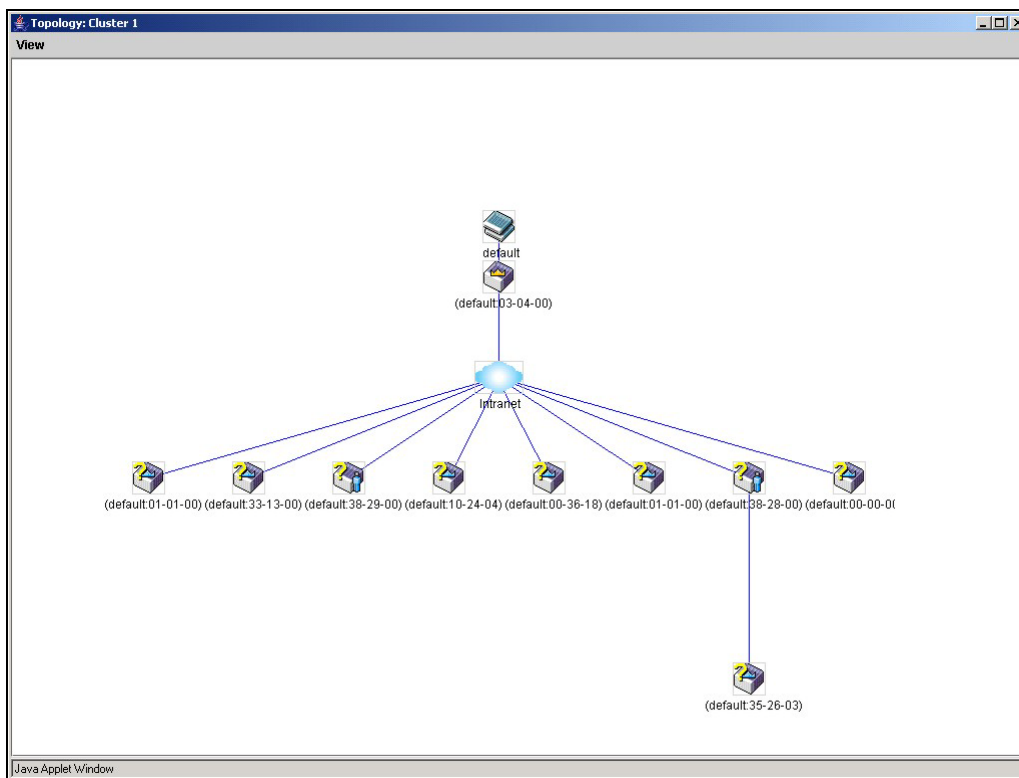


Figure 2 - 44. Topology view

This window will display how the devices within the Single IP Management Group are connected to other groups and devices. Possible icons in this window are as follows:

Icon	Description
	Group
	Layer 2 commander switch
	Layer 3 commander switch
	Commander switch of other group
	Layer 2 member switch.
	Layer 3 member switch
	Member switch of other group
	Layer 2 candidate switch
	Layer 3 candidate switch
	Unknown device
	Non-SIM devices

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example:

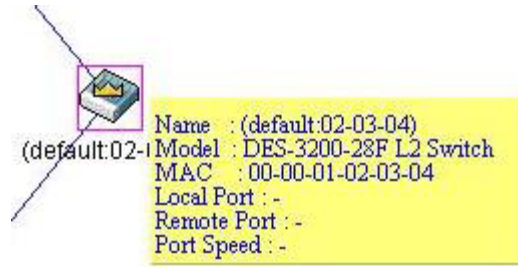


Figure 2 - 45. Device Information Utilizing the Tool Tip

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

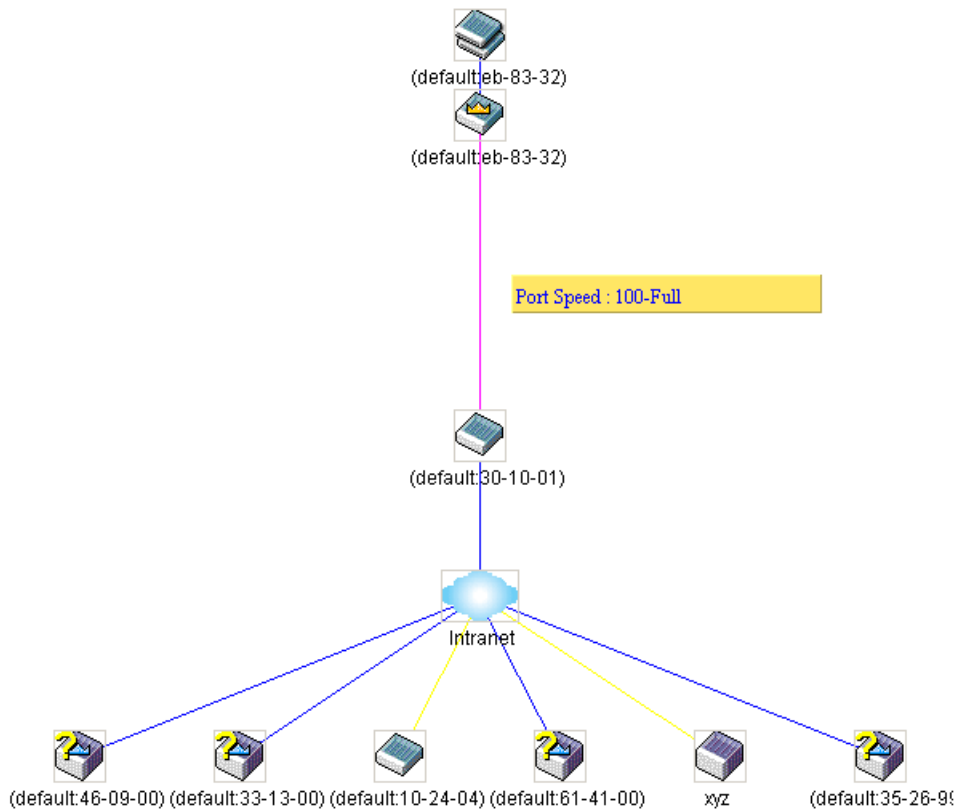


Figure 2 - 46. Port Speed Utilizing the Tool Tip

Right-Click

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

Group Icon

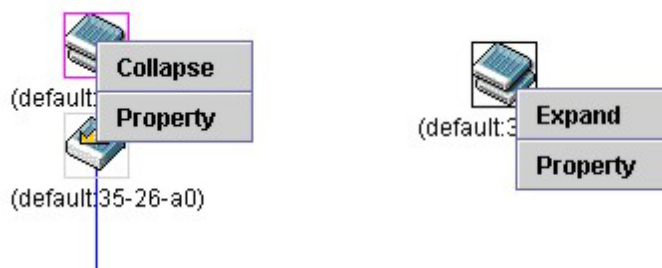


Figure 2 - 47. Right-Clicking a Group Icon

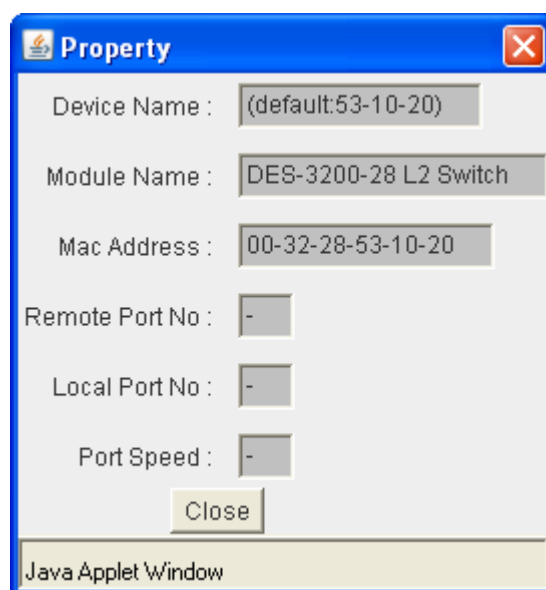


Figure 2 - 48. Property window

This window holds the following information:

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

Click **Close** to close the **Property** window.

Commander Switch Icon

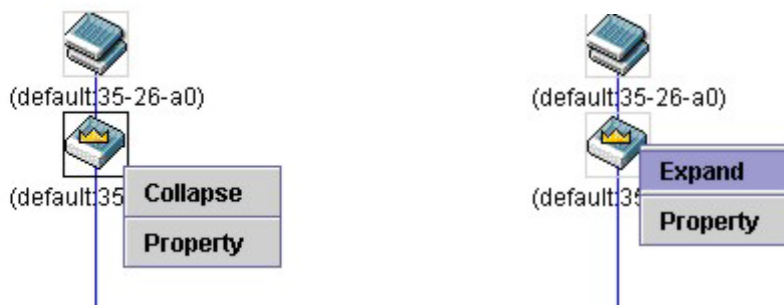


Figure 2 - 49. Right-Clicking a Commander Icon

The following options may appear for the user to configure:

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

Member Switch Icon

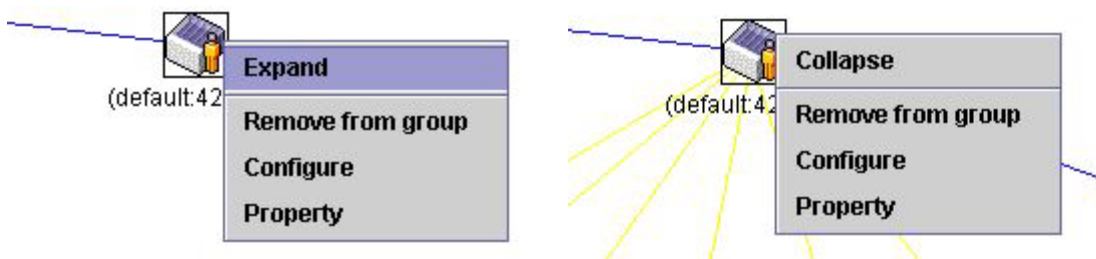


Figure 2 - 50. Right-Clicking a Member icon

The following options may appear for the user to configure:

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

Candidate Switch Icon

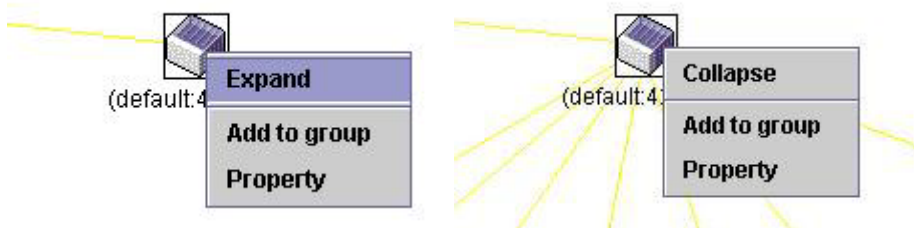


Figure 2 - 51. Right-Clicking a Candidate icon

The following options may appear for the user to configure:

- **Collapse** - To collapse the group that will be represented by a single icon.

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

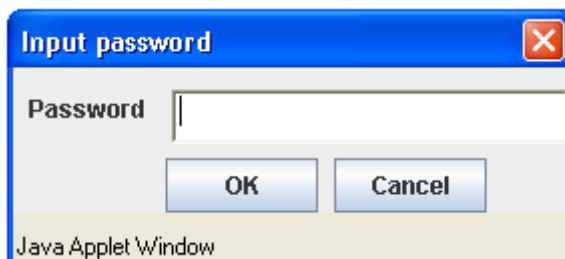


Figure 2 - 52. Input password window

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

Menu Bar

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



Figure 2 - 53. Menu Bar of the Topology View

The five menus on the menu bar are as follows.

File

- **Print Setup** - Will set the default printer properties.
- **Print Topology** - Will print the topology map.
- **Preference** - Will set display properties, such as polling interval, and the views to open at SIM startup.

Group

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

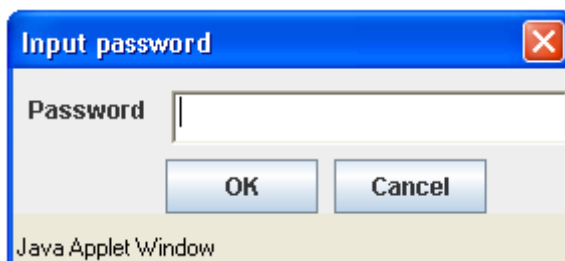


Figure 2 - 54. Input password window

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

Device

- **Configure** - Will open the web manager for the specific device.

View

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

Help

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

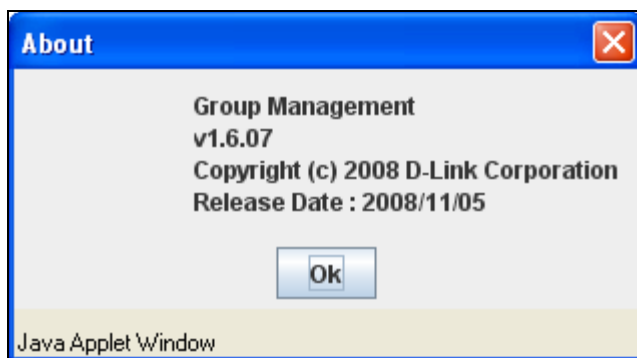


Figure 2 - 55. About window

Firmware Upgrade

This window is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by ID and Port (port on the CS where the MS resides), MAC Address, Model Name and Firmware 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 access the following window, click **Configuration > Single IP Management > Firmware Upgrade**:

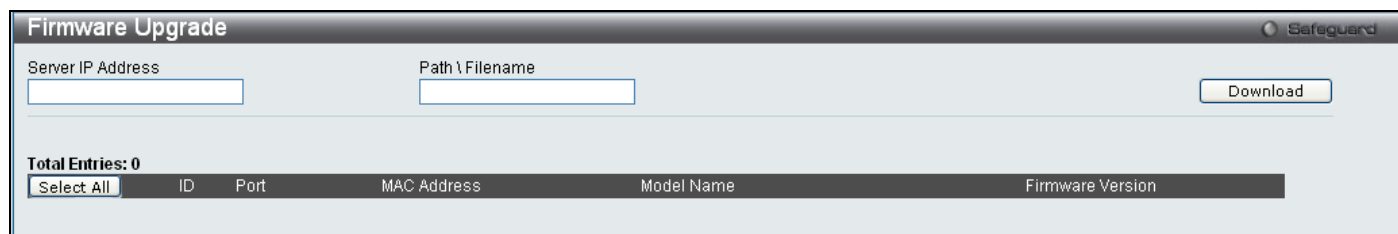


Figure 2 - 56. Firmware Upgrade window

Configuration File Backup/Restore

This window is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table 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 access the following window, click **Configuration > Single IP Management > Configuration File Backup/Restore**:

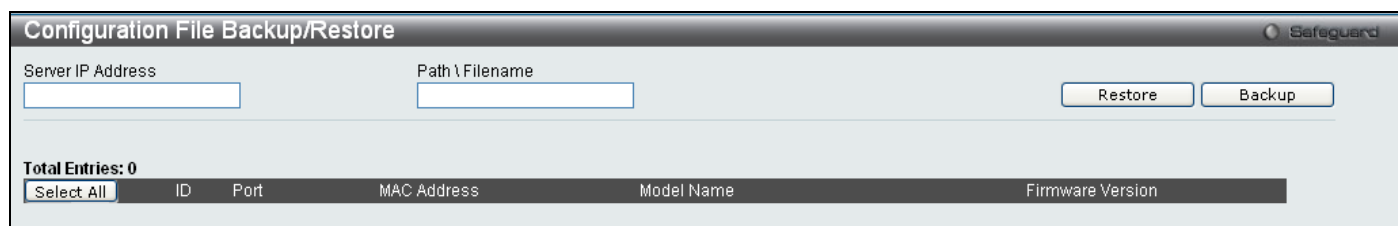


Figure 2 - 57. Configuration File Backup/Restore window

Upload Log File

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

Figure 2 - 58. Upload Log File window

Gratuitous ARP

An ARP announcement (also known as Gratuitous ARP) is a packet (usually an ARP Request) containing a valid SHA and SPA for the host which sent it, with TPA equal to SPA. Such a request is not intended to solicit a reply, but merely updates the ARP caches of other hosts which receive the packet.

This is commonly done by many operating systems on startup, and helps to resolve problems which would otherwise occur if, for example, a network card had recently been changed (changing the IP address to MAC address mapping) and other hosts still had the old mapping in their ARP cache.

Gratuitous ARP Global Settings

To view this window, click **Configuration > Gratuitous ARP > Gratuitous ARP Global Settings**:

Figure 2 - 59. Gratuitous ARP Global Settings window

The following fields can be configured:

Parameter	Description
Send On IP Interface Status Up	This is used to enable or disable the sending of gratuitous ARP request packets while an IP interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is <i>Enabled</i> .
Send On Duplicate IP Detected	This is used to enable or disable the sending of gratuitous ARP request packets while a duplicate IP is detected. By default, the state is <i>Enabled</i> . Duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address.
Gratuitous ARP Learning	This is used to enable or disable updating ARP cache based on the received gratuitous ARP packet. If a switch receives a gratuitous ARP packet, it should add or update the ARP entry. This is <i>Enabled</i> by default.

Once you have made the desired gratuitous ARP setting changes, click **Apply**.

Gratuitous ARP Settings

This window allows you to have more detailed settings for the Gratuitous ARP.

To view this window, click **Configuration > Gratuitous ARP > Gratuitous ARP Settings**:

Total Entries: 1			
IP Interface Name	Gratuitous ARP Trap	Gratuitous ARP Log	Gratuitous ARP Periodical Send Interval
System	Disabled	Enabled	0

Figure 2 - 60. Gratuitous ARP Settings window

The following fields can be set or viewed:

Parameter	Description
Gratuitous ARP Trap/Log	
Trap	The switch can trap IP conflict events to inform the administrator. By default, trap is <i>Disabled</i> .
Log	The switch can log IP conflict events to inform the administrator. By default, Log is <i>Enabled</i> .
IP Interface Name	Displays the name of the interface that is being edited.
Gratuitous ARP Periodical Send Interval	
IP Interface Name	Displays the name of the interface that is being edited.
Interval Time (0-65535)	This is used to configure the interval for the periodical sending of gratuitous ARP request packets. By default, the interval is <i>0</i> .

Click **Apply** to implement changes made.

ARP Spoofing Prevention Settings

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send the fake or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

To prevent ARP spoofing attack, the switch uses Packet Content ACL to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

To view this window, click **Configuration > ARP Spoofing Prevention Settings** as shown below:

Figure 2 - 61. ARP Spoofing Prevention Settings window

The following fields can be set or viewed:

Parameter	Description
Gateway IP Address	Enter the IP address of the gateway.
Gateway MAC Address	Enter the MAC address of the gateway.
Ports (e.g.: 1, 7-10)	Specify the switch ports for which to configure the ARP Spoofing Prevention settings. Tick the All Ports check box to configure this entry for all ports on the Switch.

Click **Apply** to implement changes made.

PPPoE Circuit ID Insertion Settings

When the setting is enabled, the system will insert the circuit ID tag to the received PPPoE discover and request packet if the tag is absent, and remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The insert circuit ID will contain the following information: Client MAC address, Device ID and Port number. Additionally, the option of user defined strings can be inserted into the circuit ID. By default, Switch IP address is used as the device ID to encode the circuit ID option.

To view this window, click **Configuration > PPPoE Circuit ID Insertion Settings** as shown below

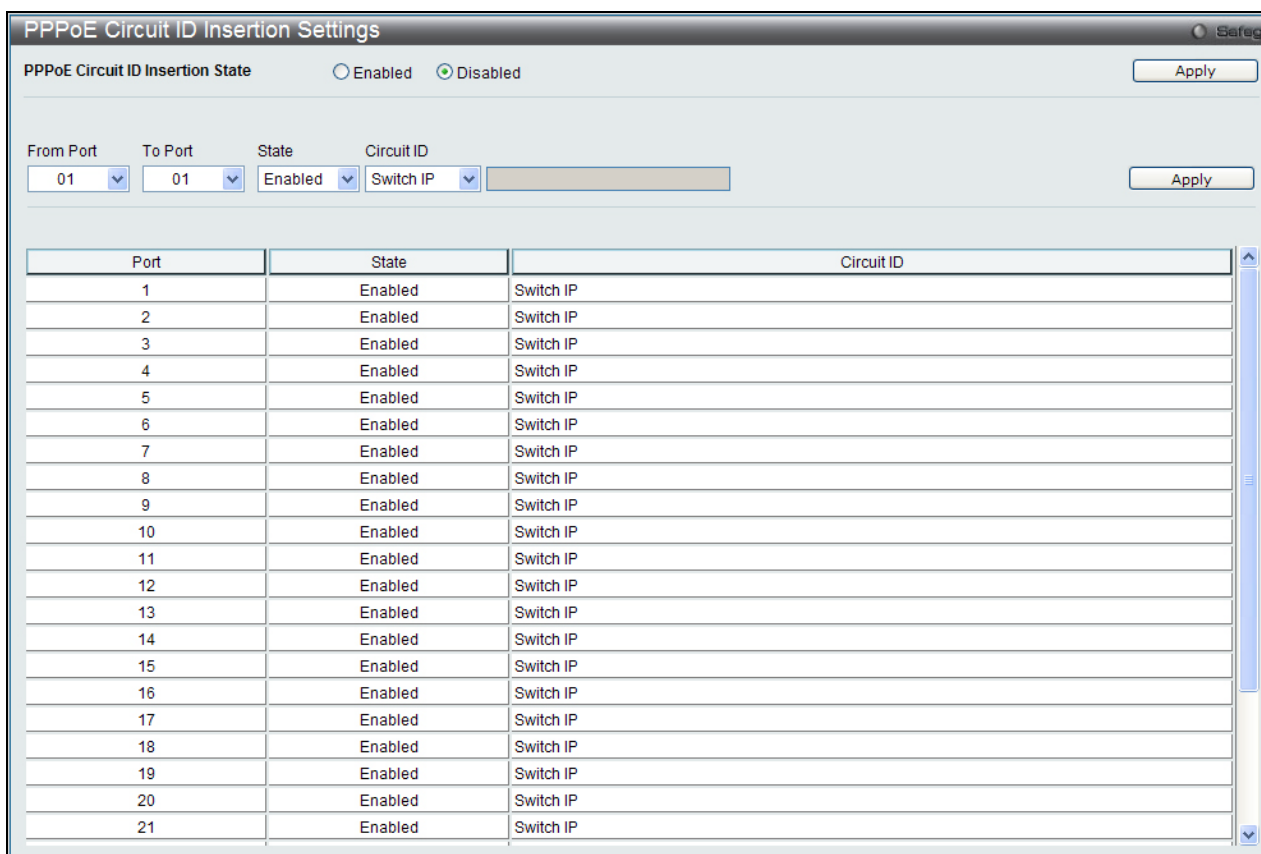


Figure 2 - 62. PPPoE Circuit ID Insertion

The following fields can be set or viewed:

Parameter	Description
From Port – To Port:	Specify the ports to be configured.
State:	Choose <i>Enable</i> or <i>Disable</i> to enable or disable PPPoE circuit ID insertion on the selected ports.
Circuit ID:	<p>Choose the device ID used for encoding of the circuit ID option. The available options are:</p> <ul style="list-style-type: none"> <i>Switch MAC</i> – Specifies that the Switch MAC address be used to encode the circuit ID option. <i>Switch IP</i> – Specifies that the Switch IP address be used to encode the circuit ID option. <i>UDF String</i> – A user defined string to be used to encode the circuit ID option. The maximum length is 32. <p>The default encoding for the device ID option is the Switch IP address.</p>

Click **Apply** to implement changes made.

Section 3

L2 Features

Jumbo Frame

802.1Q Static VLAN

Q-in-Q

802.1v Protocol VLAN

VLAN Trunk Settings

GVRP Settings

Asymmetric VLAN Settings

MAC-based VLAN Settings

PVID Auto Assign Settings

Port Trunking

LACP Port Settings

Traffic Segmentation

Layer 2 Protocol Tunneling Settings

IGMP Snooping

MLD Snooping Settings

Port Mirror

Loopback Detection Settings

Spanning Tree

Forwarding & Filtering

LLDP

Ethernet OAM

Connectivity Failure Management

ERPS Settings

The following section will aid the user in configuring Layer 2 functions for the Switch. The Switch includes various functions all discussed in detail in the following section.

Jumbo Frame

This window will enable or disable the Jumbo Frame function on the Switch. The default is Enabled. When Enabled, jumbo frames (frames larger than the standard Ethernet frame size of 1536 bytes) with a maximum size of 2048 bytes can be transmitted by the Switch.

To view this window, click **L2 Features > Jumbo Frame**:

Figure 3 - 1. Jumbo Frame window

Click **Apply** to implement changes made.

VLANs

Understanding IEEE 802.1p Priority

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

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

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

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

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

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

VLAN Description

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

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

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

Notes About VLANs

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The Switch supports IEEE 802.1Q VLANs and Port-Based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

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

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

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

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

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

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

The main characteristics of IEEE 802.1Q are as follows:

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

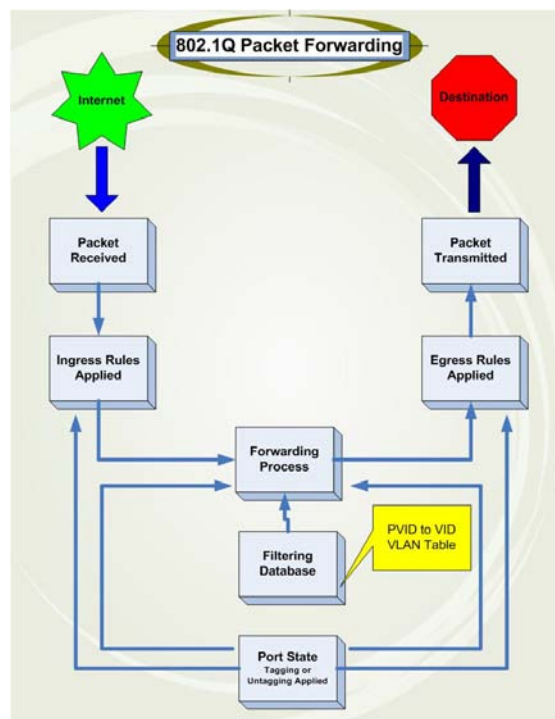


Figure 3 - 2. IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

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

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

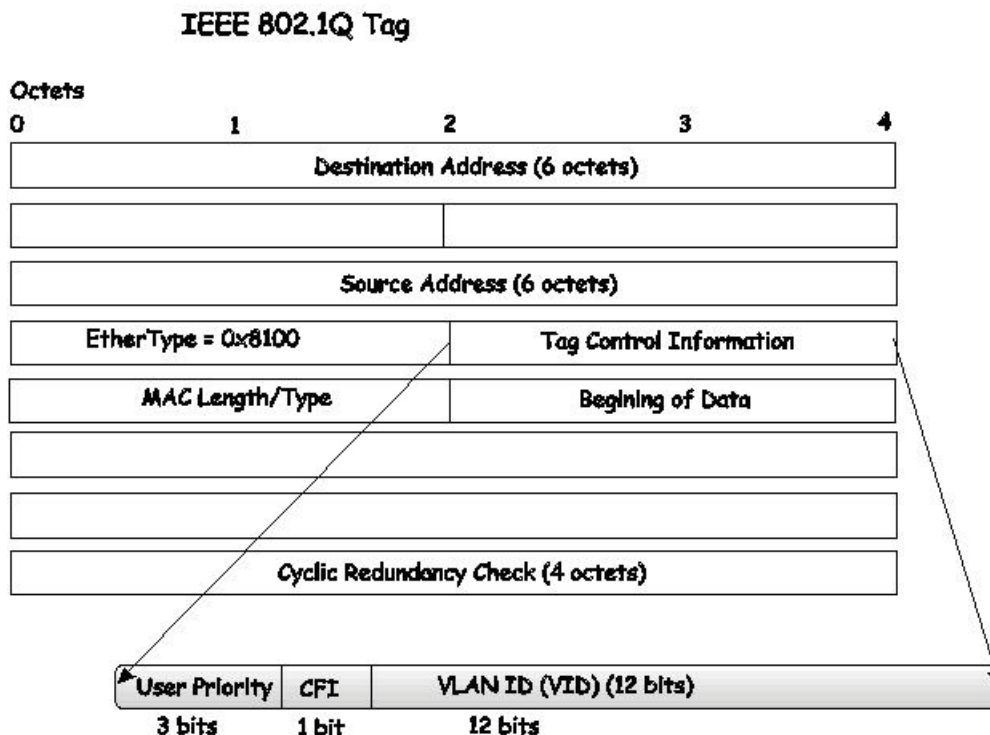


Figure 3 - 3. IEEE 802.1Q Tag

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

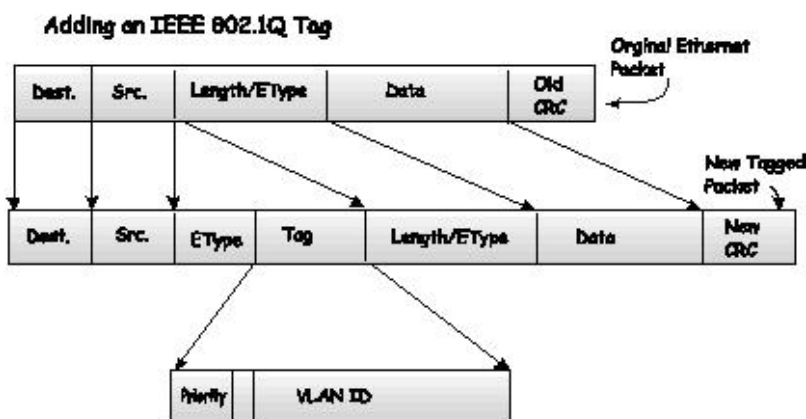


Figure 3 - 4. Adding an IEEE 802.1Q Tag

Port VLAN ID

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

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

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

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

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

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

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

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

Tagging and Untagging

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

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

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

Ingress Filtering

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

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

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

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

Default VLANs

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

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



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

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Table 3 - 1. VLAN Example - Assigned Ports

Port-based VLANs

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

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

VLAN Segmentation

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

Network resources can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, by setting VLAN 1 members to ports 1, 2, 3 and 4 and VLAN 2 members to ports 1, 5, 6 and 7, Port 1 will belong to two VLAN groups. Ports 8, 9 and 10 are not configured to any VLAN group. This means ports 8, 9 and 10 are in the same VLAN group.

VLAN and Trunk Groups

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



NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

Q-in-Q VLANs

Q-in-Q VLANs (also sometimes referred to as double VLANs) allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for

their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

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

Here is an example Q-in-Q VLAN tagged packet:

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

Consider the example below:

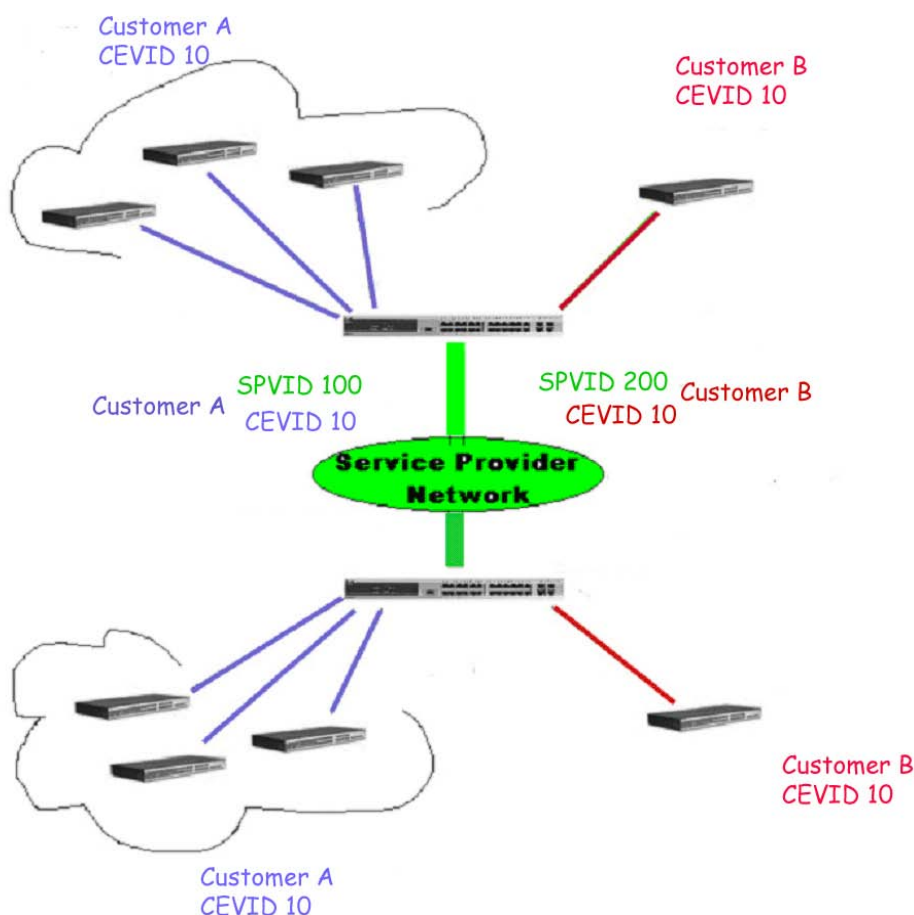


Figure 3 - 5. Q-in-Q VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Q-in-Q VLANs with different SPVIDs for specific customers (say Customer A and Customer B). Both CEVLANS (Customer VLANs), CEVID 10 are tagged with the SPVID 100 (for Customer A) or SPVID 200 (for Customer B) on the Service Provider Access Network, thus being a member of two VLANs on the Service Provider's network. In this way, the Customer can retain their normal VLAN ID's and the Service Provider can separate multiple Customer VLANs using SPVLANs, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Q-in-Q VLANs

Some rules and regulations apply with the implementation of the Q-in-Q VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both Q-in-Q and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Before Q-in-Q VLANs are enabled, users need to disable STP and GVRP manually.
7. All packets sent from the CPU to the Access ports must be untagged.

802.1Q Static VLAN

This window lists all previously configured VLANs by VLAN ID and VLAN Name.

To view this window, click **L2 Features > 802.1Q Static VLAN**:

VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports
1	default	Enabled		1,2,3,4, 5,6,7,8, 9,10,11,12...	

Figure 3 - 6. 802.1Q Static VLAN window - VLAN List tab

To create a new 802.1Q VLAN entry, click the **Add/Edit VLAN** tab at the top of the window. A new tab will appear, as shown in the first figure on the next page, to configure the port settings and to assign a unique name and number to the new VLAN.

To edit an existing 802.1Q VLAN entry, click the **Edit** button next to the corresponding VLAN entry above. A new tab will appear, as shown in the second figure on the next page.

See the table on the next page for a description of the parameters of the **802.1Q Static VLAN** window's **Add/Edit VLAN** tab.



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

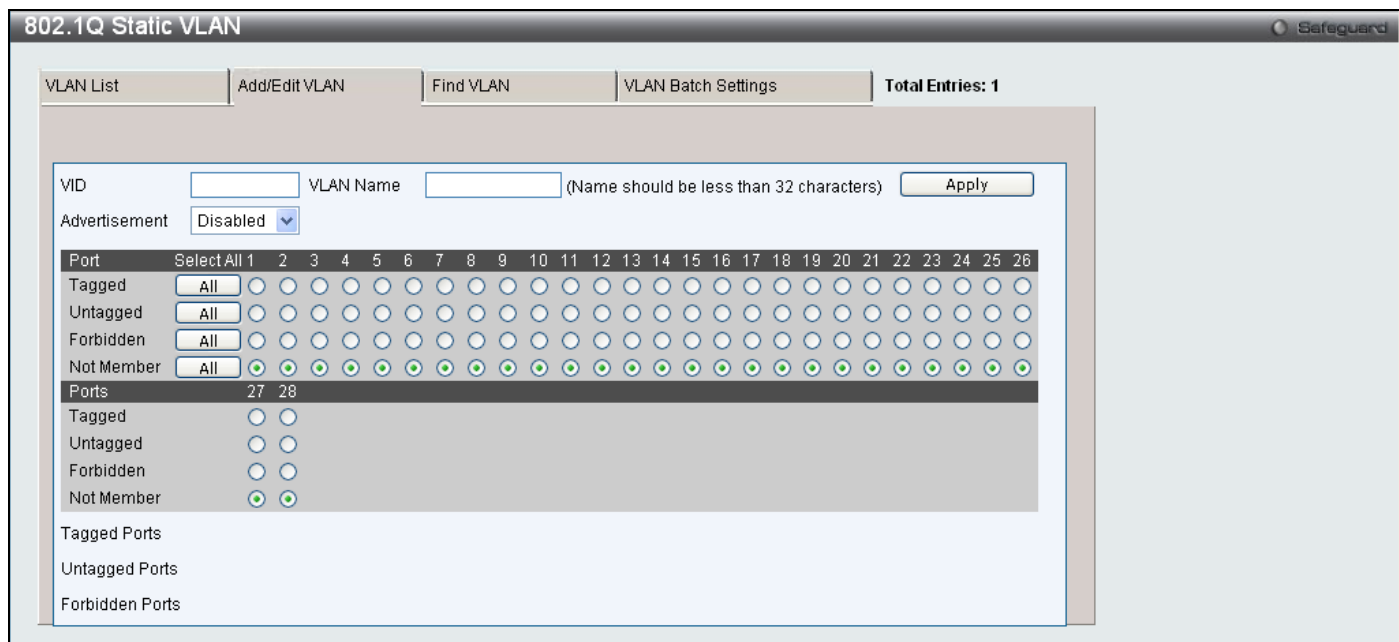


Figure 3 - 7. 802.1Q Static VLAN window – Add/Edit VLAN tab (Add)

To return to the initial **802.1Q Static VLAN** window, click the **VLAN List** tab at the top of the window. To change an existing 802.1Q static 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 window.



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

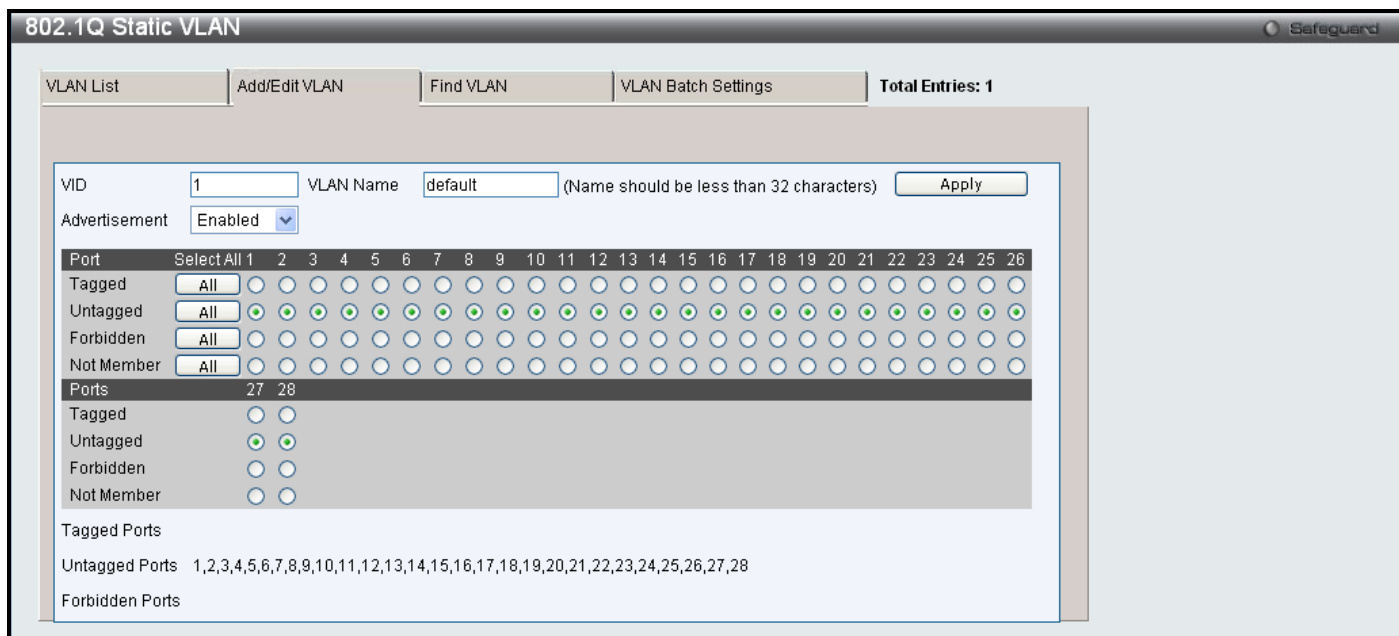


Figure 3 - 8. 802.1Q Static VLAN window – Add/Edit VLAN tab (Edit)

The following fields can then be set in the **Add/Edit VLAN** tab:

Parameter	Description
VID (VLAN ID)	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 window (see below), enter a VLAN ID, and click **Find** to display the settings for a previously configured VLAN.

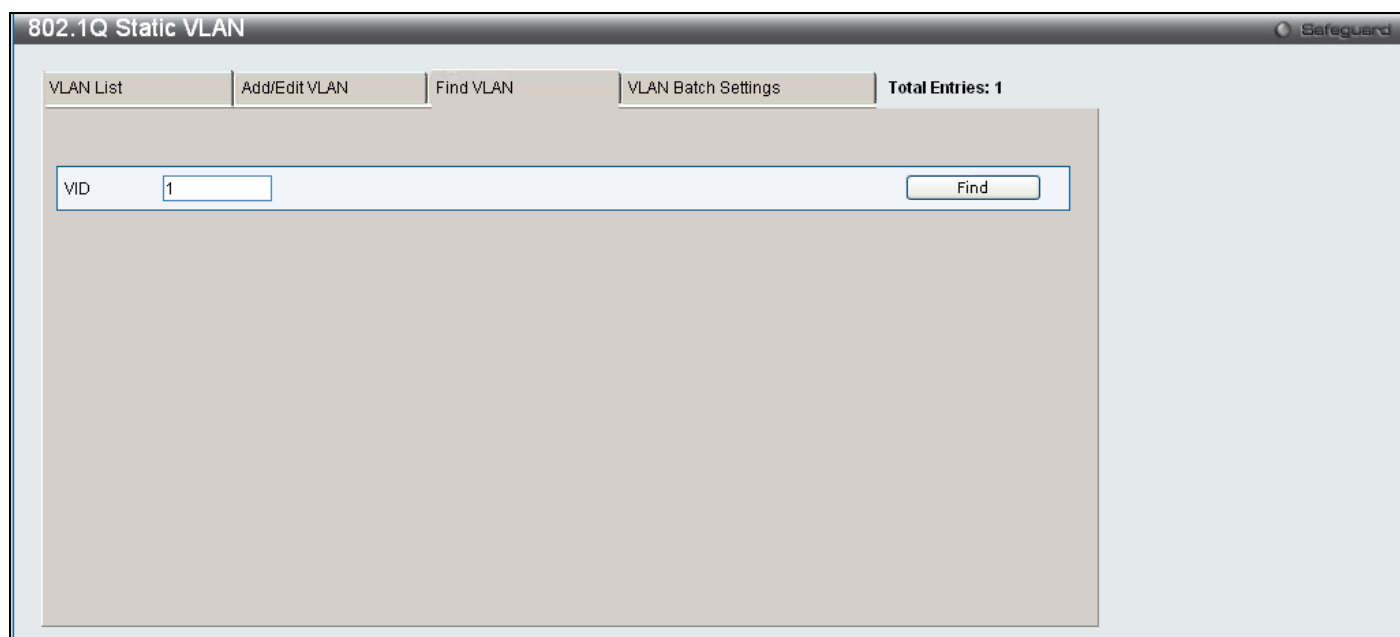


Figure 3 - 9. 802.1Q Static VLAN window – Find VLAN tab

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

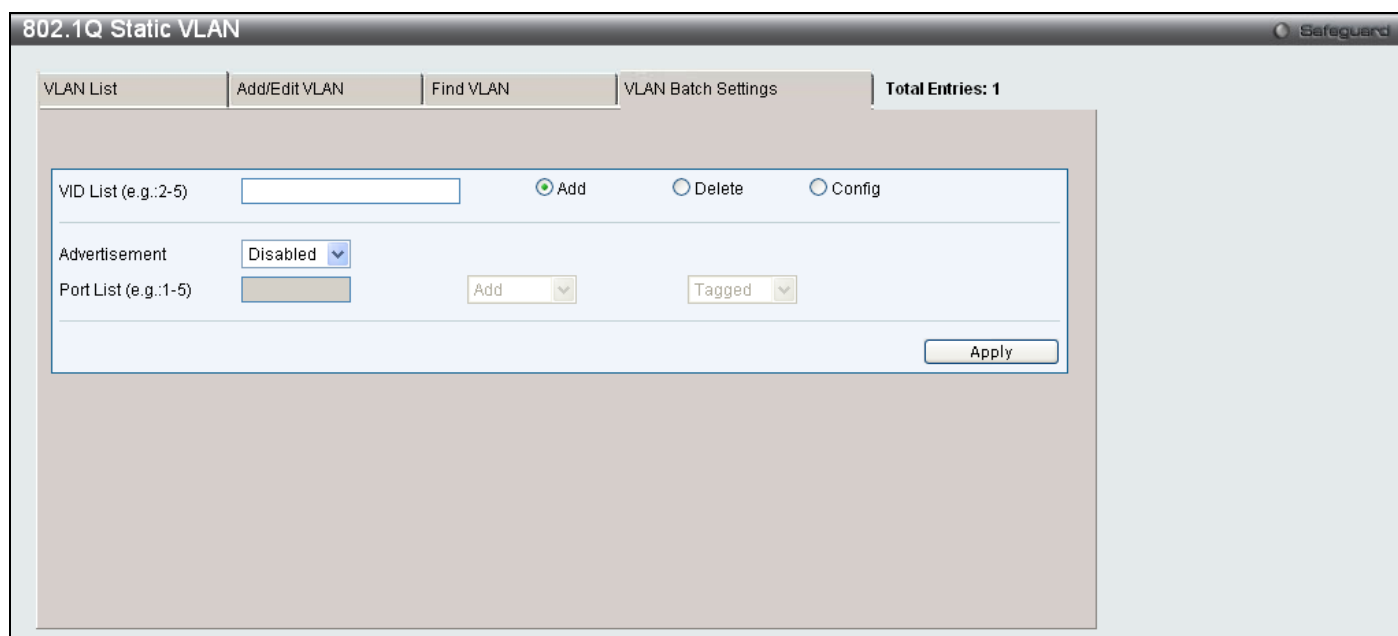


Figure 3 - 10. 802.1Q Static VLAN window – VLAN Batch Settings tab

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

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.

Q-in-Q

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.

Q-in-Q Settings

To view this window, click **L2 Features > Q-in-Q > Q-in-Q Settings**:

Port	Role	Outer TPID	Trust CVID	VLAN Translation
1	NNI	0x88a8	Disabled	Disabled
2	NNI	0x88a8	Disabled	Disabled
3	NNI	0x88a8	Disabled	Disabled
4	NNI	0x88a8	Disabled	Disabled
5	NNI	0x88a8	Disabled	Disabled
6	NNI	0x88a8	Disabled	Disabled
7	NNI	0x88a8	Disabled	Disabled
8	NNI	0x88a8	Disabled	Disabled
9	NNI	0x88a8	Disabled	Disabled
10	NNI	0x88a8	Disabled	Disabled
11	NNI	0x88a8	Disabled	Disabled
12	NNI	0x88a8	Disabled	Disabled
13	NNI	0x88a8	Disabled	Disabled
14	NNI	0x88a8	Disabled	Disabled
15	NNI	0x88a8	Disabled	Disabled
16	NNI	0x88a8	Disabled	Disabled
17	NNI	0x88a8	Disabled	Disabled
18	NNI	0x88a8	Disabled	Disabled
19	NNI	0x88a8	Disabled	Disabled
20	NNI	0x88a8	Disabled	Disabled
21	NNI	0x88a8	Disabled	Disabled
22	NNI	0x88a8	Disabled	Disabled
23	NNI	0x88a8	Disabled	Disabled
24	NNI	0x88a8	Disabled	Disabled
25	NNI	0x88a8	Disabled	Disabled
26	NNI	0x88a8	Disabled	Disabled
27	NNI	0x88a8	Disabled	Disabled
28	NNI	0x88a8	Disabled	Disabled

Figure 3 - 11. Q-in-Q Settings window

The following fields can be set:

Parameter	Description
Q-in-Q Global Settings	Click the radio button to enable or disable the Q-in-Q Global Settings.
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. <i>UNI</i> – To select a user-network interface which specifies that communication between the specified user and a specified network will occur. <i>NNI</i> – To select a network-to-network interface specifies that communication between two specified networks will occur.
Outer TPID (hex: 0x1 -0xffff)	The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.
Trust CVID	Enable or disable the Trust Customer VLAN ID (CVID). If the state is <i>Enabled</i> , use the CVID from the customer’s packet as the VLAN ID of the SPVLAN tag. The default is <i>Disabled</i> .
VLAN Translation	Enable or disable VLAN Translation. This translates the VLAN IDs carried in the data packets received from private networks into those used in the Service Provider’s network. The default is <i>Disabled</i> . Note: To use this function, Trust CVID must also be enabled.

Click **Apply** to implement changes.

VLAN Translation Settings

VLAN translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.

To view this window click **L2 Features > Q-in-Q > VLAN Translation CVID Entry Settings**:

Figure 3 - 12. VLAN Translation Settings window

The following fields can be set:

Parameter	Description
Action	Specify to <i>Add</i> or <i>Replace</i> Service Provider VLAN ID (SVID) packets.
CVID (1-4094)	The customer VLAN ID List to which the tagged packets will be added.
SVID(1-4094)	This configures the VLAN to join the Service Providers VLAN as a tagged member.

Click **Apply** to make a new entry and **Delete All** to remove a VLAN Translation entry.

802.1v Protocol VLAN

The window 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 window displays any previously created groups.

802.1v Protocol Group Settings

To view this window, click **L2 Features > 802.1v Protocol VLAN > 802.1v Protocol Group Settings**:

Figure 3 - 13. 802.1v Protocol Group Settings window

The following fields can be set:

Parameter	Description
Group ID (1-16)	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 <i>Ethernet II</i> and <i>IEEE802.3 SNAP</i> .
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 window allows the user to configure Protocol VLAN settings. The lower half of the window displays any previously created settings.

To view this window, click **L2 Features > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings**:

Figure 3 - 14. 802.1v Protocol VLAN Settings window

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 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. 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 tick 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 window click the Show All button, to clear all previously configured lists click the Delete All button.

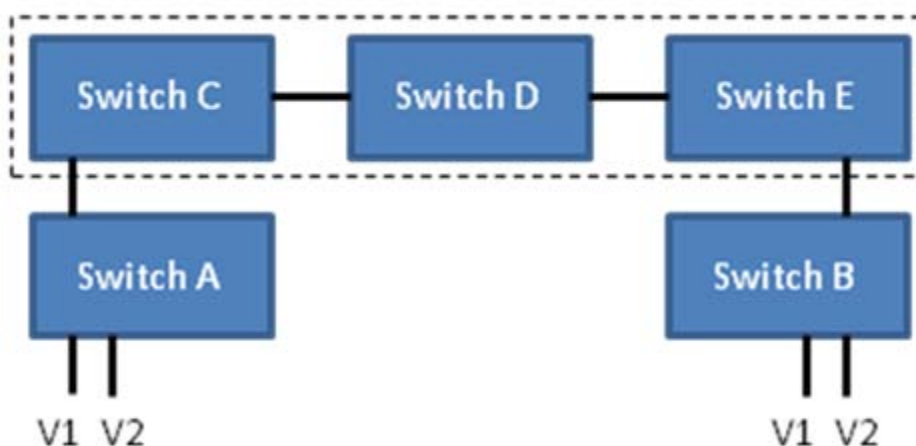


NOTE: For the current release of the DES-3200, users cannot specify a range of ports for 802.1v. The current release only allows users to specify all ports.

VLAN Trunk Settings

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

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



Users can combine a number of VLAN ports together to create VLAN trunks. To create VLAN Trunk Port settings on the Switch, select the ports to be configured, change the VLAN Trunk Global State to Enabled, and click **Apply**, the new settings will appear in the VLAN Trunk Settings table in the lower part of the window.

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

Figure 3 - 15. VLAN Trunk Settings window

The user-changeable parameters are as follows:

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

GVRP Settings

This window 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 **L2 Features > GVRP Settings**:

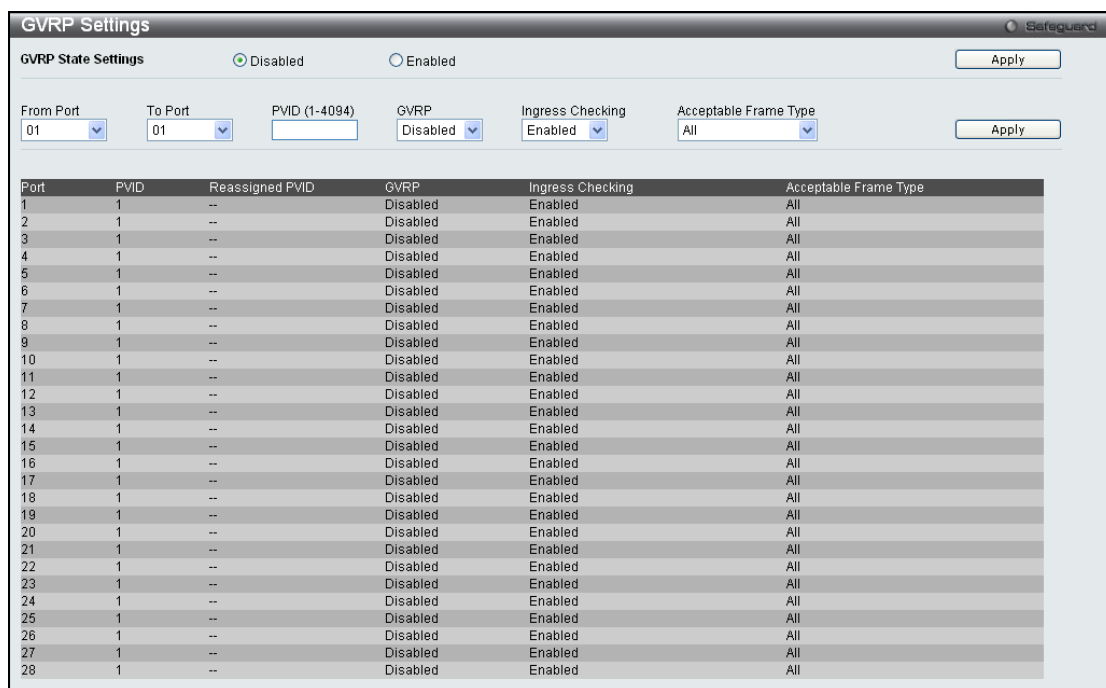


Figure 3 - 16. GVRP Settings window

The following fields can be set:

Parameter	Description
GVRP State Settings	Click the radio buttons to enable or disable the GVRP global state settings.
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.
PVID (1-4094)	Enter a 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.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is <i>Disabled</i> by default.
Ingress Checking	This field can be toggled using the space bar between <i>Enabled</i> and <i>Disabled</i> . <i>Enabled</i> 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. <i>Disabled</i> disables ingress filtering. Ingress Checking is <i>Enabled</i> by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between <i>Tagged Only</i> , which means only VLAN tagged frames will be accepted, and <i>All</i> , which mean both tagged and untagged frames will be accepted. <i>All</i> is enabled by default.

Click **Apply** to implement changes made.

Asymmetric VLAN Settings

Under normal circumstances, a pair of devices communicating in a VLAN environment will both send and receive using the same VLAN; however, there are some circumstances in which it is convenient to make use of two distinct VLANs, one used for A to transmit to B and the other used for B to transmit to A in these cases Asymmetric VLANs are needed. An example of when this type of configuration might be required would be if the client was on a distinct IP subnet, or if there was some confidentiality-related need to segregate traffic between the clients.

To view this window, click **L2 Features > Asymmetric VLAN Settings**:

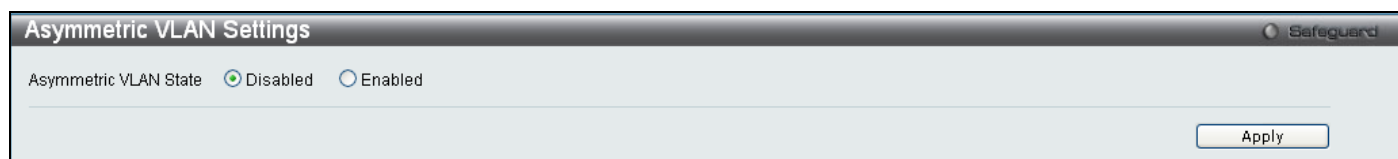


Figure 3 - 17. Asymmetric VLAN Settings window

Click **Apply** to implement changes.

MAC-based VLAN Settings

This window is used to create MAC-based VLAN entries on the switch. A MAC Address can be mapped to any existing static VLAN and multiple MAC addresses can be mapped to the same VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user is able to be serviced under the specified VLAN. Therefore each entry specifies a relationship of a source MAC address with a VLAN.

To view this window, click **L2 Features > MAC-based VLAN Settings**:

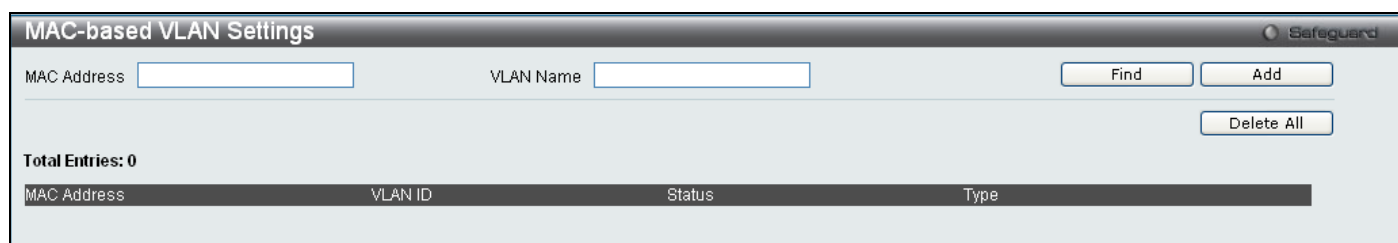


Figure 3 - 18. MAC-based VLAN Settings window

The following fields can be set

Parameter	Description
MAC Address	Specify the MAC address to be mapped.
VLAN Name	Enter the VLAN name of a previously configured VLAN.

Click **Find**, **Add** or **Delete All** for changes to take effect.

PVID Auto Assign Settings

This enables or disables PVID Auto Assign on the Switch. PVID is the VLAN that the switch will use for forwarding and filtering purposes. If PVID Auto-Assign is *Enabled*, PVID will be possibly changed by previously set PVID or VLAN configurations. When a user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. In the form of a VLAN list command, PVID is updated with the last item on the VLAN list. When a user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned to a default VLAN. When PVID Auto Assign is *Disabled*, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change the PVID. The default setting is *Enabled*.

To view this window, click **L2 Features > PVID Auto Assign Settings**:

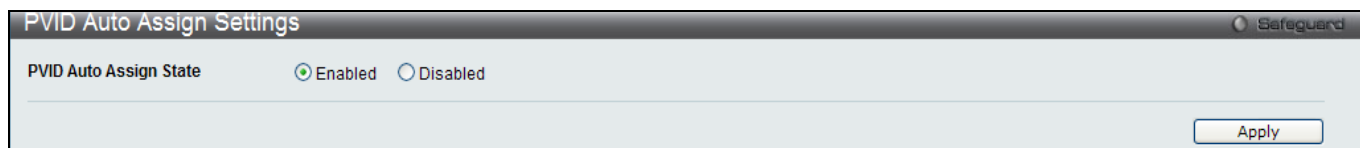


Figure 3 - 19. PVID Auto Assign Settings window

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 Switch supports up to fourteen port trunk groups with two to eight ports in each group.

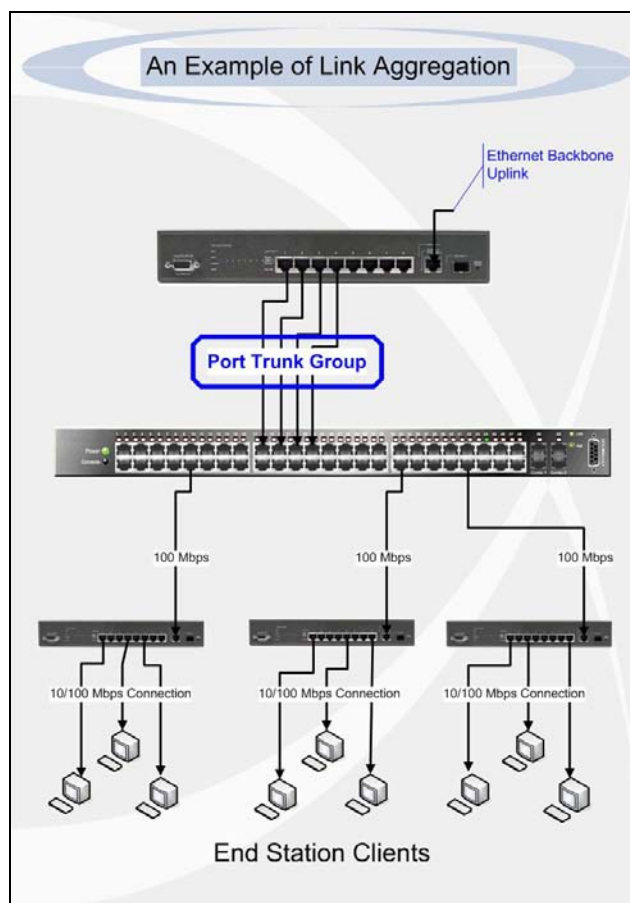


Figure 3 - 20 Example of Port Trunk Group

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



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other unlinked ports of the link aggregation group.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

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

The Switch allows the creation of up to fourteen link aggregation groups, each group consisting of two to eight links (ports). All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the 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 **L2 Features > Port Trunking**:

Figure 3 - 21. Port Trunking window

The following fields can be set

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 <i>MAC Source</i> , <i>MAC Destination</i> , <i>MAC Source Dest</i> , <i>IP Source</i> , <i>IP Destination</i> or <i>IP Source Dest</i> (See the Link Aggregation section of this manual).
Group ID (1-14)	Select an ID number for the group, between 1 and 14.
Type	This pull-down menu allows you to select between <i>Static</i> and <i>LACP</i> (Link Aggregation Control Protocol). <i>LACP</i> 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	Trunk groups can be toggled between <i>Enabled</i> and <i>Disabled</i> . This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Active Ports	Shows the ports that are currently forwarding packets.

(Member) Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Flooding Ports	These ports are designated for flooding broadcast, multicast, and DLF (unicast Destination Lookup Fail) packets from the CPU in a trunk group. The port is defined by software and doesn't actually exist in the hardware.

Click **Apply** to implement changes made.

LACP Port Settings

This window is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames.

To view this window, click **L2 Features > LACP Port Settings**:

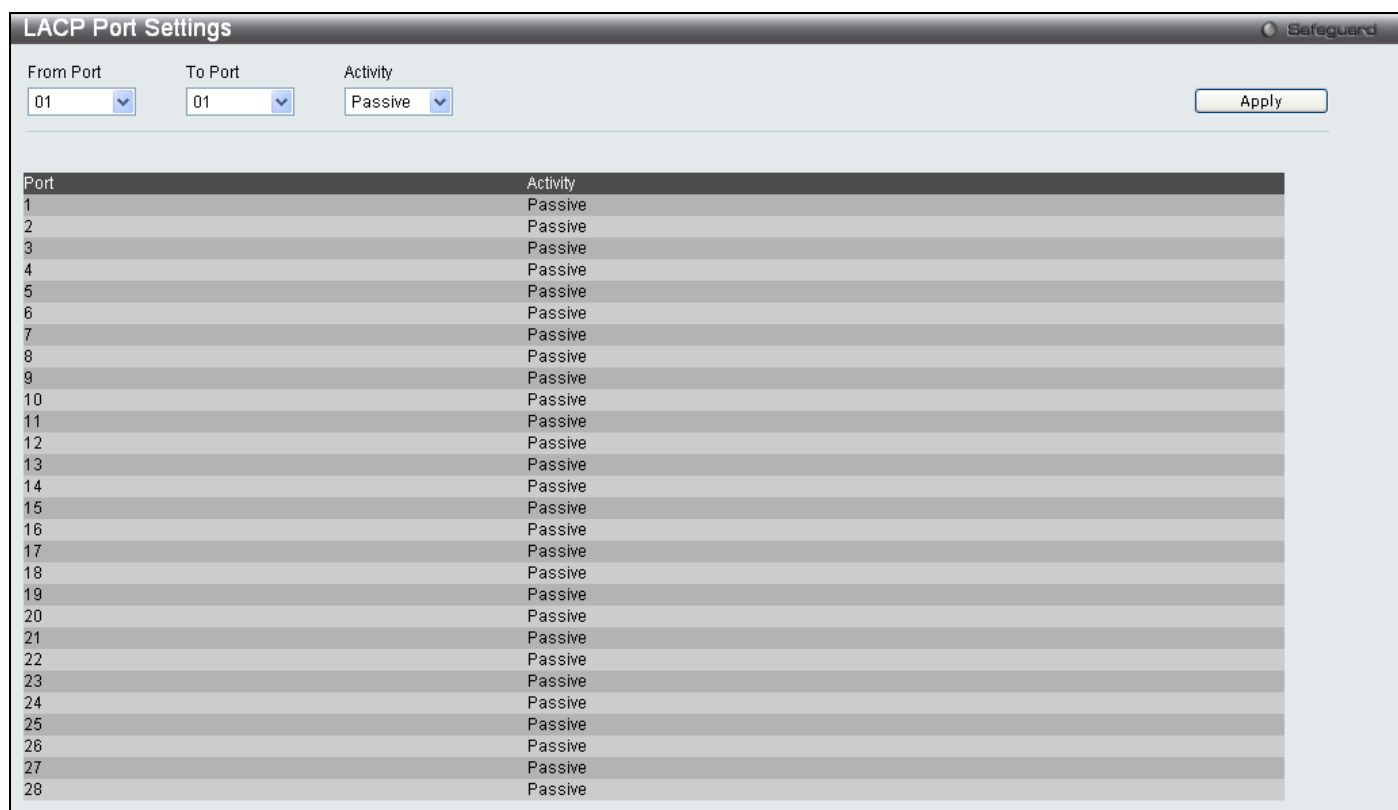


Figure 3 - 22. LACP Port Settings window

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.
Activity	<p><i>Active</i> - 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.</p> <p><i>Passive</i> - 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).</p>

Click **Apply** to implement changes made.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on the Switch. 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 Switch CPU. This window allows the user to view which ports on the Switch are allowed to forward packets to other ports on the Switch. To configure new forwarding ports for a particular port, select a port from the From Port and To Port drop-down menus and click **Apply**.

To view this window, click **L2 Features > Traffic Segmentation**:

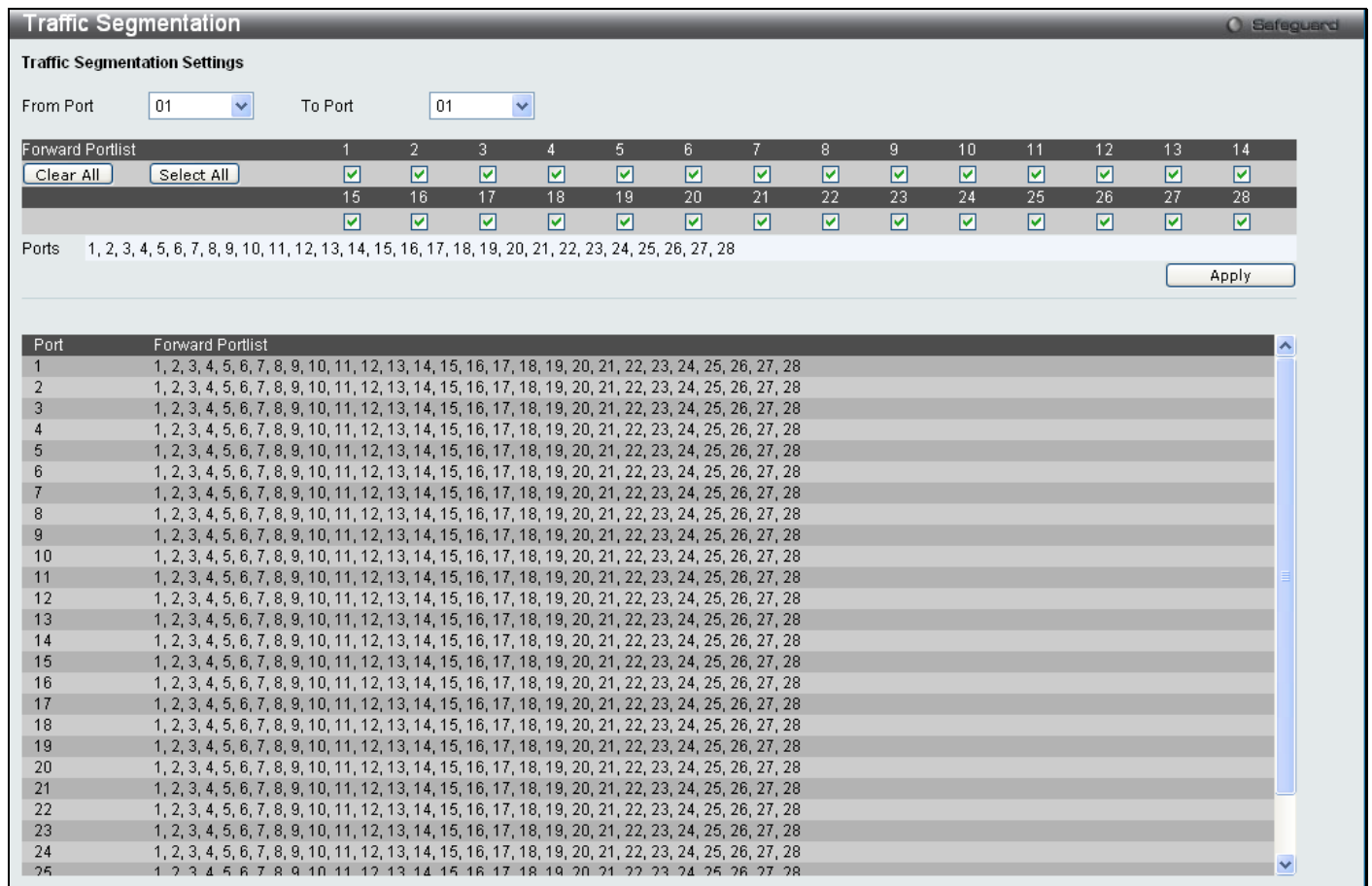


Figure 3 - 23. Traffic Segmentation window

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.

Layer 2 Protocol Tunneling Settings

To view this window, click **L2 Features > L2PT Settings**:

Figure 3 - 24. Layer 2 Tunneling Settings window

The fields that can be configured are described below:

Parameter	Description
Layer 2 Protocol Tunneling Global State:	To enable or disable the Layer 2 Protocol Tunneling state.
Port(s):	The user can select the port numbers that will be included in the Layer 2 Protocol Tunneling configuration.

Click **Apply** to implement changes made.

BPDU Attack Protection Settings

This menu is used to configure the BPDU protection function for the ports on the switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on STP-disabled port.

BPDU protection has a higher priority than the Forward BPDU setting configured in the STP Port Settings menu (**L2 Features > Spanning Tree > STP Port Settings**). That is, when a port configured to the Forward BPDU (**STP Port Settings** window) and BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the Layer 2 Protocol Tunneling port setting in the determination of BPDU handling. That is, when a port is configured as Layer 2 Protocol Tunnel port for Tunnel STP (**L2 Features > L2PT Settings**), it will forward STP BPDU. But if the port is BPDU protection enabled, then the port will not forward STP BPDU.

To view this window, click **L2 Features > BPDU Protection Settings**:

Port	State	Mode	Status
1	Disabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal
10	Disabled	Shutdown	Normal

Figure 3 - 25. BPDU Protection Settings window

The fields that can be configured are described below:

Parameter	Description
BPDU Protection Global State:	To enable or disable the BPDU Protection Global State to enable BPDU Attack Protection globally. The default state is Disabled.
Trap State:	To specify the trap state. The default state is none.
Log State:	To specify the log state. The default state is both.
Recover Time:	Specified the BPDU protection Auto-Recovery timer. The default value of the recovery timer is 60. Recover Time can be set between 60 and 1000000 seconds.
From Port – To Port:	To select a range of ports to use for this configuration.
State:	To enable or disable the mode for a specific port.
Mode:	Specified the BPDU protection mode. The default mode is shutdown. <i>Drop</i> – Drop all received BPDU packets when the port enters under attack state. <i>Block</i> – Drop all packets (include BPDU and normal packets) when the port enters under attack state. <i>Shutdown</i> – Shut down the port when the port enters under attack state.

Click **Apply** for the menu being configured to implement changes made.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can add or remove 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. Then, fine-tune the settings for each VLAN using the **IGMP Snooping** windows in the **L2 Features** 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 this window to enable or disable IGMP snooping on the Switch. The IGMP Snooping State under IGMP Snooping Global Settings can be enabled or disabled and a Max Learning Entry Value between 1 and 1024 can be entered in the field under IGMP Data Driven Learning Settings. Click **Apply** to modify the settings.

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Settings**:

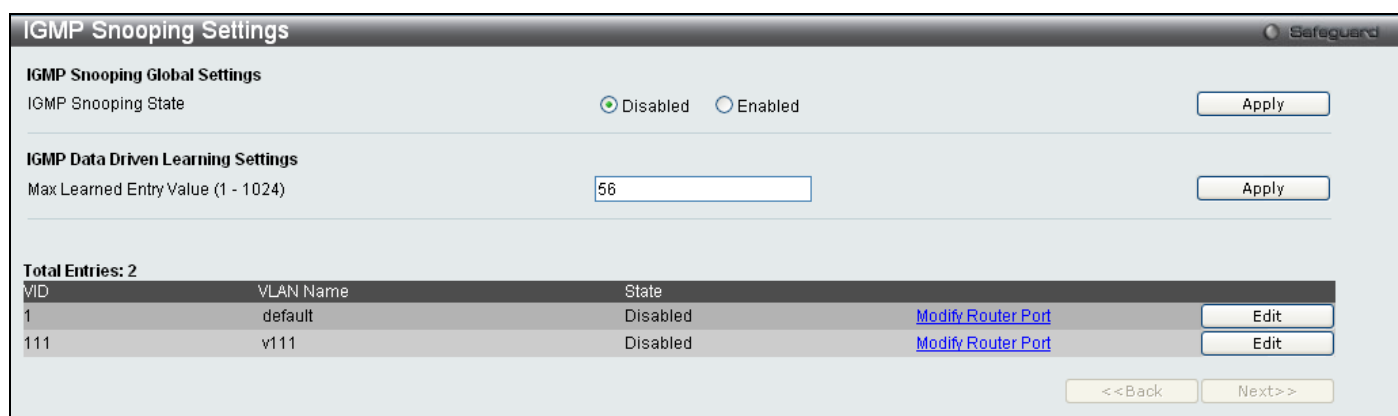


Figure 3 - 26. IGMP Snooping Settings window

Clicking the **Edit** button will open this window:

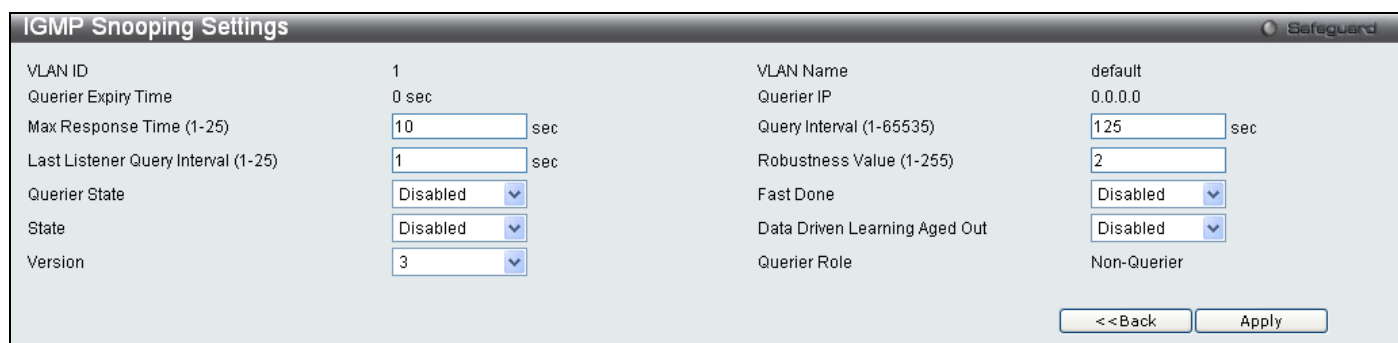


Figure 3 - 27. IGMP Snooping Settings (Edit) window

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.
Querier Expiry Time	Displays the querier expiry time.
Querier IP	The IP address of the device which acts as the IGMP querier for the network.
Max Response Time (1-25)	This determines the maximum amount of time in seconds to wait for reports from members. The Max Response Time field allows an entry between 1 and 25 (seconds). The default is 10.
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. The default is 125.
Last Listener Query Interval (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is 1.
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. The default is 2.
Querier State	Choose <i>Enabled</i> to enable transmitting IGMP query packets or <i>Disabled</i> to disable the transmitting of IGMP query packets. The default is <i>Disabled</i> .
Fast Done	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 <i>Disabled</i> .
State	Select <i>Enabled</i> to implement IGMP Snooping. This field is <i>Disabled</i> by default.
Data Driven Learning Aged Out	Allows users to enable or disable aged out of IGMP Snooping data driven learning for the specified VLAN.
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 Switch for sending query packets. Querier will denote that the Switch is sending out IGMP query packets. Non-Querier will denote that the Switch is not sending out IGMP query packets. This field will only read Querier when the Querier State and the State fields have been <i>Enabled</i> .

To modify the IGMP Snooping Router Port Settings, click on the [Modify Router Port](#) hyperlink, which will show the following window for the user to configure:

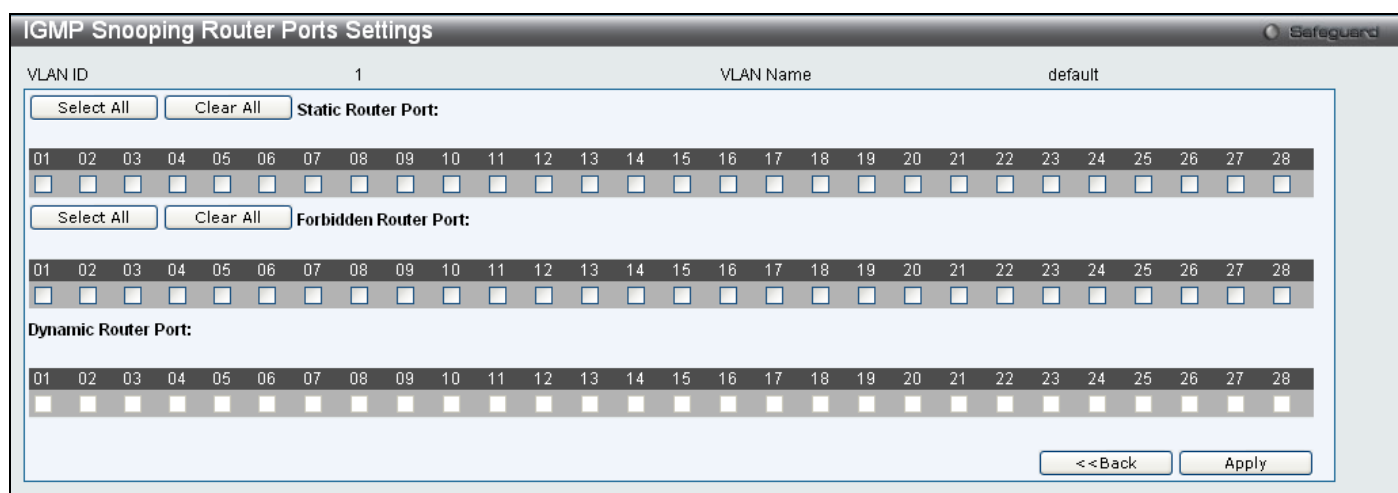


Figure 3 - 28. IGMP Snooping Router Ports Settings window

Select the desired member ports and click **Apply**. Click **<<Back** to go back to the **IGMP Snooping Settings** window.

IGMP Access Control Settings

This window is used to configure IGMP Access Control settings on the Switch.

To view this window, click L2 Features > IGMP Snooping > IGMP Access Control Settings:

From Port	To Port	State	Apply
01	01	Enable	Apply

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
27	Disabled
28	Disabled

Figure 3 - 29. IGMP Access Control Settings window

Parameter	Description
From Port/To Port	Select a range of ports.
State	Enable or disable the IGMP Access Control. When <i>Enable</i> is selected and the Switch receives an IGMP Join request, the Switch will send the access request to the RADIUS server to do the authentication.

Click **Apply** to implement changes made.

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 **L2 Features > IGMP Snooping > IGMP Snooping Multicast VLAN Settings**:

Figure 3 - 30. IGMP Snooping Multicast VLAN Settings window

The following fields can be set

Parameter	Description
ISM VLAN Global State	Click the Enabled or Disabled radio button to enable or disable multicast VLAN.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to add or 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 add or modify the IGMP Snooping Settings for.
State	Enable or disable multicast VLANs for the chosen VLAN.
Replace Source IP	With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will not be replaced.
Member Port (e.g.: 1-4, 6)	A range of member ports to add to the multicast VLAN. They will become the untagged member ports of the ISM VLAN.
Source Port (e.g.: 1-4, 6)	Select the source Port for the multicast VLAN.
Tagged Member Port (e.g.: 1-4, 6)	Specifies the ports that will be tagged as members of the multicast VLAN.
Untagged Source Port (e.g.: 1-4, 6)	A range of untagged source ports to add to the multicast VLAN. The reassigned PVID of the untagged source port will be automatically changed to the multicast VLAN.
Remap Priority (Value 0-7)	The remap priority is associated with the data traffic to be forwarded on the multicast VLAN. If <i>None</i> is selected, the packet's original priority will be used. The default setting is <i>None</i> .
Replace Priority	Tick this option so that the packet's priority will be changed based on the remap priority by the Switch. This option takes effect only when remap priority is set.

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

To add a multicast VLAN to a profile that has been created, click the corresponding hyperlinked [Group List](#) to reveal the following window:

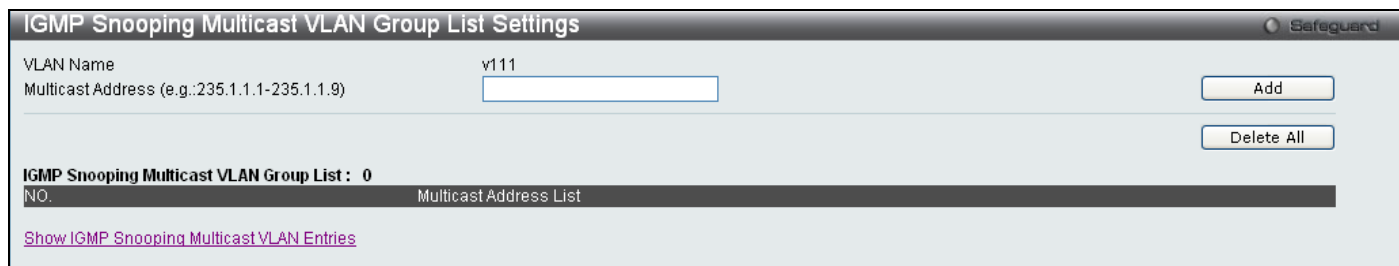


Figure 3 - 31. IGMP Snooping Multicast VLAN Group List Settings window

Enter a Multicast Address and click **Add**. The new information will be displayed in the table at the bottom of the window. Click [Show IGMP Snooping Multicast VLAN Entries](#) to return to the **IGMP Snooping Multicast VLAN Settings** window. Click **Delete All** to remove all the entries on this window.

IP Multicast Profile Settings

This window allows the user to add a profile to which multicast IP address reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP Multicast address or range of IP Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view this window, click **L2 Features > IGMP Snooping > IP Multicast Profile Settings**:

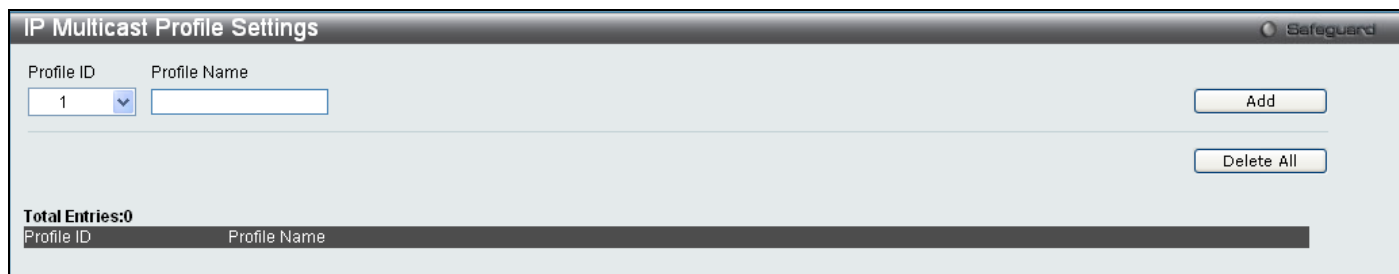


Figure 3 - 32. IP Multicast Profile Settings window

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 IP Multicast Profile.

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

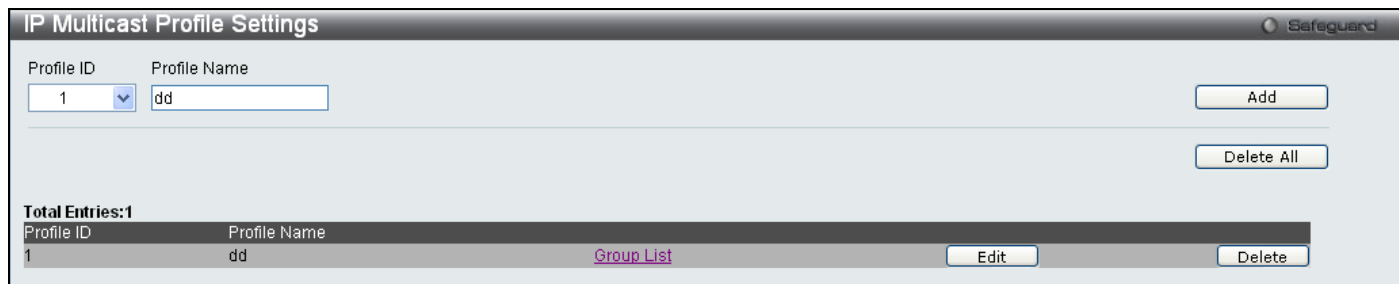


Figure 3 - 33. IP Multicast Profile Settings (Edit) window

To configure the Group List Settings click the hyperlinked [Group List](#). The following window will appear:



Figure 3 - 34. Multicast Address Group List Settings window

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.

Limited Multicast Range Settings

This window enables the user to configure the ports on the Switch that will be involved in the Limited IP Multicast Range. The user can configure the range of ports and associate an IP Multicast Profile to allow or disallow IGMP join requests to multicast groups defined in the profile.

To configure these settings, click **L2 Features > IGMP Snooping > Limited Multicast Range Settings**:

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

Figure 3 - 35. Limited Multicast Range Settings window

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

Max Multicast Group Settings

This window allows users to configure the ports on the Switch that will be a part of the maximum number of multicast groups that can be learned. To add a new Max Multicast Group, enter the information and click **Apply**.

To view this window, click **L2 Features > IGMP Snooping > Max Multicast Group Settings**:

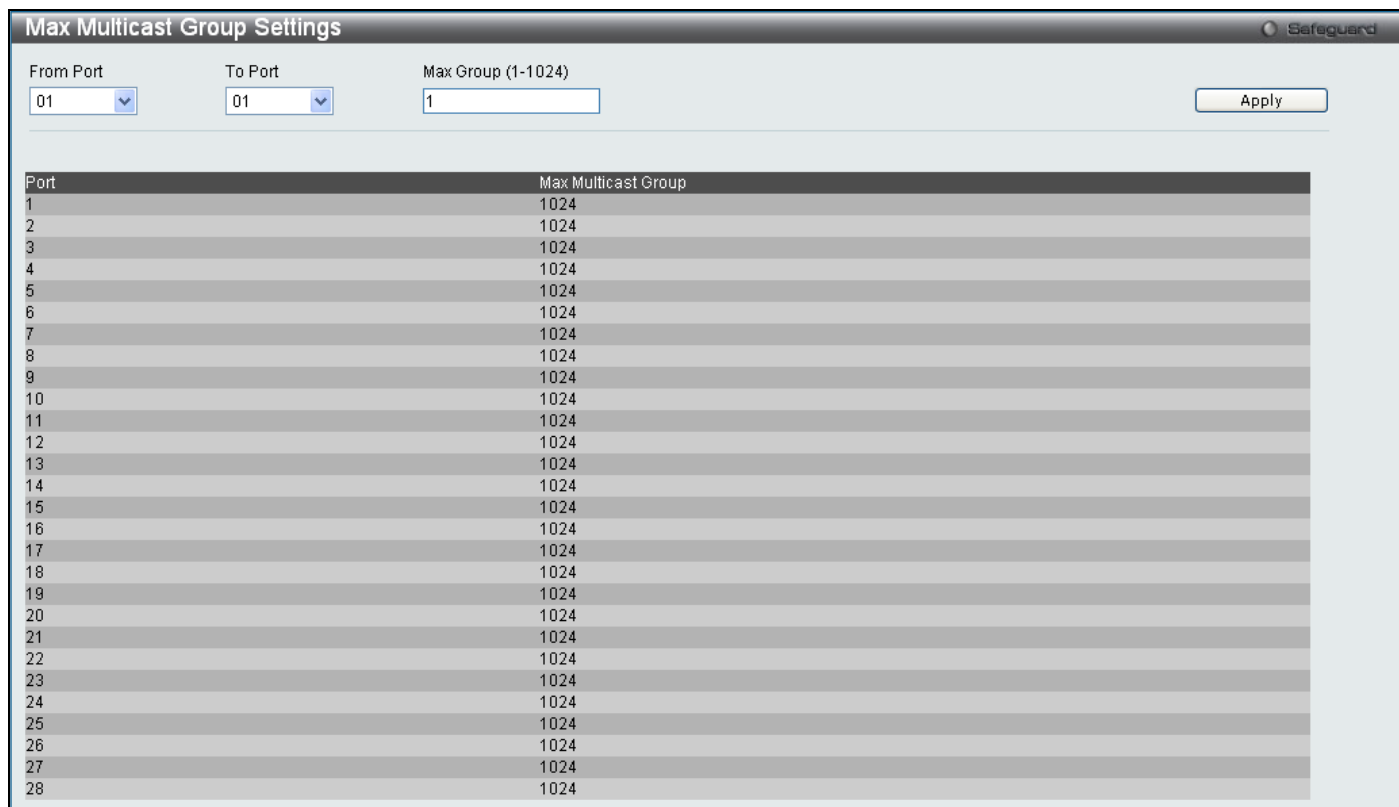


Figure 3 - 36. Max Multicast Group Settings window

The following fields can be set:

Parameter	Description
From Port/To Port	Use the drop-down menus to choose a range of ports.
Max Group (1-1024)	Enter the maximum number of the multicast groups. The range is from 1 to 1024.

MLD Snooping Settings

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.

The Switch supports both MLD Snooping version 1 and MLD version 2.

MLD Control Messages

If implementing MLD snooping version 1, three types of messages are transferred between devices. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131, and 132.

1. **Multicast Listener Query, Version 1** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.

2. **Multicast Listener Report, Version 1** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

If implementing MLD snooping version 2, two types of messages are transferred between devices. The two messages are defined by two ICMPv6 packet headers, labeled 130 and 143.

1. **Multicast Listener Query, Version 2** – Similar to the IGMPv3 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. With MLD snooping version 2, there are three types of MLD query messages emitted by the router, as described below:
 - The router sends a General Query message to learn which multicast addresses have listeners on an attached link. In a General Query, both the Multicast Address field and the Number of Sources field are set to zero.
 - The router sends a Multicast Address Specific Query message to learn if a particular multicast address has any listeners on an attached link. In a Multicast Address Specific Query, the Multicast Address field contains the multicast address that the router is interested in, while the Number of Sources field is set to zero.
 - The router sends a Multicast Address and Source Specific Query to learn if any of the sources from the specified list for the particular multicast address has any listeners on an attached link or not. In a Multicast Address and Source Specific Query the Multicast Address field contains the multicast address that the router is interested in, while the Source Address field(s) contain(s) the source address(es) that the router is interested in.
2. **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

This window is used to enable MLD Snooping on the Switch and to configure the settings for MLD snooping. To enable the MLD Snooping State, click the Enable radio button under MLD Snooping Global Settings and click **Apply**.

To view this window, click **L2 Features > MLD Snooping Settings**:

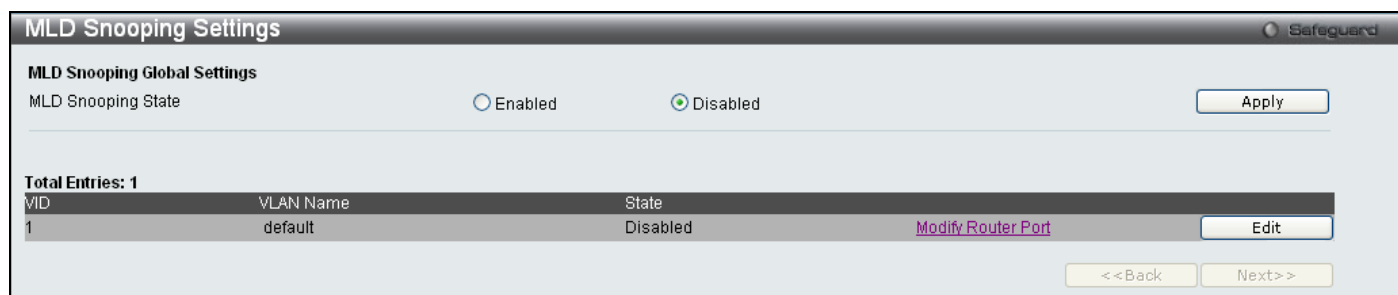


Figure 3 - 37. MLD Snooping Settings window

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



Figure 3 - 38. MLD Snooping Settings (Edit) window

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 the user wishes to modify the MLD 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 MLD Snooping Settings.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting MLD queries. Entries between 1 and 65535 seconds are allowed. The default is 125.
Max Response Time (1-25)	This determines the maximum amount of time in seconds to wait for reports from members. The Max Response Time field allows an entry between 1 and 25 (seconds). The default is 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. The default is 2.
Last Listener Query Interval (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is 1.
Fast Done	This parameter allows the user to enable the Fast Leave function. <i>Enabled</i> , this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Listener Query Interval) when an MLD Leave Report Packet is received by the Switch. The default is <i>Disabled</i> .
State	Select <i>Enabled</i> to implement MLD Snooping. This field is <i>Disabled</i> by default.
Version	The read-only field displays the MLD version used on the Switch, 2.
Querier Role	This read-only field describes the behavior of the Switch for sending query packets. Querier will denote that the Switch is sending out MLD query packets. Non-Querier will denote that the Switch is not sending out MLD query packets.

Click **Apply** to implement any changes made and **<<Back** to return to the initial **MLD Snooping Settings** window.

To modify the MLD Snooping Router Port Settings, click on the hyperlinked [Modify Router Port](#), which will show the following window for the user to configure:

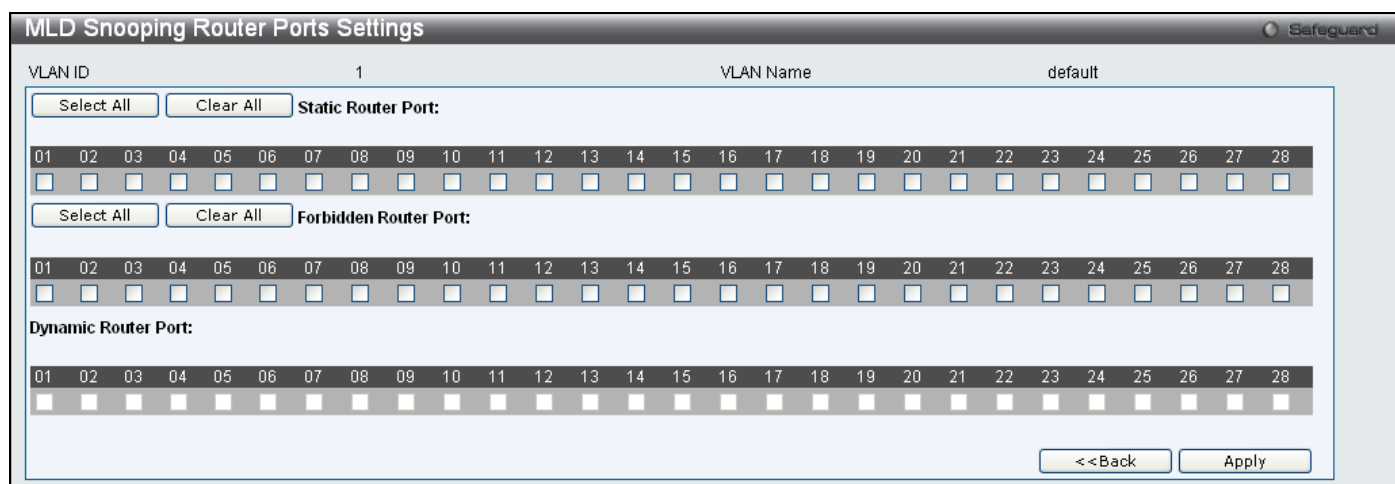


Figure 3 - 39. MLD Snooping Router Ports Settings window

Select the desired router ports and then click **Apply** to implement any changes made. To select either all of the static router ports or all of the forbidden router ports, click the corresponding **Select All** button. To clear either all of the selected static router ports or all of the selected forbidden router ports, click the corresponding **Clear All** button. Click **<<Back** to return to the **MLD Snooping Settings** window.

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 **Layer 2 Features > Port Mirror**:

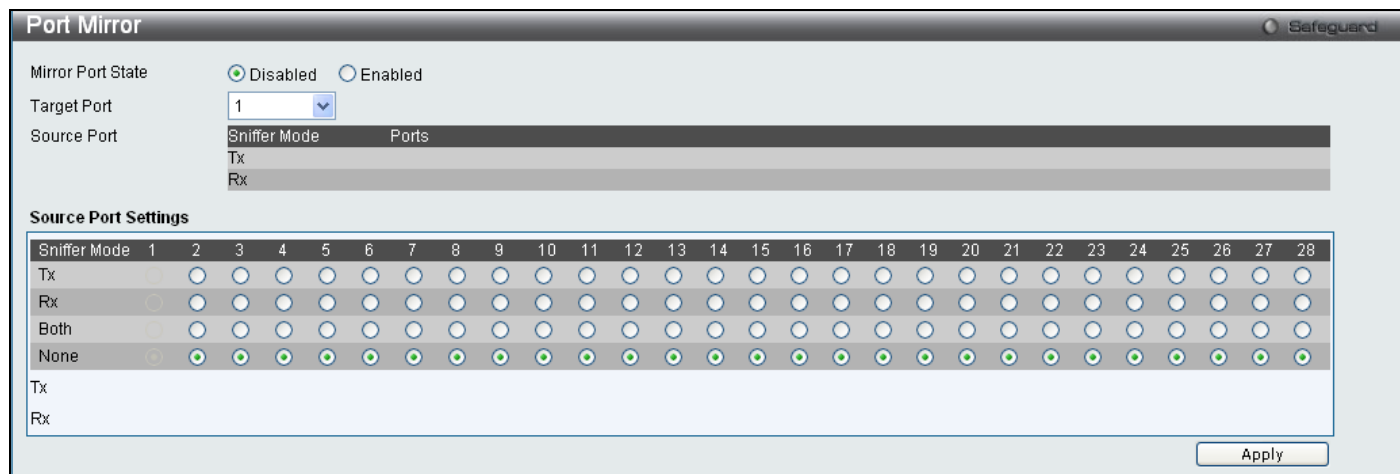


Figure 3 - 40. Port Mirror window

To configure a mirror port:

1. Change the status to Enabled.
2. Select the Target Port, which receives the copies from the source port.
3. Select the Source Port from where the frames come from.
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.

Loopback Detection Settings

The Loopback Detection function is used to detect the loop created by a specific port. Choose the loopback detection operation mode. Two modes are supported, port based and VLAN based. In the port-based mode, the port will be shut-down (be disabled) when a loop is detected; in VLAN-based mode, the port cannot process packets on the VLAN on which the loop is detected. The default mode is port-based. The Loopback Detection port or VLAN will restart (be able to forwarding) 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 **L2 Features > Loopback Detection Settings**:

Port	Loopdetect Detection State	Loop Status
1	Enabled	Normal
2	Enabled	Normal
3	Enabled	Normal
4	Enabled	Normal
5	Enabled	Normal
6	Enabled	Normal
7	Enabled	Normal
8	Enabled	Normal
9	Enabled	Normal
10	Enabled	Normal
11	Enabled	Normal
12	Enabled	Normal
13	Enabled	Normal
14	Enabled	Normal
15	Enabled	Normal
16	Enabled	Normal
17	Enabled	Normal
18	Enabled	Normal
19	Enabled	Normal
20	Enabled	Normal
21	Enabled	Normal
22	Enabled	Normal
23	Enabled	Normal
24	Enabled	Normal

Figure 3 - 41. Loopback Detection Settings window

Parameter	Description
State	Use the drop-down menu to enable or disable loopback detection. The default is <i>Disabled</i> .
Interval (1-32767)	Set a loop-detect Interval between 1 and 32767 seconds. The default is 10 seconds.
Mode	Choose <i>Port Based</i> or <i>VLAN Based</i> .
Recover Time (0 or 60-1000000)	Time allowed (in seconds) for recovery when a loopback is detected. The Loop-detect 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	Use the drop-down menu to select a beginning port number.
To Port	Use the drop-down menu to select an ending port number.
State	Use the drop-down menu to toggle between <i>Enabled</i> and <i>Disabled</i> .
Trap Status	Choose the condition for sending traps. The options are: <i>Loop Detected</i> - Trap is sent when the loop condition is detected. <i>Loop Cleared</i> - Trap is sent when the loop condition is cleared. <i>None</i> – Do not send a trap for loopback detection. This is the default status. <i>Both</i> – Send both cleared and detected traps.

Click **Apply** to implement changes made.

Spanning Tree

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

802.1Q-2005 MSTP

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

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **MSTI Config Information** window when configuring MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998, however the advantages of using RSTP will be lost.

The Rapid Spanning Tree Protocol (RSTP) evolved from the STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in STP and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. The table below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of STP is this absence of immediate feedback from adjacent bridges.

MSTP	RSTP	STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Blocking</i>	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Listening</i>	No	No
<i>Learning</i>	<i>Learning</i>	<i>Learning</i>	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

Table 3 - 1. 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/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

STP/RSTP/MSTP Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to STP format when necessary. However, any segment using STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

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

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

STP Bridge Global Settings

To open the following window, click **L2 features > Spanning Tree > STP Bridge Global Settings**:

Figure 3 - 42. STP Bridge Global Settings window

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: <i>STP</i> - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. <i>RSTP</i> - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. <i>MSTP</i> – Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be <i>Enabled</i> or <i>Disabled</i> . When <i>Enabled</i> , it allows the forwarding of STP BPDU packets from other network devices. The default is <i>Enabled</i> .
Bridge Max Age (6-40)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. 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 Forward Delay (4-30)	The Forward Delay can be from 4 to 30 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
Tx Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is 6.
Max Hops (6-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default is 20.

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

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

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

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

- From Port: 01
- To Port: 01
- External Cost (0=Auto): 0
- Migrate: Yes
- Edge: Auto
- P2P: Auto
- Port STP: Enabled
- Restricted Role: False
- Restricted TCN: False
- Forward BPDU: Enabled
- Hello Time (1-2): 2 sec

Below the configuration options is a table with the following columns: Port, External Cost, Edge, P2P, Port STP, Restricted Role, Restricted TCN, Forward BPDU, and Hello Time. The table lists settings for ports 1 through 22, with values such as Auto/200000 for External Cost, Auto/No for Edge, Auto/Yes for P2P, Enabled for Port STP, False for Restricted Role and Restricted TCN, Enabled for Forward BPDU, and 2/2 for Hello Time.

Legend: Port field : M=Trunk Master ; T= Trunk Member External Cost, Edge, P2P and Hello Time fields : Value1/Value2 (Value1=Configured value ; Value2=Actual value)

Figure 3 - 43. STP Port Settings window

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)	<p>External Cost - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</p> <p>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.</p> <p>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.</p>
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 <i>True</i> 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 <i>Auto</i> parameter will indicate that the port will be able to automatically enable edge port status if needed.
P2P	Choosing the <i>True</i> 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 <i>false</i> indicates that the port cannot have p2p status. <i>Auto</i> 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 <i>False</i> . The default setting for this parameter is <i>True</i> . The default value <i>True</i> is equivalent to the <i>Auto</i> value.
Port STP	Allows STP to be <i>Enabled</i> or <i>Disabled</i> for the ports.
Restricted Role	Toggle between <i>True</i> and <i>False</i> to set the restricted role state of the packet. The default value is <i>False</i> .
Restricted TCN	Toggle between <i>True</i> and <i>False</i> to set the restricted TCN of the packet. The default value is <i>False</i> .
Forward BPDU	This field can be <i>Enabled</i> or <i>Disabled</i> . When <i>Enabled</i> , it allows the forwarding of STP BPDU packets from other network devices. The default is <i>Enabled</i> .
Hello Time (1-2)	The Hello Time can be set from 1 to 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. The default value is 2.

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 **L2 Features > Spanning Tree > MST Configuration Identification**:

Figure 3 - 44. MST Configuration Identification window

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 (1-8)	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. <i>Add VID</i> - Select this parameter to add VLANs to the MSTI ID, in conjunction with the VID List parameter. <i>Remove VID</i> - Select this parameter to remove VLANs 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** for changes to take effect.

STP Instance Settings

The following window displays MSTIs currently set on the Switch.

To view the following table, click **L2 Features > Spanning Tree > STP Instance Settings**:

Instance Type	Instance Status	Instance Priority
CIST	Disabled	32768(Bridge Priority : 32768, SYS ID Ext : 0)

STP Instance Operational Status			
MSTP ID	--	Designated Root Bridge	--
External Root Cost	--	Regional Root Bridge	--
Internal Root Cost	--	Designated Bridge	--
Root Port	--	Max Age	--
Forward Delay	--	Remaining Hops	--
Last Topology Change	--	Topology Changes Count	--

Figure 3 - 45. STP Instance Settings window

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). This value is created in the MST Configuration menu (see above). Values allowed for MSTI ID range from 1 - 8.
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:

Instance Type	Instance Status	Instance Priority
CIST	Enabled	32768(Bridge Priority : 32768, SYS ID Ext : 0)

STP Instance Operational Status			
MSTP ID	0	Designated Root Bridge	32768/00-21-91-AF-EA-00
External Root Cost	0	Regional Root Bridge	32768/00-21-91-AF-EA-00
Internal Root Cost	0	Designated Bridge	32768/00-21-91-AF-EA-00
Root Port	None	Max Age	20
Forward Delay	15	Remaining Hops	--
Last Topology Change	7	Topology Changes Count	1

Figure 3 - 46. STP Instance Settings - View window

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 the following window, click **L2 Features > Spanning Tree > MSTP Port Information**:

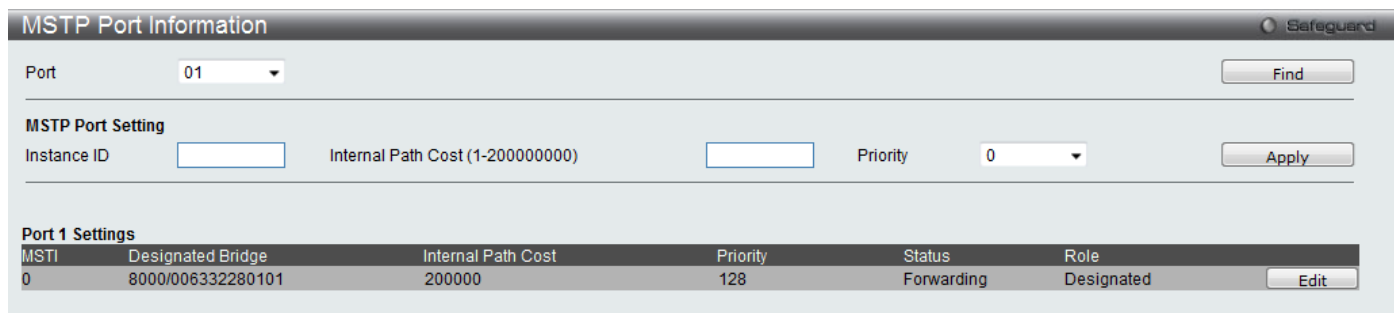


Figure 3 - 47. MSTP Port Information window

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. 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. A lower Internal cost represents a quicker transmission.
Priority	Select 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.

Forwarding & Filtering

This folder contains windows for Unicast Forwarding and Multicast Forwarding.

Unicast Forwarding Settings

To view this window, click **L2 Features > Forwarding & Filtering > Unicast Forwarding Settings**:

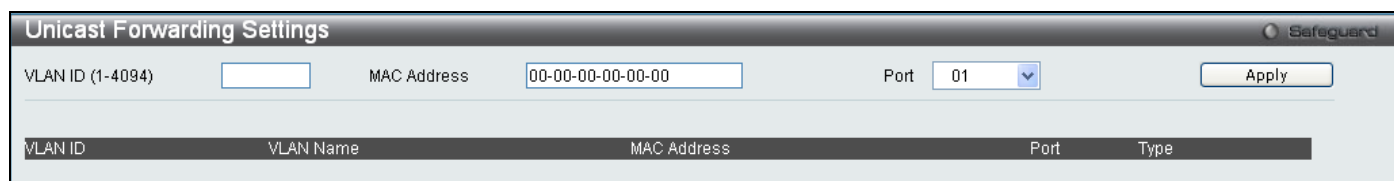


Figure 3 - 48. Unicast Forwarding Settings window

To add or edit an entry, define the following parameters and then click **Add/Modify**:

Parameter	Description
VLAN ID (1-4094)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port	Select the port number on which the MAC address entered above resides.
VLAN Name	The VLAN Name associated with the subnet.

Click **Apply** to implement the changes made. The new entries will be displayed on the bottom half of the window.

Multicast Forwarding Settings

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Forwarding Settings**:

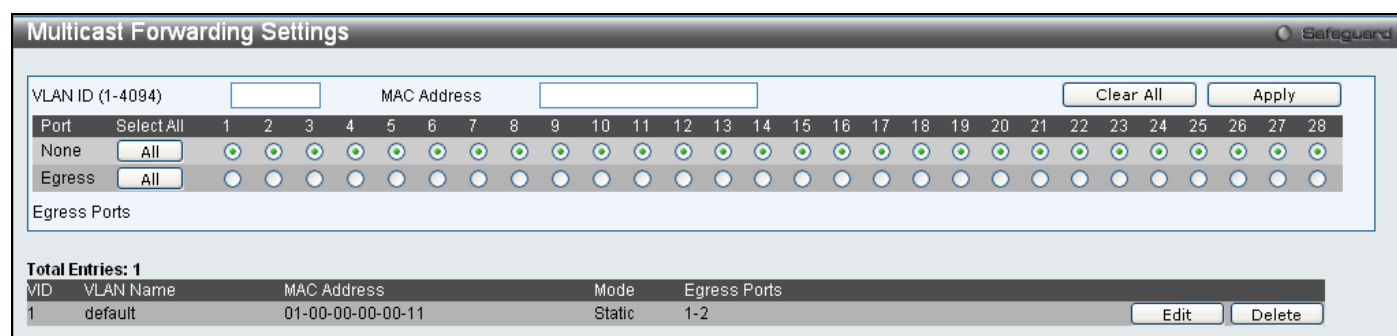


Figure 3 - 49. Multicast Forwarding Settings window

The following parameters can be set:

Parameter	Description
VLAN ID (1-4094)	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
MAC Address	The MAC address that will be added to the multicast forwarding table.
Port Settings	<p>Allows the selection of ports that will be members of the static multicast group. The options are:</p> <p><i>None</i> - 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.</p> <p><i>Egress</i> - The port is a static member of the multicast group.</p> <p>Click All to choose either all of the ports selected as None or all of the ports selected as Egress. Click Clear All to clear all the settings at the top of this window.</p>

Click **Apply** to implement the changes made. To delete an entry in the static multicast forwarding table, click the corresponding **Delete** button. To modify an entry in the static multicast forwarding table, click the corresponding **Edit** button and make the desired changes at the top of the window before clicking the **Apply** button.

Multicast Filtering Mode

Users can configure the multicast filtering mode.

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Filtering Mode:**

Port	Multicast Filtering Mode
1	Forward Unregistered Groups
2	Forward Unregistered Groups
3	Forward Unregistered Groups
4	Forward Unregistered Groups
5	Forward Unregistered Groups
6	Forward Unregistered Groups
7	Forward Unregistered Groups
8	Forward Unregistered Groups
9	Forward Unregistered Groups
10	Forward Unregistered Groups
11	Forward Unregistered Groups
12	Forward Unregistered Groups
13	Forward Unregistered Groups
14	Forward Unregistered Groups
15	Forward Unregistered Groups
16	Forward Unregistered Groups
17	Forward Unregistered Groups
18	Forward Unregistered Groups
19	Forward Unregistered Groups
20	Forward Unregistered Groups
21	Forward Unregistered Groups
22	Forward Unregistered Groups
23	Forward Unregistered Groups
24	Forward Unregistered Groups
25	Forward Unregistered Groups
26	Forward Unregistered Groups
27	Forward Unregistered Groups
28	Forward Unregistered Groups

Figure 3 - 50. Multicast Filtering Mode window

The following parameters can be set:

Parameter	Description
From Port/To Port	The range of ports to be configured.
Filtering Mode	<p>This drop-down menu instructs the Switch what action to take when it receives a multicast packet that requires forwarding to a port.</p> <p><i>Forward Unregistered Groups</i> – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.</p> <p><i>Filter Unregistered Groups</i> – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above..</p>

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

NLB Settings

The Network Load Balancing commands are used to configure the Switch to support Network Load Balancing (NLB), a proprietary Microsoft implementation of server clustering and load balancing, suitable for various stateless applications such as FTP, VPN and Web servers. Client requests for such applications can be distributed among multiple servers in a cluster that share a single IP address and a single destination MAC address. Client requests are forwarded to all servers in the cluster but only one will actually process the request.

The Switch operates NLB in unicast mode or multicast mode. Unicast is the default operation mode. To support this mode the switch between clients and servers must allow L2 unicast packets to be forwarded to multiple NLB servers. The other mode is multicast mode. With multicast mode the NLB servers share identical unicast IP address called Cluster IP and a multicast MAC address called Flooding MAC. In both modes, a shared destination MAC address is used as the destination MAC address in the client request frame, however the server that actually processes the request will use its own MAC address in the reply frame.

Please consult Microsoft’s server documentation for more information on using and setting up NLBS on Windows servers.

To view this window, click **L2 Features > NLB Settings**:

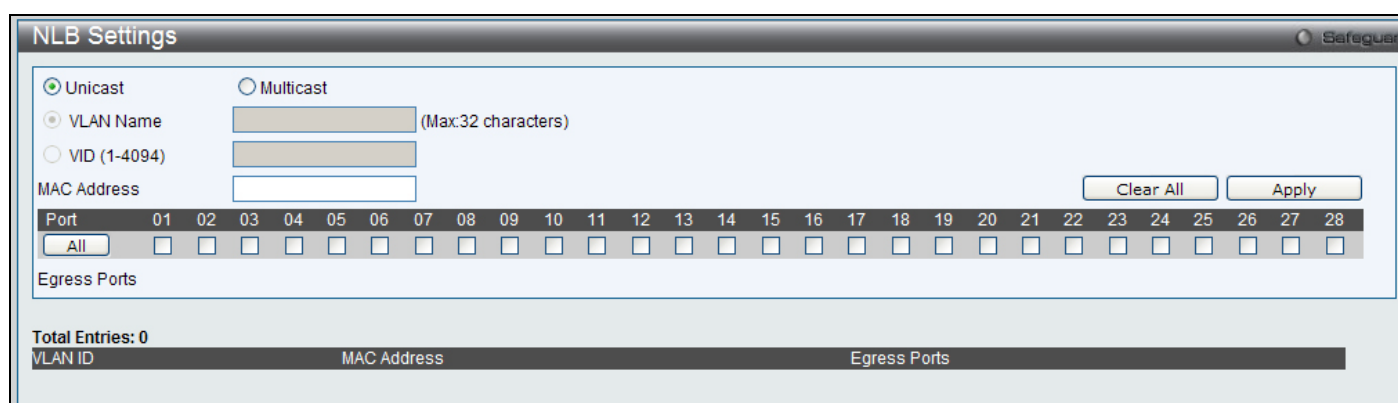


Figure 3 - 51. NLB Settings window

The following parameters can be set:

Parameter	Description
Unicast/Multicast	Click on the radio button for mode in which NLB will operate.
VLAN Name	Enter the name for the VLAN of the NLB multicast FDB entry being created.
VID	Enter the VLAN ID of the NLB multicast FDB entry being created.
MAC Address	Type the MAC address to enter into the NLB Forwarding Data Base.
Port	Choose the forwarding ports to be used for the configured NLB unicast FDB entry.

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

LLDP

The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station’s point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) through a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP Global Settings

To view this window, click **L2 Features > LLDP > LLDP Global Settings**:

Figure 3 - 52. LLDP Global Settings window

The following parameters can be set:

Parameter	Description
LLDP State	Used to enable or disable LLDP on the Switch.
LLDP Forward Message	When LLDP is Disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message Tx Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (5 to 32768).
Message Tx Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP Reinit Delay (1-10)	The LLDP reinitialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP Reinit Delay, enter a value in seconds (1 to 10).
LLDP Tx Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (1 to 8192).
LLDP Notification Interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (5 to 3600).

Click **Apply** to implement changes made.

LLDP Port Settings

To view this window, click **L2 Features > LLDP > LLDP Port Settings**:

LLDP Port Settings

From Port: 01 To Port: 01 Notification: Disabled Admin Status: Tx and Rx
 Subtype: IPv4 Action: Disabled Address:

Note: The IPv4/IPv6 Address should be the Switch's Address.

Port ID	Notification	Admin Status	Subtype	Address
1	Disabled	Tx and Rx	IPv4	
2	Disabled	Tx and Rx	IPv4	
3	Disabled	Tx and Rx	IPv4	
4	Disabled	Tx and Rx	IPv4	
5	Disabled	Tx and Rx	IPv4	
6	Disabled	Tx and Rx	IPv4	
7	Disabled	Tx and Rx	IPv4	
8	Disabled	Tx and Rx	IPv4	
9	Disabled	Tx and Rx	IPv4	
10	Disabled	Tx and Rx	IPv4	
11	Disabled	Tx and Rx	IPv4	
12	Disabled	Tx and Rx	IPv4	
13	Disabled	Tx and Rx	IPv4	
14	Disabled	Tx and Rx	IPv4	
15	Disabled	Tx and Rx	IPv4	
16	Disabled	Tx and Rx	IPv4	
17	Disabled	Tx and Rx	IPv4	
18	Disabled	Tx and Rx	IPv4	
19	Disabled	Tx and Rx	IPv4	
20	Disabled	Tx and Rx	IPv4	
21	Disabled	Tx and Rx	IPv4	
22	Disabled	Tx and Rx	IPv4	
23	Disabled	Tx and Rx	IPv4	
24	Disabled	Tx and Rx	IPv4	
25	Disabled	Tx and Rx	IPv4	
26	Disabled	Tx and Rx	IPv4	
27	Disabled	Tx and Rx	IPv4	
28	Disabled	Tx and Rx	IPv4	

Figure 3 - 53. LLDP Port Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Notification	Use the pull-down menu to enable or disable the status of the LLDP notification. This function controls the SNMP trap, however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This function controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains <i>Tx</i> , <i>Rx</i> , <i>Tx and Rx</i> or <i>Disabled</i> . <i>Tx</i> : the local LLDP agent can only transmit LLDP frames. <i>Rx</i> : the local LLDP agent can only receive LLDP frames. <i>Tx and Rx</i> : the local LLDP agent can both transmit and receive LLDP frames. <i>Disabled</i> : the local LLDP agent can neither transmit nor receive LLDP frames. The default value is <i>Tx and Rx</i> .
Subtype	This read-only field displays IPv4, the type of the IP address.
Action	Used to <i>Enable</i> or <i>Disable</i> the advertise management address function base port.
Address	The address must be the management IP-address. For multi IP-addresses, you can enter any IP or create a new IP interface that you want to add.

Click **Apply** to implement changes made.

LLDP Basic TLVs Settings

This window is used to enable the settings for the Basic TLVs Settings.

To view this window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**:

Port	Port Description	System Name	System Description	System Capabilities
1	Disabled	Disabled	Disabled	Disabled
2	Enabled	Enabled	Enabled	Enabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled
25	Disabled	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled	Disabled

Figure 3 - 54. LLDP Basic TLVs Settings window

Use the drop-down menus to enable or disable the settings for the Basic TLVs Settings. Click **Apply** to implement changes made.

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Port Description	Use the drop-down menu to enable or disable port description.
System Name	Use the drop-down menu to enable or disable system name.
System Description	Use the drop-down menu to enable or disable system description.
System Capabilities	Use the drop-down menu to enable or disable system capabilities.

Click **Apply** to implement changes made.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**:

Port	PVID State	Port and Protocol VID State	VID	VLAN Name State	VID	Protocol Identity State	Protocol Identity
1	Disabled	Disabled		Disabled		Disabled	
2	Enabled	Disabled		Enabled	1-4094	Enabled	EAPOL, LAC...
3	Disabled	Disabled		Disabled		Disabled	
4	Disabled	Disabled		Disabled		Disabled	
5	Disabled	Disabled		Disabled		Disabled	
6	Disabled	Disabled		Disabled		Disabled	
7	Disabled	Disabled		Disabled		Disabled	
8	Disabled	Disabled		Disabled		Disabled	
9	Disabled	Disabled		Disabled		Disabled	
10	Disabled	Disabled		Disabled		Disabled	
11	Disabled	Disabled		Disabled		Disabled	
12	Disabled	Disabled		Disabled		Disabled	
13	Disabled	Disabled		Disabled		Disabled	
14	Disabled	Disabled		Disabled		Disabled	
15	Disabled	Disabled		Disabled		Disabled	
16	Disabled	Disabled		Disabled		Disabled	
17	Disabled	Disabled		Disabled		Disabled	
18	Disabled	Disabled		Disabled		Disabled	
19	Disabled	Disabled		Disabled		Disabled	
20	Disabled	Disabled		Disabled		Disabled	
21	Disabled	Disabled		Disabled		Disabled	
22	Disabled	Disabled		Disabled		Disabled	
23	Disabled	Disabled		Disabled		Disabled	
24	Disabled	Disabled		Disabled		Disabled	
25	Disabled	Disabled		Disabled		Disabled	
26	Disabled	Disabled		Disabled		Disabled	

Figure 3 - 55. LLDP Dot1 TLVs Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
PVID	Use the drop-down menu to enable or disable the advertise PVID.
Protocol VLAN ID	Use the drop-down menu to enable or disable the advertise Protocol VLAN ID.
VLAN Name	Use the drop-down menu to enable or disable the advertise VLAN Name.
Protocol Identity	Use the drop-down menu to enable or disable the advertise Protocol Identity.

Click **Apply** to implement changes made.

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**:

Port	MAC/PHY Configuration Status	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled
2	Enabled	Enabled	Enabled
3	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled
25	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled

Figure 3 - 56. LLDP Dot3 TLVs Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the drop-down menu to select a range of ports to be configured.
MAC/PHY Configuration Status	This TLV optional data type indicates that the LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is <i>Disabled</i> .
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is <i>Disabled</i> .
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is <i>Disabled</i> .

Click **Apply** to implement changes made.

Ethernet OAM

Ethernet OAM (Operations, Administration, and Maintenance) is a data link layer protocol which provides network administrators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions on point-to-point and emulated point-to-point Ethernet link.

Ethernet OAM Port Settings

To view this window, click **L2 Features > Ethernet OAM > Ethernet OAM Port Settings**:

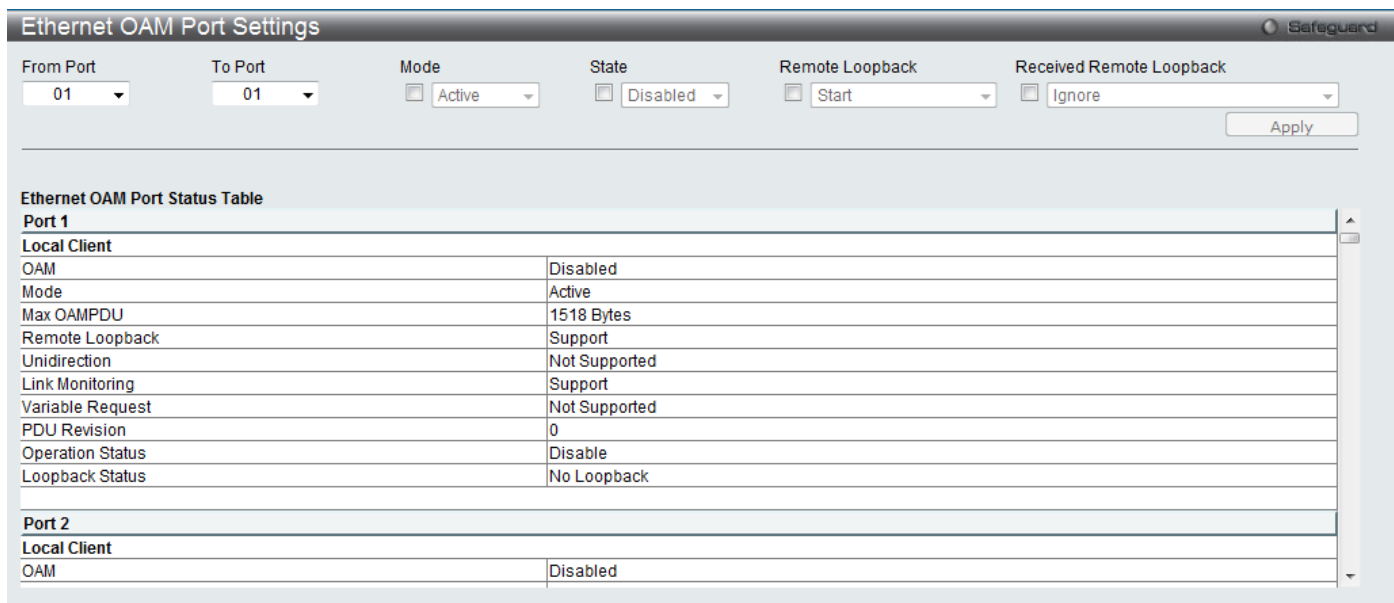


Figure 3 - 57. Ethernet OAM Port Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Specified a range of ports to be configured.
Mode	Specify to operate in either active mode or passive mode The default mode is active.
State	Specify to enable or disable the OAM function. The default state is disabled.
Remote Loopback	If start is specified, it will request the peer to change to the remote loopback mode. If stop is specified, it will request the peer to change to the normal operation mode.
Received Remote Loopback	Specify whether to process or to ignore the received Ethernet OAM remote loopback command. The default method is <i>ignore</i> .

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

Ethernet OAM Event Configuration

To view this window, click **L2 Features > Ethernet OAM > Ethernet OAM Event Configuration**:

Figure 3 - 58. Ethernet OAM Event Configuration window

The following parameters can be set:

Parameter	Description
From Port/To Port	Specified a range of ports to be configured.
Link Event	Choose the type of Link Event, <i>Link Monitor</i> or <i>Critical Link Event</i> , to configure.
Link Monitor	The option is used to configure ports Ethernet OAM link monitoring error symbols, error frames, error frame period, and error frame seconds. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. If the number of error symbols or error frames is equal to or greater than the specified threshold within the period specified by the Window option, and the event notification state (Notify) is enabled, it generates an event to notify the remote OAM peer. Use the Link Monitor menu to define the type of link monitor, and set the threshold, window and notifications status.
Critical Link Event	The <i>Critical Event</i> option refers to an unspecified critical event. The <i>Dying Gasp</i> option specifies detection of an unrecoverable event has occurred, such as a power failure of the remote device.
Threshold	Specify the number of error symbols, error frames, error frame period, or error frame seconds in the period that is required to be equal to or greater than in order for the event to be generated. Threshold value can range from 0 – 4294967295.
Window:	For error symbol and error frame, the available range is 1000 to 60000 ms and default value 1000ms. For error frame period the range is 14881 to 89286000, the default value is 148810 for FE port. For error frame seconds the range is 10000 to 900000, the default value is 60000.
Notify	Specify to enable or disable the event notification. The default state is <i>Enabled</i> .

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

Connectivity Fault Management (CFM)

Connectivity Fault Management (CFM) or Ethernet Connectivity Fault Management is an end-to-end Ethernet layer OAM protocol. CFM is defined by IEEE 802.1ag and includes connectivity monitoring, fault notification and means of isolating faults on large Ethernet metropolitan-area networks (MANs) and WANs.

Ethernet has traditionally operated on isolated enterprise LANs. As Ethernet has been expanded to operate on the much larger scale carrier networks that encompass multiple administrative domains, the demands of the much larger and more complex networks required a new set of OAM capabilities. Since these larger scale networks have a very large user base, carry more diversified network applications and typically span a much larger geographical area than traditional enterprise Ethernet LANs where link uptime is crucial, a means of dealing with connectivity faults able to operate in Ethernet became necessary. Since none of the existing OAM protocols could adequately address this new circumstance, Ethernet Connectivity Fault Management has been developed in order to meet the new operational management needs created by the application of Ethernet technologies to MANs and WANs.

Ethernet CFM provides Ethernet network service providers with various benefits such as end-to-end service-level OAM and lower operating expenses, all operated on top of a familiar Ethernet platform.

CFM introduces some new terms and concepts to Ethernet, these are briefly described below.

Maintenance Domain

A maintenance domain is generic term referring to a management area created for the purpose of managing and administering a network. A maintenance domain is operated by a single entity or “owner” and defined by a boundary with a set of ports internal to this boundary.

An Ethernet CFM maintenance domain, referred to in this manual simply as an MD, exists in a hierarchical relationship to other MDs. Typically a large MAN or WAN can be partitioned into a hierarchy based on the size of domain that mirrors the structural relationship of customers, service providers and operators. The service providers have end-to-end service responsibility while operators provide service transport across subnetworks. The hierarchy is defined by a maintenance level value ranging from 0 to 7 where 7 is the highest level and 0 the lowest level. The larger the MD is, the higher its maintenance level will be. For example, if the customer domain is the largest MD, it should be assigned a maintenance level of 7, the operator MD being the smallest, receives a maintenance level of 0 with the service provider domain being in between these values. Maintenance levels are manually assigned by the network administrator. All levels of the MD hierarchy must operate together.

Nesting of MDs is allowed, however they cannot intersect since this violates the requirement that management of MDs be done by a single owner. If two or more domains are nested, the outer domain must be assigned a higher maintenance level than the nested domains.

CFM operations and message exchanges are conducted on a per-domain basis. This means for example, that CFM operating at level 3 does not allow discovery of the level 3 network by higher levels.

Maintenance Association

A maintenance association (MA) in CFM is a set of MEPs that have been configured with the same management domain level and maintenance association identifier (MAID).

Different MAs in an MD must have different MA Names. Different MAs in different MDs may have the same MA Name. The MEP list specified for a MA can be located in different devices. MEPs must be created on ports of these devices explicitly. A MEP will transmit CCM packets periodically across the MA. The receiving MEP will verify these received CCM packets from other MEPs against this MEP list for configuration integrity check.

Maintenance Point

A maintenance point in CFM is a point of demarcation on a port within a maintenance domain. Maintenance points filter CFM frames within the boundaries of an MD by dropping frames that do not belong to the correct maintenance level. There are two types of maintenance points, **Maintenance Endpoints** (MEPs) and **Maintenance Intermediate Points** (MIPs). MEPS and MIP are manually configured by a network administrator.

A MEP exists at the edge of a maintenance domain, defining the boundary of the MD. MEP functions include filtering CFM messages so that they are confined to the MD. A MEP can be configured to transmit Connectivity Check Messages (CCMs) and will transmit treacroute and loopback messages if configured to do so. A MEP can be *Inward* facing or *Outward* facing.

An Inward facing MEP source CFM frames toward the bridge relay function, not through the bridge port on which the MEP is configured. An Inward facing MEP drops all CFM frames at its level or lower that are received from the Inward side; and forwards all CFM frames at a higher level regardless of the origin of the frame, Inward or Outward. If the port on which the inward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can no longer transmit or receive CFM messages.

An Outward facing MEP source frames toward the bridge port and can only be configured on routed ports. An Outward facing port drops all CFM frames at it level or lower coming from the bridge relay function side. It processes all CFM frames at its level, and drops all CFM frames at a lower level, coming from the bridge port. An Outward facing port forwards all CFM frames at higher levels regardless of which direction the frames come in. If the port on which the outward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can still transmit and receive CFM messages through the bridge port.

A MIP is a maintenance point that is internal to an MD, not at the boundary. A MIP receives CFM frames from other MIPs and from MEPs. These frames are cataloged and forwarded using the bridge relay function and bridge port. All CFM frames at a lower level than the MIP are blocked and dropped regardless of the origin. All CFM frames at a higher level are forwarded regardless of the origin. If the port on which a MIP is configured is blocked by Spanning-Tree Protocol, the MIP cannot receive CFM messages or relay them toward the bridge relay function side. The MIP can, however, receive and respond to CFM messages from the bridge port.

CFM messages include Continuity Check Messages (CCMs), Loopback Messages (LBMs) and Link Trace Messages (LTMs). CFM uses standard Ethernet frames that can be sourced, terminated, processed and relayed by bridges. Routers support limited CFM functions.

Continuity Check Messages (CCMs) are multicast messages exchanged among MEPs. CCMs allow discovery of MEPs for other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a maintenance domain. CCMs are cataloged by MIPs at the same maintenance level and terminated by remote MEPs at the same maintenance level. They are unidirectional (no response solicitation) and carry the status of the port on which the MEP is configured. LBMs are similar to Ping or ICMP messages in that they indicate only whether a destination is reachable and do not allow discovery of each hop.

Link Trace Messages (LTMs) are multicast CFM frames sent by MEPs to identify adjacency relationships with remote MEPs and MIPs at the same maintenance level. The message body of an LTM includes a destination MAC address of a target MEP that terminates the linktrace. When a MIP or MEP receives an LTM, it generates a unicast Link Trace Reply (LTR) to the initiating MEP. It also forwards the LTM to the target MEP destination MAC address. An LTM effectively traces the path to the target MEP or MIP.

Loopback Messages (LBMs) are similar to Ping or ICMP messages in that they indicate only whether a destination is reachable and do not allow the discovery of each hop.

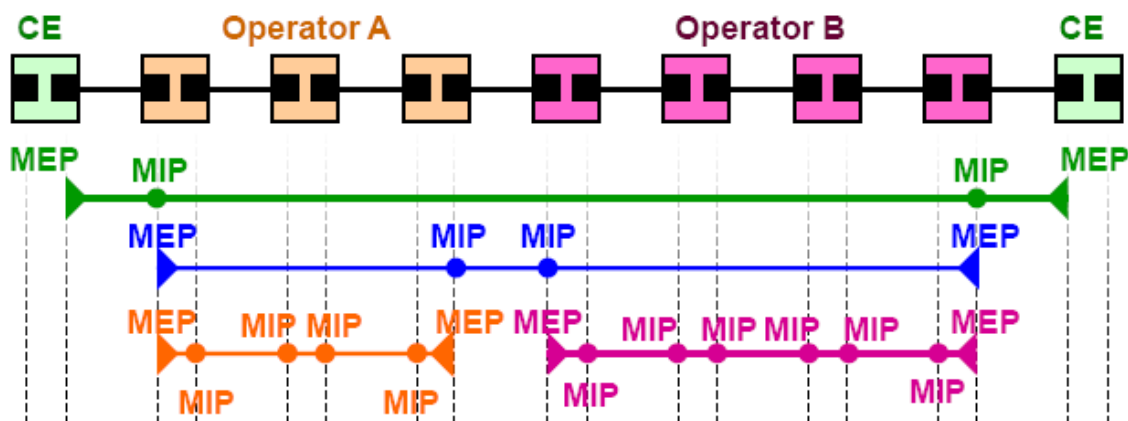


Figure 3 - 59. OAM Domain Architecture

- Maintenance Association (MA) – Boundaries of an Administrator’s scope of monitoring part of the network
- Maintenance Domain (MD) – A level of monitoring within the hierarchy
- Maintenance End Points (MEP) – End Points of the MA or MD
- Maintenance Intermediate Points (MIP) – Intermediate Points within MA or MD

Note: CE = Customer Equipment

CFM Settings

To view this window, click **L2 Features > CFM > CFM Settings**:

Figure 3 - 60. CFM Settings window

The following parameters can be set:

Parameter	Description
CFM State	To enable or disable the CFM feature.
All MPs Reply LTRs	To enable or disable all Maintenance Points (MEPs and MIPs) to reply Link Trace Reply (LTR) message. These are used with Link Trace Messages to trace a path from a MEP to another MEP or MIP.
CFM MD	To enter the maintenance domain name. A maintenance domain name can be up to 22 characters long.
Level	To select the maintenance domain level. Levels are set between 0 and 7 where 0 is the lowest and 7 is the highest.
MIP	This is the control creations of MIPs. <i>None</i> – Don’t create MIPs. This is the default value. <i>Auto</i> – MIPs can always be created on any ports in this MD, if that port is not configured with a MEP of this MD. For the intermediate switch in a MA, the setting must be auto in order for the MIPs to be created on this device. <i>Explicit</i> – MIPs can be created on any ports in this MD, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MD.
SenderID TLV	This is the control transmission of the SenderID TLV. <i>None</i> – Don’t transmit sender ID TLV. This is the default value. <i>Chassis</i> – Transmit sender ID TLV with chassis ID information. <i>Manage</i> – Transmit sender ID TLV with managed address information. <i>Chassis Manage</i> – Transmit sender ID TLV with chassis ID information and manage address information.

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

CFM MA Settings

To view this window, click on **L2 Features > CFM > CFM Settings > Add MA** button:

VID	MA Name	MIP	Sender ID	CCM	MEP ID(s)
1	MA1	Defer	Defer	10 seconds	

Figure 3 - 61. CFM MA Settings window

The following parameters can be set:

Parameter	Description
MA	To enter the maintenance association name.
VLAN ID	VLAN Identifier. Different MA must be associated with different VLANs.

Click **Add** to implement the changes made. To re-configure the MA, select it and click on the **Edit** button. To add a MEP, click the **Add MEP** button.

MA information presented in the table includes the following:

Parameter	Description
MIP This is the control creation of MIPs.	<p><i>None</i> - Don't create MIPs.</p> <p><i>Auto</i> - MIPs can always be created on any ports in this MA, if that port is not configured with a MEP of that MA.</p> <p><i>Explicit</i> - MIP can be created on any ports in this MA, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MA.</p> <p><i>Defer</i> - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.</p>
SenderID This is the control transmission of the sender ID TLV.	<p><i>None</i> - Don't transmit sender ID TLV. This is the default value.</p> <p><i>Chassis</i> - Transmit sender ID TLV with chassis ID information.</p> <p><i>Manage</i> - Transmit sender ID TLV with manage address information.</p> <p><i>Chassis Manage</i> - Transmit sender ID TLV with chassis ID information and manage address information.</p> <p><i>Defer</i> - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.</p>
CCM: This is the CCM interval.	<p><i>10ms</i> - 10 milliseconds. Not recommended. For test purpose.</p> <p><i>100ms</i> - 100 milliseconds. Not recommended. For test purpose.</p> <p><i>1sec</i> - One second.</p> <p><i>10sec</i> - Ten seconds. This is the default value.</p> <p><i>1min</i> - One minute.</p> <p><i>10min</i> - Ten minutes.</p>
MEP ID(s) This is to specify the MEP IDs contained in the maintenance association.	<p><i>Add</i> - Add MEP ID(s).</p> <p><i>Delete</i> - Delete MEP ID(s).</p> <p>By default, there is no MEP ID in a newly created maintenance association.</p> <p>The range of the MEP ID is 1 to 8191.</p>

Click **Apply** to implement changes made.

To view the MIP Port Table, click on the **MIP Port Table** button:

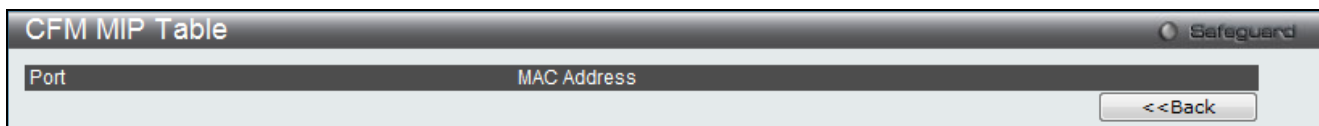


Figure 3 - 62. CFM MIP Table window

CFM MEP Settings

To view this window, click on the **Add MEP** button in the **CFM MA Settings** window (**L2 Features > CFM > CFM Settings**):

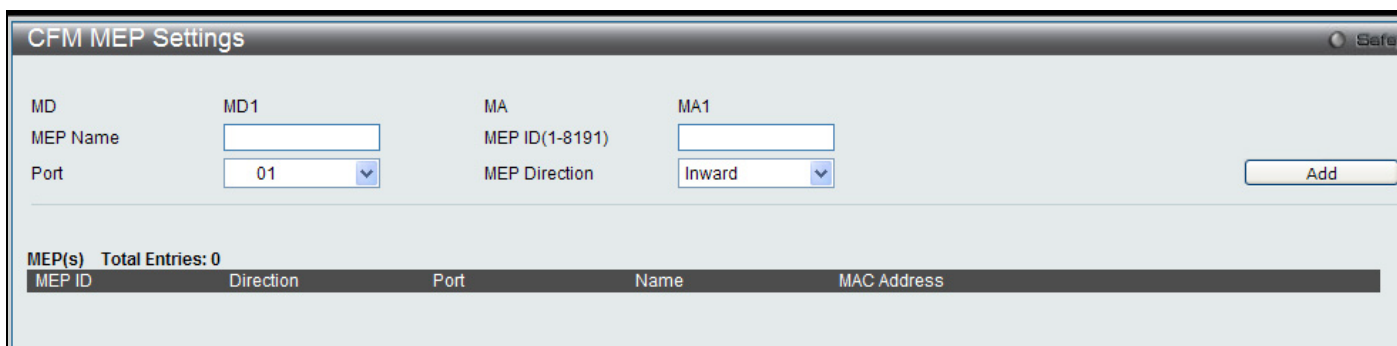


Figure 3 - 63. CFM MEP Settings window

Parameter	Description
MEP Name	MEP name. It is unique among all MEPs configured on the device.
MEP ID	MEP MEPID. It should be configured in the MA's MEP ID list.
Port	Port number. This port should be a member of the MA's associated VLAN.
MEP Direction	<p>This is the MEP direction.</p> <p><i>Inward</i> - Inward facing (up) MEP. An Inward facing MEP drops all CFM frames at its level or lower that are received from the Inward side; and forwards all CFM frames at a higher level regardless of the origin of the frame, Inward or Outward.</p> <p><i>Outward</i> - Outward facing (down) MEP. An Outward facing port drops all CFM frames at its level or lower coming from the bridge relay function side. It processes all CFM frames at its level, and drops all CFM frames at a lower level, coming from the bridge port. An Outward facing port forwards all CFM frames at higher levels regardless of which direction the frames come in.</p>

To view detailed information about the MEP entry, click on the **View Detail** link.

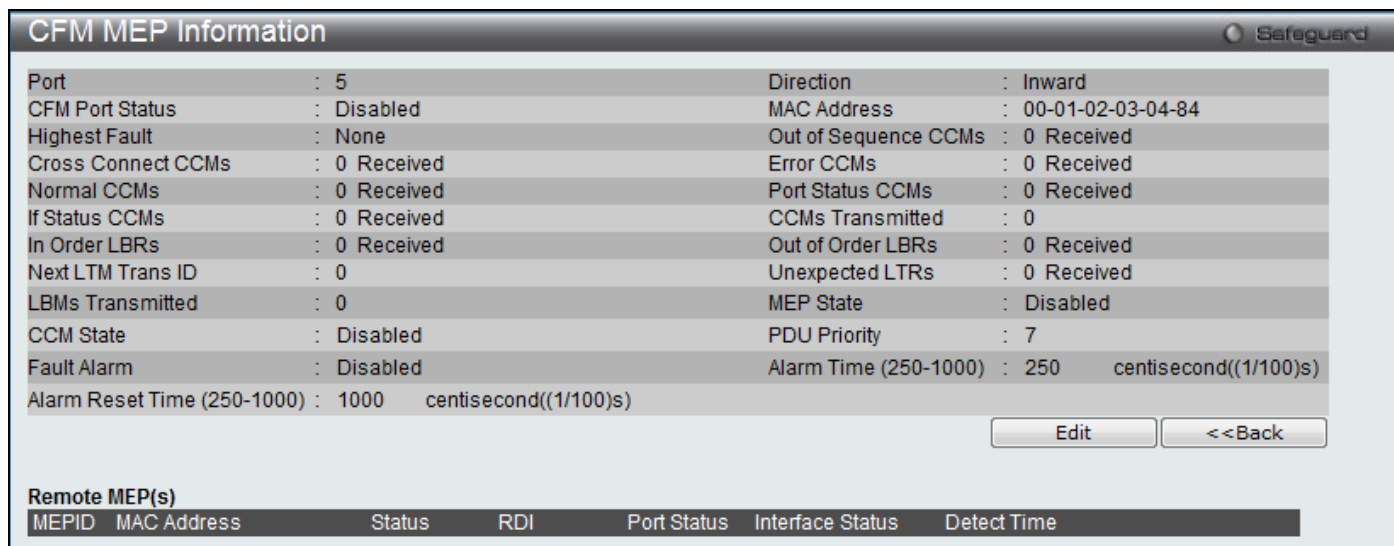


Figure 3 - 64. CFM MEP Information window

To re-configure the MEP entry, click on the **Edit** button.

Parameter	Description
MEP State	This is the MEP administrative state. <i>Enable</i> - MEP is enabled. <i>Disable</i> - MEP is disabled. This is the default value.
CCM State	This is the CCM transmission state. <i>Enable</i> - CCM transmission enabled. <i>Disable</i> - CCM transmission disabled. This is the default value.
PDU Priority	The 802.1p priority is set in the CCMs and the LTM's messages transmitted by the MEP. The default value is 7.
Fault Alarm	This is the control types of the fault alarms sent by the MEP. <i>All</i> - All types of fault alarms will be sent. <i>Mac Status</i> - Only the fault alarms whose priority is equal to or higher than "Some Remote MEP MAC Status Error" are sent. <i>Remote CCM</i> - Only the fault alarms whose priority is equal to or higher than "Some Remote MEP Down" are sent. <i>Errors CCM</i> - Only the fault alarms whose priority is equal to or higher than "Error CCM Received" are sent. <i>Xcon CCM</i> - Only the fault alarms whose priority is equal to or higher than "Cross-connect CCM Received" are sent. <i>None</i> - No fault alarm is sent. This is the default value.
Alarm Time	This is the time that a defect must exceed before the fault alarm can be sent. The unit is in centiseconds, the range is 250-1000. The default value is 250.
Alarm Reset Time	This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is in centiseconds, the range is 250-1000. The default value is 1000.
Remote MEP Table	Read-only information for remote MEPs is listed here. Information includes, Remote MEPID, MAC Address, Status, RDI, Port Status, Interface Status, Last CCM Serial Number, Sender Chassis ID, Sender Management Address, and Detect Time.

CFM Port Settings

To view this window, click **L2 Features > CFM > CFM Port Settings**:

From Port	To Port	State	Apply
01	01	Disabled	Apply

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
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
27	Disabled
28	Disabled

Figure 3 - 65. CFM Port Settings window

The fields that can be configured are described below:

Parameter	Description
From Port/To Port	To select the port range used for this configuration.
State	To enable or disable the state of specific port regarding the CFM configuration. The default State is <i>Disabled</i> .

Click **Apply** to implement changes made.

CFM Loopback Settings

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

Figure 3 - 66. CFM Loopback Settings window

The fields that can be configured are described below:

Parameter	Description
MEP Name:	To enter the MEP name.
MEP ID	To enter the MEP ID.
MD	To enter the maintenance domain name.
MA	To enter the maintenance association name.
MAC Address	To enter the destination MAC address.
LBMs Number	Number of LBMs to be sent. The default value is 4. The range is 1-65535.
LBM Payload Length	The payload length of LBM to be sent. The default is 0.
LBM Payload Pattern	An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.
LBMs Priority	The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.

Click **Apply** to implement changes made.

CFM Linktrace Settings

On this page the user can configure the CFM link track message.

To view this window, click **L2 Features > CFM > CFM Linktrace Settings:**

Figure 3 - 67. CFM Linktrace Settings window

The fields that can be configured are described below:

Parameter	Description
MEP Name	To enter the MEP name.
MEP ID	To enter the MEP ID.
MD Name	To enter the maintenance domain name.
MA Name	To enter the maintenance association name.
MAC Address	To enter the destination MAC address.
TTL	Link-trace message TTL value. The default value is 64. The range is 2-255.
PDU Priority	The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MEP.

Click **Apply** to implement changes made. Type the MEP Name or MA Name and MEP ID in the spaces provided and click on **Find** to view details for the linktrace in the table below.

Click on the **View Detail** link to display the details of any listed CFM Linktrace set.

ERPS Settings

This page is used to enable the Ethernet Ring Protection Switching (ERPS) function on the Switch. STP and LBD should be disabled on the ring ports before enabling ERPS.

The ERPS cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when ERPS is enabled.

To view this window, click **L2 Features > ERPS Settings**:

Figure 3 - 68. ERPS Settings window

The fields that can be configured are described below:

Parameter	Description
ERPS State	To enable or disable the ERPS State.
ERPS Log	To enable or disable the ERPS Log.
ERPS Trap	To enable or disable the ERPS Trap.
R-APS VLAN	Specify the VLAN which will be the R-APS VLAN. Enter the R-APS VLAN ID, West Port, East port, RPL Owner status, Ring MEL*, Protected VLAN, Hold Off Timer, Guard Time, and WTR Time.
West Port	Specifies the port as the west ring port. ERPS uses cardinal direction terms “East” and “West” to designate how the ports on nodes in the ring are oriented to the ring itself. Each node on the ring has an East port and West port. The West port of one node is linked to the East port of the adjacent node in the ring.
East Port	Specifies the port as the east ring port. ERPS uses cardinal direction terms “East” and “West” to designate how the ports on nodes in the ring are oriented to the ring itself. Each node on the ring has an East port and West port. The East port of one node is linked to the West port of the adjacent node in the ring.

* If CFM (Connectivity Fault Management) and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU. The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP (maintenance entity group end point) with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.

Click **Apply** to implement changes apply the enable or disable state for ERPS, ERPS log and ERPS trap settings.

To create a new R-APS VLAN, enter the required settings in the window and click on the **Create** button.

(ERPS Settings continued)

Parameter	Description
RPL Port	Specifies the ring port as the Ring Protection Link (RPL) port. The RPL remains idle and blocks traffic when all links on the ring are functioning. If there is a link failure on the ring however, the RPL port is unblocked by the RPL Owner node in order to allow an alternate path around the ring.
RPL Owner	Enable/Disable the device as an RPL owner node. This node blocks or unblocks the RPL as required by network conditions. An Ethernet Ring Automatic Protection Switching (R-APS) message protocol coordinates protection activities for all nodes on the ring. In the event of a link failure, the RPL Owner uses these messages to block a failed link and unblock the RPL. There can be only one RPL Owner on a ring.
Ring MEL	Specifies the ring Maintenance Entity Group (MEG) level (MEL) of the R-APS function.
Protected VLANs	This command is used to configure the VLANs that are protected by the ERPS function.
Hold Off Time	Specifies the hold off time of the R-APS function. A hold off timer is used in order to coordinate timing of ERPS at multiple levels. The purpose is to allow, for example, a server layer switch to be able to fix the problem before switching at a client layer. When a new defect or more severe defect is detected, the event will not be reported immediately, instead, after the hold off timer expires, the trail that started the timer will be checked to see if the defect still exists. If it exists, the defect is reported and the ERPS goes into effect.
Guard Time	Specifies the guard time of the R-APS function. While the Guard timer is running, received R-APS messages are NOT forwarded to the RPL Owner. The purpose of this is to prevent the possibility a loop forming in the event that two or more R-APS signal fail messages are sent simultaneously from different ends of the ring.
WTR Time	Specifies the wait-to-restore (WTR) time of the R-APS function. The WTR time defines the amount of time mandated to pass after conditions clear. After the WTR time expires, the RPL returns to idle state (blocking). This is used to prevent too frequent operation of ERPS due to an intermittent signal failure defect.

Click **Apply** to implement changes apply the enable or disable state for ERPS, ERPS log and ERPS trap settings.

To create a new R-APS VLAN, enter the required settings in the menu and click on the **Create** button.

Section 4

QoS

Bandwidth Control

Traffic Control

Queue Bandwidth Control Settings

802.1p Default Priority

802.1p User Priority

QoS Scheduling Settings

Priority Mapping

TOS Mapping

DSCP Map Settings

The Switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

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 amount of 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 larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements 802.1P priority queuing.

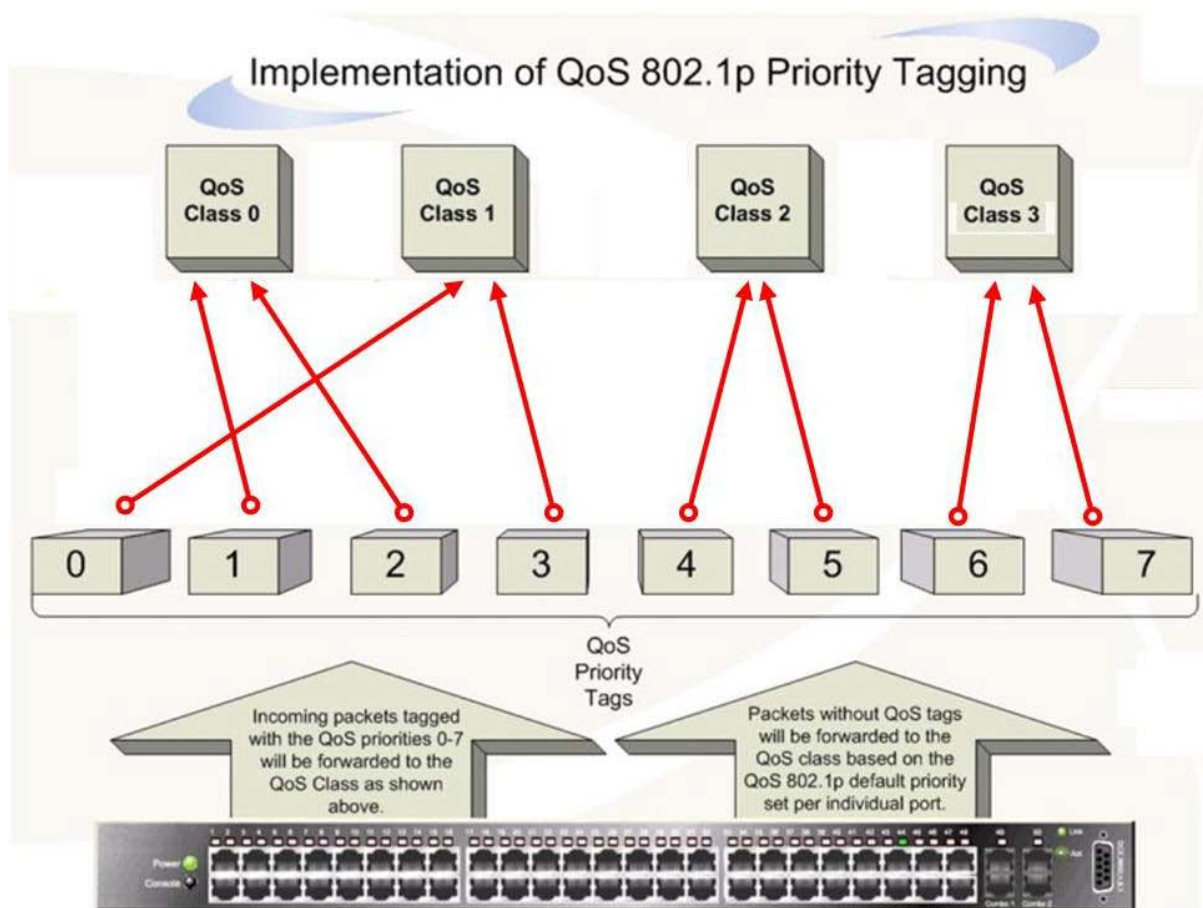


Figure 4 - 1. Mapping QoS on the Switch

The previous picture shows the default priority setting for the Switch. Class 3 has the highest priority of the four priority queues on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag tagged. Then the user may forward these tagged packets to designated queues on the Switch where they will be emptied, based on priority.

For example, if a user wishes to have a videoconference between two remotely set computers, the administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result for the end user is receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has four priority queues. These priority queues are labeled from 0 to 3, with 3 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 Q1 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q0 queue.
- Priority 3 is assigned to the Switch's Q1 queue.
- Priority 4 is assigned to the Switch's Q2 queue.
- Priority 5 is assigned to the Switch's Q2 queue.
- Priority 6 is assigned to the Switch's Q3 queue.
- Priority 7 is assigned to the Switch's Q3 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 four QoS queues, A~D with their respective weight value: 4~1, the packets are sent in the following sequence: A1, B1, C1, D1, A2, B2, C2, A3, B3, A4.

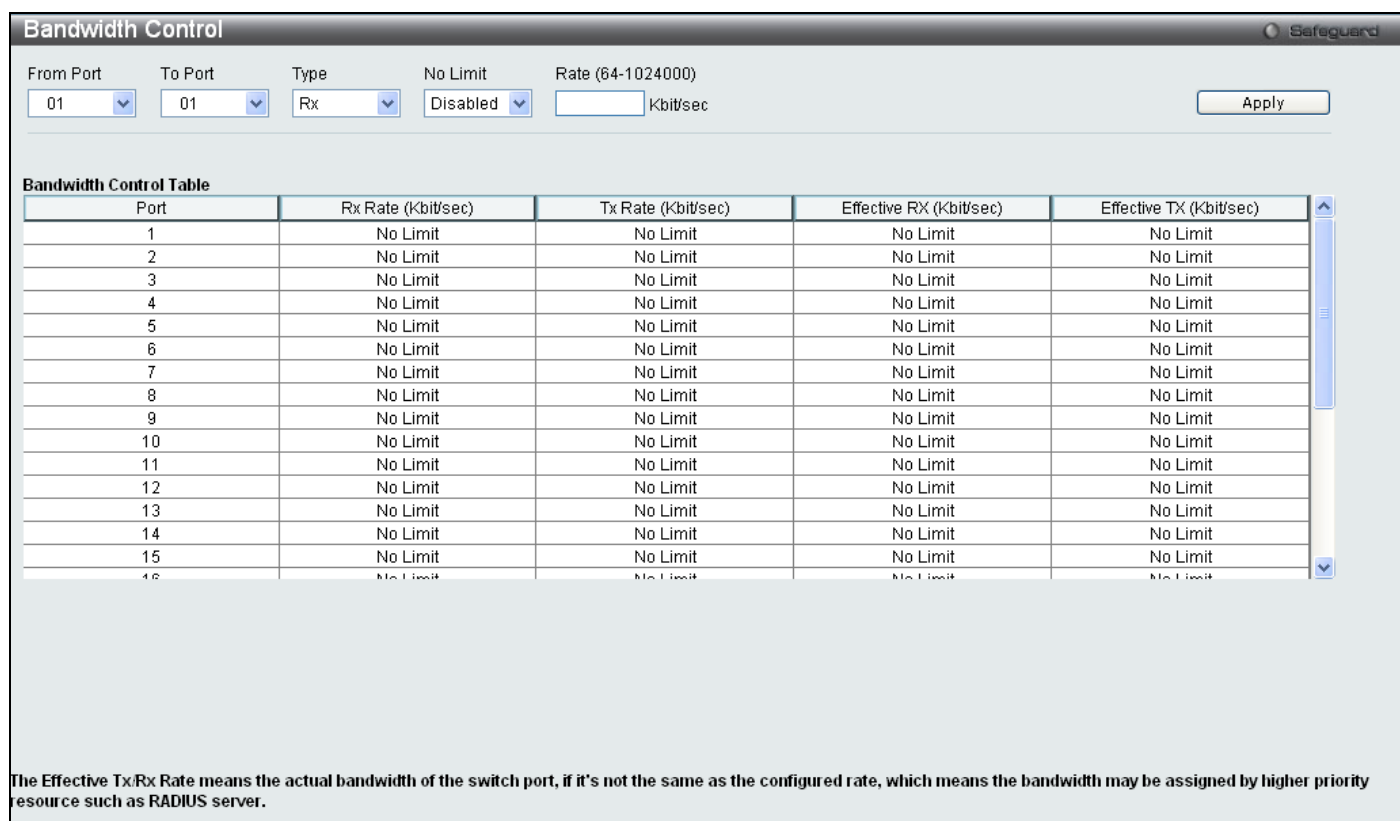
For weighted round robin queuing, if each QoS queue has the same weight value, then each QoS queue has an equal opportunity to send packets just like round robin queuing.

The Switch has four priority queues (and eight Classes of Service) for each port.

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**:



Bandwidth Control

From Port: 01 To Port: 01 Type: Rx No Limit: Disabled Rate (64-1024000): Kbit/sec Apply

Port	Rx Rate (Kbit/sec)	Tx Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
7	No Limit	No Limit	No Limit	No Limit
8	No Limit	No Limit	No Limit	No Limit
9	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit
11	No Limit	No Limit	No Limit	No Limit
12	No Limit	No Limit	No Limit	No Limit
13	No Limit	No Limit	No Limit	No Limit
14	No Limit	No Limit	No Limit	No Limit
15	No Limit	No Limit	No Limit	No Limit
16	No Limit	No Limit	No Limit	No Limit

The Effective Tx/Rx Rate means the actual bandwidth of the switch port, if it's not the same as the configured rate, which means the bandwidth may be assigned by higher priority resource such as RADIUS server.

Figure 4 - 2. Bandwidth Control window

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 <i>Rx</i> (receive), <i>Tx</i> (transmit), and <i>Both</i> . This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	Use the drop-down menu to specify the selected port has limited or 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 62.5 up to 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.

Traffic 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.

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 Rest mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Rest mode, the port will be recovered after 5 minutes, or the user manually resets the port 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 **QoS > Traffic Control**:

The screenshot shows the 'Traffic Control' window with the following settings:

- Traffic Control Settings:**
 - From Port: 01
 - To Port: 01
 - Action: Drop
 - Count Down (0 or 5-30): 0 min
 - Time Interval (5-30): 5 sec
 - Threshold (64-1000000): 64 kbit/s
 - Storm Control Type: None
- Traffic Trap Settings:** None

Below the settings is a table with the following columns: Port, Storm Control Type, Action, Threshold, Count Down, Interval, and Shutdown Forever. The table lists configurations for ports 1 through 23.

Port	Storm Control Type	Action	Threshold	Count Down	Interval	Shutdown Forever
1	None	Drop	64	0	5	
2	None	Drop	64	0	5	
3	None	Drop	64	0	5	
4	None	Drop	64	0	5	
5	None	Drop	64	0	5	
6	None	Drop	64	0	5	
7	None	Drop	64	0	5	
8	None	Drop	64	0	5	
9	None	Drop	64	0	5	
10	None	Drop	64	0	5	
11	None	Drop	64	0	5	
12	None	Drop	64	0	5	
13	None	Drop	64	0	5	
14	None	Drop	64	0	5	
15	None	Drop	64	0	5	
16	None	Drop	64	0	5	
17	None	Drop	64	0	5	
18	None	Drop	64	0	5	
19	None	Drop	64	0	5	
20	None	Drop	64	0	5	
21	None	Drop	64	0	5	
22	None	Drop	64	0	5	
23	None	Drop	64	0	5	

Figure 4 - 3. Traffic Control window

The following parameters can be set or are displayed:

Parameter	Description
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: <i>Drop</i> – 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. <i>Shutdown</i> – 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 Rest mode. The port will be recovered after 5 minutes, or the user manually resets the port using the Port Configuration window in the Configuration 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.
Count Down (0 or 5-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. Only the switch continues to experience a traffic storm during this countdown period and the switch will shutdown the port. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are 0, 5 to 30 minutes. Zero means that the port will not enter shutdown rest mode.
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 (64- 1000000)	This value represents the upper threshold at which the specified traffic control is switched on. The threshold value is measured in Kbit/sec when the action is set to drop mode; it is measured in pps(packets/sec) when the action is set to shutdown mode. That is, the number of broadcast/multicast/Unknown unicast packets, received by the Switch that will trigger the storm traffic control measures. The configurable threshold range is from 64 to 1000000 with a default setting of 64. Actual rate = rate entered/ minimum granularity * minimal granularity, for example: 62.5= 100/62.5 *62.5” number implies the closest smaller integer.
Storm Control Type	Select the type of Storm Type to detect: <i>Broadcast, Multicast, Unknown Unicast, Broadcast + Multicast, Broadcast + Unknown Unicast, Multicast + Unknown Unicast, Broadcast + Multicast + Unknown Unicast</i> , or <i>None</i> . Once selected, use the pull-down menu to enable or disable this storm detection.
Traffic Trap Setting	
Storm Trap	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: <i>None</i> – Will not send any Storm trap warning messages regardless of action taken by the Traffic Control mechanism. <i>Storm Occurred</i> – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. <i>Storm Cleared</i> – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. <i>Both</i> – 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 <i>Drop</i> 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 rest 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 rest mode will be seen as link down in all windows and screens until the user recovers these ports.

Queue Bandwidth Control Settings

The queue bandwidth control settings are used to place a ceiling on the transmitting data rates for the priority queue of the port.

To view this window, click **QoS > Queue Bandwidth Control Settings:**

Queue Bandwidth Control Settings

From Port: 01 To Port: 01 From CoS: 0 To CoS: 0 Max Rate (64-1024000): No Limit Apply

Queue Bandwidth Control Table On Port 1

Queue	Max Rate(Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit

Queue Bandwidth Control Table On Port 2

Queue	Max Rate(Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit

Queue Bandwidth Control Table On Port 3

Queue	Max Rate(Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit

Queue Bandwidth Control Table On Port 4

Queue	Max Rate(Kbit/sec)
0	No Limit
1	No Limit
2	No Limit
3	No Limit

Queue Bandwidth Control Table On Port 5

Figure 4 - 4. Queue Bandwidth Control Settings window

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.
From Cos/To CoS	Use to define the range of CoS value configured for the selected ports.
No Limit	Use the No Limit check box to specify the selected port has limited or unlimited bandwidth.
Max Rate (64–1024000)	Max rate is a limitation. When it is specified, packet transmitted from the queue will not exceed the specified limitation even though the bandwidth is available. The value must be between 64 and 1024000. Actual rate = rate entered/ minimum granularity * minimal granularity, for example: 62.5= 100/62.5 *62.5 number implies the closest smaller integer.

Click **Apply** to set the changes.

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**:

Port	Priority	Effective Priority
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0

Figure 4 - 5. 802.1p Default Priority window

This window allows assignment of a default 802.1p priority to any given port on the Switch. The priority values are numbered from 0, the lowest priority, to 7, the highest priority. Click **Apply** to implement the 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**:

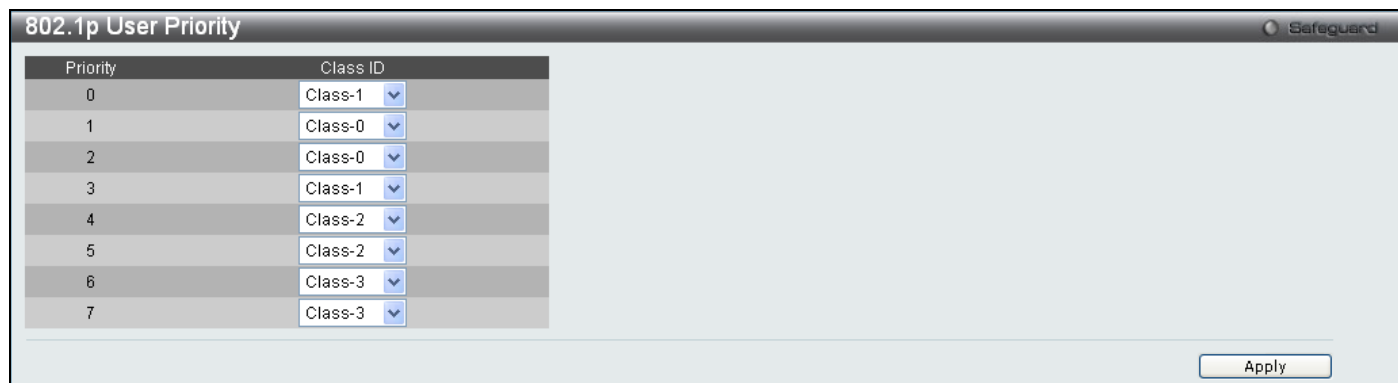


Figure 4 - 6. 802.1p User Priority window

Once a priority has been assigned to the port groups on the Switch, assign this Class to each of the eight levels of 802.1p priorities.

The following parameter may be set:

Parameter	Description
Class ID	This field is used to enter a Class ID between <i>Class-0</i> and <i>Class-3</i> .

Click **Apply** to set the changes.

QoS Scheduling Settings

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 Settings**:

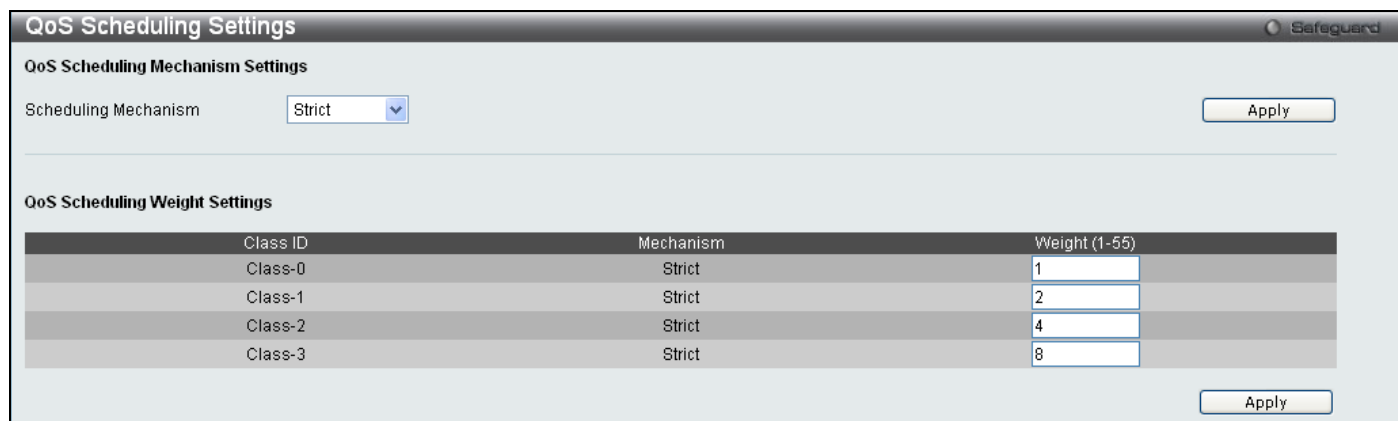


Figure 4 - 7. QoS Scheduling Settings window

The Scheduling Mechanism has the following parameters.

Parameter	Description
Scheduling Mechanism	Toggle between <i>Strict</i> and <i>Weight Fair</i> . <i>Strict</i> is the highest class of service and the first to process traffic. That is, the highest class of service will finish before other queues empty. <i>Weight Fair</i> uses the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service.
Weight (1-55)	Enter a Weight value between 1 and 55.

Click **Apply** to set the changes.

Priority Mapping

This window is used to set up Priority Mapping.

To view this window, click **QoS > Priority Mapping**:

Port	Ethernet Priority	IP Priority
1	802.1p	Off
2	802.1p	Off
3	802.1p	Off
4	802.1p	Off
5	802.1p	Off
6	802.1p	Off
7	802.1p	Off
8	802.1p	Off
9	802.1p	Off
10	802.1p	Off
11	802.1p	Off
12	802.1p	Off
13	802.1p	Off
14	802.1p	Off
15	802.1p	Off
16	802.1p	Off
17	802.1p	Off
18	802.1p	Off
19	802.1p	Off
20	802.1p	Off
21	802.1p	Off
22	802.1p	Off
23	802.1p	Off
24	802.1p	Off
25	802.1p	Off
26	802.1p	Off
27	802.1p	Off
28	802.1p	Off

Figure 4 - 8. Priority Mapping window

The following parameter may be set:

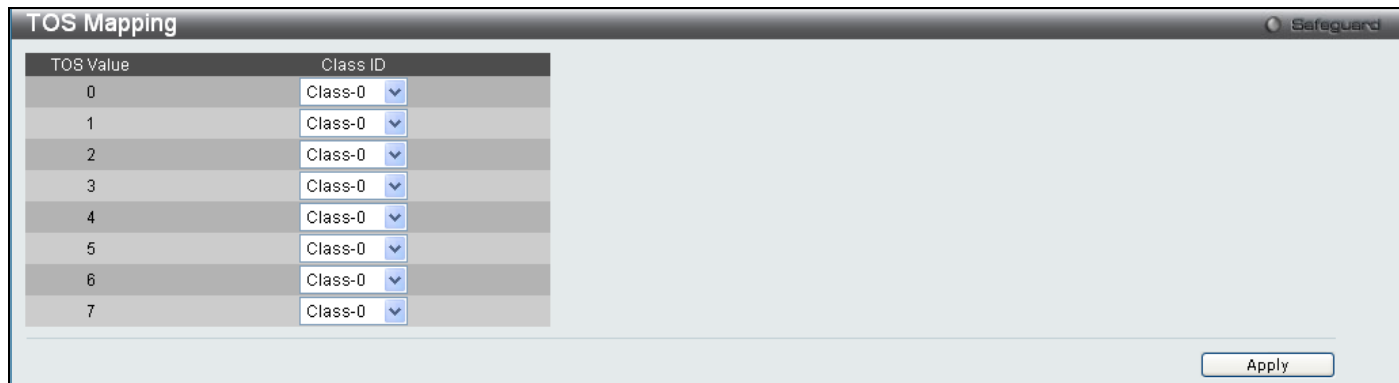
Parameter	Description
From Port/To Port	Select a range of ports to configure.
Priority	Tick the None check box neither Ethernet nor IP Priority mapping is desired.
Ethernet Priority	Tick the Ethernet Priority check box to set up 802.1p mapping.
IP Priority	Tick the IP Priority check box and then use the drop-down menu to select either <i>TOS</i> or <i>DSCP</i> mapping.

Click **Apply** to set the changes.

TOS Mapping

This window is used to set up Type of Service (TOS) Mapping.

To view this window, click **QoS > ToS Mapping**:



TOS Value	Class ID
0	Class-0
1	Class-0
2	Class-0
3	Class-0
4	Class-0
5	Class-0
6	Class-0
7	Class-0

Figure 4 - 9. TOS Mapping window

The following parameter may be set:

Parameter	Description
Class ID	This field is used to enter a Class ID between <i>Class-0</i> and <i>Class-3</i> .

Click **Apply** to set the changes.

DSCP Mapping

This window is used to set up DSCP Mapping.

To view this window, click **QoS > DSCP Mapping**:

DSCP	Class ID
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
29	0

Figure 4 - 10. DSCP Mapping window

The following parameters may be set:

Parameter	Description
DSCP Value	This field is used 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 main, or part of, the criterion for forwarding. The user may choose a value between 0 and 63.
Class ID	This field is used to enter a Class ID between <i>Class-0</i> and <i>Class-3</i> .

Section 5

Security

Safeguard Engine

Trusted Host

IP-MAC-Port Binding

Port Security

802.1X

RADIUS Attributes Assignment

SSL Settings

SSH

Access Authentication Control

MAC-based Access Control

DoS Prevention Settings

DHCP Server Screening Settings

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP storm) or other methods. These attacks may affect normal traffic flow. 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 during an attack, therefore making it capable of forwarding essential packets over the network with limited bandwidth. To achieve this, the Safeguard Engine uses threshold values to place the Switch in Exhausted or Normal mode.

The Switch will be placed in Exhausted mode when the CPU utilization exceeds the Rising Threshold. In Exhausted mode, the Switch will limit the bandwidth for ARP packets, therefore allowing more bandwidth for essential packets.

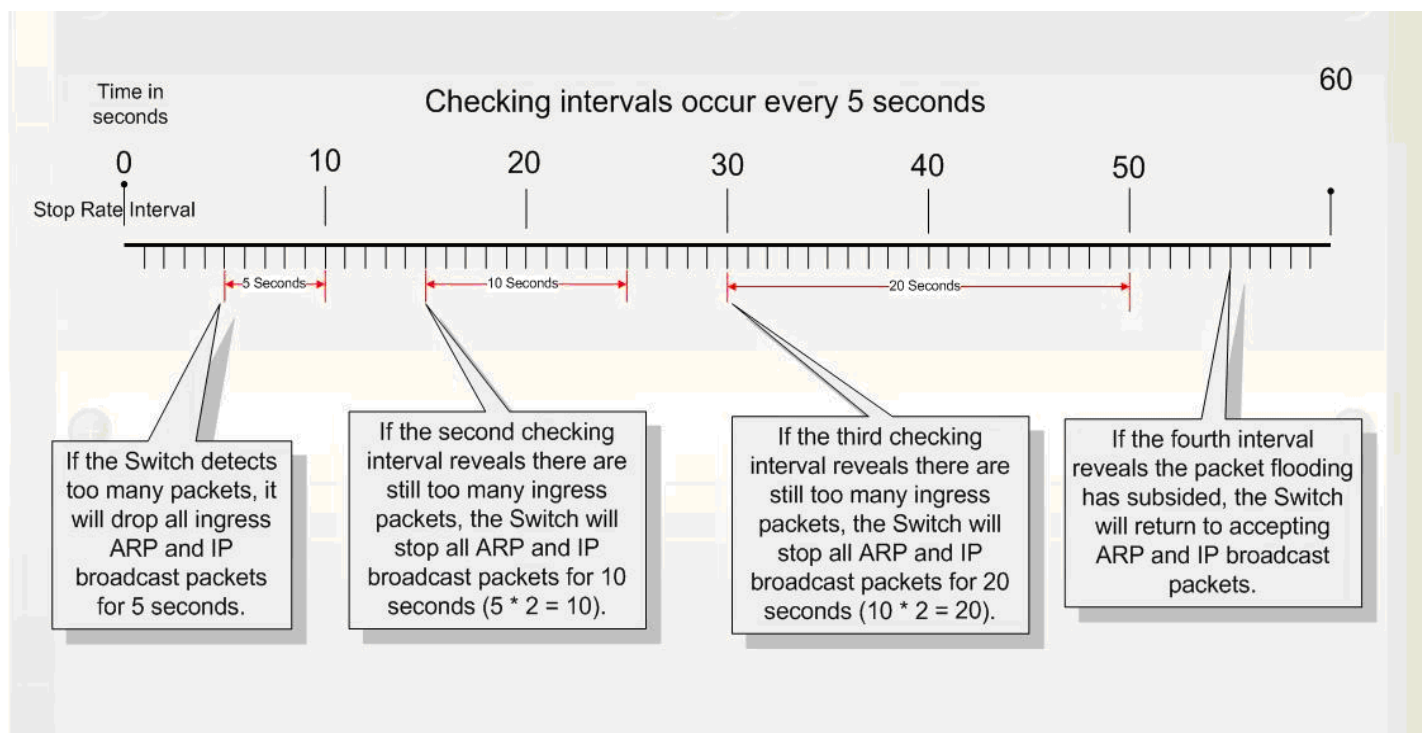


Figure 5 - 1. Safeguard Engine Checking Interval Example on the Switch

In Exhausted mode, two modes can be implemented to limit the bandwidth assigned to ARP packets, “Strict” and “Fuzzy”.

In Strict mode, the Switch will drop all ARP packets. The Switch will reluctantly process any packets not destined for the Switch and broadcast packets, no matter what is causing the high utilization rate on the CPU, which may not be an ARP storm.

In Fuzzy mode, the Switch uses an algorithm to assign different bandwidth levels for ARP packets. In Fuzzy mode, the Switch will analyze the rate of received ARP traffic to adjust the bandwidth dynamically. 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 a small amount of processed packets and then return to a normal packet flow

In both Strict mode and Fuzzy mode the Safeguard Engine will check for packet flooding issues at regular intervals. For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will accept a few ingress ARP packets. In the example above, the Switch doubled the time for dropping ARP 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 packets will return to 5 seconds and the process will resume.

To configure the Safeguard Engine for the Switch, click **Security > Safeguard Engine**, which will open the following window:

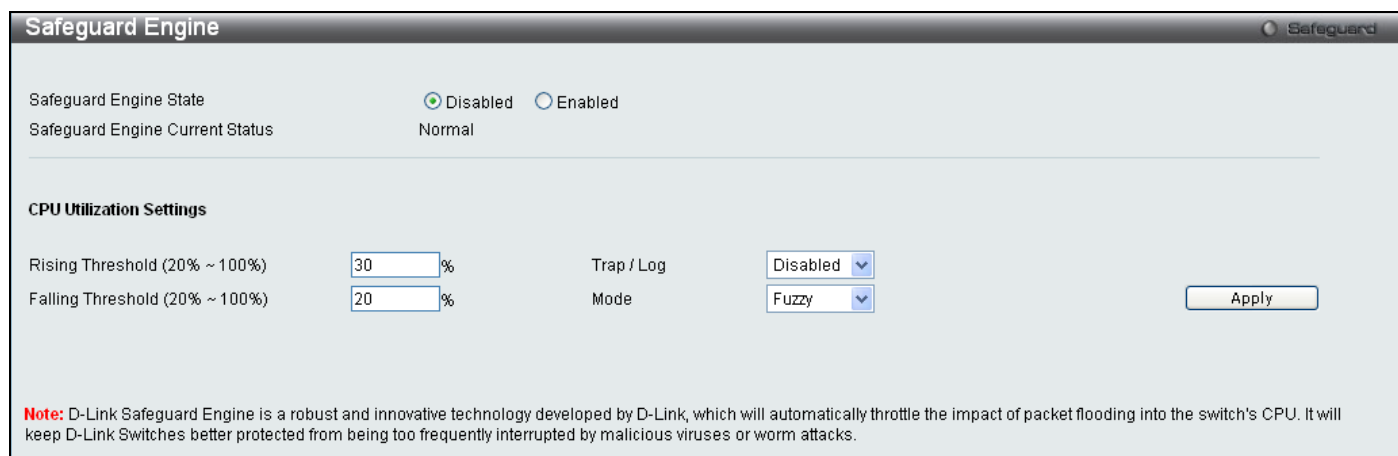


Figure 5 - 2. Safeguard Engine window

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 <i>Strict</i> or <i>Fuzzy</i> 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 one or more designated management stations are defined by the user, only the chosen stations, as defined by IP address, will be allowed management privilege through the Web manager, Telnet session, or SNMP manager. 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**:

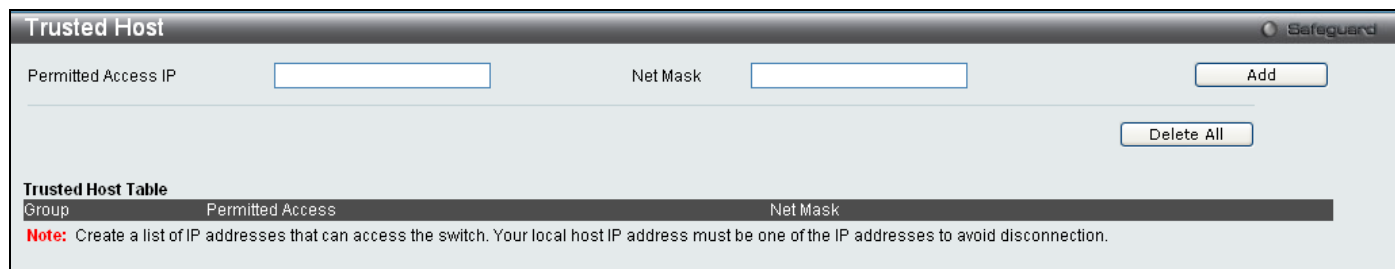


Figure 5 - 3. Trusted Host window

To delete an entry, click the corresponding **Delete** button. To delete all the entries on the Trusted Host Table, click the **Delete All** button.

IP-MAC-Port Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict access to the Switch to a number of authorized users. Only authorized clients can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC-port binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-port binding entries is dependent on chip capability (e.g. the ARP table size) and storage size of the device. Active and inactive entries use the same database. The maximum entry number is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

IMP Binding Global Settings

This window is used to enable or disable the Trap Log State and DHCP Snoop state on the Switch. The Trap/Log field will enable and disable the sending of trap log messages for IP-MAC-port binding. When enabled, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.

To view this window click, **Security > IP-MAC-Port Binding > IMP Binding Global Settings**:

Figure 5 - 4. IMP Binding Global Settings window

The following parameters can be set:

Parameter	Description
Trap / Log	This field will enable and disable the sending of trap log messages for IP-MAC-port binding. When <i>Enabled</i> , the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.
DHCP Snoop State	Use the pull-down menu to enable or disable the DHCP Snooping State for IP-MAC-port binding.
ARP Inspection	When this is <i>Enabled</i> , the Switch will filter ARP packets which have unauthorized sender MACs, IP addresses, and ingress ports. ARP inspection is only active on IP-MAC-port binding-enabled ports.
Recover Learning Ports (e.g.: 1, 7-12)	Enter the ports for which the ARP check function has stopped. This will allow recovery, or an unfreezing, of the ARP check on the ports listed in this field. Alternatively, tick All to force the recovery of all learning ports.

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

IMP Binding Port Settings

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with the State, Allow Zero IP, Forward DHCP Packet, Mode, and SLT fields, and configure the port's Max Entry value.

To view this window click, **Security > IP-MAC-Port Binding > IMP Binding Port Settings**:

Port	State	Allow Zero IP	Forward DHCP Packet	Mode	SLT/Mode	Max Entry
1	Disabled	Not Allow	Forward	ARP	500/Normal	5
2	Disabled	Not Allow	Forward	ARP	500/Normal	5
3	Disabled	Not Allow	Forward	ARP	500/Normal	5
4	Disabled	Not Allow	Forward	ARP	500/Normal	5
5	Disabled	Not Allow	Forward	ARP	500/Normal	5
6	Disabled	Not Allow	Forward	ARP	500/Normal	5
7	Disabled	Not Allow	Forward	ARP	500/Normal	5
8	Disabled	Not Allow	Forward	ARP	500/Normal	5
9	Disabled	Not Allow	Forward	ARP	500/Normal	5
10	Disabled	Not Allow	Forward	ARP	500/Normal	5
11	Disabled	Not Allow	Forward	ARP	500/Normal	5
12	Disabled	Not Allow	Forward	ARP	500/Normal	5
13	Disabled	Not Allow	Forward	ARP	500/Normal	5
14	Disabled	Not Allow	Forward	ARP	500/Normal	5
15	Disabled	Not Allow	Forward	ARP	500/Normal	5
16	Disabled	Not Allow	Forward	ARP	500/Normal	5
17	Disabled	Not Allow	Forward	ARP	500/Normal	5
18	Disabled	Not Allow	Forward	ARP	500/Normal	5
19	Disabled	Not Allow	Forward	ARP	500/Normal	5
20	Disabled	Not Allow	Forward	ARP	500/Normal	5
21	Disabled	Not Allow	Forward	ARP	500/Normal	5
22	Disabled	Not Allow	Forward	ARP	500/Normal	5
23	Disabled	Not Allow	Forward	ARP	500/Normal	5
24	Disabled	Not Allow	Forward	ARP	500/Normal	5
25	Disabled	Not Allow	Forward	ARP	500/Normal	5

Note:FDP:Forward DHCP Packet, SLT:Stop Learning Threshold

Figure 5 - 5. IMP Binding Port Settings window

The following fields can be set or modified:

Parameter	Description
From Port/To Port	Select a port or range of ports to set for IP-MAC Binding.
State	Use the pull-down menu to Enable or Disable these ports for IP-MAC Binding. <i>Enabled (Strict)</i> – This mode provides a stricter method of control. If the user selects this mode, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the S/W learns the entries for the ports. The port will check ARP packets and IP packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is <i>Enabled (Strict)</i> if not specified. <i>Enabled (Loose)</i> – This mode provides a looser way of control. If the user selects loose mode, ARP packets and IP Broadcast packets will be sent to the CPU. The packets will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.

Allow Zero IP	Use the drop-down menu to enable or disable this feature. Zero IP configures the state which allows ARP packets with 0.0.0.0 source IP to bypass.
FDP	By default, the DHCP packet with broadcast DA will be flooded. When set to <i>Disabled</i> , the broadcast DHCP packet received by the specified port will not be forwarded.
Mode	The user may set the mode for this IP-MAC-port binding settings by choosing <i>ARP</i> or <i>ACL</i> . When configuring the mode of the port to <i>ACL</i> , the Switch will create an ACL access entry corresponding to the entries of this port. If the port changes to <i>ARP</i> , all the ACL entries will be deleted automatically. The default mode is <i>ARP</i> .
SLT (0-500)	Enter a Stop-learning Threshold value between 0 and 500. The default SLT for each port is 500.
Max Entry (1-50)	Specifies the maximum number of IP-MAC-port binding entries between 1 and 50. The default is 5. Alternatively, tick the No Limit check box.

IMP Binding Entry Settings

This window is used to create static IP- MAC-port binding entries on the Switch.

To view this window click, **Security > IP-MAC-Port Binding > IMP Binding Entry Settings**:

Figure 5 - 6. IMP Binding Entry Settings window

The following fields can be set or modified:

Parameter	Description
IP Address	Enter the IP address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Ports	Specify the Switch ports for which to configure this IP-MAC-port binding entry (IP Address + MAC Address). Tick the All Ports check box to configure this entry for all ports on the Switch.

Click **Apply** for implement changes, click **Find** to search for an entry, click **Show All** for the table to display all entries and click **Delete** to remove an entry.

DHCP Snooping Entries

This window is used to view dynamic entries on specific ports. To view particular port settings, enter the port number and click **Find**. To view all entries click **View All**, and to delete an entry, click **Clear**.

To view this window click, **Security > IP-MAC-Port Binding > DHCP Snooping Entries**:

Figure 5 - 7. DHCP Snooping Entries window

MAC Block List

This window is used to view unauthorized devices that have been blocked by IP-MAC binding restrictions. To find an unauthorized device that has been blocked by the IP-MAC binding restrictions, enter the VID and MAC Address in the appropriate fields and click **Find**. To delete an entry, click the delete button next to the entry's port. To display all the MAC blocked entries, click **View All**. To delete all the entries in the window, click **Delete All**.

To view this window click, **Security > IP-MAC-Port Binding > MAC Block List**:

Figure 5 - 8. MAC Block List window

Port Security

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.

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.

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

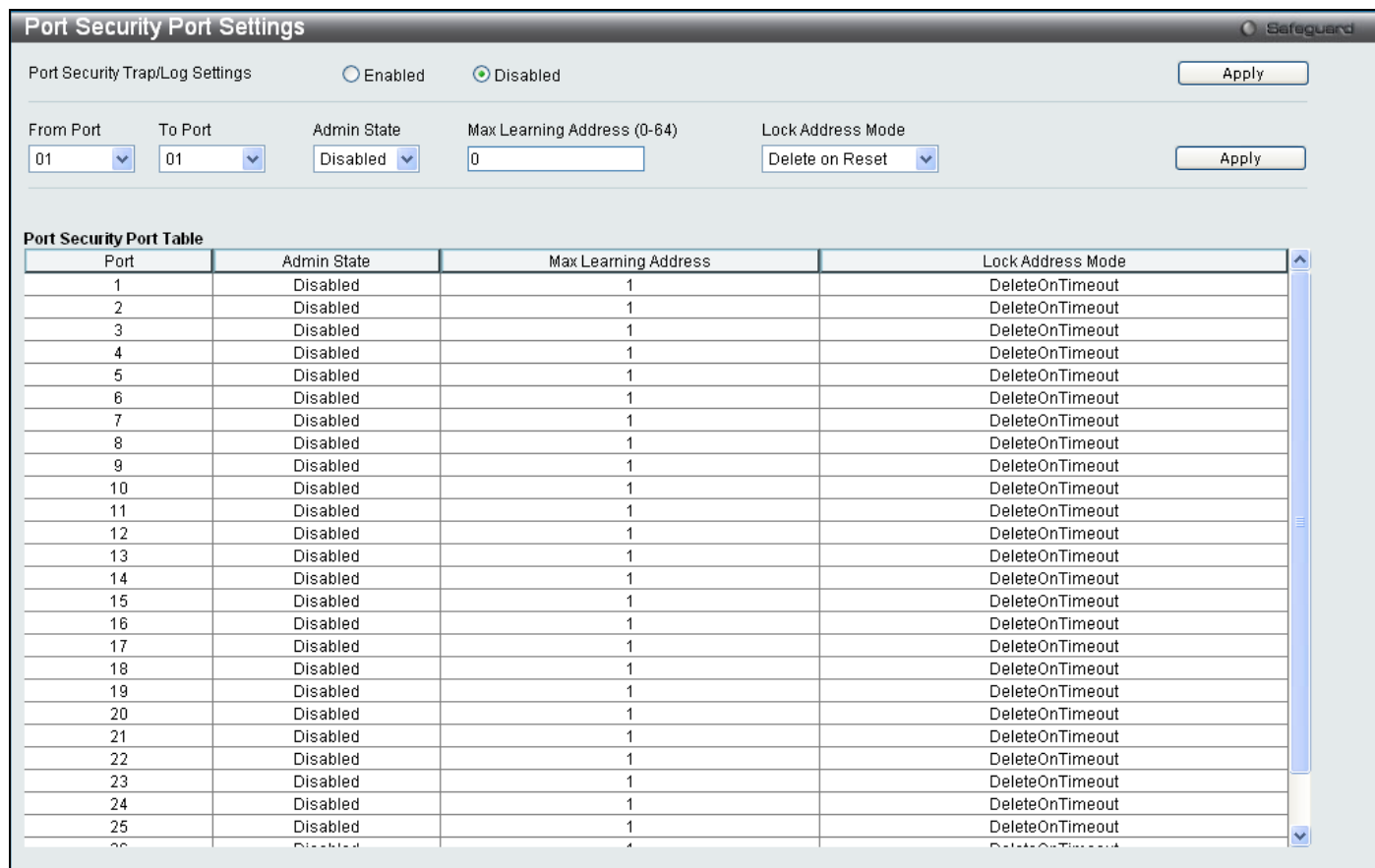


Figure 5 - 9. Port Security Port Settings window

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).
Max. Learning Address (0-64)	The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of 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: <ul style="list-style-type: none"> ▪ <i>Permanent</i> – The locked addresses will not age out after the aging timer expires. ▪ <i>Delete on Timeout</i> – The locked addresses will age out after the aging timer expires. ▪ <i>Delete on Reset</i> – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

Port Security FDB Entries

This window is used to clear the Port Lock Entries by individual ports. To clear entries enter the range of ports and click **Clear**.

To view the following window click, **Security > Port Security > Port Security FDB Entries**:

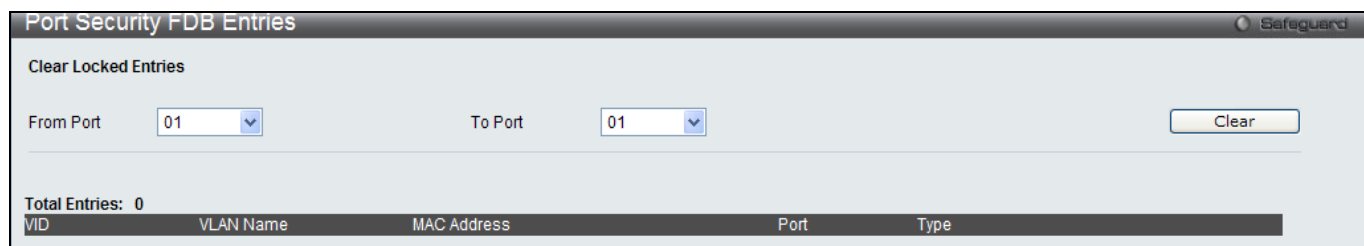


Figure 5 - 10. Port Security FDB Entries window

802.1X

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

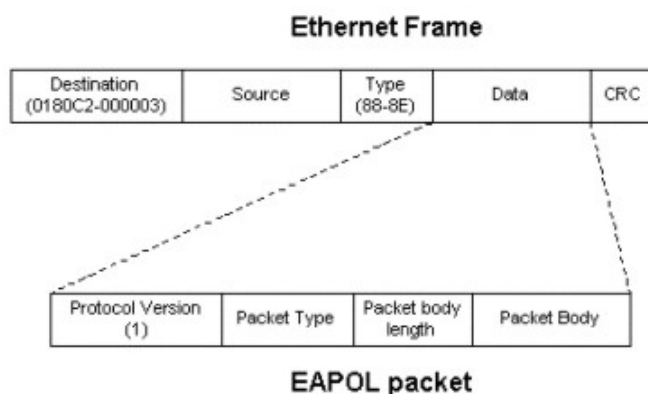


Figure 5 - 11. The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method holds three roles, each of which are vital to creating and maintaining a stable and working Access Control security method.

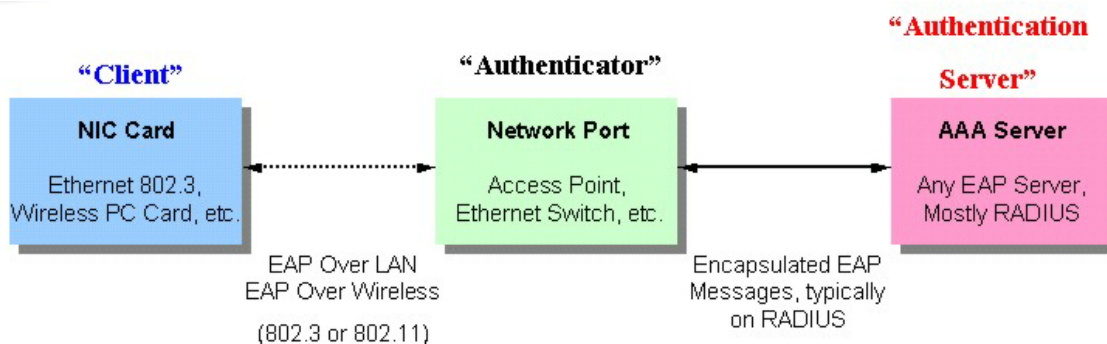


Figure 5 - 12. The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

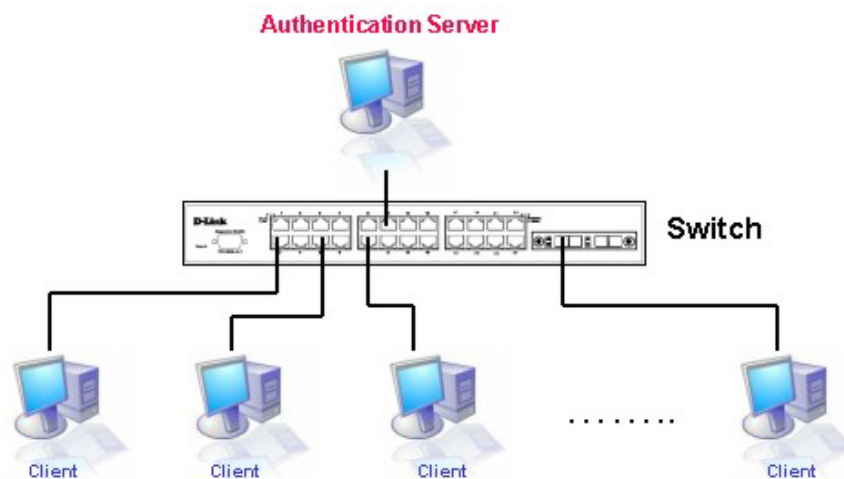


Figure 5 - 13. The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X state must be *Enabled*. (**Security / 802.1X / 802.1X Settings**)
2. The 802.1X settings must be implemented by port (**Security / 802.1X / 802.1X Settings**)
3. A RADIUS server must be configured on the Switch. (**Security / 802.1X / Authentic RADIUS Server**)

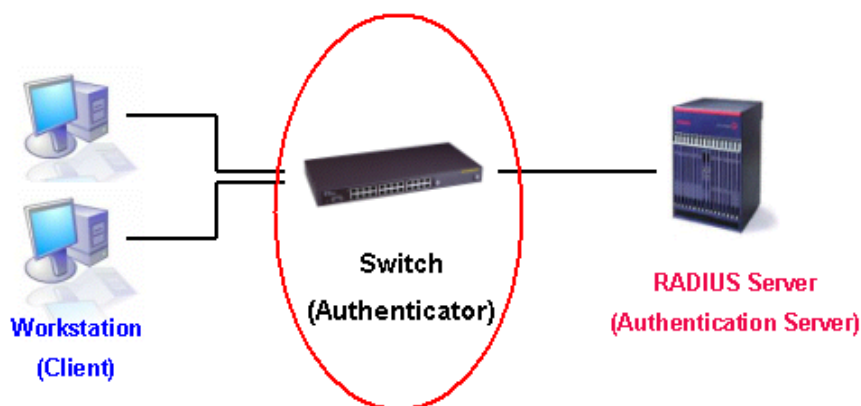


Figure 5 - 14. The Authenticator



NOTE: When configuring the Authentication Protocol as local, the Switch has two roles: Authenticator and Authentication Server.

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows XP, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

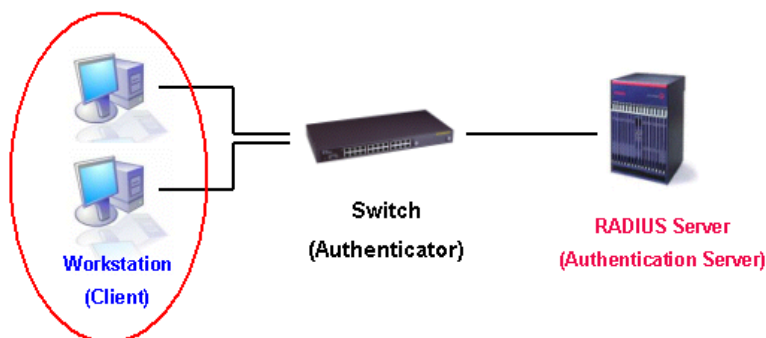


Figure 5 - 15. The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

802.1X Authentication process

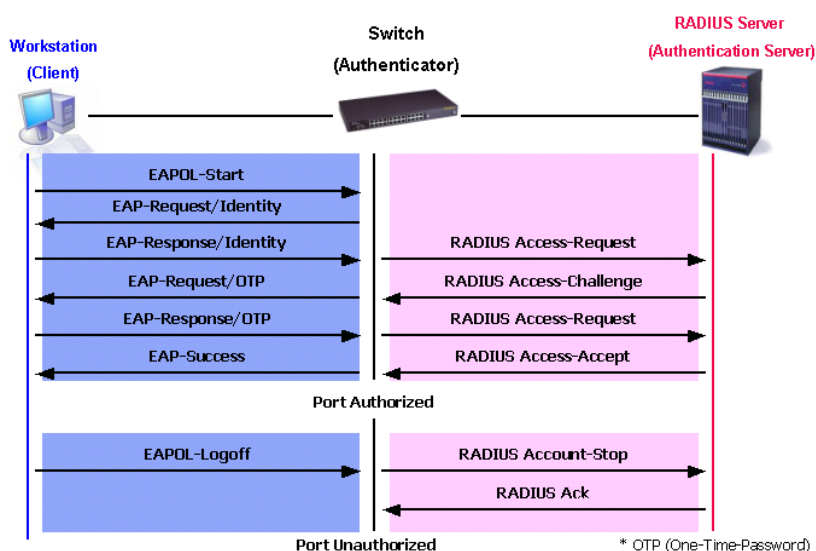


Figure 5 - 16. The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1. Port-based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. Host-based Access Control – Using this method, the Switch will automatically learn up to 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

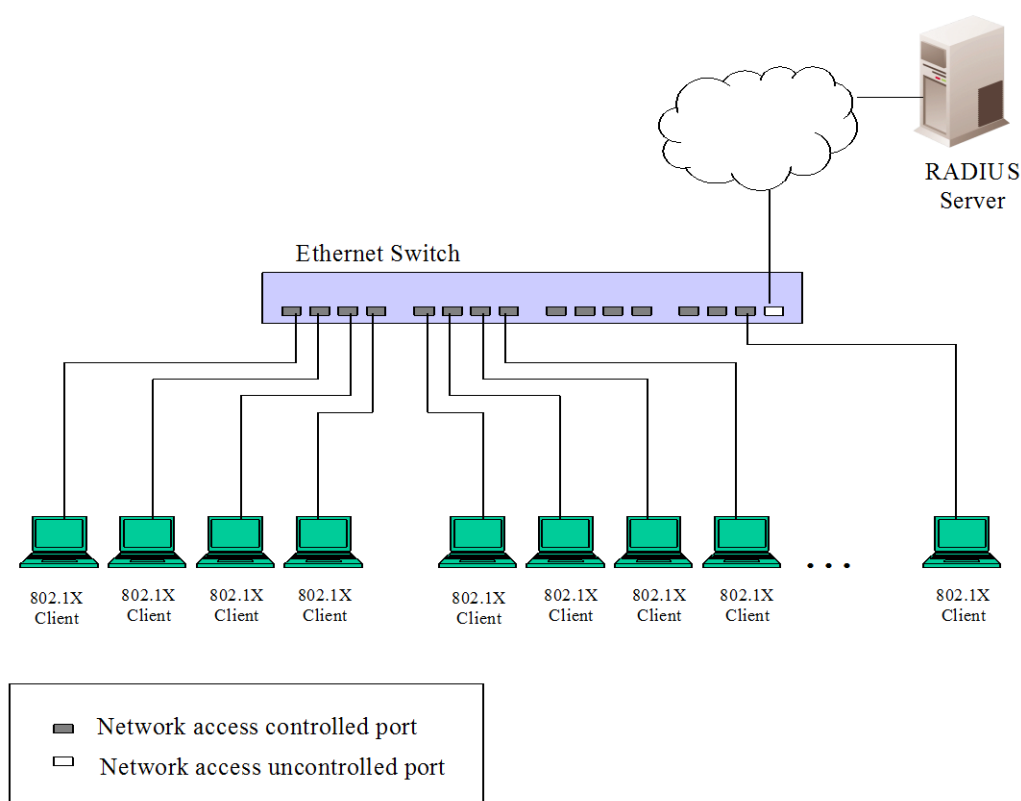


Figure 5 - 17. Example of Typical Port-based Configuration

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

Host-based Network Access Control

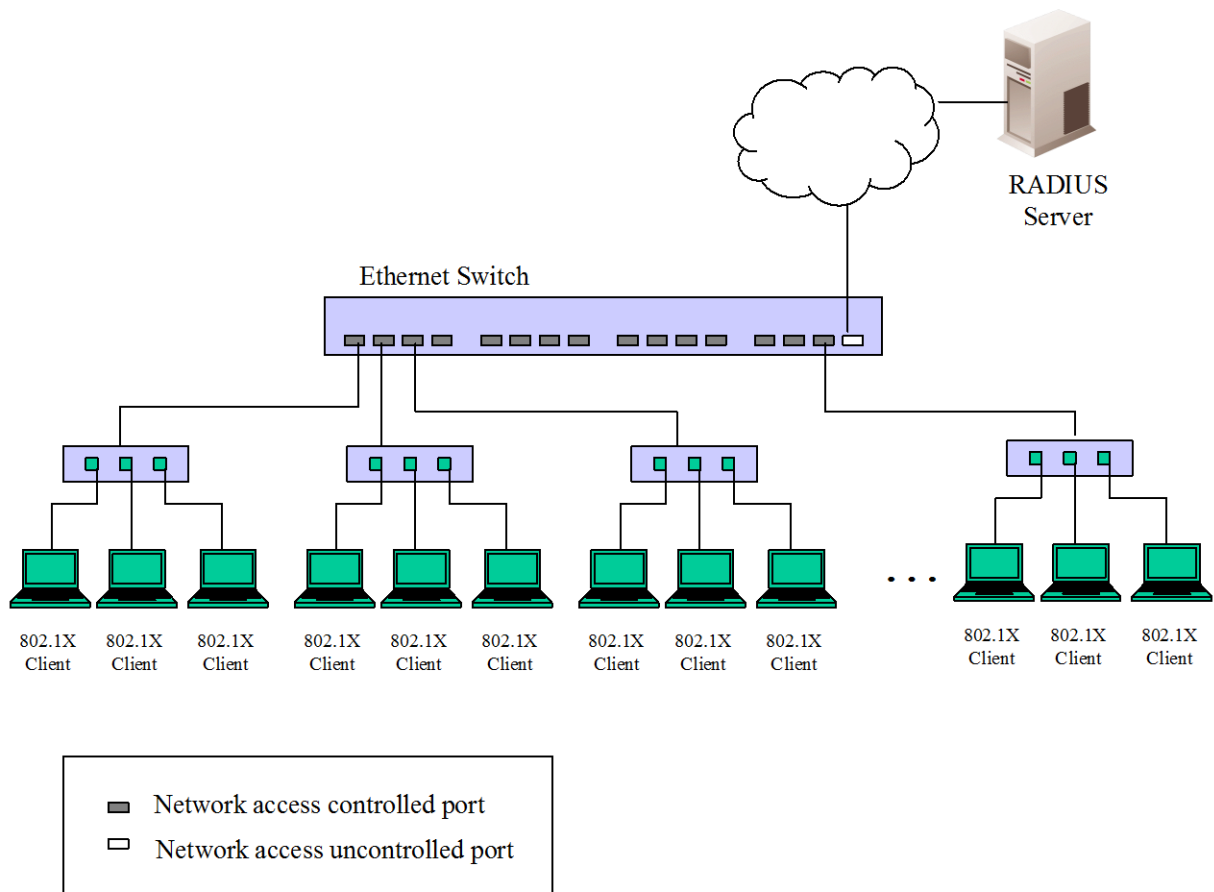


Figure 5 - 18. Example of Typical Host-based Configuration

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

802.1X Settings

To configure the 802.1X Settings, click **Security > 802.1X > 802.1X Settings**:

Port	AdmDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuthentication	Capability
1	Both	Auto	30	60	30	30	2	3600	Disabled	None
2	Both	Auto	30	60	30	30	2	3600	Disabled	None
3	Both	Auto	30	60	30	30	2	3600	Disabled	None
4	Both	Auto	30	60	30	30	2	3600	Disabled	None
5	Both	Auto	30	60	30	30	2	3600	Disabled	None
6	Both	Auto	30	60	30	30	2	3600	Disabled	None
7	Both	Auto	30	60	30	30	2	3600	Disabled	None
8	Both	Auto	30	60	30	30	2	3600	Disabled	None
9	Both	Auto	30	60	30	30	2	3600	Disabled	None
10	Both	Auto	30	60	30	30	2	3600	Disabled	None
11	Both	Auto	30	60	30	30	2	3600	Disabled	None
12	Both	Auto	30	60	30	30	2	3600	Disabled	None
13	Both	Auto	30	60	30	30	2	3600	Disabled	None
14	Both	Auto	30	60	30	30	2	3600	Disabled	None

Figure 5 - 19. 802.1X Settings window

This window allows you to set the following features:

Parameter	Description
802.1X	Use the radio buttons to enable or disable 802.1X.
Auth Mode	Choose the 802.1X authentication mode, <i>Port Based</i> , or <i>MAC Based</i> .
Auth Protocol	Choose the authentication protocol, <i>Local</i> or <i>RADIUS EAP</i> .
From Port/To Port	Enter the port or ports to be set.
QuietPeriod (0-65535)	This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is 60 seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is 30 seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is 2.
TxPeriod	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines

(1-65535)	the period of an EAP Request/Identity packet transmitted to the client. The default setting is 30 seconds.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.
ReAuthentication	Determines whether regular reauthentication will take place on this port. The default setting is <i>Disabled</i> .
Port Control	<p>This allows you to control the port authorization state.</p> <p>Select <i>ForceAuthorized</i> to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.</p> <p>If <i>ForceUnauthorized</i> is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.</p> <p>If <i>Auto</i> is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.</p> <p>The default setting is <i>Auto</i>.</p>
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select <i>Authenticator</i> to apply the settings to the port. When the setting is activated A user must pass the authentication process to gain access to the network. Select <i>None</i> disable 802.1X functions on the port.
Direction	<p>Sets the administrative-controlled direction to either <i>in</i> or <i>both</i>.</p> <p>If <i>In</i> is selected, control is only exerted over incoming traffic through the port you selected in the first field.</p> <p>If <i>Both</i> are selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.</p>
Forward EAPOL PDU On Port	This enables or disables the Switch retransmit EAPOL PDU Request on a per port basis.

Click **Apply** to implement your configuration changes.

802.1X User

To create a new 802.1X User enter a user name and password then reconfirm the password and click **Apply**, the new user will be displayed in the lower half of the table. To delete an entry click the corresponding **Delete** button.

To configure the 802.1X User, click **Security > 802.1X > 802.1X User**:

Figure 5 - 20. 802.1X User window

Authentication RADIUS Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

To configure the 802.1X User, click **Security > 802.1X > Authentication RADIUS Server**:

Figure 5 - 21. Authentication RADIUS Server window

This window displays the following information:

Parameter	Description
Index	Choose the desired RADIUS server to configure: 1, 2 or 3.
IP Address	Set the RADIUS Server IP.
Authentic Port (1-65535)	Set the RADIUS authentic server(s) UDP port. The default port is 1812.
Accounting Port (1-65535)	Set the RADIUS account server(s) UDP port. The default port is 1813.
Timeout (1-255)	Enter the timeout value in seconds (1 to 255) the default value is 5.
Retransmit (1-255)	Set the retransmit value in seconds (1 to 255) the default value is 2.
Key (Max. length 32 bytes)	Set the key the same as that of the RADIUS server. Maximum length of the entry is 32 bytes.

Guest VLAN Configuration

On 802.1X security enabled networks, there is a need for non 802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or lower operating systems, or the need for guests to gain access to the network without full authorization. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN. If authenticated and the authenticator possesses the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

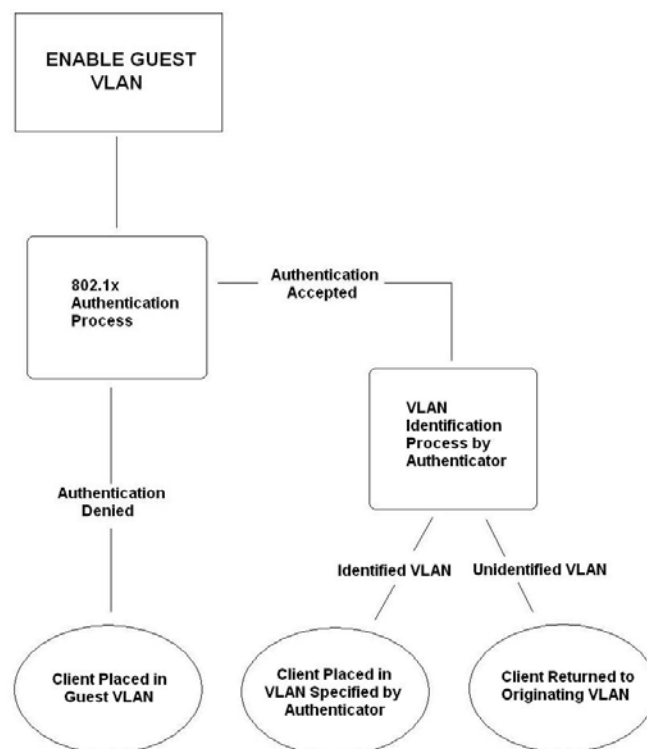


Figure 5 - 22. Guest VLAN Authentication Process

Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.
4. If a port is a member of multiple VLANs, it cannot become a member of the Guest VLAN.

Guest VLAN

To view the following window, click, **Security > 802.1X > Guest VLAN**:

Figure 5 - 23. Guest VLAN window

The following fields may be modified to enable the 802.1X Guest VLAN:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as an 802.1X Guest VLAN.
Port List	Set the individual port(s) to be enabled for the 802.1X Guest VLAN or click All .

Click **Apply** to implement the 802.1X Guest VLAN. Once properly configured, the Guest VLAN Name and associated ports will be listed in the lower part of the window.



NOTE: For more information and configuration examples for the 802.1X Guest VLAN function, please refer to the Guest VLAN Configuration Example located on the D-Link Website.

Initialize Port(s)

Existing 802.1X port and MAC-based settings are displayed and can be configured using the two windows below.

To initialize ports for the port side of 802.1X, the user must first enable 802.1X by port in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Initialize Port(s)**:

Figure 5 - 24. Initialize Port(s) window for Port-based 802.1X

This window allows initialization of a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s). To initialize ports, choose the range of ports in the From Port and To Port fields. To begin the initialization, click **Apply**.

To initialize ports for the MAC-based side of 802.1X, the user must first enable 802.1X by MAC address in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Initialize Port(s)**:

Figure 5 - 25. Initialize Port(s) window for MAC-based 802.1X

To initialize ports, choose the range of ports in the From Port and To Port fields. Next, the user must specify the MAC address to be initialized by entering it into the MAC Address field and ticking the corresponding check box. To begin the initialization, click **Apply**.



NOTE: The user must first globally enable 802.1X in the **802.1X Settings** window (**Security > 802.1X > 802.1X Settings**) before initializing ports. Information in the **Initialize Port(s)** windows cannot be viewed before enabling 802.1X for either Port-based 802.1X or MAC-based 802.1X.

The **Initialize Port(s)** windows display the following information:

Parameter	Description
From Port	The beginning port in a range of ports to be initialized.
To Port	The ending port in a range of ports to be initialized.
Port	A read-only field indicating a port on the Switch.
Auth PAE State	The Authenticator PAE State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.</i>
Backend_State	The Backend Authentication State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.</i>
Port Status	The status of the controlled port can be <i>Authorized, Unauthorized, or N/A.</i>
MAC Address	The authenticated MAC address of the client connected to the corresponding port, if any.

Reauthenticate Port(s)

Users can display and configure reauthenticate ports for 802.1X port and MAC-based using the two windows below.

To reauthenticate ports for the port side of 802.1X, the user must first enable 802.1X by port in the **802.1X Settings** window

To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**:

Figure 5 - 26. Reauthenticate Port(s) window for Port-based 802.1X

This window allows reauthentication of a port or group of ports by using the drop-down menus From Port and To Port and clicking **Apply**. The Reauthenticate Port Table displays the current status of the reauthenticated port(s) once **Apply** has been clicked.



NOTE: The user must first globally enable 802.1X in the **802.1X Settings** window (**Security > 802.1X > 802.1X Settings**) before reauthenticating ports. Information in the **Reauthenticate Port(s)** window cannot be viewed before enabling 802.1X.

To reauthenticate ports for the MAC-based side of 802.1X, the user must first enable 802.1X by MAC address in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**:

Figure 5 - 27. Reauthenticate Port(s) window for MAC-based 802.1X

To reauthenticate ports, first use the From Port and To Port drop-down menus to choose the range of ports. Then the user must specify the MAC address to be reauthenticated by entering it into the MAC Address field and ticking the corresponding check box. To begin the reauthentication, click **Apply**.

This window displays the following information:

Parameter	Description
From Port	The beginning port in a range of ports to be reauthenticated.
To Port	The ending port in a range of ports to be reauthenticated.
MAC Address	Displays the physical address of the Switch where the port resides.
Auth PAE State	The Authenticator State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.</i>
Backend_State	The Backend State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.</i>
Port Status	The status of the controlled port can be <i>Authorized, Unauthorized, or N/A.</i>

SSL Settings

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

Key Exchange: The first part of the cyphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.

Encryption: The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

- Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
- CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

Hash Algorithm: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Download Certificate

This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. The Switch is shipped with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

Ciphersuite

This window will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the Switch. A *ciphersuite* is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible ciphersuites for the SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://10.90.90.90) Any other method will result in an error and no access can be authorized for the web-based management.

To view this window, click **Security > SSL Settings**:

Figure 5 - 28. SSL Settings window

To set up the SSL function on the Switch, configure the following parameters and click **Apply**.

Parameter	Description
SSL Settings	
SSL Status	Enable or Disable the SSL status on the switch. The default is disabled.
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is 600 seconds.
SSL Ciphersuite Settings	

RSA with RC4_128_MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
DHE DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
SSL Certificate Download	
Server IP Address	Enter the IP address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)



NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SSH

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1. Create a user account with admin-level access using the User Accounts window in the **Configuration** folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
2. Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication** window. There are three choices as to the method SSH will use to authorize the user, which are *Host Based*, *Password* and *Public Key*.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the **SSH Authmode and Algorithm Settings** window.
4. Finally, enable SSH on the Switch using the **SSH Settings** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Settings

The following window is used to configure and view settings for the SSH server.

To view this window, click **Security > SSH > SSH Settings**:

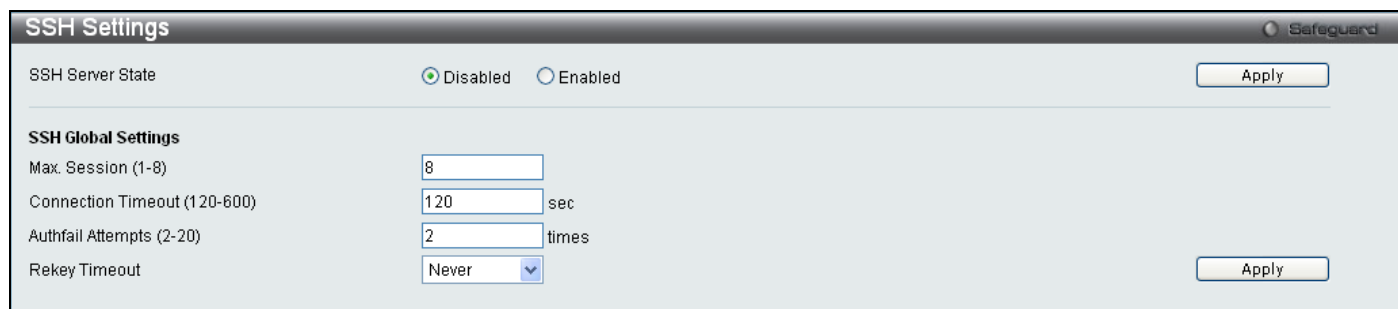


Figure 5 - 29. SSH Settings window

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

Parameter	Description
SSH Server State	Enable or disable SSH on the Switch. The default is <i>Disabled</i> .
Max Session (1-8)	Enter a value between 1 and 8 to set the number of users that may simultaneously access the Switch. The default setting is 8.
Connection Timeout (120-600)	Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default setting is 120 seconds.
Authfail Attempts (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between 2 and 20. The default setting is 2.
Rekey Timeout	Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are <i>Never, 10 min, 30 min, and 60 min</i> . The default setting is <i>Never</i> .

Click **Apply** to implement changes made.

SSH Authmode and Algorithm Settings

The SSH Algorithm window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are four categories of algorithms listed and specific algorithms of each may be enabled or disabled by checking the boxes. All algorithms are enabled by default.

To view this window, click **Security > SSH > SSH Authmode and Algorithm Settings**:

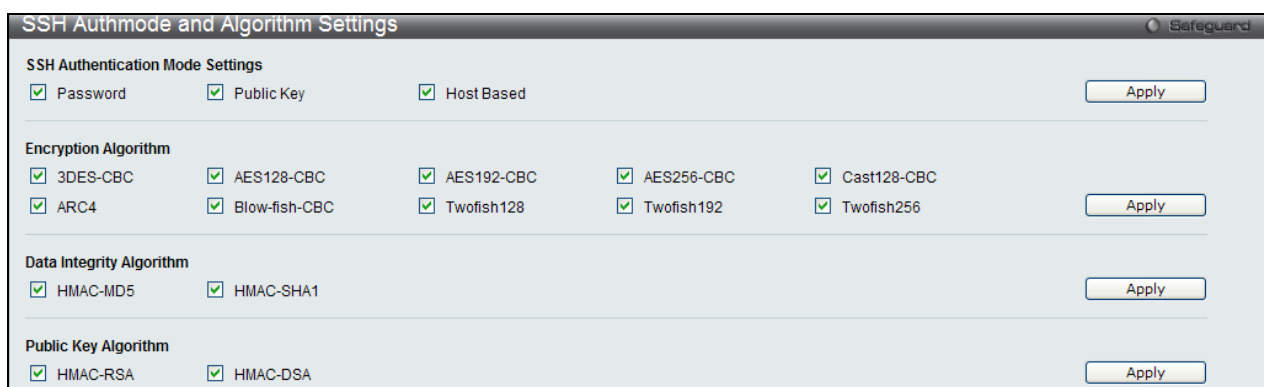


Figure 5 - 30. SSH Authmode and Algorithm Settings window

The following algorithms may be set:

Parameter	Description
SSH Authentication Mode Settings	
Password	This parameter may be enabled if the administrator wishes to use a locally configured password for authentication on the Switch. The default is enabled.
Public Key	This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch. The default is enabled.
Host-based	This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. The default is enabled.
Encryption Algorithm	
3DES-CBC	Tick the check box to enable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish CBC	Tick the check box to enable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Tick the check box to enable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Tick the check box to enable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Tick the check box to enable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Tick the check box to enable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.
Cast128-CBC	Tick the check box to enable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Tick the check box to enable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Tick the check box to enable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Tick the check box to enable the twofish256 encryption algorithm. The default is enabled.
Data Integrity Algorithm	
HMAC-SHA1	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.
HMAC-MD5	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.
Public Key Algorithm	
HMAC-RSA	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. The default is enabled.

Click **Apply** to implement changes made.

SSH User Authentication Lists

The following windows are used to configure parameters for users attempting to access the Switch through SSH.

To access the following window, click **Security > SSH > SSH User Authentication Lists**:

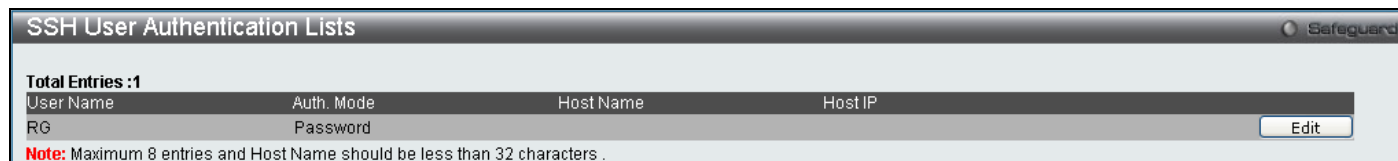


Figure 5 - 31. SSH User Authentication Lists window

In the example above, the User Account “RG” has been previously set using the **User Accounts** window in the **Configuration** folder. A User Account **MUST** be set in order to set the parameters for the SSH user. To edit the parameters for a SSH user, click on the corresponding **Edit** button, which will reveal the following window to configure:



Figure 5 - 32. SSH User Authentication Lists (Edit) window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Auth. Mode	<p>The administrator may choose one of the following to set the authorization for users attempting to access the Switch.</p> <p><i>Host Based</i> – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.</p> <ul style="list-style-type: none"> ▪ <i>Host Name</i> – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. ▪ <i>Host IP</i> – Enter the corresponding IP address of the SSH user. <p><i>Password</i> – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.</p> <p><i>Public Key</i> – This parameter should be chosen if the administrator wishes to use the public key on a SSH server for authentication.</p>
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.

Click **Apply** to implement changes made.



NOTE: To set the SSH User Authentication parameters on the Switch, a User Account must be previously configured. For more information on configuring local User Accounts on the Switch, see the User Accounts section of this manual located in the Configuration section.

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 logs in to the device successfully through TACACS/XTACACS/TACACS+server or none method, the "user" privilege 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 logs in 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 can not 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 window offers 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 access the following window, click **Security > Access Authentication Control > Authentication Policy Settings**:

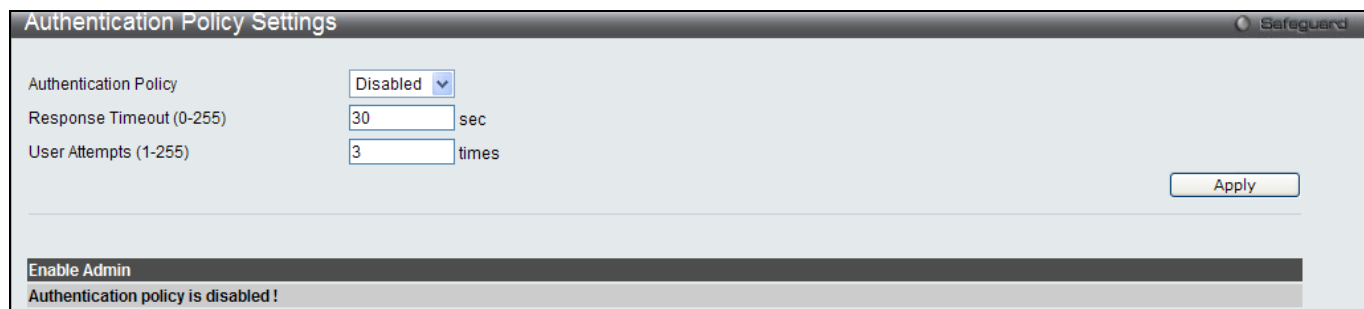


Figure 5 - 33. Authentication Policy Settings window

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 the following window, click **Security > Access Authentication Control > Application Authentication Settings**:

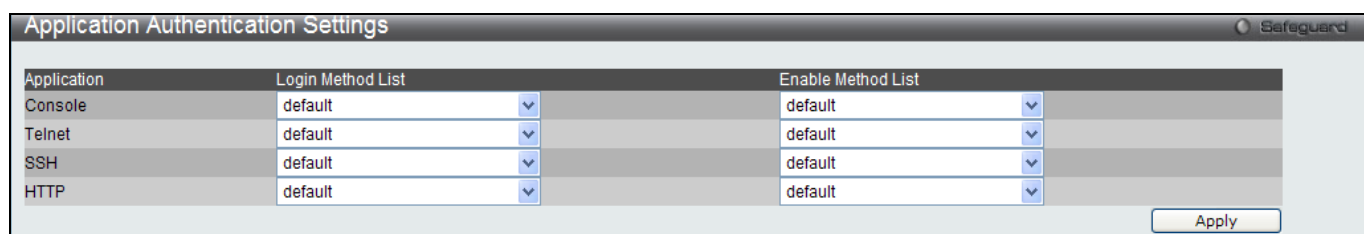


Figure 5 - 34. Application's Authentication Settings window

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 authentications server hosts may be added to any particular group.

To view the following window, click **Security > Access Authentication Control > Authentication Server Group**:

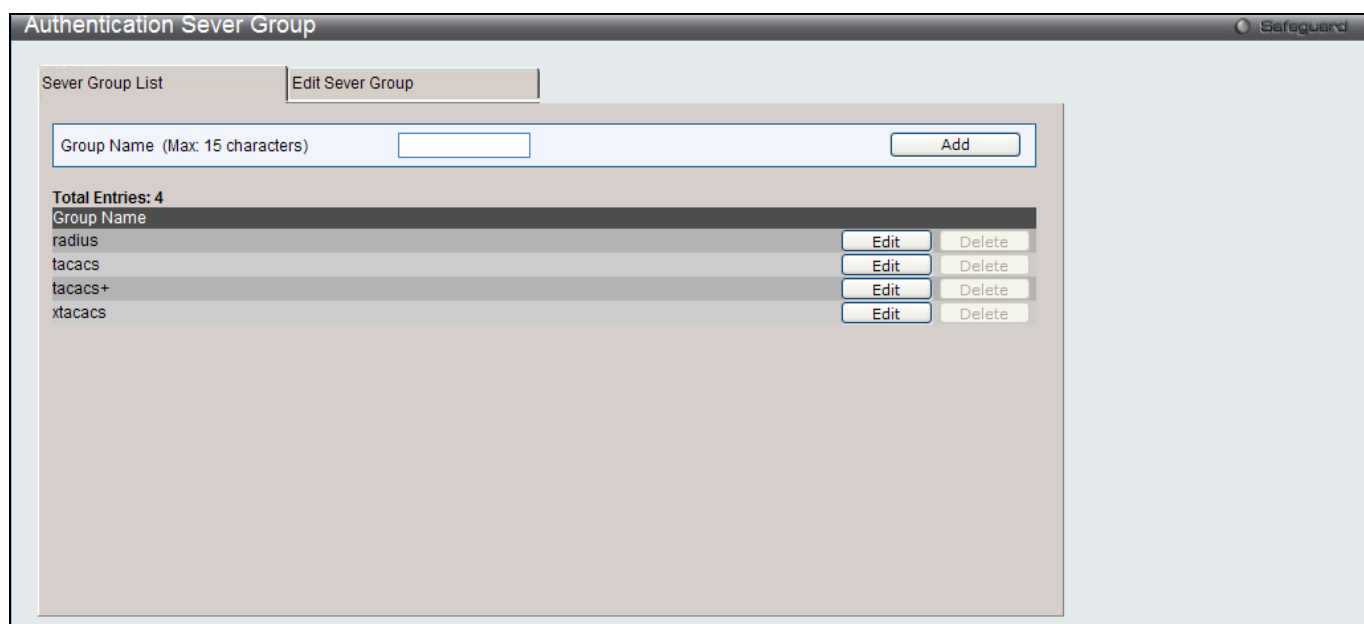


Figure 5 - 35. Authentication Server Group Settings window – Server Group List tab

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 tab will be displayed:

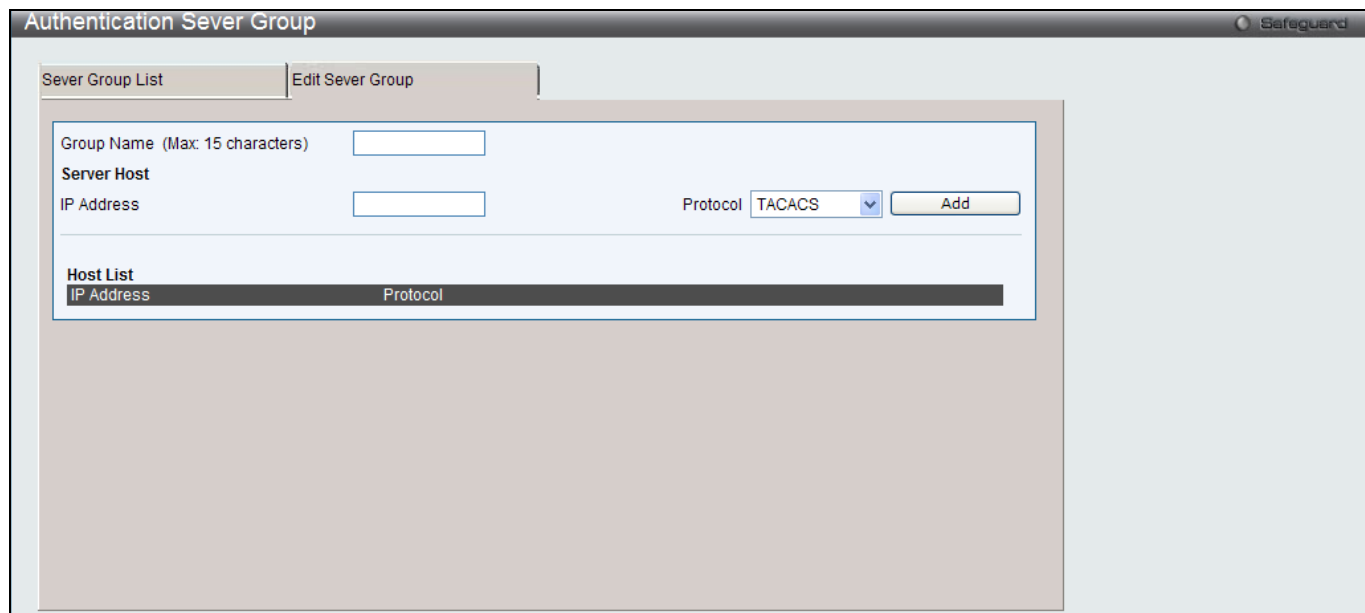


Figure 5 - 36. Authentication Server Group window – Edit Server Group tab

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 the following window, click **Security > Access Authentication Control > Authentication Server:**



Figure 5 - 37. Authentication Server Settings window

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: <ul style="list-style-type: none"> ▪ 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 window is used to 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 dependent on the local account privilege configured on the Switch.

When the user logs in 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 logs in to the device successfully through RADIUS server or local method, three kinds of privilege levels can be assigned to the user and the user can not use the **Enable Admin** window to promote to admin privilege level.

To view the following window, click **Security > Access Authentication Control > Login Method Lists**:

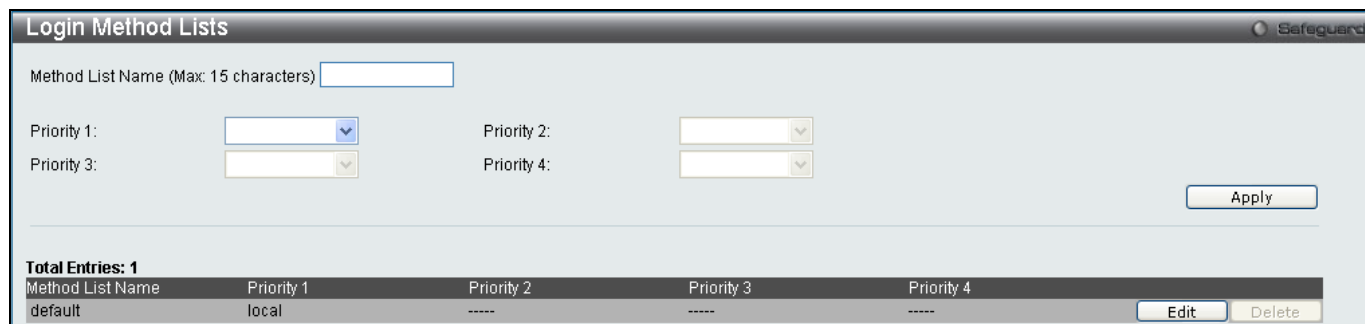


Figure 5 - 38. Login Method Lists window

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 corresponding **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	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. ▪ <i>xtacacs</i> - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. ▪ <i>tacacs+</i> - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. ▪ <i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. ▪ <i>server_group</i> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. ▪ <i>local</i> - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. ▪ <i>none</i> - Adding this parameter will require no authentication to access the Switch.

Enable Method Lists

This 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**:

Figure 5 - 39. Enable Method Lists window

To delete an Enable Method List defined by the user, click the **Delete** button. To modify an Enable Method List, click on 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	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <ul style="list-style-type: none"> ▪ <i>local_enable</i> - 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. ▪ <i>none</i> - Adding this parameter will require no authentication to access the Switch. ▪ <i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. ▪ <i>tacacs</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. ▪ <i>xtacacs</i> - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. ▪ <i>tacacs+</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. ▪ <i>server_group</i> - 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 the following window, click **Security > Access Authentication Control > Local Enable Password Settings**:

Figure 5 - 40. Local Enable Password Settings window

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

Parameter	Description
Old Local Enable Password (Max: 15 characters)	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.

MAC-based Access Control

MAC-based Access Control is a method to authenticate and authorize access using either a port or host. For port-based MAC, the method decides port access rights, while for host-based MAC, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In MAC-based Access Control, MAC user information in a local database or a RADIUS server database is searched for authentication. Following the authentication result, users achieve different levels of authorization.

Notes About MAC-based Access Control

There are certain limitations and regulations regarding the MAC-based Access Control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.
2. If a port is granted clearance for a MAC address in a VLAN that is not a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the Switch.
3. Ports that have been enabled for Link Aggregation, Port Security, or GVRP authentication cannot be enabled for MAC-based Authentication.

MAC-based Access Control Settings

The following window is used to set the parameters for the MAC-based Access Control function on the Switch. Here the user can set the running state, method of authentication, RADIUS password, and view the Guest VLAN configuration to be associated with the MAC-based Access Control function of the Switch.

To enable the MAC-based Access Control Global Settings on the Switch, click **Security > MAC-based Access Control > MAC-based Access Control Settings**:

Figure 5 - 41. MAC-based Access Control Settings window

The following parameters may be viewed or set:

Parameter	Description
Settings	
MBA Global State	Use the radio button to globally enable or disable the MAC-based Access Control function on the Switch.
Method	Use the pull-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: <i>Local</i> – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based Access Control. This MAC address list can be configured in the MAC-based Access Control Local Database Settings window. <i>RADIUS</i> – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is <i>default</i> .
Authentication Failover	By default, authentication failover is <i>Disabled</i> . If RADIUS servers are unreachable, authentication will fail. When authentication failover is <i>Enabled</i> , if RADIUS server authentication is unreachable, the local database will do the authentication.
Max User (1–128)	Enter a value for the maximum number of users, between 1 and 128. The default is 128.

Authorization Attributes	When enabled, authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server or local database. Which attributes will be accepted depends on the individual module's setting. Authorization for attributes is disabled by default.
RADIUS Authorization	If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted when the global authorization status is enabled.
Local Authorization	If specified to enable, the authorized attributes assigned by the local database will be accepted if the global authorization status is enabled.
Trap	Use this pull-down menu to enable or disable traps to be sent for MAC-based Access Control.
Log	Use this pull-down menu to enable or disable logging for MAC-based Access Control.

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

Config Guest VLAN	
VLAN Name	Enter a Guest VLAN name. Clicking the hyperlinked name will send the Web manager to the Guest VLAN configuration window.
VLAN ID (1-4094)	Enter a VLAN ID number between 1 and 4094.
Member Ports (e.g.: 1-5, 9)	Displays the list of ports that have been configured for the Guest VLAN.
Port Settings	
From Port/To Port	Enter the Port range.
State	Use the pull-down menu to enable or disable the MAC-based Access Control function on individual ports.
Mode	Toggle between <i>Port Based</i> and <i>Host Based</i> .
Aging Time (1-1440)	Enter an aging value between 1 and 1440 minutes. The default is 1440. Tick the Infinite check box for no aging time.
Hold Time (1-300)	Enter a hold value between 1 and 300 seconds. The default is 300. Tick the Infinite check box for no hold time.
Max User (1-128)	Enter a value for the maximum number of users, between 1 and 128. The default is 128. Tick the No Limit check box for no maximum user limit.

MAC-based Access Control Local Settings

The following window is used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

To enable the MAC-based Access Control Local MAC Settings on the switch, click **Security > MAC-based Access Control > MAC-based Access Control Local Settings**:

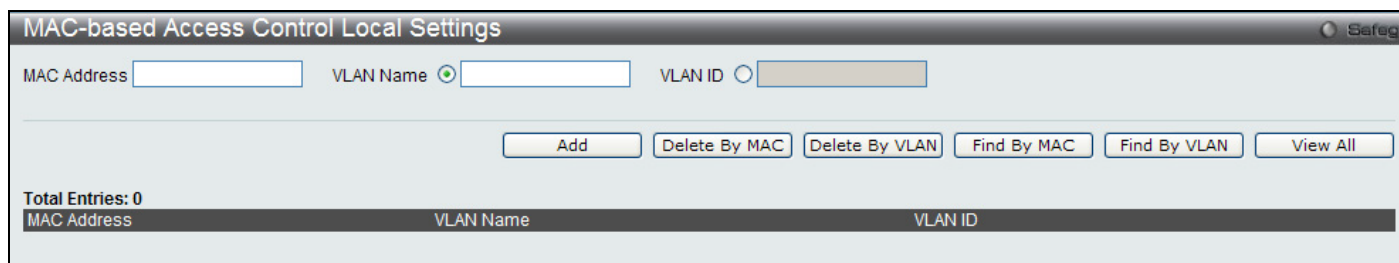


Figure 5 - 42. MAC-based Access Control Local Settings window

To add a MAC address to the local authentication list, enter the MAC address and the target VLAN name into their appropriate fields and click **Add**. To change a MAC address or a VLAN in the list, click the corresponding **Edit By Name** or **Edit By ID** button. To delete a MAC address entry, enter its parameters into the appropriate fields and click **Delete By MAC**, to delete a VLAN, enter its parameters into the appropriate fields and click **Delete By VLAN**. To search for a MAC or a VLAN enter the information in the appropriate fields and click **Find By MAC** or **Find By VLAN**.

Click on the **View All** button to display all current MAC-based Access Control Local Settings entries listed by MAC Address, VLAN Name and VLAN ID.

DoS Prevention Settings

The Switch supports Denial of Service (DoS) prevention to mitigate DoD attacks from hackers or other malicious sources.

To view this window, click **Security > DoS Prevention Settings**:

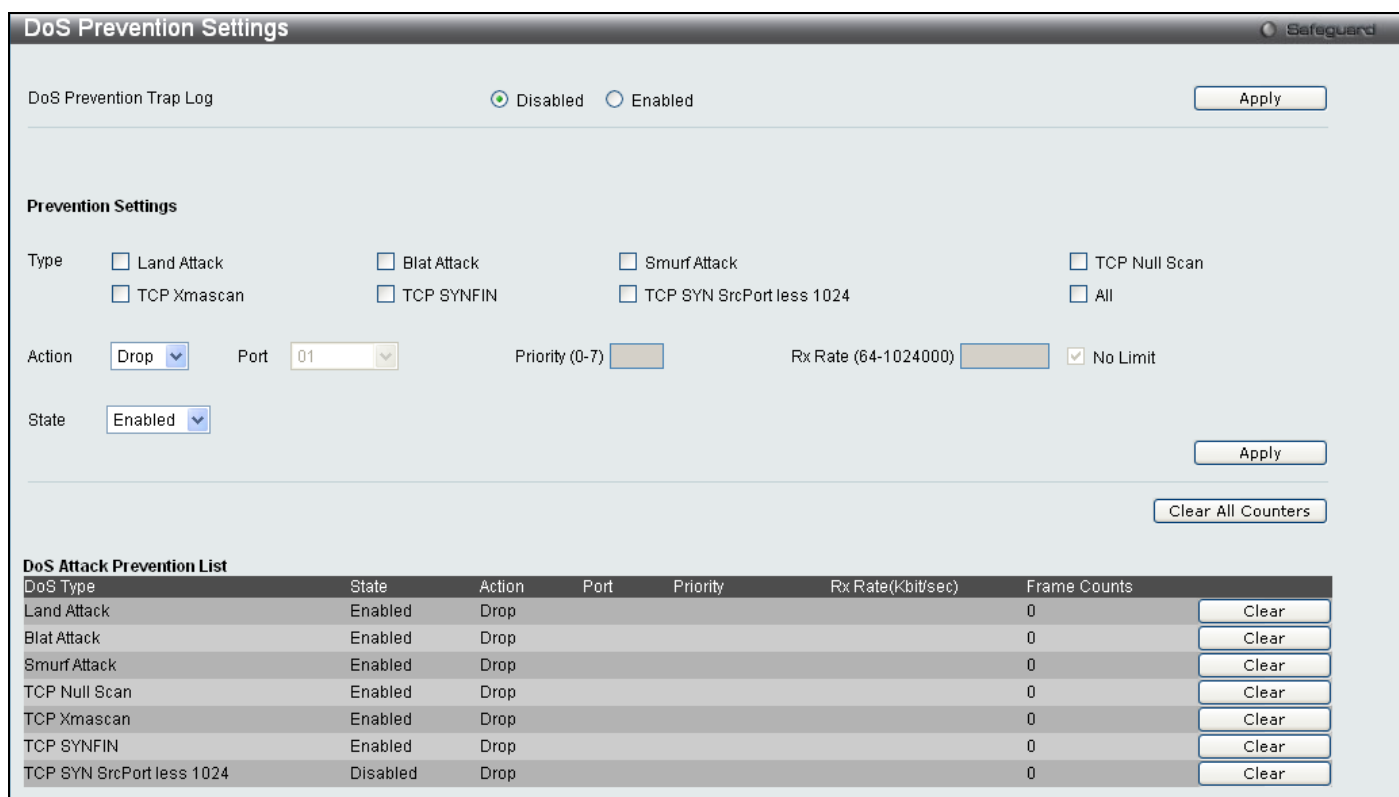


Figure 5 - 43. DoS Prevention Settings window

Set the following parameters and then click **Apply**:

Parameter	Description
DoS Prevention Trap Log	Use the radio button to enable or disable this feature.
Type	Tick the check box for each type of DoS attack: Land Attack, Blat Attack, Smurf Attack, TCP Null Scan, TCP Xmascan, TCP SYNFIN, TCP SYN SrcPort less 1024, and All.

Action	Toggle between <i>Drop</i> and <i>Mirror</i> .
Port	Select the Port which the log will be mirrored to.
Priority (0-7)	Select the Priority for the mirror port.
Rx Rate (64-1024000)	Enter a value between 64 and 1024000 or tick the No Limit check box.
State	Toggle to enable or disable DoS Prevention.
Clear	Click to clear the DoS prevention trap logs for the corresponding types of DoS attacks.

DHCP Server Screening Settings

This function allows the user to not only restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

The DHCP Server Screening folder contains two windows: **DHCP Server Screening Port Settings** and **DHCP Offer Permit Entry Setting**.

DHCP Server Screening Port Settings

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers. When the DHCP server screening function is enabled, all DHCP server packets will be filtered from a specific port.

To view this window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings** as shown below:

DHCP Server Screening Port Settings Safeguard

DHCP Server Screening Trap State Enabled Disabled
 DHCP Server Screening Log State Enabled Disabled
 Illegal Server Log Suppress Duration 1 min 5 mins 30 mins

From Port To Port State

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
27	Disabled
28	Disabled

Figure 5 - 44. DHCP Screening Port Settings

Use the radio buttons at the top of the menu to enable or disable the DHCP Server Screening trap and log state. Set the **Illegal Server Log Suppression Duration** time to 1 minute, 5 minutes (default) or 30 minutes. Click the **Apply** button to apply the settings.

To configure per port screening settings, use the pull-down menus to configure the following parameters:

Parameter	Description
From Port / To Port	A consecutive group of ports may be configured starting with the selected port.
State	Choose <i>Enabled</i> to enable the DHCP Server Screening function or <i>Disabled</i> to disable it. The default is Disabled.

After setting the previous parameters, click **Apply** to allow your changes to be implemented. The **DHCP Port Information Table** shows which ports are enabled or disabled for **DHCP Sever Screening**.

DHCP Offer Permit Entry Setting

This function allows the user not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

To view this window, click **Security > DHCP Server Screening > DHCP Offer Permit Entry Setting** as shown below:

Figure 5 - 45. DHCP Offer Permit Entry Setting menu

The user may set the following parameters:

Parameter	Description
Server IP Address	The IP address of the DHCP server.
Client's MAC Address	The MAC address of the DHCP client. Only multiple legal DHCP servers on the network need to be entered in this field. If there is only one legal DHCP server on the network, no input to this field is allowed.
Ports	Choose the range of ports that you want to use as the DHCP server, or check the All Ports box if you wish to use all the ports on the Switch.

Click **Apply** to implement changes.

Section 6

ACL

ACL Configuration Wizard

Access Profile List

CPU Access Profile List

ACL Finder

ACL Flow Meter

Access profiles allow the user 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.

ACL Configuration Wizard

This window 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**:

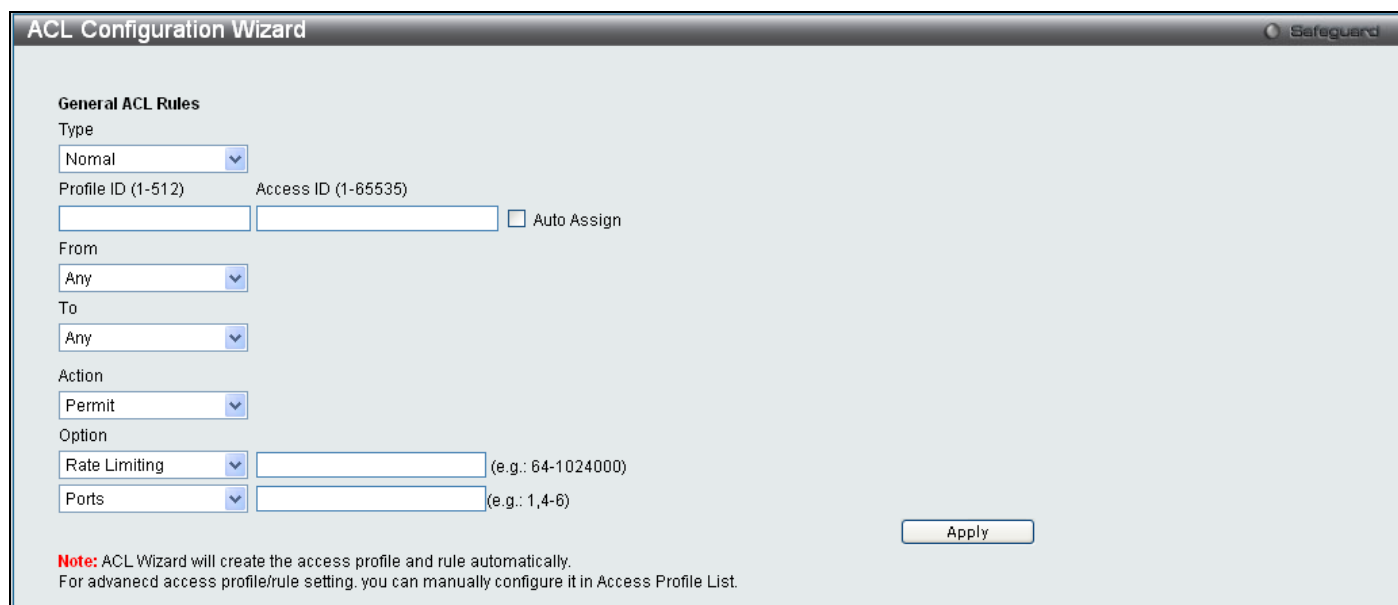


Figure 6 - 1. ACL Configuration Wizard window

The following parameters can be configured:

Parameter	Description
Type	Select the type of ACL you wish to create, either <i>Normal</i> or <i>CPU</i> .
Profile ID (1-512)	Enter a unique identifier number for this profile set. This value can be set from 1 to 512.
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from 1 to 65535.
From	Use the drop-down menu to select from <i>MAC Address</i> , <i>IPv4 Address</i> , <i>IPv6</i> , or <i>Any</i> .
To	Use the drop-down menu to select from <i>MAC Address</i> , <i>IPv4 Address</i> , or <i>Any</i> . When IPv6 is selected the user can only enter the IPv6 source address or the IPv6 destination address at any one time.

Service Type	Use the drop-down menu to select from <i>VLAN Name</i> , <i>Ethernet Type</i> , <i>802.1P</i> , or <i>Any</i> .
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> 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	Select between <i>Rate Limiting</i> , <i>Change 1P Priority</i> , and <i>Replace DSCP</i> .
Ports	Enter a range of ports to be configured.

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 display the currently configured Access Profiles on the Switch, click **ACL > Access Profile Lists**:



Figure 6 - 46. initial Access Profile List window

To add an ACL Profile, click the **Add ACL Profile** button, which will display the window below:

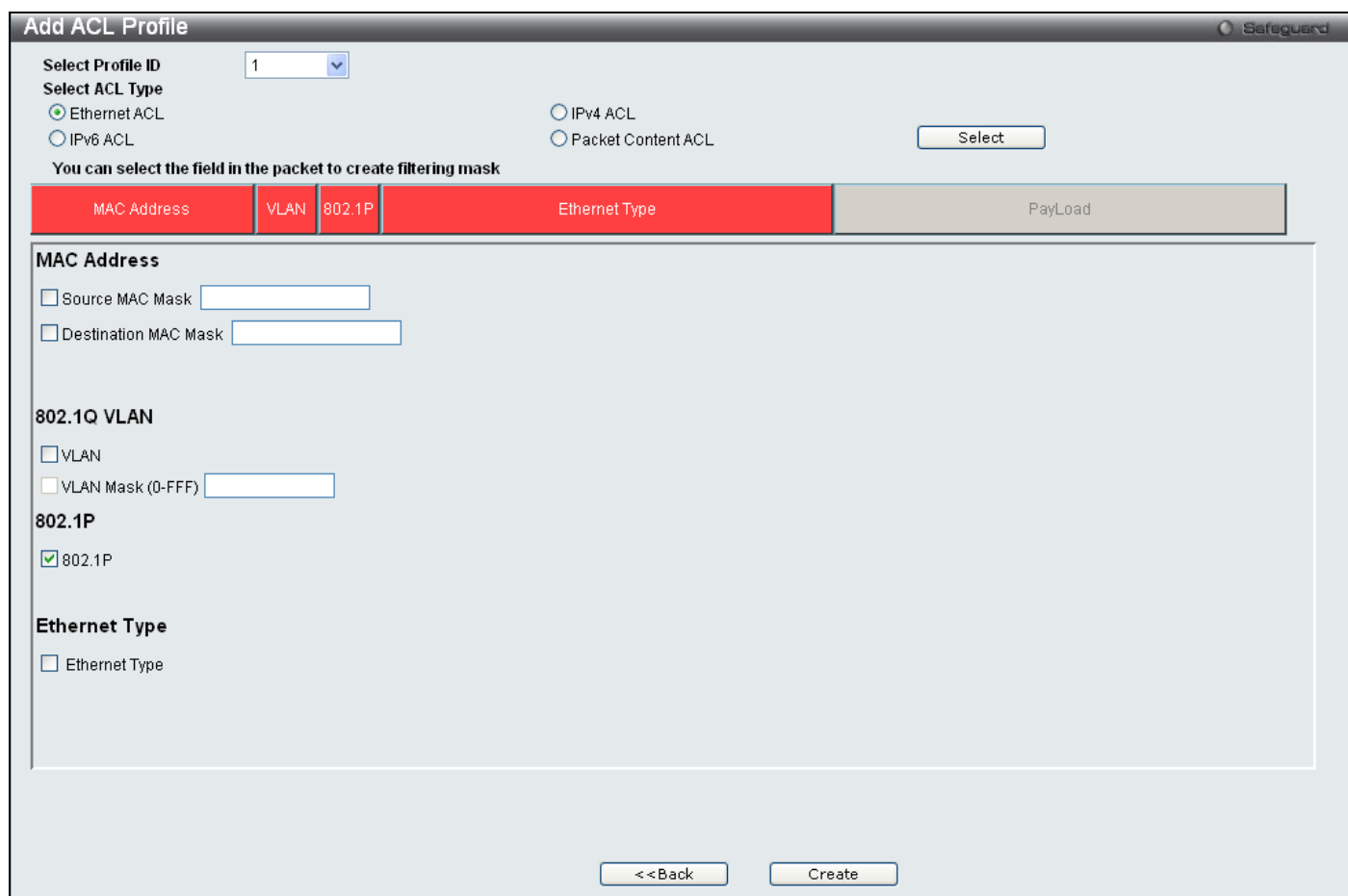


Figure 6 - 47. Add ACL Profile window for Ethernet example

There are four sets of Access Profile configuration windows; one for Ethernet (or MAC address-based) profile configuration, one for IP (IPv4) address-based profile configuration, one for the Packet Content and one for IPv6. Explore the four types of Access Profile configuration options by using the drop-down menu to select a Profile ID between 1 and 512 (1 has been selected in this example), using the radio button to select an ACL Type (Ethernet ACL has been selected in this example), and then clicking **Select**. Next, click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration (MAC Address, 802.1Q VLAN, 802.1p, and Ethernet Type have been selected in this example). At least one mask must then be selected before clicking the **Create** button (802.1p has been ticked in this example). To return to the Access Profile List window, click **<<Back**.

The following parameters can be configured for Ethernet ACL:

Parameter	Description
Select ACL Type	<p>Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 or packet content mask. This will change the window according to the requirements for the type of profile.</p> <ul style="list-style-type: none"> ▪ Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. ▪ Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. ▪ Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. ▪ Select Packet Content ACL to specify a mask to hide the content of the packet header.
MAC Address	<p>Tick either Source MAC Mask and enter the source MAC address mask or Destination MAC Mask and enter the destination MAC address mask.</p>
802.1Q VLAN	<p>VLAN - Specifies a VLAN. VLAN Mask (0-FFF) - Specifies a VLAN mask.</p>

	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.

Clicking **Create** on the previous **Add ACL Profile** window inserts a new Access Profile List entry in the **Access Profile List** window 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. To remove all listed profiles, click on the **Delete All** button.

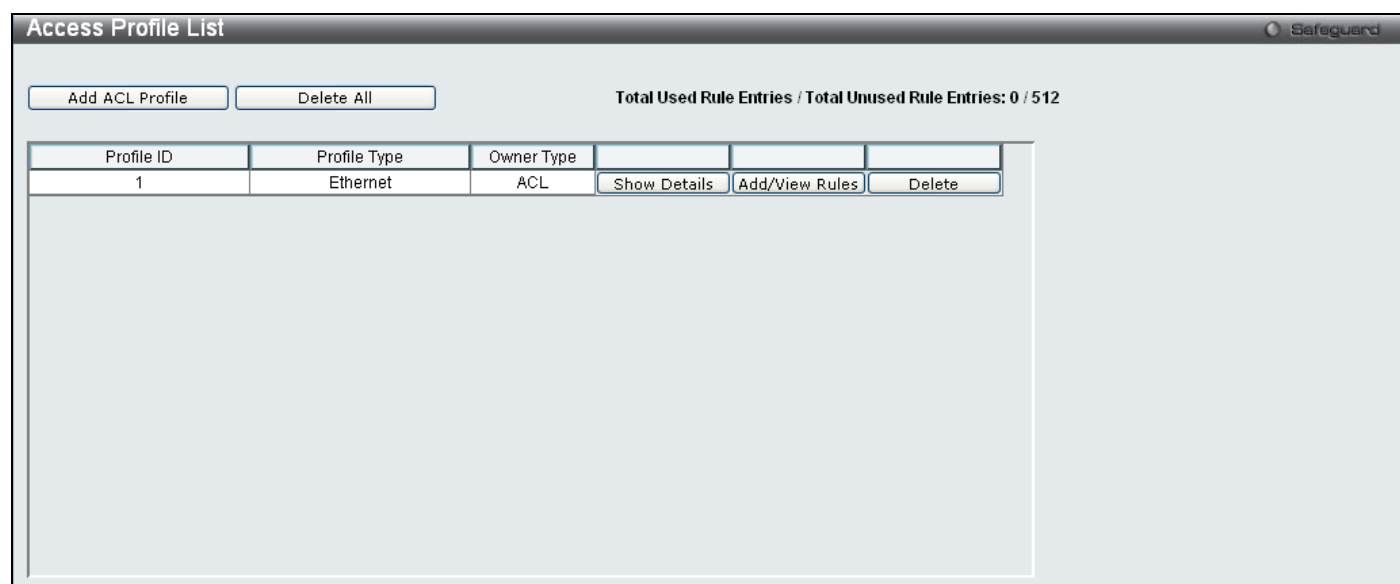


Figure 6 - 48. Access Profile List window for Ethernet example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

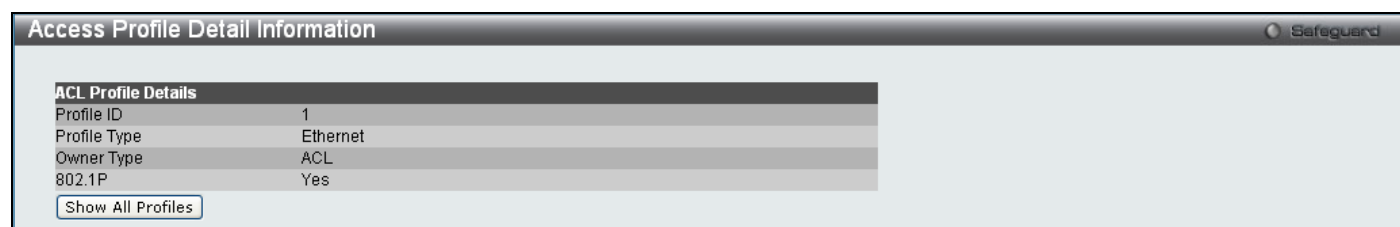


Figure 6 - 49. Access Profile Detail Information window for Ethernet example

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

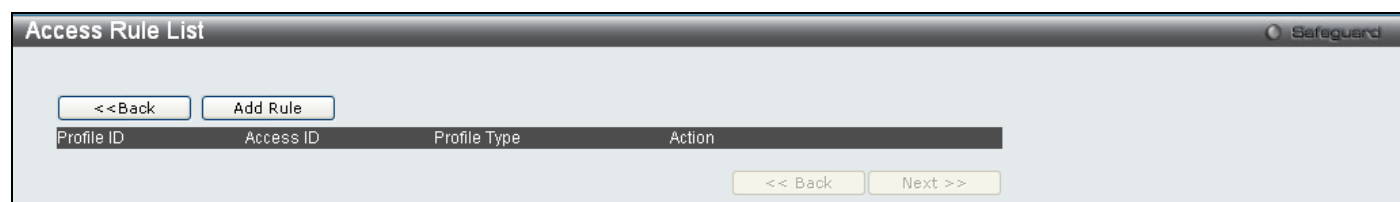


Figure 6 - 50. initial Access Rule List window

Click **Add Rule**, which will reveal the following window:

Figure 6 - 51. Add Access Rule window for Ethernet example

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

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from 1 to 65535. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	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
VLAN ID (1-4094)	Mask ____ (0-FFF) – Specifies a VLAN ID.
VLAN ID	Allows the entry of a VLAN ID for a previously configured VLAN.
Source MAC Address	Specifies a MAC address mask for the source MAC address.
Source MAC Mask	Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.
Destination MAC Address	Specifies a MAC address for the destination MAC address.
Destination MAC Mask	Specifies a MAC address mask for the destination MAC address.
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.
Ethernet Type (0-FFFF)	Enter a value that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> 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 user 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. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority 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.
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	Specifies whether counter feature will be enabled or disabled. This is optional, the default is disabled.
Ports	Enter a range of ports to be configured.

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

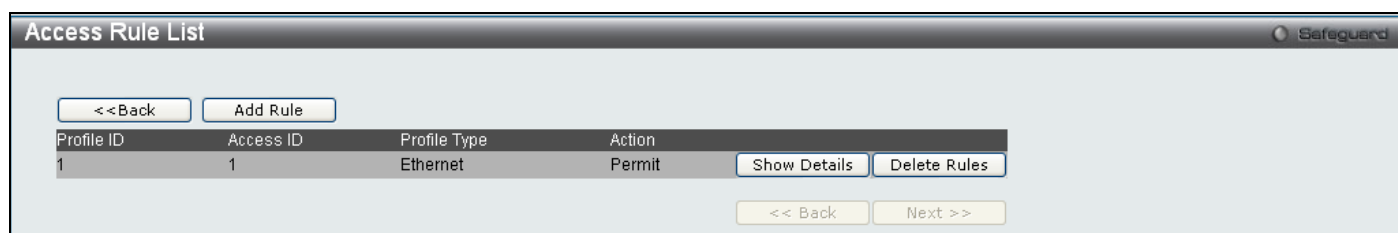


Figure 6 - 52. Access Rule List window for Ethernet example

To view the configurations for previously configured rules, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

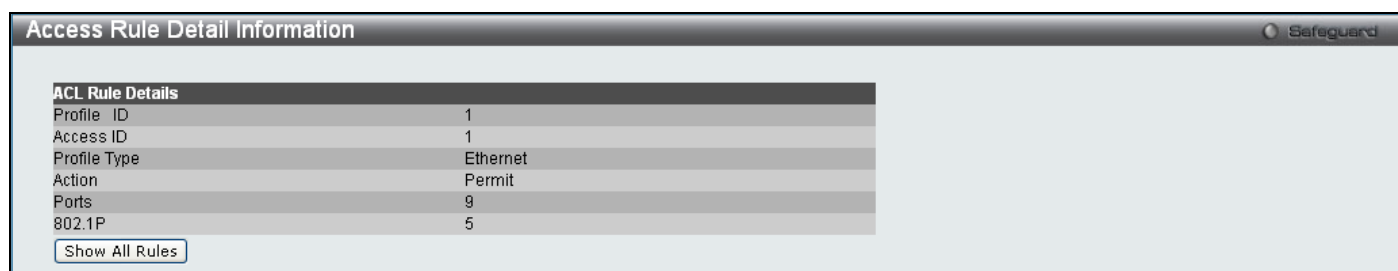


Figure 6 - 53. Access Rule Detail Information window for Ethernet example

To create an IPv4 ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between 1 and 512, click the IPv4 ACL radio button, and then use the drop-down menu to select a protocol *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID*. Click **Select** and the following window will appear (this window will vary depending on whether *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID* has been selected):

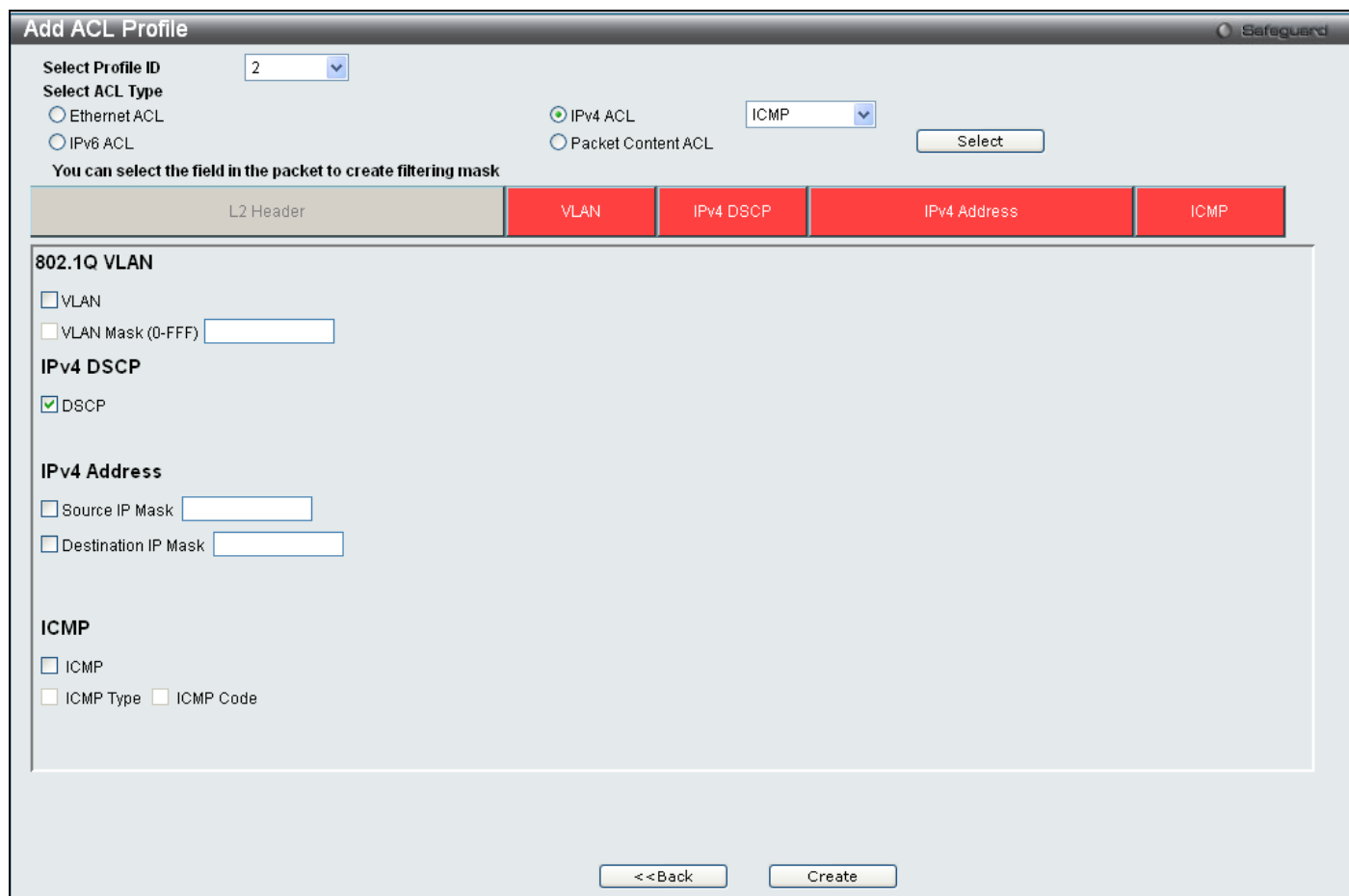


Figure 6 - 54. Add ACL Profile window for IPv4 example

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

The following parameters can be set for IPv4:

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.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Address	Tick either Source IP Mask and enter the IPv4 source address mask or Destination IP Mask and enter the IPV4 destination address mask.
ICMP	Tick ICMP to specify that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet. Tick ICMP Type to specify that the access profile will apply to this ICMP type value. Tick ICMP Code to specify that the access profile will apply to this ICMP code value.
IGMP	Tick IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Tick IGMP Type to further specify that the access profile will apply an IGMP type value.
TCP	Tick TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Ticking TCP requires specifying 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. <ul style="list-style-type: none"> Source Port Mask (0-FFFF) – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff).

	<ul style="list-style-type: none"> Destination Port Mask (0-FFFF) – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff). TCP Flag Bits – Tick URG (urgent), ACK (acknowledgement), PSH (push), RST (reset), SYN (synchronize), FIN (finish), or Check All to filter certain flag bits within the packets.
UDP	<p>Tick UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Ticking UDP requires specifying a source port mask and/or a destination port mask.</p> <ul style="list-style-type: none"> Source Port Mask – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). Destination Port Mask – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff).
Protocol ID	<p>Tick Protocol ID Mask and enter a value defining the protocol ID in the packet header to mask.</p> <ul style="list-style-type: none"> Protocol ID Mask (0-FF) – Tick and 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** window 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. To remove all listed profiles, click on the **Delete All** button.

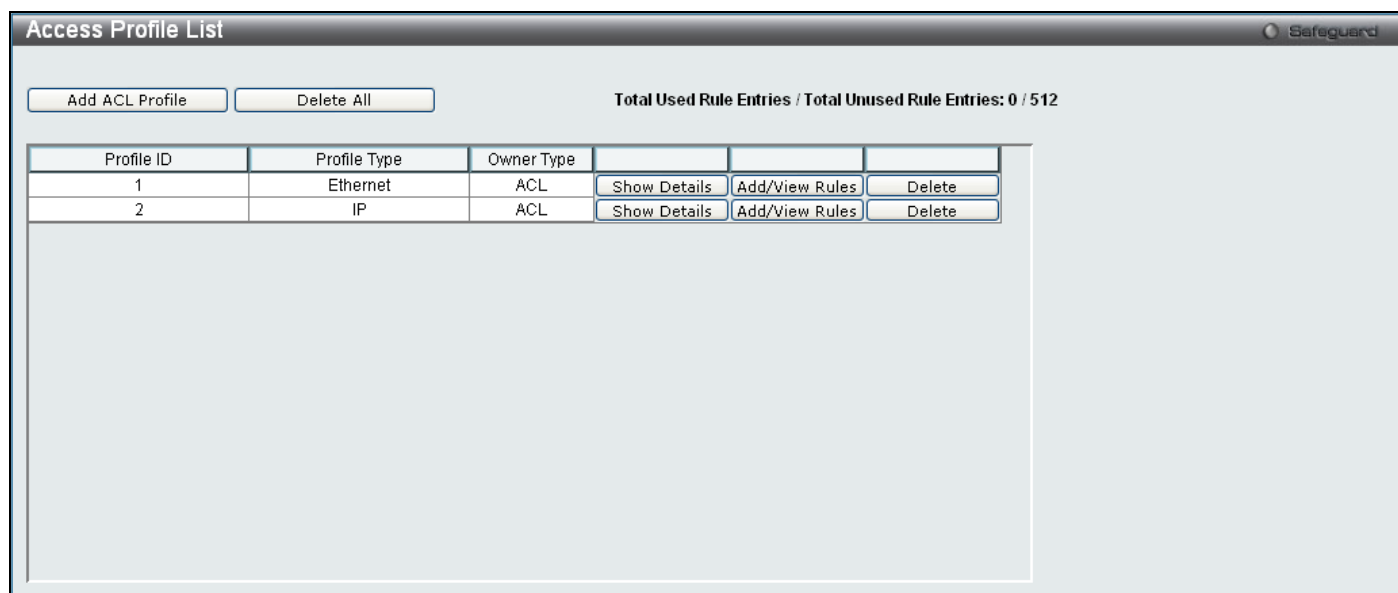


Figure 6 - 55. Access Profile List window for IPv4 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

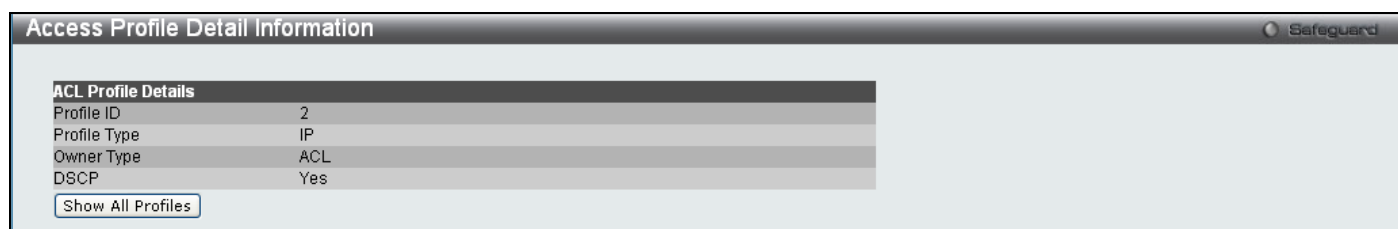


Figure 6 - 56. Access Profile Detail Information window for IPv4 example

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

Figure 6 - 57. Add Access Rule window for IPv4 example

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

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from 1 to 65535.
VLAN Name	Specifies a VLAN name.
VLAN ID (1-4094)	Mask ____ (0-FFF) – Specifies a VLAN ID.
Source IP Address	Specifies an IP address for the source IP address.
Source IP Mask	Specifies an IP address mask for the source IP address.
Destination IP Address	Specifies an IP address for the destination IP address.
Destination IP Mask	Specifies a destination IP address mask for the destination IP address.
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 <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. ICMP Type - Specifies that the Switch will examine each frame's ICMP Type field. ICMP Code - Specifies that the Switch will examine each frame's ICMP Code field.
IGMP	Type ____ e.g. (0-255) - Specifies that the Switch will examine each frame's IGMP Type field.
TCP	Source Port - Specifies a TCP port for the source port. Mask (0-FFFF) - Specifies a TCP port mask for the source port. Destination Port - Specifies a TCP port for the destination port. Mask (0-FFFF) - Specifies a TCP port mask for the destination port. Flag Bits - Enter the appropriate flag mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. URG/ACK/PSH/RST/SYN/FIN – Choose among <i>urg</i> (urgent), <i>ack</i> (acknowledgement), <i>psb</i> (push), <i>rst</i> (reset), <i>syn</i> (synchronize) and <i>fin</i> (finish)

UDP	Source Port - Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field for the source port. Mask (0-FFFF) - Specifies a UDP port mask for the destination port. Destination Port - Specifies a UDP port for the destination port. Mask (0-FFFF) - Specifies a UDP port mask for the destination port.
Protocol ID	Protocol ID ____ e.g. (0-255) - Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> 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 user 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. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority 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.
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	Enter a range of ports to be configured.

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

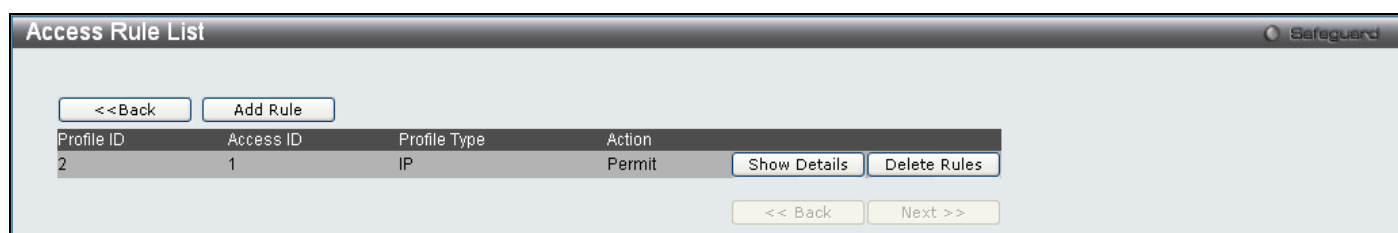


Figure 6 - 58. Access Rule List window for IPv4 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

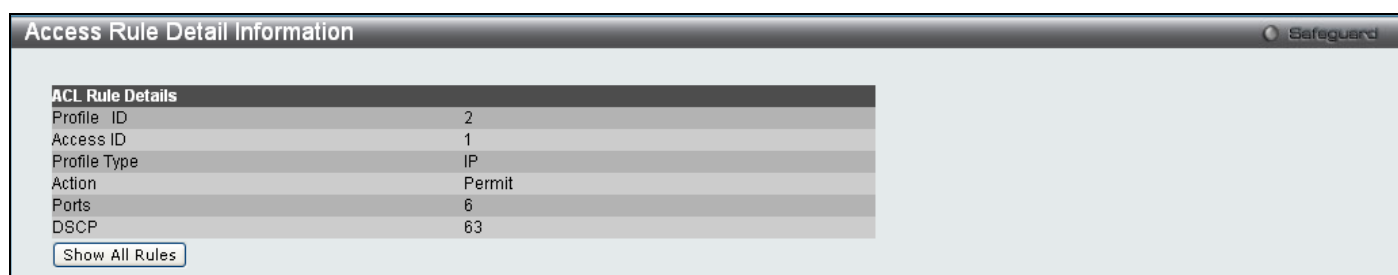


Figure 6 - 59. Access Rule Detail Information window for IPv4 example

To create an IPv6 ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between 1 and 512, click the IPv6 ACL radio button, and then use the drop-down menu to select

a protocol *TCP* or *UDP*. Click **Select** and the following window will appear (this window will vary depending on whether *TCP* or *UDP* has been selected):

Figure 6 - 60. Add ACL Profile window for IPv6 example

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** window, 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. The 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. The 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 Address	Ticking this check box will instruct the Switch to examine the IPv6 Source Address.
IPv6 TCP	Ticking this check box will specify that the rule applies to TCP traffic. The user can tick and 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 tick and enter a specific UDP Source Port Mask or UDP Destination Port Mask.

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window 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. To remove all listed profiles, click on the **Delete All** button.

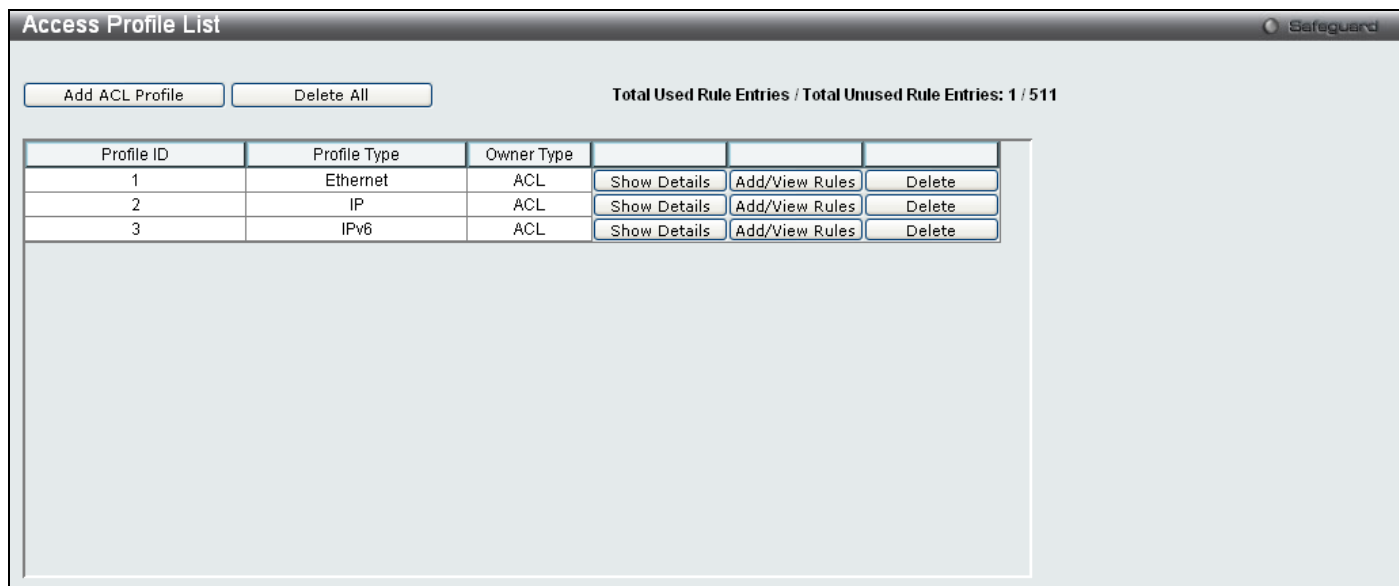


Figure 6 - 61. Access Profile List window for IPv6 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

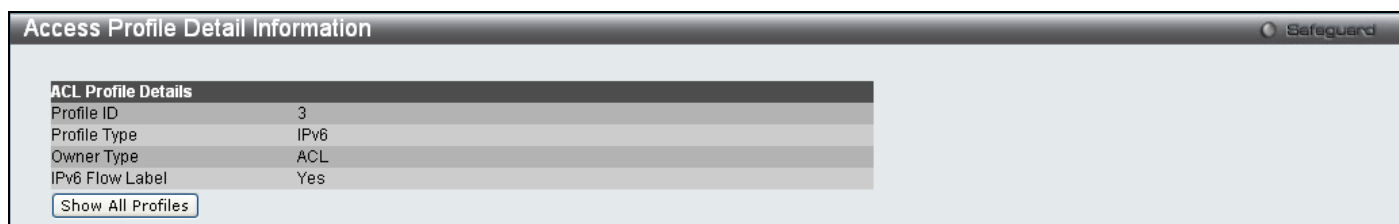


Figure 6 - 62. Access Profile Detail Information window for IPv6 example

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

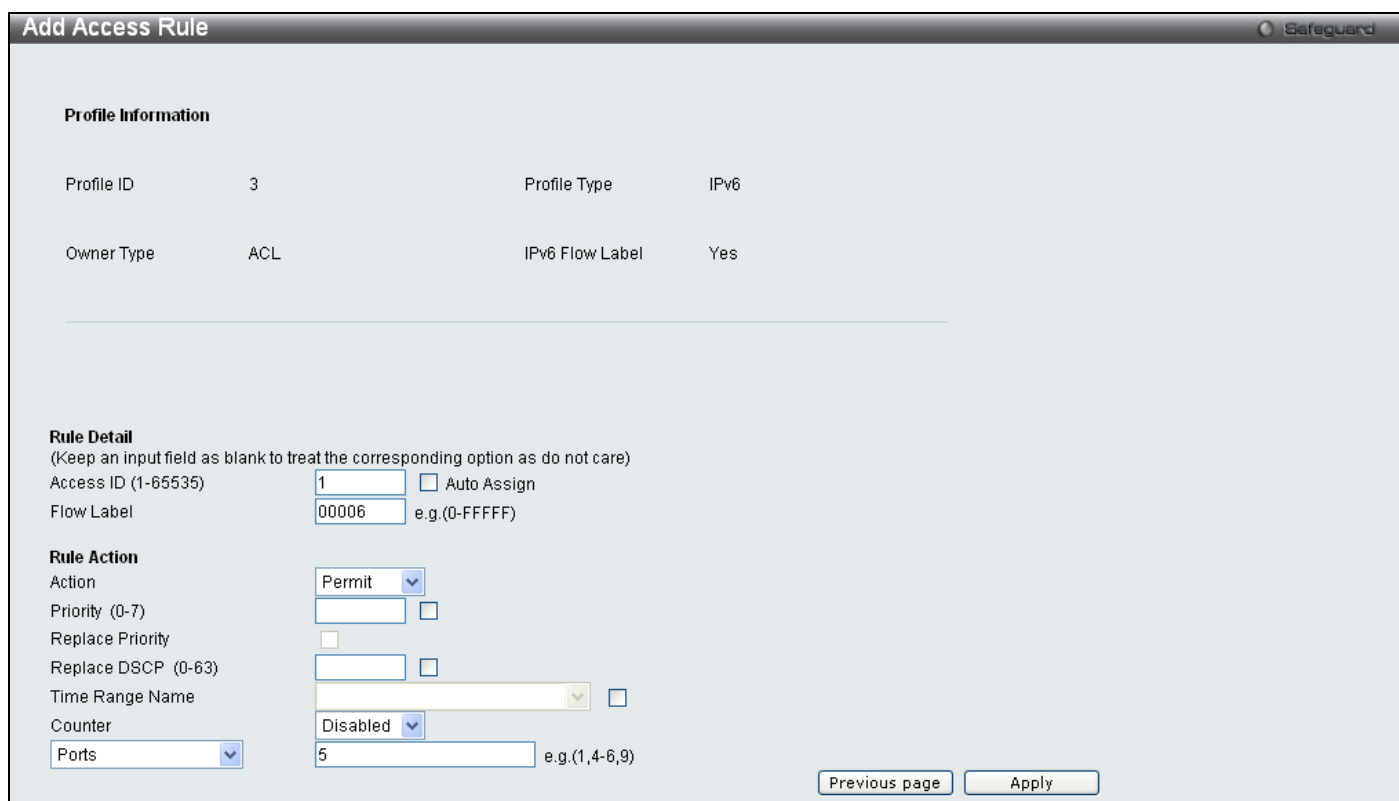


Figure 6 - 63. Add Access Rule window for IPv6 example

The following parameters may be configured for IPv6:

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from 1 to 65535. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Class	Entering a class will instruct the Switch to examine the <i>class</i> 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.
Flow Label	Specifies the IPv6 Flow Label. Enter a value between 0 – FFFFF.
IPv6 Source Address	Specifies an IPv6 address for the IPv6 source address.
IPv6 Source Mask	Specifies an IPv6 source submask. The device only supports filtering of the last 44 bits (LSB) of the source IPv6 address.
TCP	Source Port - Specifies an IPv6 L4 TCP source port submask. Destination Port - Specifies an IPv6 L4 TCP destination port submask.
UDP	Source Port - Specifies an IPv6 L4 UDP source port submask. Destination Port - Specifies an IPv6 L4 UDP destination port submask.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> 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 user 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. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority 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.
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	Enter a range of ports to be configured.

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



Figure 6 - 64. Access Rule List window for IPv6 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

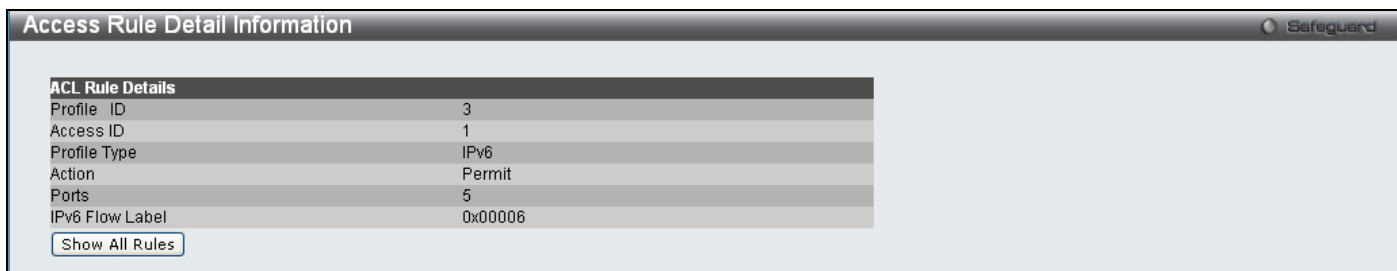


Figure 6 - 65. Access Rule Detail Information window for IPv6 example

To create a Packet Content ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between 1 and 512 and click the Packet Content ACL radio button. Click **Select** and the following window will appear:

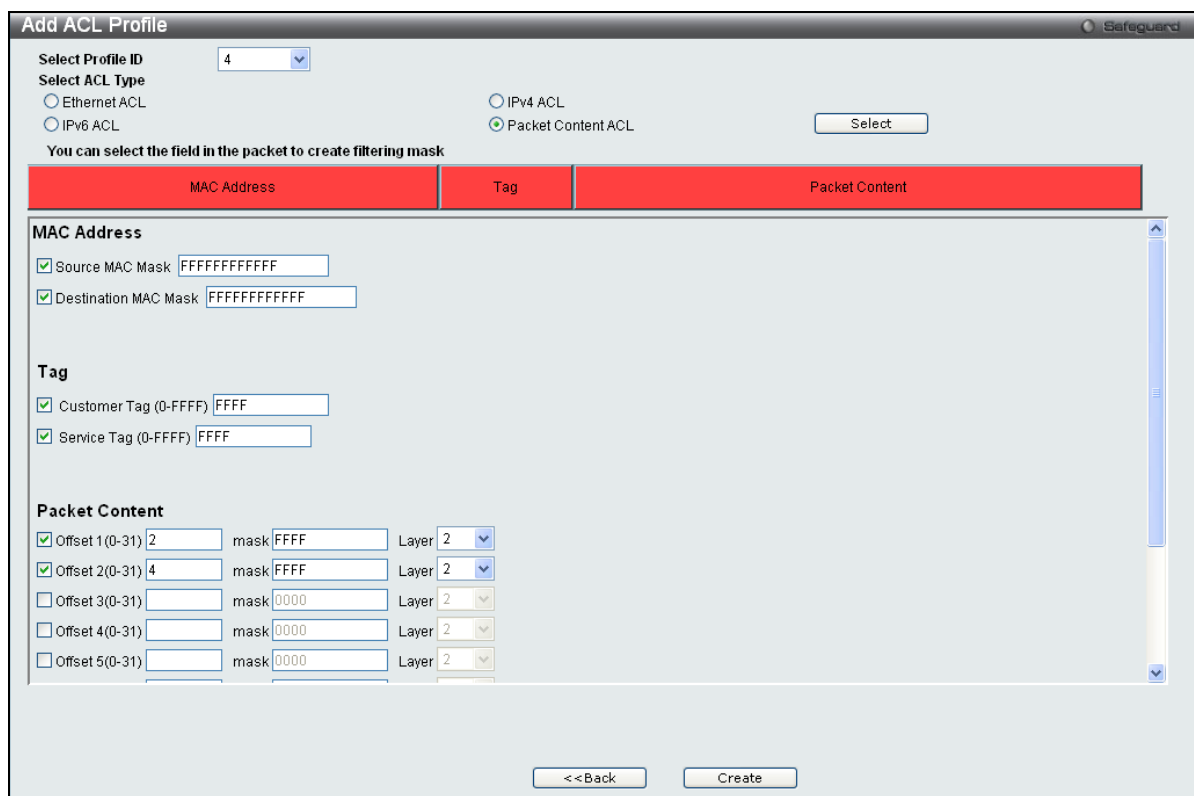


Figure 6 - 66. Add ACL Profile window for Packet Content example

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** window, click **<<Back**.

The following parameters can be set for Packet Content:

Parameter	Description
MAC Address	Tick either Source MAC Mask and enter the MAC source address mask or Destination MAC Mask and enter the MAC destination address mask.
Tag	Tick Customer Tag (0-FFFF) and enter the appropriate customer tag, in hex form (hex 0x0-0xffff), and/or Service Tag (0-FFFF) and enter the appropriate service tag, in hex form (hex 0x0-0xffff).
Packet Content	<p>Allows users to examine up to eleven specified offset packet content chunks within a packet at one time and specifies the frame content offset, mask, and layer. There are eleven packet content chunk offsets that can be configured. A packet content chunk mask presents two bytes. Up to eleven packet content offset chunks can be selected:</p> <p>Offset 1 (0-31) ____mask____ Layer ____, Offset 2 (0-31) ____mask____ Layer ____, Offset 3 (0-31) ____mask____ Layer ____, Offset 4 (0-31) ____mask____ Layer ____, Offset 5 (0-31) ____mask____ Layer ____, Offset 6 (0-31) ____mask____ Layer ____, Offset 7 (0-31) ____mask____ Layer ____, Offset 8 (0-31) ____mask____ Layer ____, Offset 9 (0-31) ____mask____ Layer ____, Offset 10 (0-31) ____mask____ Layer ____, Offset 11 (0-31) ____mask____ Layer ____</p> <p>With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link xStack® 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.</p>

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window 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. To remove all listed profiles, click on the **Delete All** button.

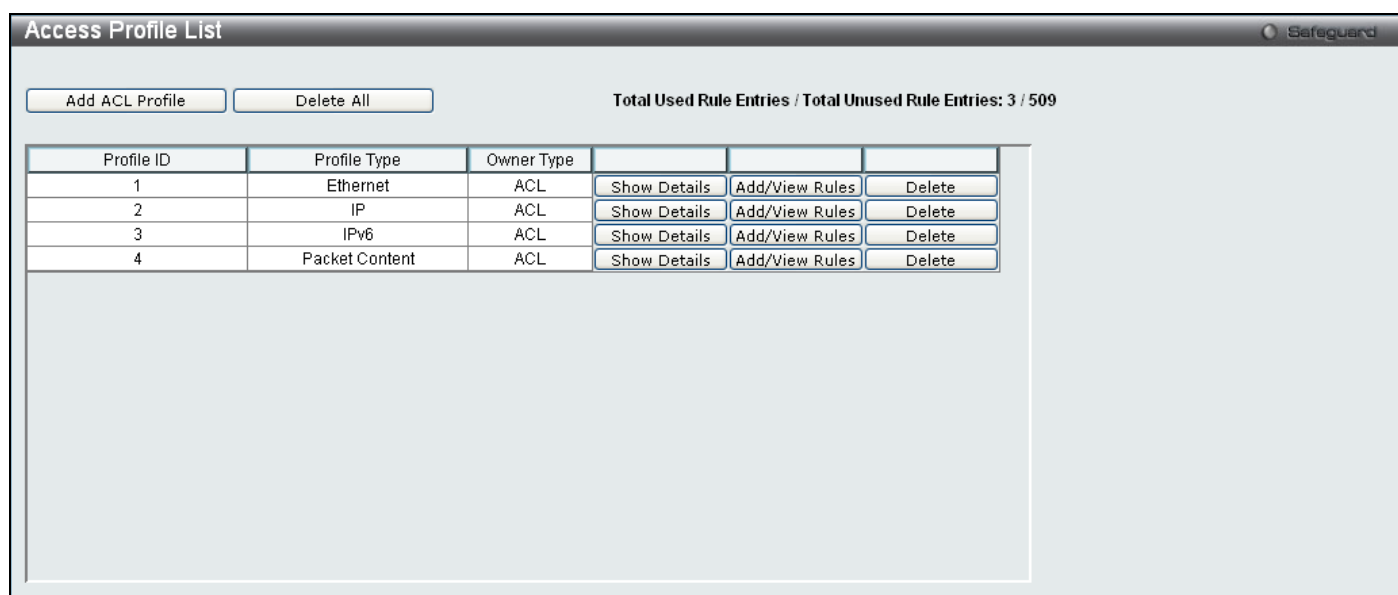


Figure 6 - 67. Access Profile List window for Packet Content example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

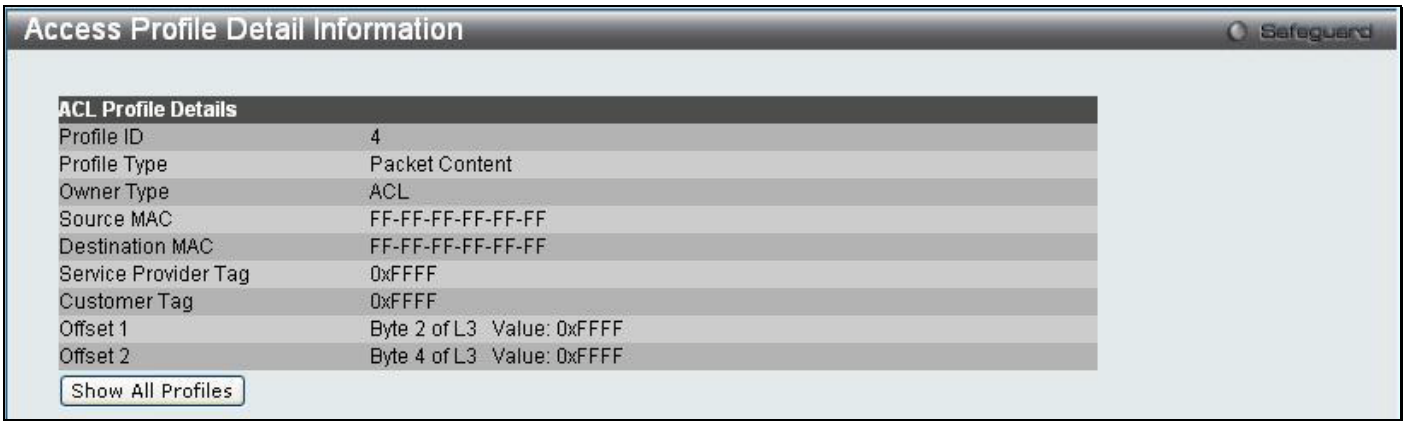


Figure 6 - 68. Access Profile Detail Information window for Packet Content example

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

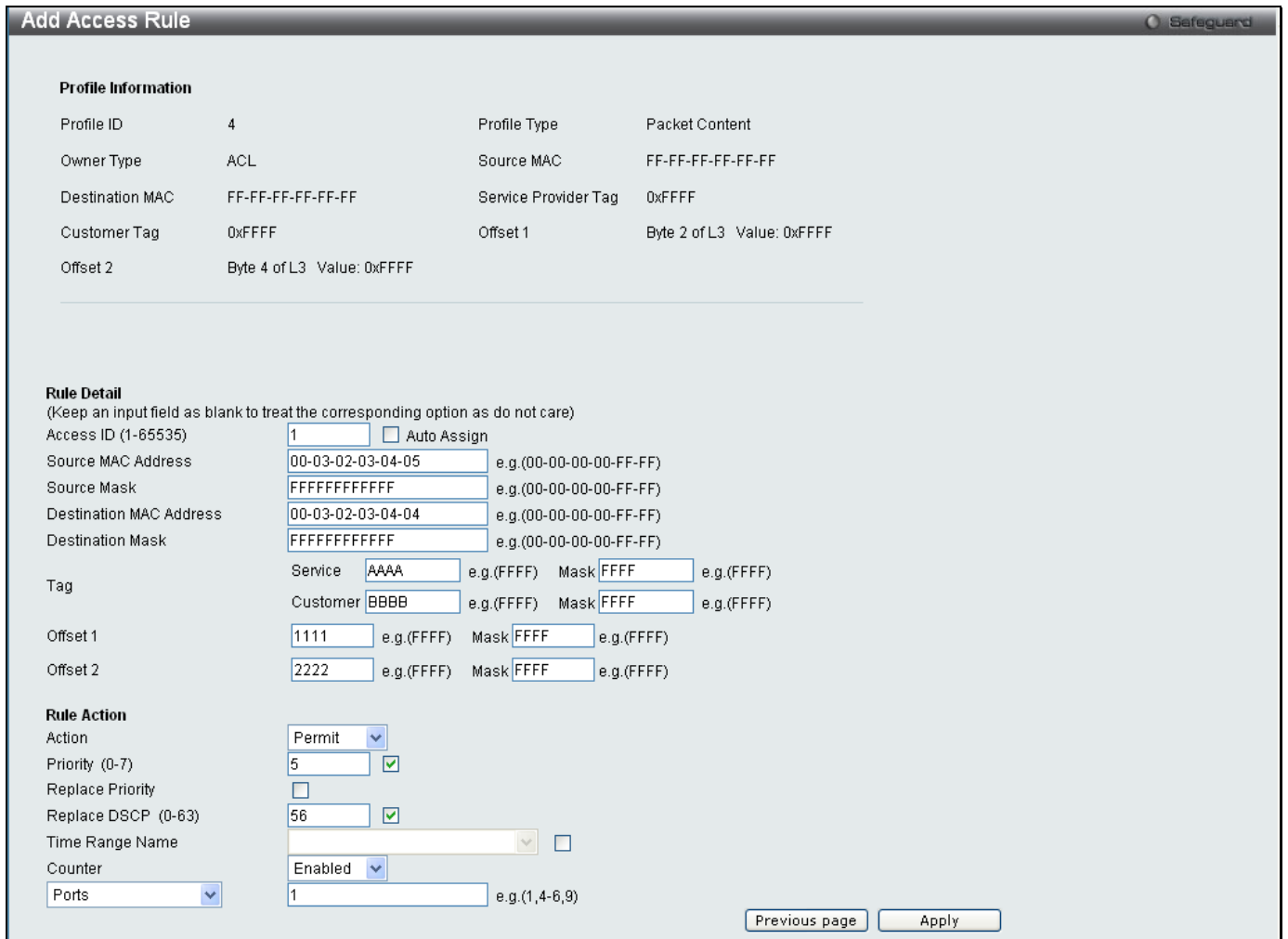


Figure 6 - 69. Add Access Rule window for Packet Content example

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

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from 1 to 65535.
Source MAC Address	Specify the source MAC address of the packets that needed to be examined.
Source Mask	Specify a mask for the source MAC address. The filter is the result of the AND operation between this mask and the source MAC address.
Destination MAC Address	Specify the destination MAC address of the packets that need to be examined.
Destination Mask	Specify a mask for the destination MAC address. The filter is the result of the AND operation between this mask and the destination MAC address.
Tag	Specify the values for customer and service tags which need to be examined. The “mask” options can be used to mask the tag values. That is, the final filter is the result of the AND operation between the customer/service tag values and their corresponding masks.
Offset	Specifies the 2-byte value of the chunk which needs to be examined. The mask option can be used to mask the 2-byte value of the chunk. The final filter is the result of the AND operation between the chunk value and the mask.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> 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 user 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. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Click on the box to enable this option and manually enter the replacement value used to re-write the 802.1p user priority 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.
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 for this ACL rule.
Ports	Enter a range of ports to be configured.

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

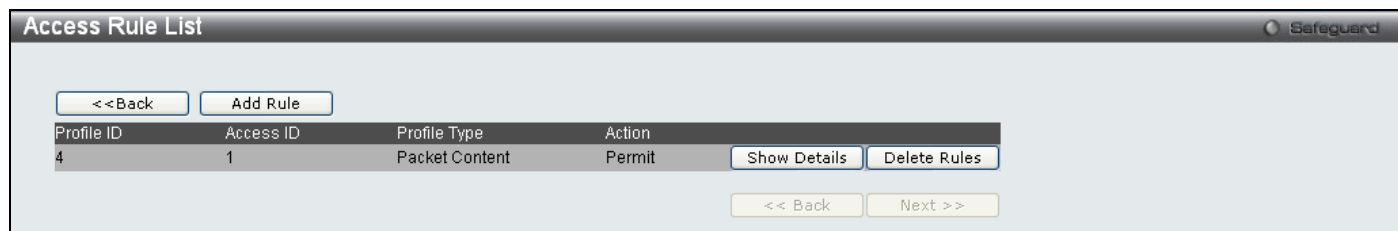


Figure 6 - 70. Access Rule List window for Packet Content example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

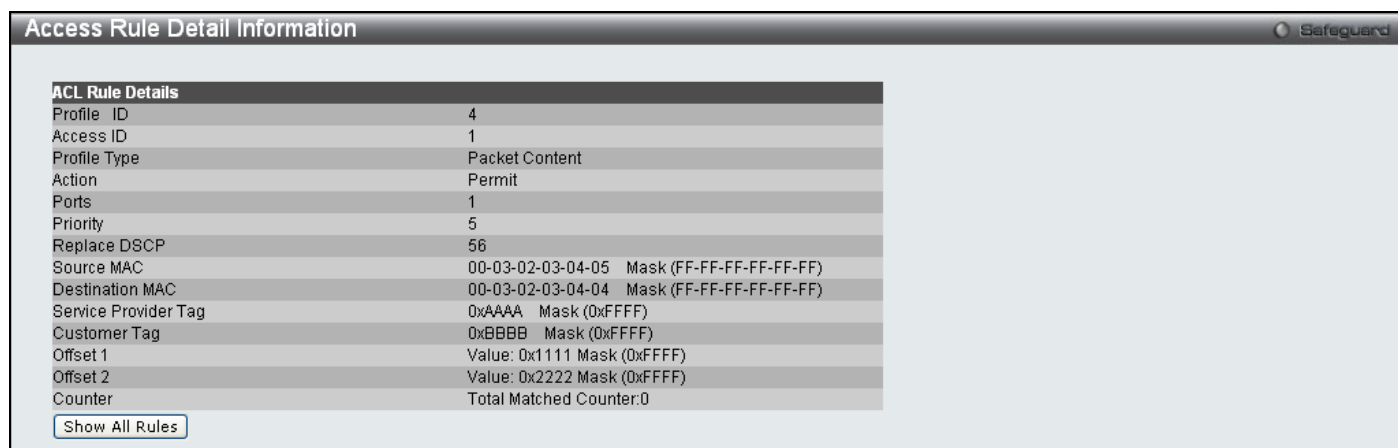


Figure 6 - 71. Access Rule Detail Information window for Packet Content example



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 the section titled ARP Spoofing Prevention Settings on page 58.

CPU Interface Filtering

Due to a chipset limitation and needed extra switch security, the Switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user's implementation. As an added feature for the CPU Filtering, the Switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

Creating an access profile for the CPU is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.

CPU Access Profile List

In the following window, the user may globally enable or disable the CPU Interface Filtering State mechanism by using the radio buttons to change the running state.

To access this window, click **ACL > CPU Access Profile List**

Choose Enabled to enable CPU packets to be scrutinized by the Switch and Disabled to disallow this scrutiny.



Figure 6 - 72. CPU Access Profile List window

This window displays the CPU Access Profile List entries created on the Switch. To view the configurations for an entry, click the corresponding **Show Details** button (once an entry has been created).

To add an entry to the **CPU Access Profile List** window, click the **Add CPU ACL Profile** button. This will open the **Add CPU ACL Profile** window. Click the **Select** button to see the window, as shown below. To remove all CPU Access Profile List entries, click the **Delete All** button.

The Switch supports four CPU Access Profile types: Ethernet (or MAC address-based) profile configuration, IP (IPv4) address-based profile configuration, IPv6 address-based profile configuration, and Packet Content Mask.

The window shown below is the **Add CPU ACL Profile** window for Ethernet:

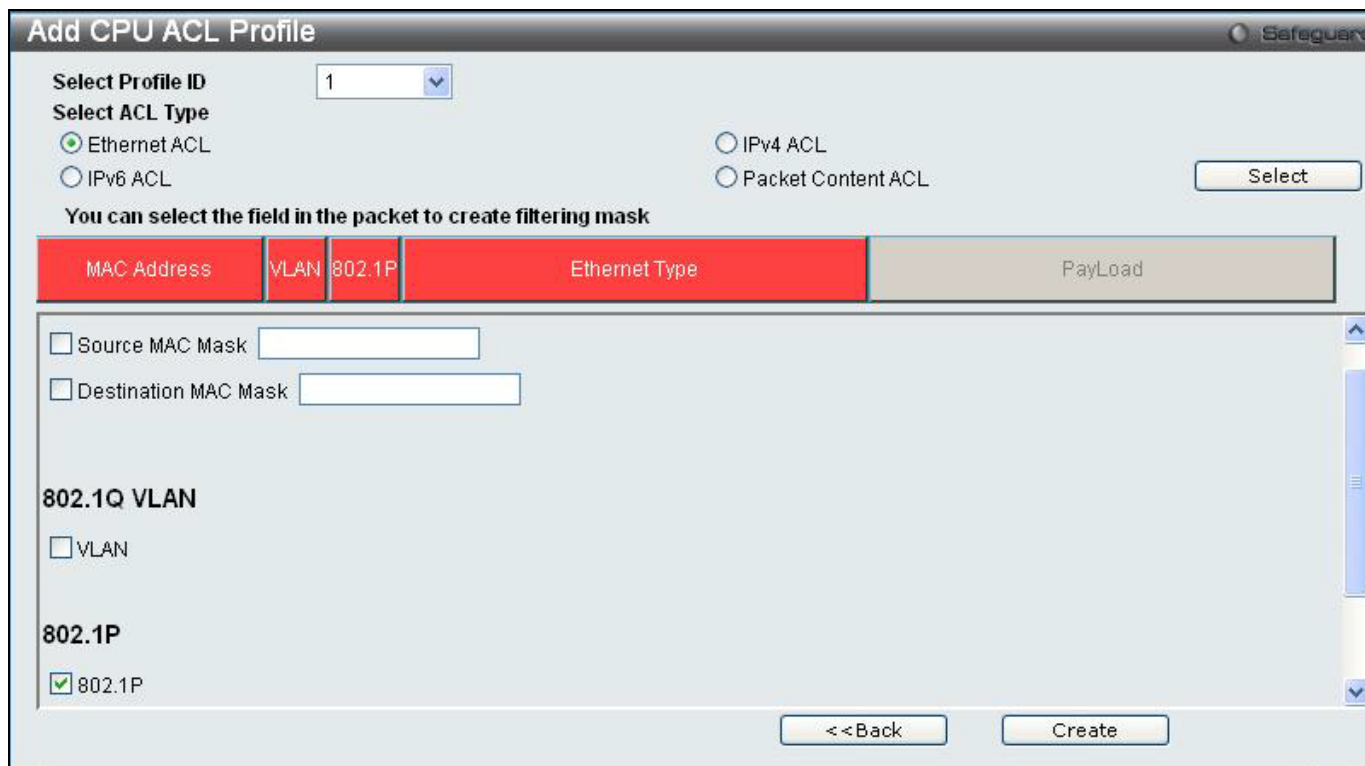


Figure 6 - 73. Add CPU ACL Profile window for Ethernet example

Parameter	Description
Select Profile ID (1-3)	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from 1 to 3.
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 ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content ACL to specify a mask to hide the content of the packet header.
MAC Address	Tick either Source MAC Mask and enter a source MAC address mask for the source MAC address or Destination MAC Mask and enter a destination MAC address mask for the destination MAC address.
802.1Q VLAN	Ticking 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	Ticking this option instructs the Switch to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Ticking this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **Apply** to set this entry in the Switch's memory.

The following **CPU Access Profile List** window opens:



Figure 6 - 74. CPU Access Profile List window for Ethernet example

To view the settings of a previously correctly created profile, click the corresponding **Show Details** button on the following **CPU Access Profile List** window above. The following window opens:

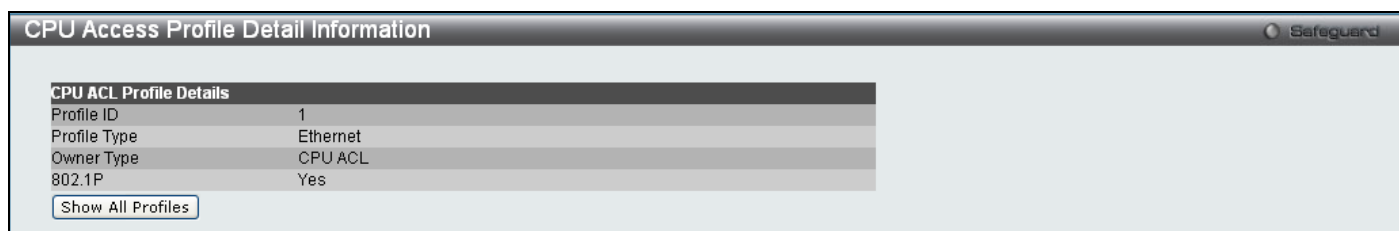


Figure 6 - 75. CPU Access Profile Detail Information window for Ethernet

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

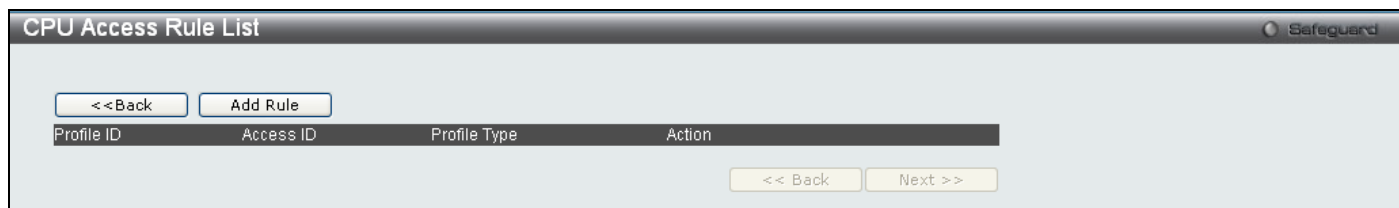


Figure 6 - 76. initial CPU Access Rule List window

Click **Add Rule**, which will reveal the following window:

Figure 6 - 77. (CPU) Add Access Rule window for Ethernet example

Profile Information and the available configuration parameters viewable in the menu will vary depending on the options that were chosen in the **Add CPU Access Profile** menu. To set the **Access Rule for Ethernet**, adjust the following parameters as applicable for the CPU Access Profile being configured and click **Apply**.

Parameter	Description
Access ID (1-5)	Type in a unique identifier number for this access. This value can be set from 1 to 5.
VLAN	Use this to specify that the access profile will apply to only to the VLAN in the VLAN Name field.
MAC Address	Specify that the access profile will apply to the Source MAC Address , and/or Destination MAC Address .
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.
Ethernet Type	Specify access profile is applied to the Ethernet type value in each frame's header.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

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



Figure 6 - 78. CPU Access Rule List window for Ethernet example

To view the configurations for previously configured rules, click on the corresponding **Show Details** button, which will display the following **CPU Access Rule Detail Information** window:

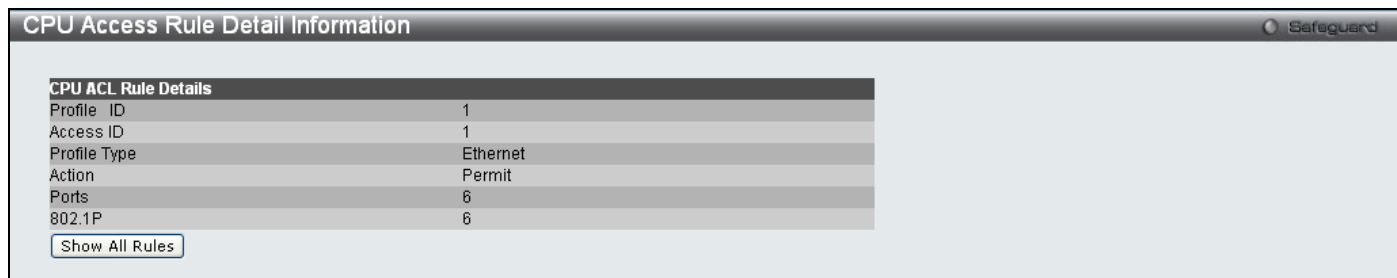


Figure 6 - 79. CPU Access Rule Detail Information window for Ethernet example

To create an IPv4 ACL, click **Add CPU ACL Profile** in the **CPU Access Profile List** window. This will open the **Add CPU ACL Profile** window. Use the drop-down menu to select a Profile ID between 1 and 3, click the IPv4 ACL radio button, and then use the drop-down menu to select a protocol *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID*. Click **Select** and the following window will appear (this window will vary depending on whether *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID* has been selected):

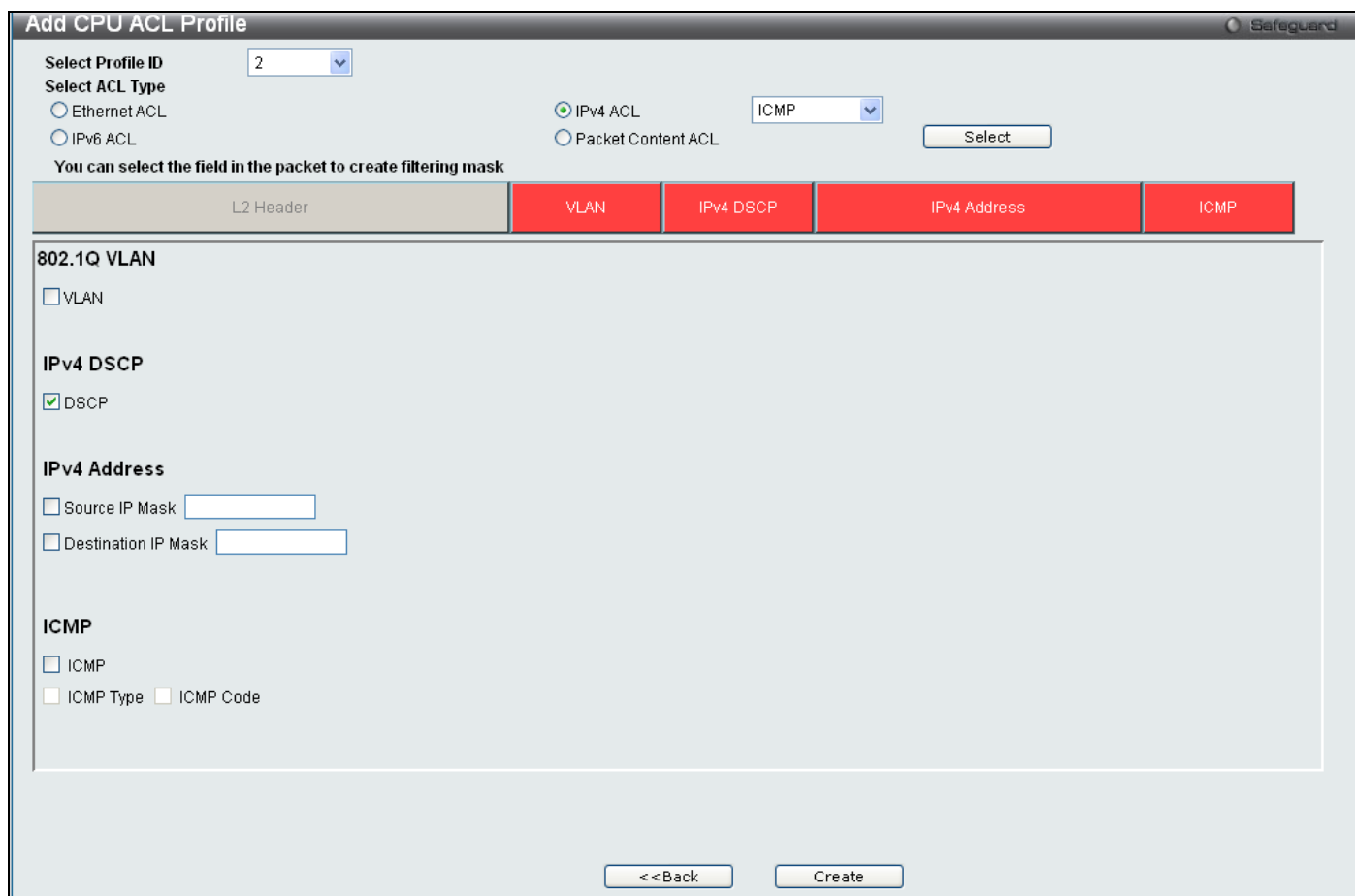


Figure 6 - 80. Add CPU ACL Profile window for IPv4 example

Click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration. To create a new entry, enter the appropriate information and click **Create**. To return to the **CPU Access Profile List**, menu click **<<Back**.

The following parameters can be set for IPv4:

Parameter	Description
Select Profile ID	Enter an integer used to identify the access profile that will be configured with this command.
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Address	Tick either Source IP Mask and enter the IPv4 source address mask or Destination IP Mask and enter the IPV4 destination address mask.
ICMP	Tick ICMP to specify that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet. Tick ICMP Type to specify that the access profile will apply to this ICMP type value. Tick ICMP Code to specify that the access profile will apply to this ICMP code value.
IGMP	Tick IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Tick IGMP Type to further specify that the access profile will apply an IGMP type value.
TCP	Tick TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Ticking TCP requires specifying 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. T <ul style="list-style-type: none"> ▪ Source Port Mask (0-FFFF) – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). ▪ Destination Port Mask (0-FFFF) – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff). ▪ TCP Flag Bits – Tick URG (urgent), ACK (acknowledgement), PSH (push), RST (reset), SYN (synchronize), FIN (finish), or Check All to filter certain flag bits within the packets.
UDP	Tick UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Ticking UDP requires specifying a source port mask and/or a destination port mask. <ul style="list-style-type: none"> ▪ Source Port Mask – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). ▪ Destination Port Mask – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff).
Protocol ID	Tick Protocol ID Mask and enter a value defining the protocol ID in the packet header to mask. Protocol ID Mask (0-FF) – Tick and enter a value defining the mask options behind the IP header. User Define (0-FFFFFFFF) – Tick and enter a user-defined value.

Click **Apply** to implement changes made.

Click **Create** to view the new CPU Access Profile List entry in the **CPU Access Profile List** window shown below. To add another Access Profile click **Add CPU 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 CPU Access Profile entry, click the **Add/View Rules** button.

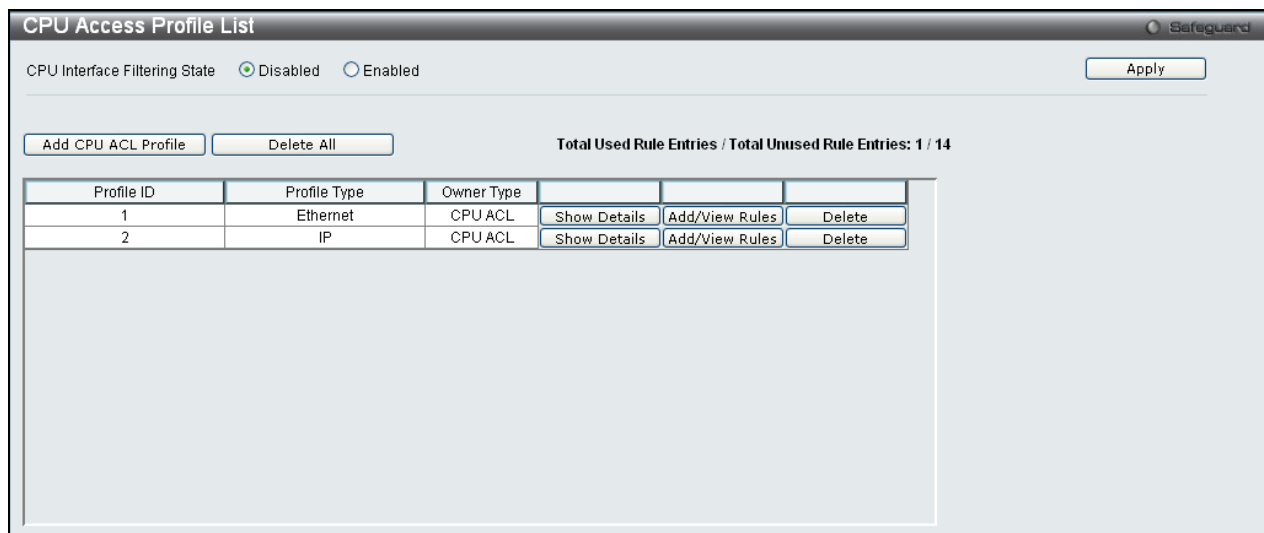


Figure 6 - 81. CPU Access Profile List window for IPv4 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

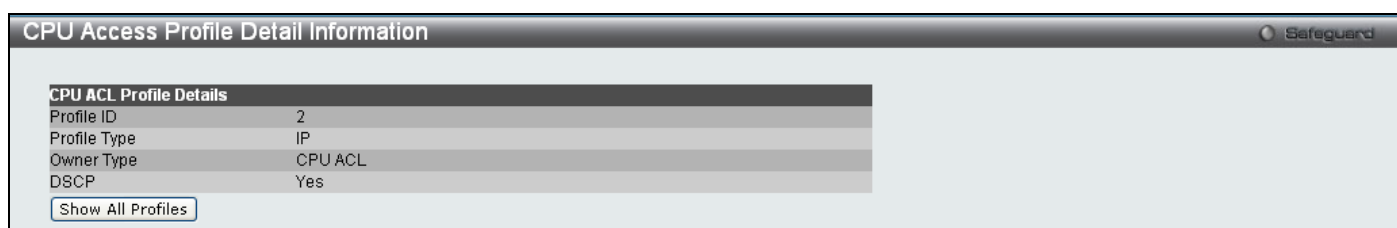


Figure 6 - 82. CPU Access Profile Detail Information window for IPv4 example

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

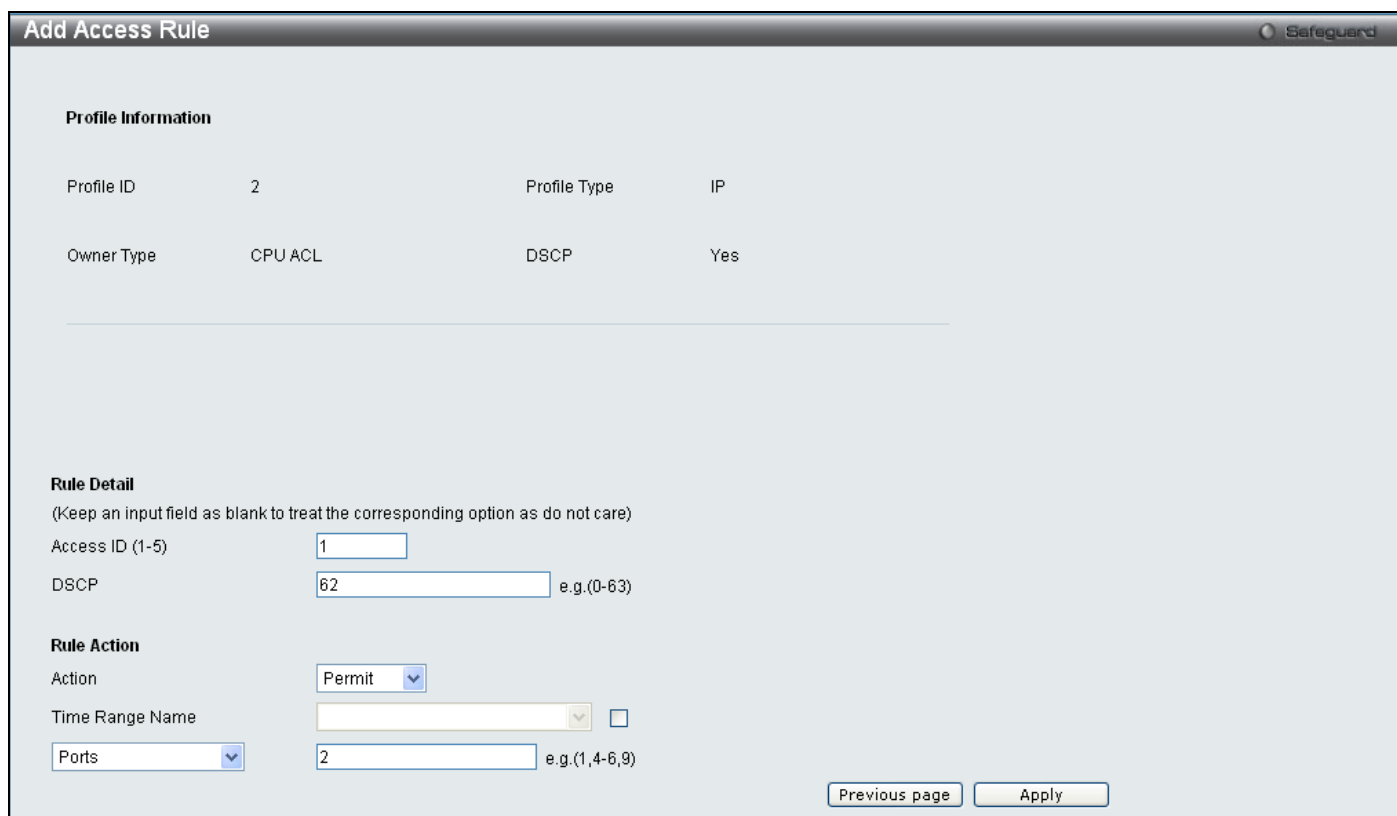


Figure 6 - 83. (CPU) Add Access Rule window for IPv4 example

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

Parameter	Description
Access ID (1-5)	Type in a unique identifier number for this access. This value can be set from 1 to 5.
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.
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.
IP Address	Select the option and enter the Source IP Address or the Destination IP Address. This will be used as the criteria for forwarding decisions.
IGMP	Tick <i>IGMP</i> to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Tick <i>IGMP Type</i> to further specify that the access profile will apply an IGMP type value.
UDP	Tick <i>TCP</i> to use the TCP port number contained in an incoming packet as the forwarding criterion. Ticking TCP requires specifying 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.
TCP	Tick <i>UDP</i> to use the UDP port number contained in an incoming packet as the forwarding criterion. Ticking UDP requires specifying a source port mask and/or a destination port mask.
ICMP	Select <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **CPU Access Rule List** window:



Figure 6 - 84. CPU Access Rule List window for IPv4 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **CPU Access Rule Detail Information** window:

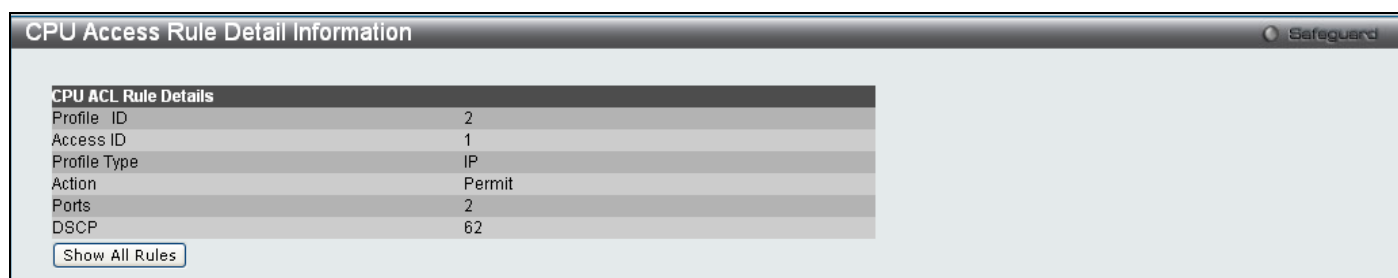


Figure 6 - 85. CPU Access Rule Detail Information window for IPv4 example

To create an IPv6 ACL, click **Add CPU ACL Profile** in the **CPU Access Profile List** window and then use the drop-down menu to select a Profile ID between 1 and 3 and click the IPv6 ACL radio button. Click **Select** and the following window will appear:

Figure 6 - 86. Add CPU ACL Profile window for IPv6 example

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 **CPU Access Profile List** window, click **<<Back**.

The following parameters can be set for IPv6:

Parameter	Description
Select Profile ID	Enter an integer used to identify the access profile that will be configured with this command.
IPv6 Class	Ticking this check box will instruct the Switch to examine the class field of the IPv6 header. The 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. The 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 Address	IPv6 Source Address – Enter an IPv6 address to be used as the source address. IPv6 Destination Address – Enter an IPv6 address that will be used as the destination address.

Click **Apply** to implement changes made.

Click **Create** to view the new CPU Access Profile List entry in the **CPU Access Profile List** window shown below. To add another Access Profile, click **Add CPU 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 CPU Access Profile entry, click the **Add/View Rules** button.

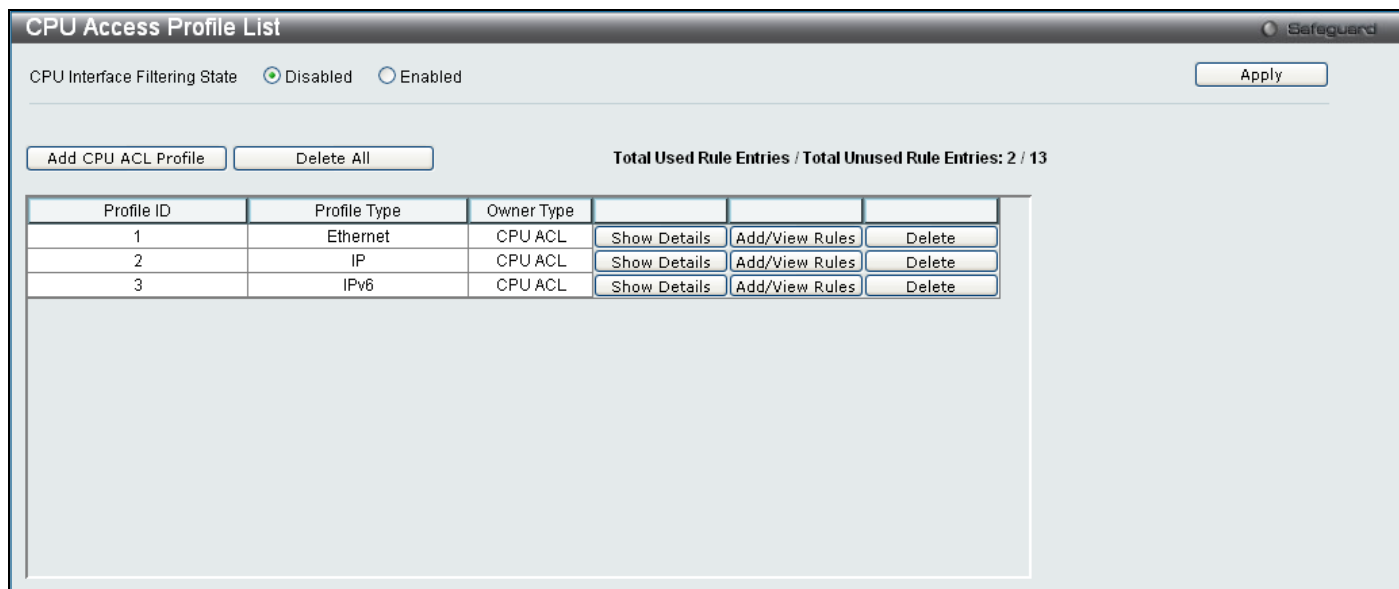


Figure 6 - 87. CPU Access Profile List window for IPv6 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

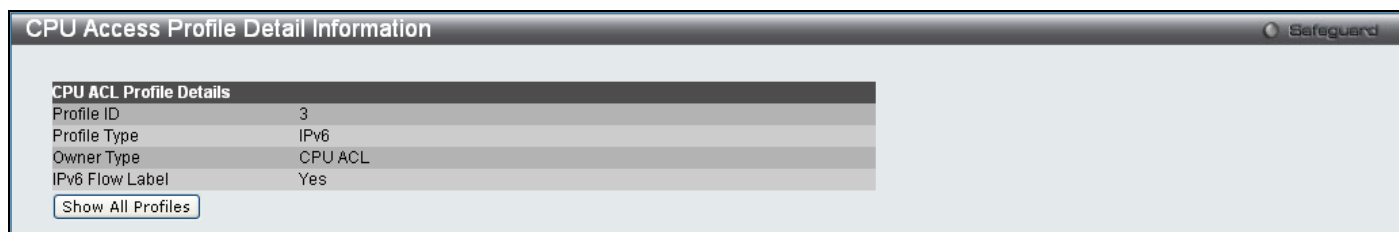


Figure 6 - 88. CPU Access Profile Detail Information window for IPv6 example

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

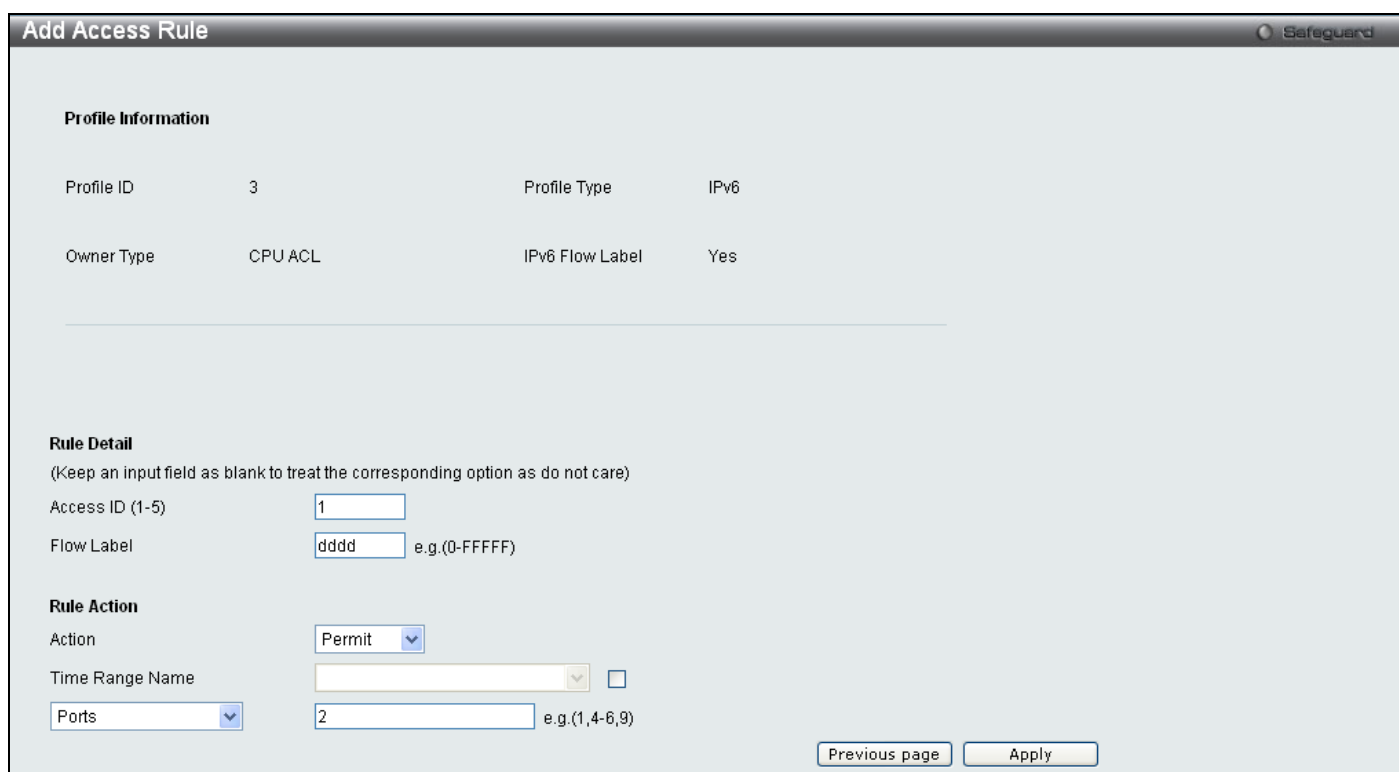


Figure 6 - 89. (CPU) Add Access Rule window for IPv6 example

The following parameters may be configured for the IPv6:

Parameter	Description
Access ID (1-5)	Type in a unique identifier number for this access. This value can be set from 1 to 5.
Flow Label	Specifies the IPv6 Flow Label. Enter a value between 0 – FFFFF.
IPv6 Address	Denotes that IPv6 packets will have Source or Destination IPv6 Address examined by the Switch for forwarding or filtering based on the rules configured. IPv6 packets may be identified by the following:
Class	Entering this parameter will instruct the Switch to examine the class field of the IPv6 header that is similar to the Type of Service (ToS) or Precedence bits field in Ipv4.
Action	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

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

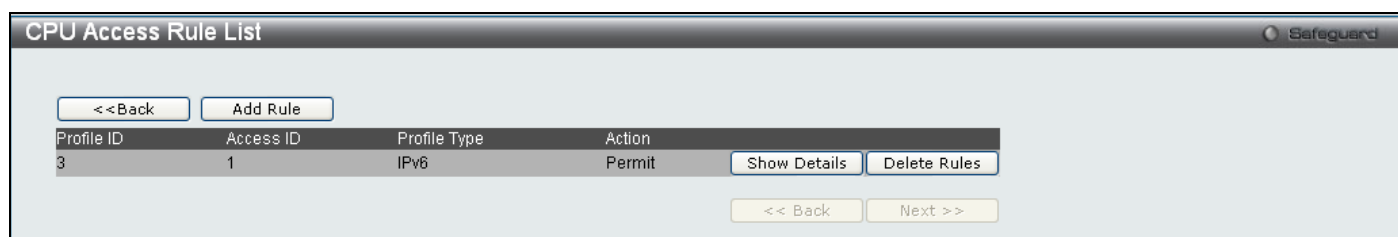


Figure 6 - 90. CPU Access Rule List window for IPv6 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **CPU Access Rule Detail Information** window:

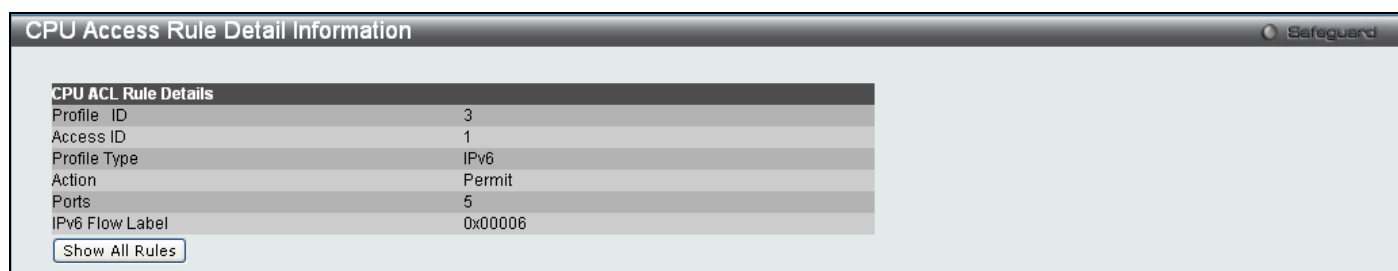


Figure 6 - 91. CPU Access Rule Detail Information window for IPv6 example

To create a Packet Content ACL, click **Add CPU ACL Profile** in the **CPU Access Profile List** window and then use the drop-down menu to select a Profile ID between 1 and 3 and click the Packet Content ACL radio button. Click **Select** and the following window will appear:

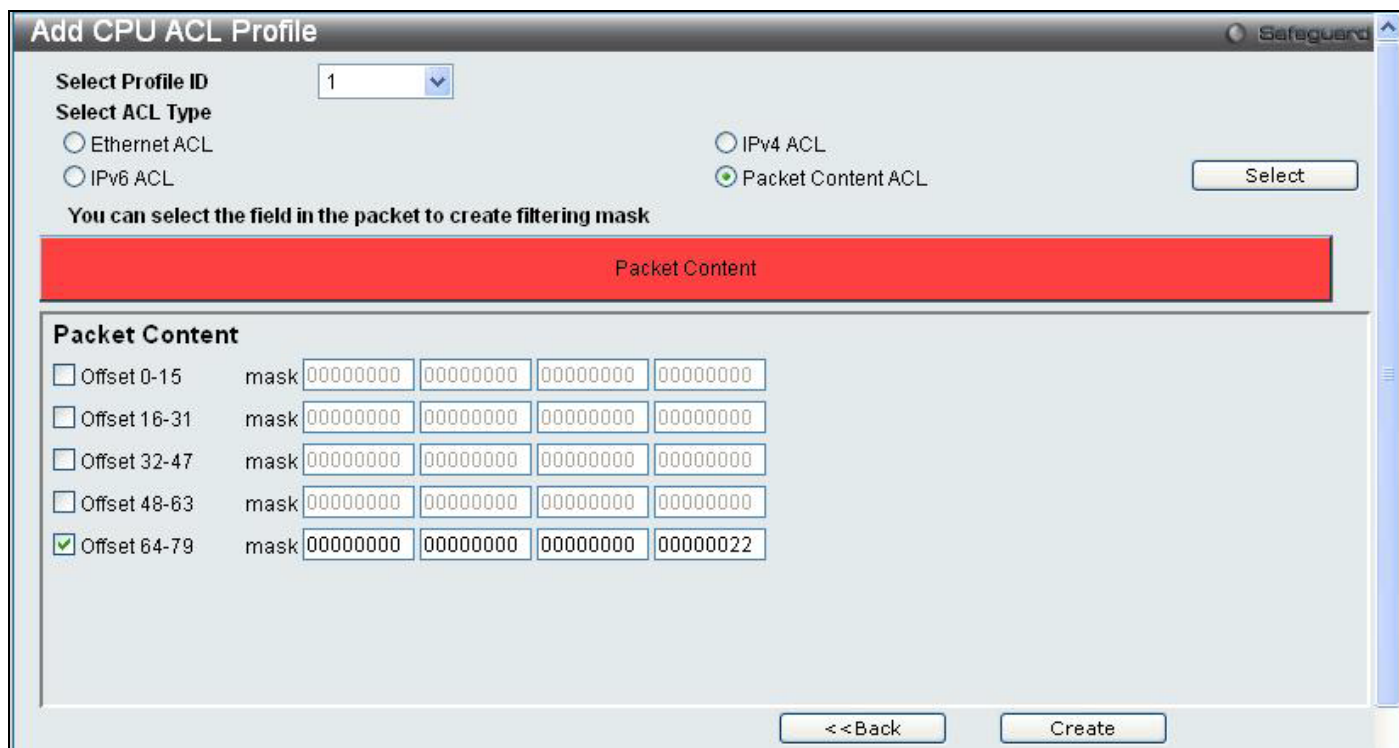


Figure 6 - 92. Add CPU ACL Profile window for Packet Content example

Click on the box 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 **CPU Access Profile List** window, click **<<Back**.

The following parameters can be set for Packet Content:

Parameter	Description
Select Profile ID	Enter an integer used to identify the access profile that will be configured with this command.
Packet Content	<p>Allows users to examine up to five specified offset packet content chunks within a packet at one time and specifies the frame content offset, mask, and layer. There are five packet content chunk offsets that can be configured. A packet content chunk mask presents four bytes. Up to five packet content offset chunks can be selected:</p> <p>Offset 0-15 mask - Enter a value in hex form to mask the packet from byte 0 to byte 15.</p> <p>Offset 16-31 mask - Enter a value in hex form to mask the packet from byte 16 to byte 31.</p> <p>Offset 32-47 mask - Enter a value in hex form to mask the packet from byte 32 to byte 47.</p> <p>Offset 48-63 mask - Enter a value in hex form to mask the packet from byte 48 to byte 63.</p> <p>Offset 64-79 mask - Enter a value in hex form to mask the packet from byte 64 to byte 79.</p> <p>Note: Only one packet content mask profile can be created.</p> <p>With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link xStack® 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.</p>

Click **Apply** to implement changes made.

Click **Create** to view the new CPU Access Profile List entry in the **CPU Access Profile List** window shown below. To add another CPU Access Profile, click **Add CPU 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 CPU Access Profile entry, click the **Add/View Rules** button.

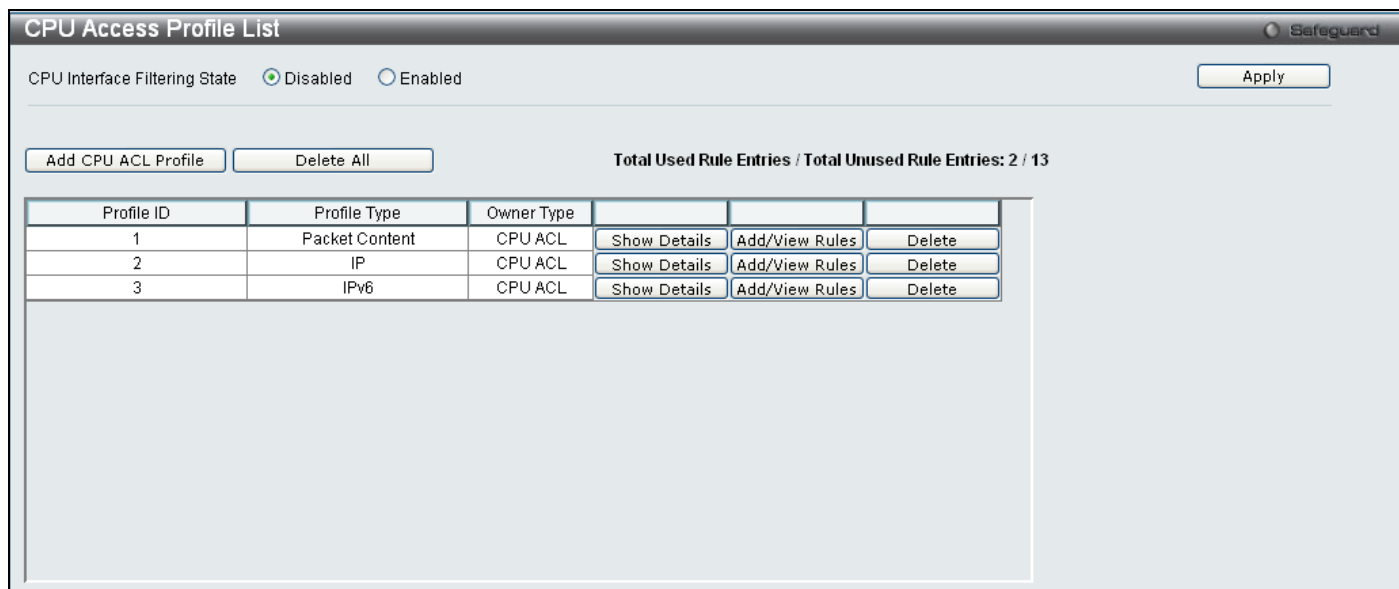


Figure 6 - 93. CPU Access Profile List window for Packet Content example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

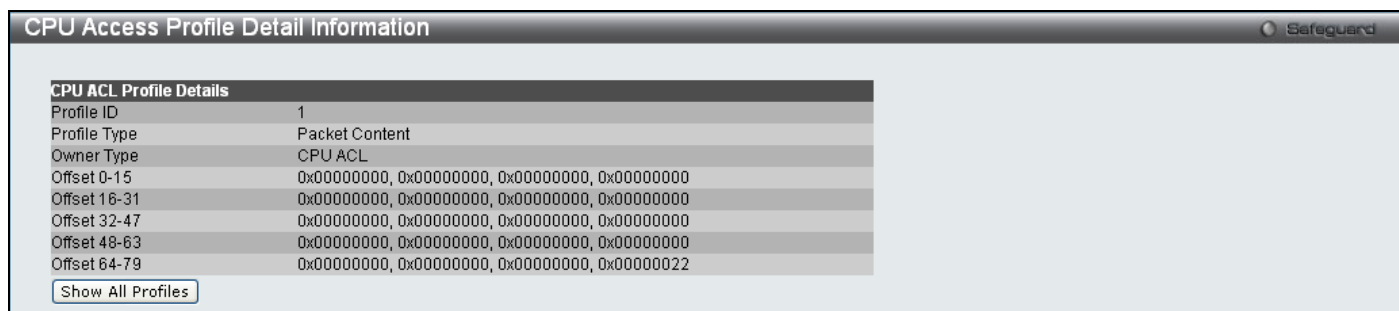


Figure 6 - 94. CPU Access Profile Detail Information window for Packet Content example

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

Add Access Rule
Safeguard

Profile Information

Profile ID	1	Profile Type	Packet Content
Owner Type	CPU ACL	Offset 0-15	0x00000000, 0x00000000, 0x00000000, 0x00000000
Offset 16-31	0x00000000, 0x00000000, 0x00000000, 0x00000000	Offset 32-47	0x00000000, 0x00000000, 0x00000000, 0x00000000
Offset 48-63	0x00000000, 0x00000000, 0x00000000, 0x00000000	Offset 64-79	0x00000000, 0x00000000, 0x00000000, 0x00000022

Rule Detail
(Keep an input field as blank to treat the corresponding option as do not care)

Access ID (1-5)

Offset 0-15
 Offset 16-31
 Offset 32-47
 Offset 48-63
 Offset 64-79

Rule Action

Action: Permit

Time Range Name:

Ports: 9 e.g.(1,4-6,9)

Previous page
Apply

Figure 6 - 95. (CPU) Add Access Rule window for Packet Content example

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

Parameter	Description
Select Profile ID	Enter an integer used to identify the access profile that will be configured with this command.
Rule Detail	<p>This field will instruct the Switch to mask the packet header beginning with the offset value specified:</p> <p>Offset 0-15 – Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte.</p> <p>Offset 16-31 – Enter a value in hex form to mask the packet from byte 16 to byte 31.</p> <p>Offset 32-47 – Enter a value in hex form to mask the packet from byte 32 to byte 47.</p> <p>Offset 48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63.</p> <p>Offset 64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79.</p>
Action	<p>Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).</p> <p>Select <i>Deny</i> to specify the packets that match the access profile are not forwarded by the Switch and will be filtered.</p>
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **CPU Access Rule List** window:

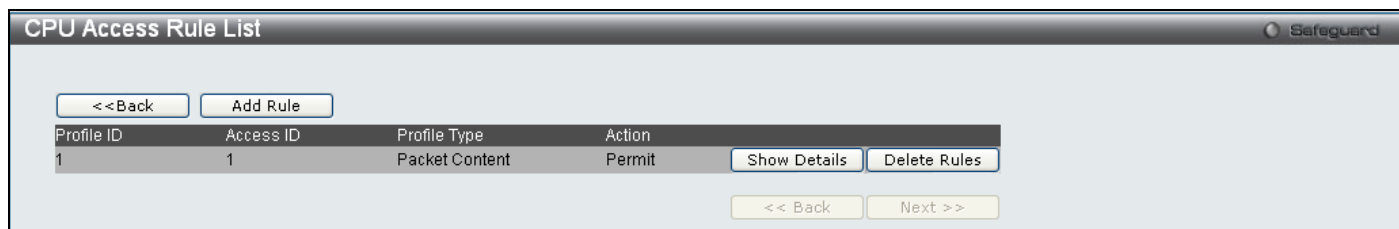


Figure 6 - 96. CPU Access Rule List window for Packet Content example

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

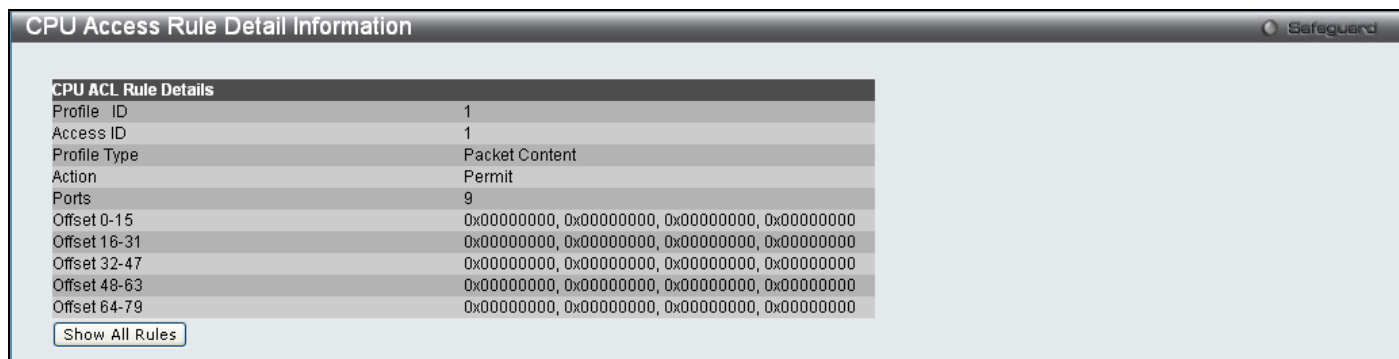


Figure 6 - 97. CPU Access Rule Detail Information window for Packet Content example

ACL Finder

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

To open this window, click **ACL > ACL Finder**

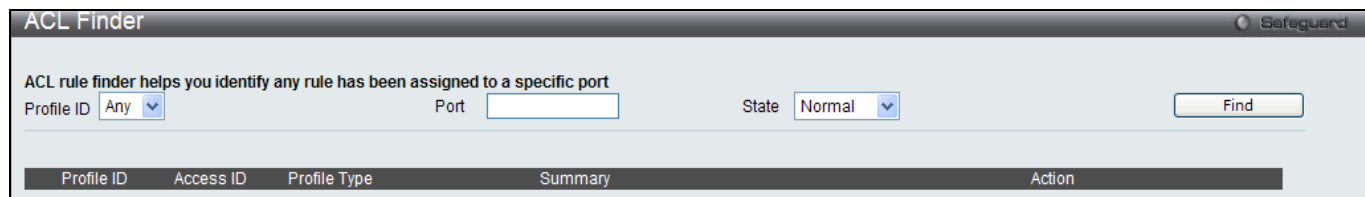


Figure 6 - 98. ACL Finder window

ACL Flow Meter

This window offers flow bandwidth control used to limit the bandwidth of the ingress traffic. When users create an ACL rule to filter packets, a metering rule can be created to associate with this ACL rule to limit traffic. The step of bandwidth is 64kbps. Due to limited metering rules, not all ACL rules can associate with a metering rule.

To open this window, click **ACL > ACL Flow Meter**

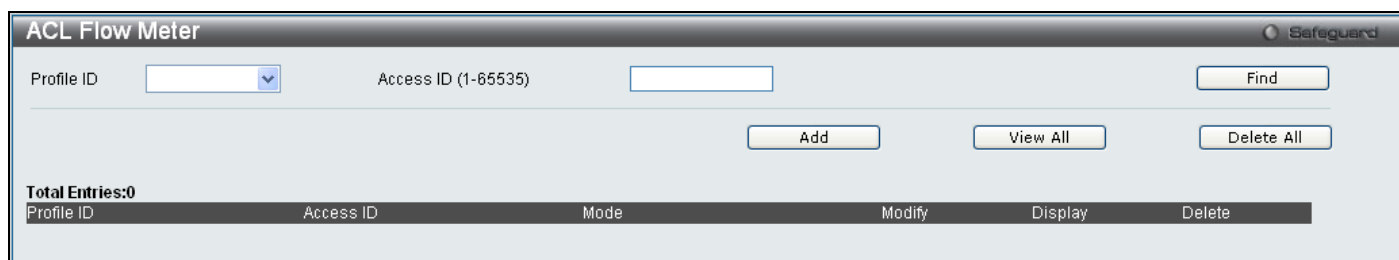


Figure 6 - 99. ACL Flow Meter window

The following fields may be configured:

Parameter	Description
Profile ID	The pre-configured Profile ID for which to configure the Flow Metering parameters.
Access ID (1-65535)	The pre-configured Access ID for which to configure the Flow Metering parameters.

Enter the appropriate information and click **Find**. The entries will be displayed on the lower half of the table. To edit an entry, click the corresponding **Modify** button. To delete an entry, click the corresponding **Delete** button. To add a new entry, click the **Add** button, which will display the following window for the user to configure:

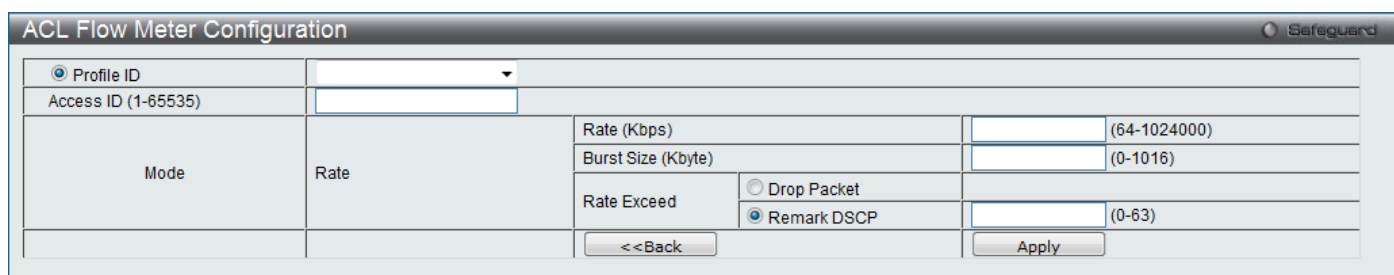


Figure 6 - 100. ACL Flow Meter Configuration window

The following fields may be configured:

Parameter	Description
Profile ID	Use the drop-down menu to select the pre-configured Profile ID that will be used to configure the Flow Metering parameters.
Access ID (1-65535)	Enter the Access ID that will be used to configure the Flow Metering parameters, enter a value between 1 and 65535.
Mode	Single-rate Two-Color Marker, marks packets green or red based on a rate and burst size. This is useful when only burst size matters. <ul style="list-style-type: none"> Rate (64-1024000) Kbps – Specifies the committed bandwidth in Kbps for the flow. The range is from 64 to 1024000. The unit is Kbps. Burst Size (0-1016) Kbyte – Specifies the burst size for this flow. The range is from 0 to 1016. The unit is Kbyte.
Action	Violate – Specifies the action when the packet is in “red color” mode. <ul style="list-style-type: none"> Remark DSCP – Change the DSCP of the packet. Drop – Drops the packet.

Click **Apply** to implement changes made, click **<<Back** to return to the **ACL Flow Meter** window.

Section 7

Monitoring

Cable Diagnostics

CPU Utilization

Port Utilization

Packet Size

Memory Utilization

Packets

Errors

Port Access Control

Browse ARP Table

Browse VLAN

IGMP Snooping

LLDP

Ethernet OAM

Connectivity Fault Management

MAC-based Access Authentication State

Browse Session Table

MAC Address Table

System Log

Cable Diagnostics

This window displays the details of copper cables attached to specific ports on the Switch. If there is an error in the cable this feature can determine the type of error and the position where the error has occurred.

To view this window, click **Monitoring > Cable Diagnostics**:

Port	Type	Link Status	Test Result	Cable Length(M)
<p>The Cable Diagnostic is designed primarily for administrators or customer service representative to view tests on copper cables, it can rapidly determine where errors occurred in the cable and the type of cable error which occurred.</p> <p>Note: The Cable Fault Distance is calculated from switch side.</p>				

Figure 7 - 1. Cable Diagnostics window

Enter the range of ports to test and click **Test**. The results will be displayed in the table on the lower half of the window.



NOTE: If the Link Status field for an interface displays "Link Up", the value displayed in the Cable Length field may not be accurate for the interface.

CPU Utilization

This 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 **Monitoring > CPU Utilization**:

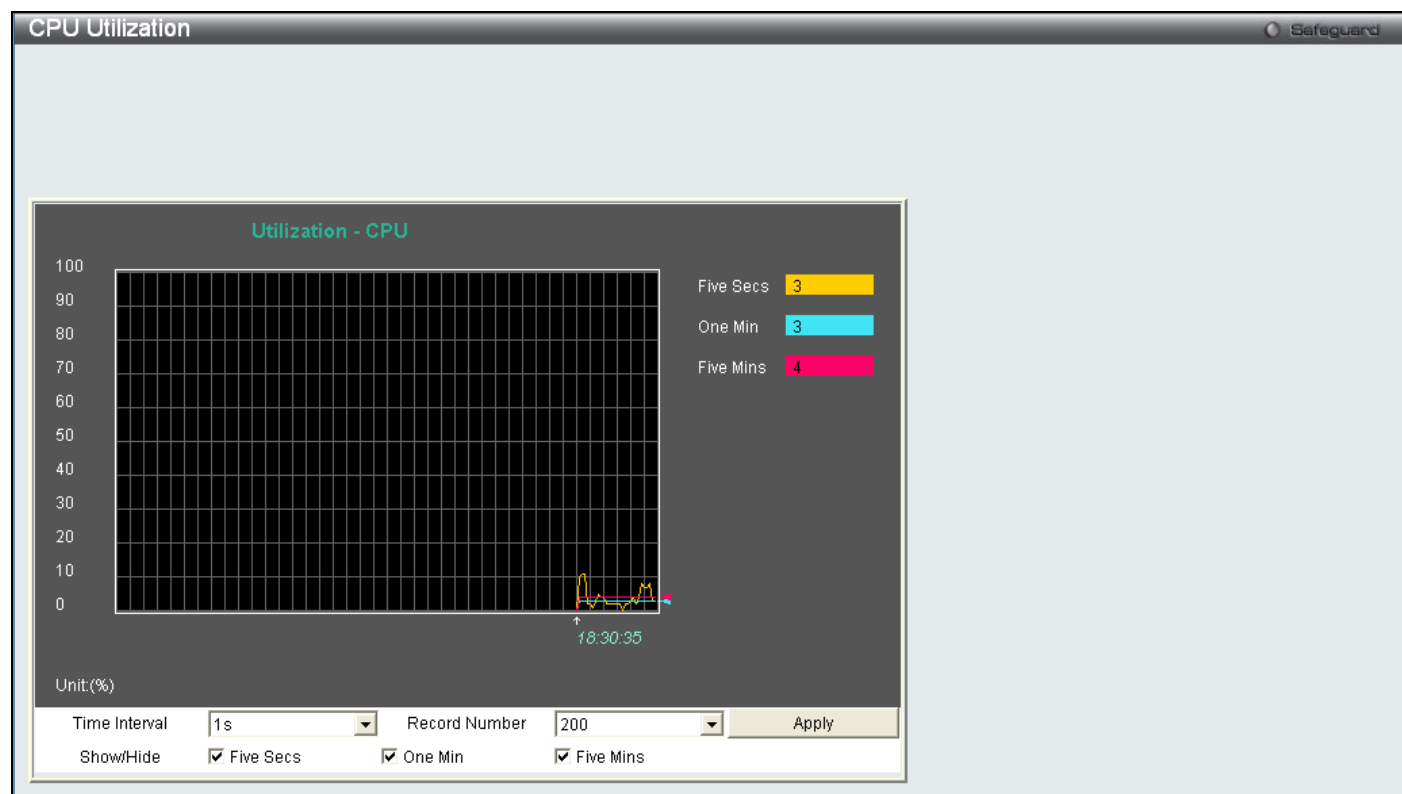


Figure 7 - 2. CPU Utilization window

To view the CPU utilization by port, use the real-time graphic of the Switch 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

This window displays the percentage of the total available bandwidth being used on the port.

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

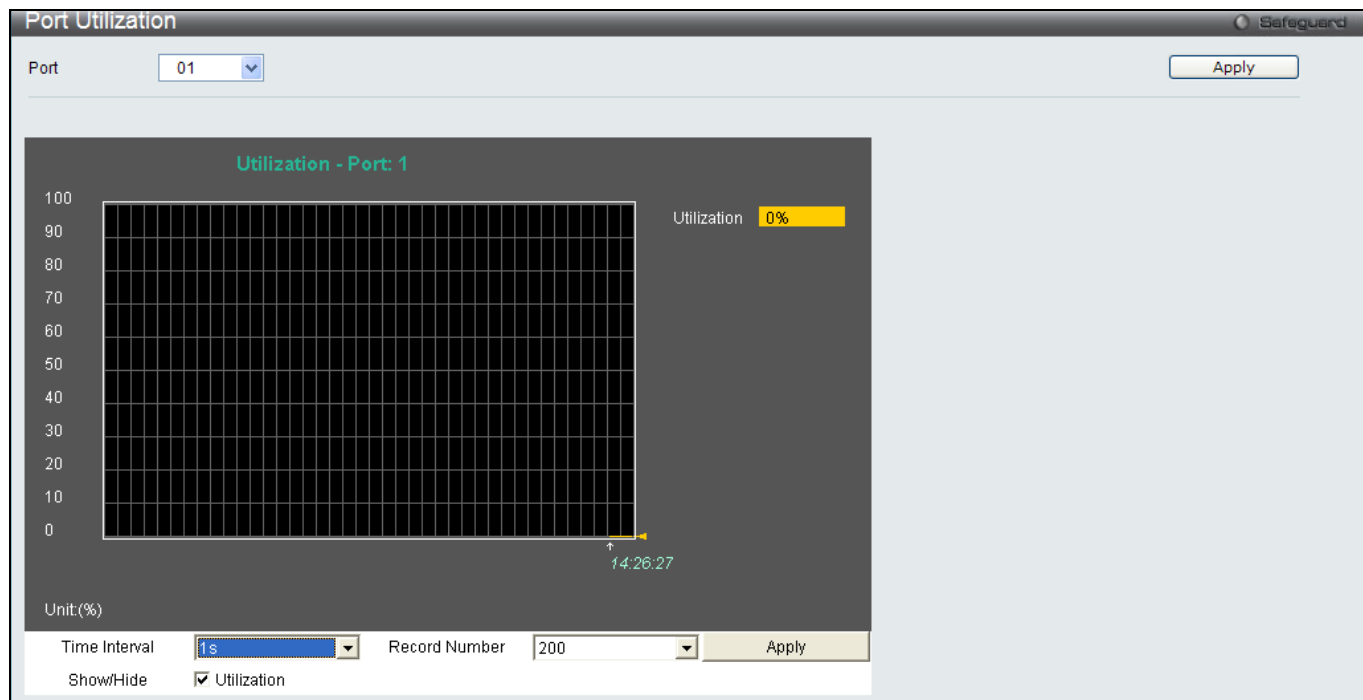


Figure 7 - 3. Port Utilization window

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

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 <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is <i>200</i> .
Show/Hide	Check whether or not to display Utilization.

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 the packet size windows, click **Monitoring > Packet Size**:

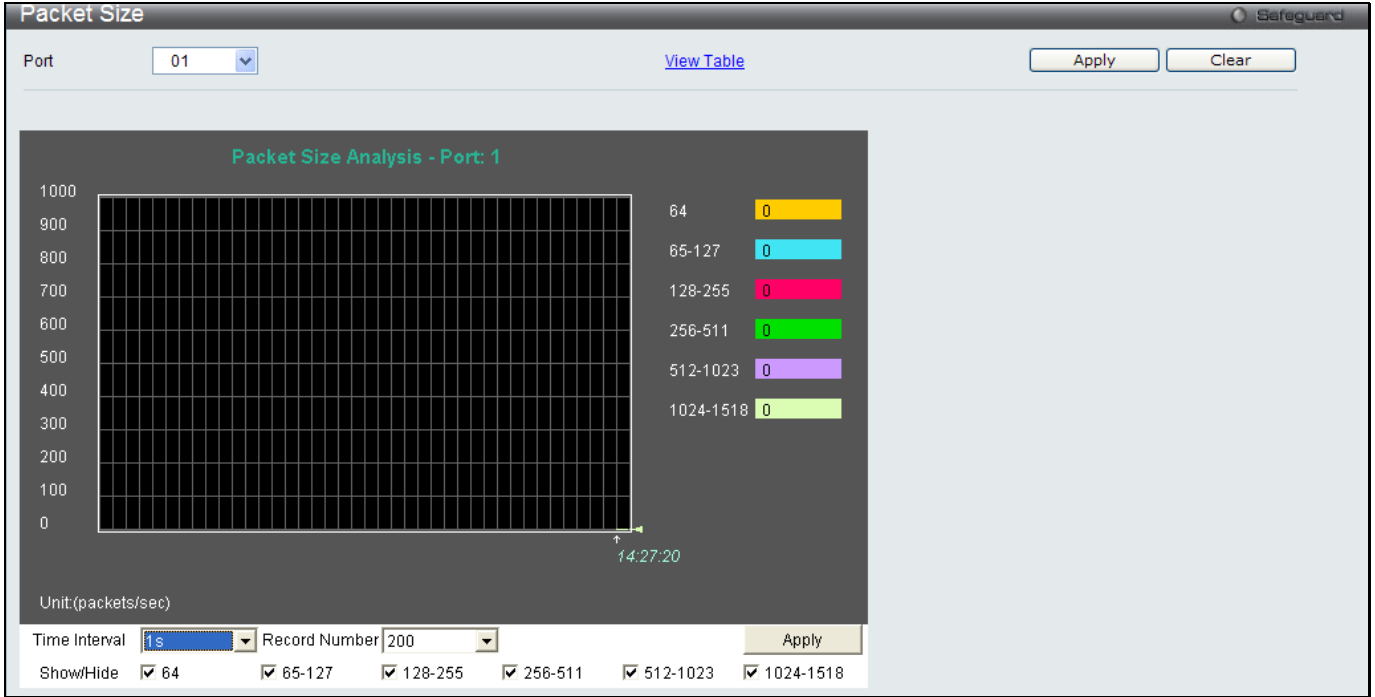


Figure 7 - 4. Packet Size window

To view the **Packet Size Table** window, click the link [View Table](#), which will show the following table:

The screenshot shows the 'Packet Size Table' window. At the top, there is a 'Port' dropdown menu set to '01', a 'View Graphic' link, and 'Apply' and 'Clear' buttons. The main area contains a table with the following data:

Frame Size	Frame Counts	Frames/sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0

At the top of the table area, there is a 'Port: 1' label, a '1s' dropdown menu, and an 'OK' button.

Figure 7 - 5. Packet Size Table window

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.

Memory Utilization

The Switch displays memory utilization information for DRAM and Flash.

To view this window, click **Monitoring > Memory Utilization**:

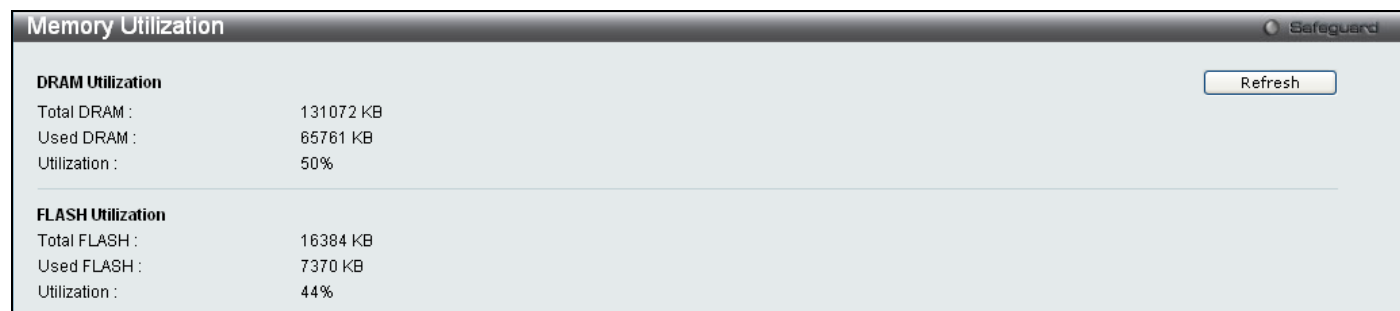


Figure 7 - 6. Memory Utilization window

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (Rx)

These windows display 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 the following graph of packets received on the Switch, click **Monitoring > Packets > Received (Rx)**:

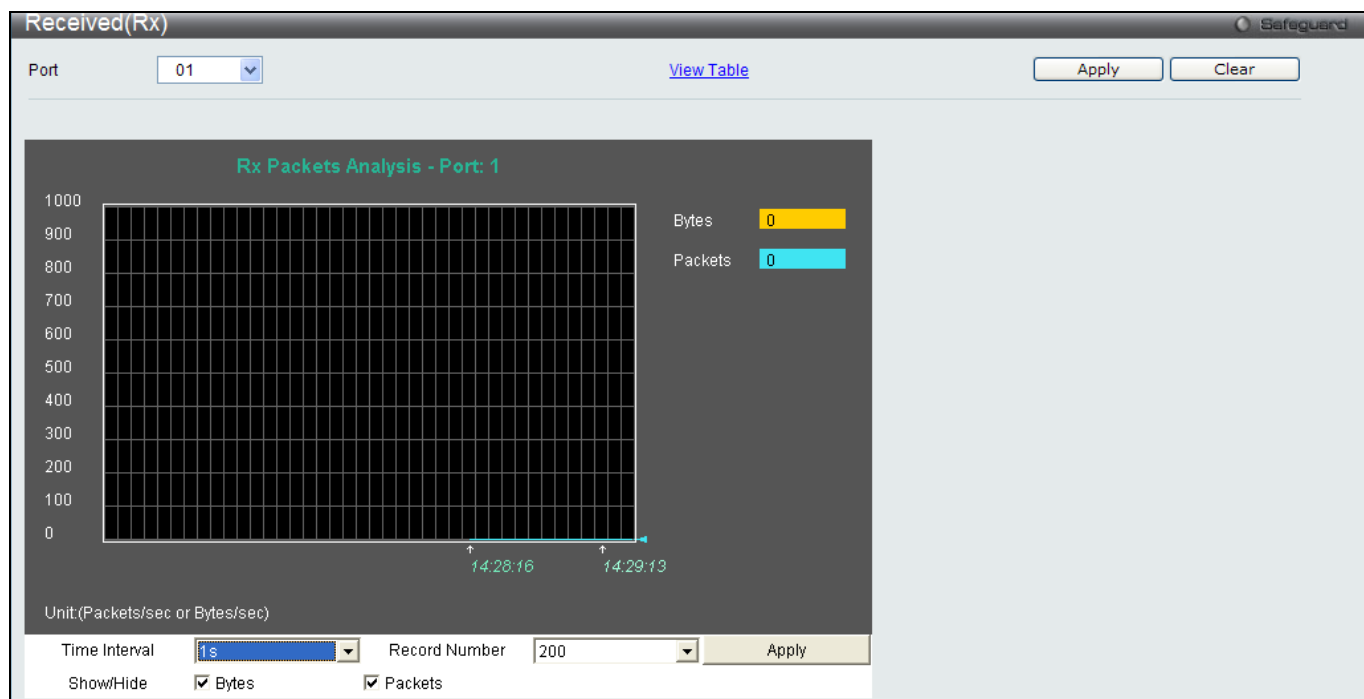


Figure 7 - 7. Received (Rx) window (for Bytes and Packets)

To view the **Received (Rx) Table** window, click [View Table](#).

The screenshot shows the 'Received(Rx) Table' window. At the top, there is a 'Port' dropdown menu set to '01', a 'View Graphic' link, and 'Apply' and 'Clear' buttons. Below this, there is a sub-section for 'Port: 1' with a '1s' dropdown and an 'OK' button. The main content is a table with three sections:

Rx Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

Rx Packets	Total	Total/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

Tx Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

Figure 7 - 8. Received (Rx) Table window (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)

These windows display 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 the following graph of UMB cast packets received on the Switch, click **Monitoring > Packets > UMB_cast (Rx)**:

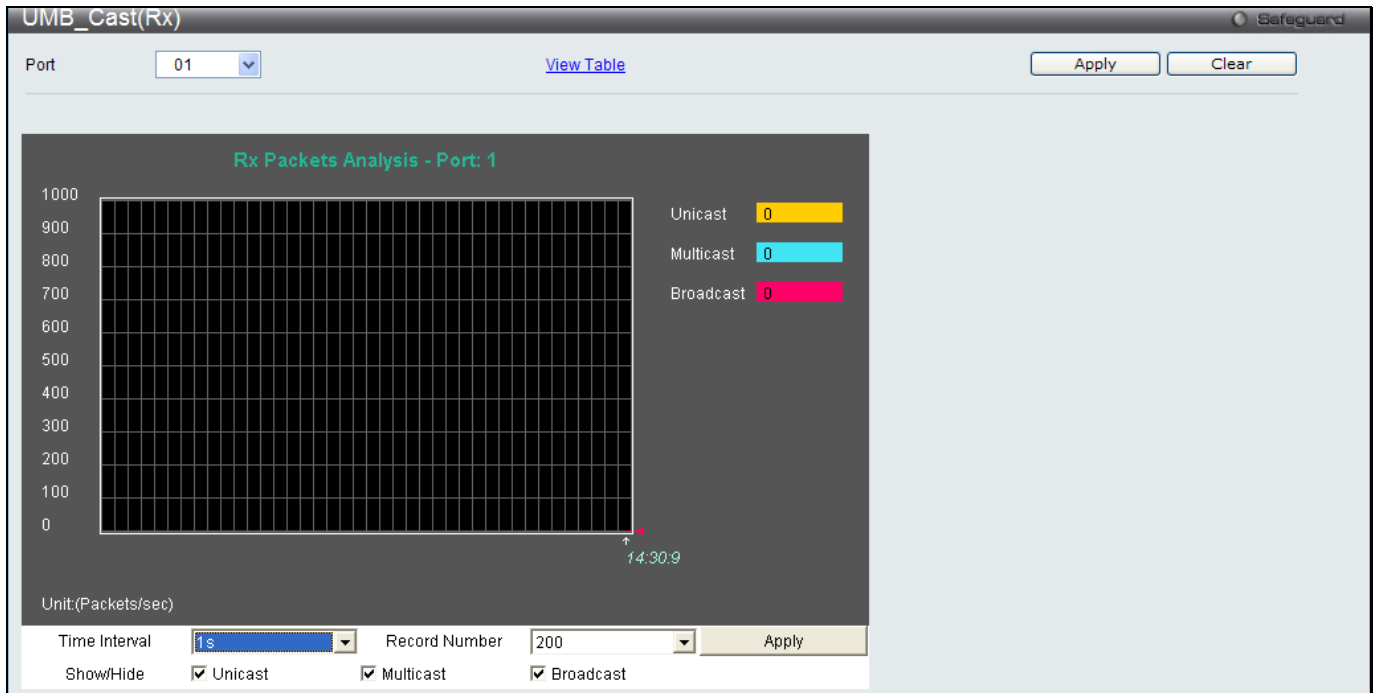


Figure 7 - 9. UMB_cast (Rx) window (for Unicast, Multicast, and Broadcast Packets)

To view the **UMB_cast (Rx) Table** window, click the [View Table](#) link.

The screenshot shows the 'UMB_cast(Rx) Table' window with a 'Port' dropdown set to '01'. A 'View Graphic' link is visible. The main area contains a table with the following structure:

Port: 1		
Rx Packets	Total	Total/sec
Bytes	0	0
Packets	0	0
Rx Packets	Total	Total/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0
Tx Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

At the top of the table area, there is a 'Port: 1' dropdown, a '1s' time interval dropdown, and an 'OK' button. 'Apply' and 'Clear' buttons are also present at the top right of the window.

Figure 7 - 10. UMB_cast (Rx) Table window (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.
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)

These windows display the Transmitted (Tx) 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 the following graph of packets transmitted from the Switch, click **Monitoring > Packets > Transmitted (Tx)**:

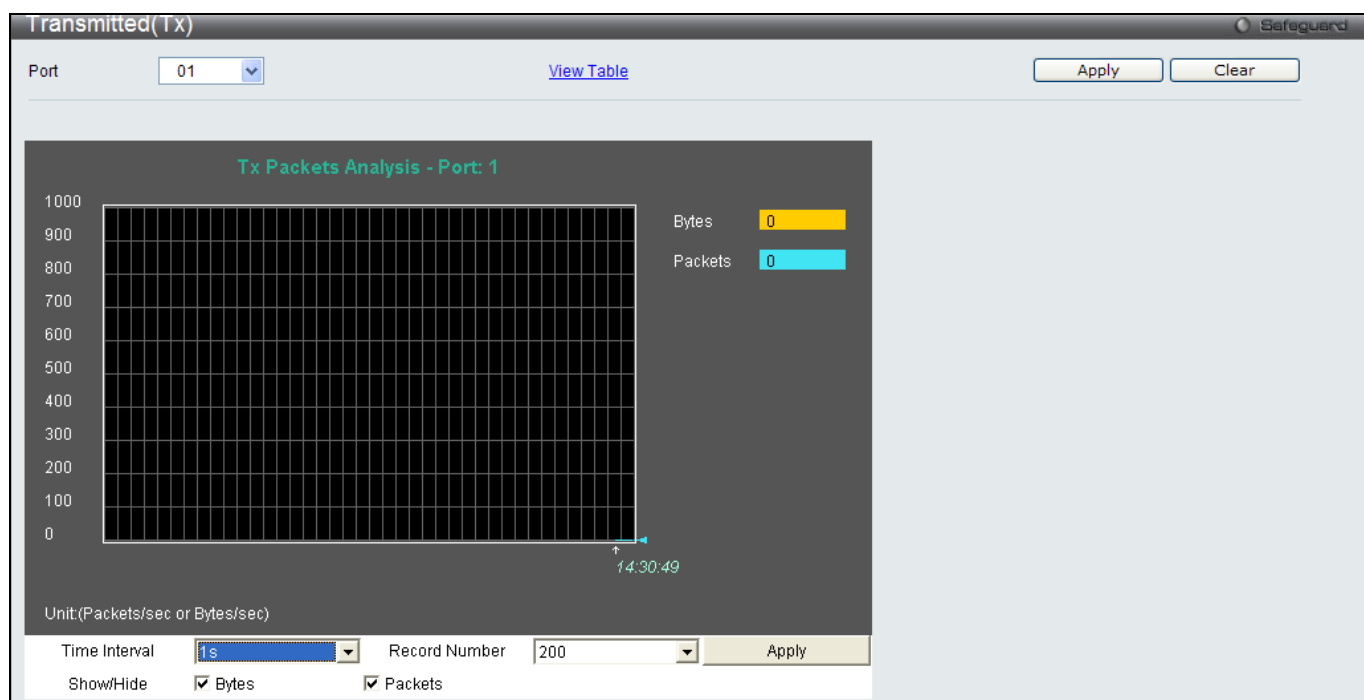


Figure 7 - 11. Transmitted (Tx) window (for Bytes and Packets)

To view the **Transmitted (Tx) Table** window, click the link [View Table](#).

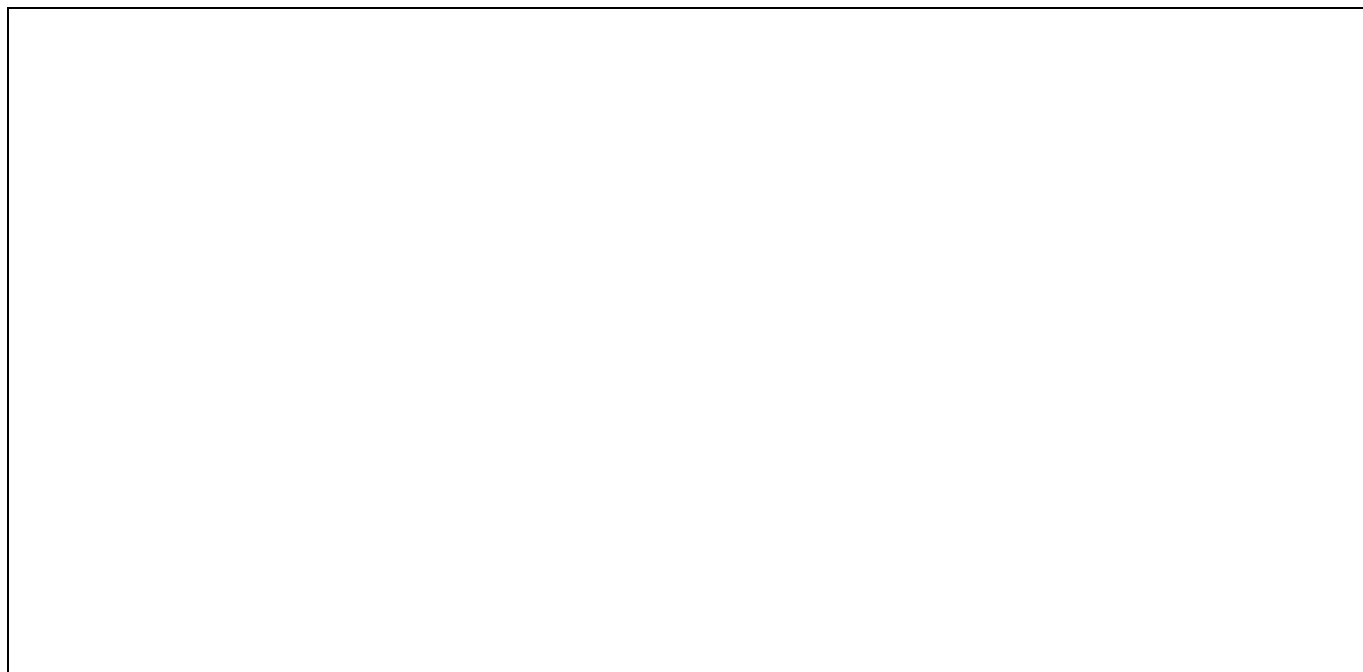


Figure 7 - 12. Transmitted (Tx) Table window (for Bytes and Packets)

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.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of error packets received on the Switch, click **Monitoring > Errors > Received (RX)**:

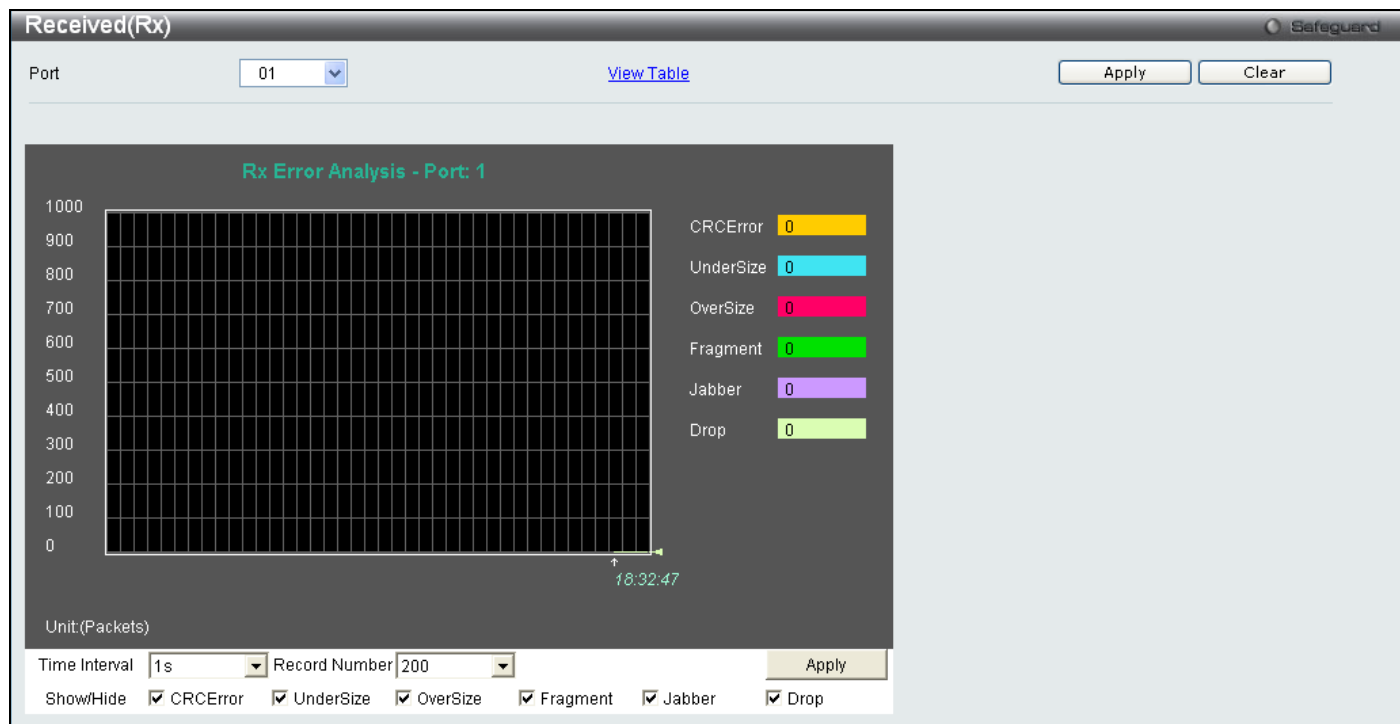


Figure 7 - 13. Received (Rx) window (for errors)

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

The screenshot shows the 'Received(RX) Table' window with a port dropdown set to '01'. Below the dropdown is a 'View Graphic' link and 'Apply' and 'Clear' buttons. The main area contains a table with the following data:

Rx Error	RX Frame
CRCError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Drop	0

At the top of the table area, there are controls for 'Port: 1', 'Time Interval' (set to 1s), and an 'OK' button.

Figure 7 - 14. Received (Rx) Table window (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.
CRCErr	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.
Show/Hide	Check whether or not to display CRCErr, 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 the following graph of error packets received on the Switch, click the **Monitoring > Errors > Transmitted (Tx)** :

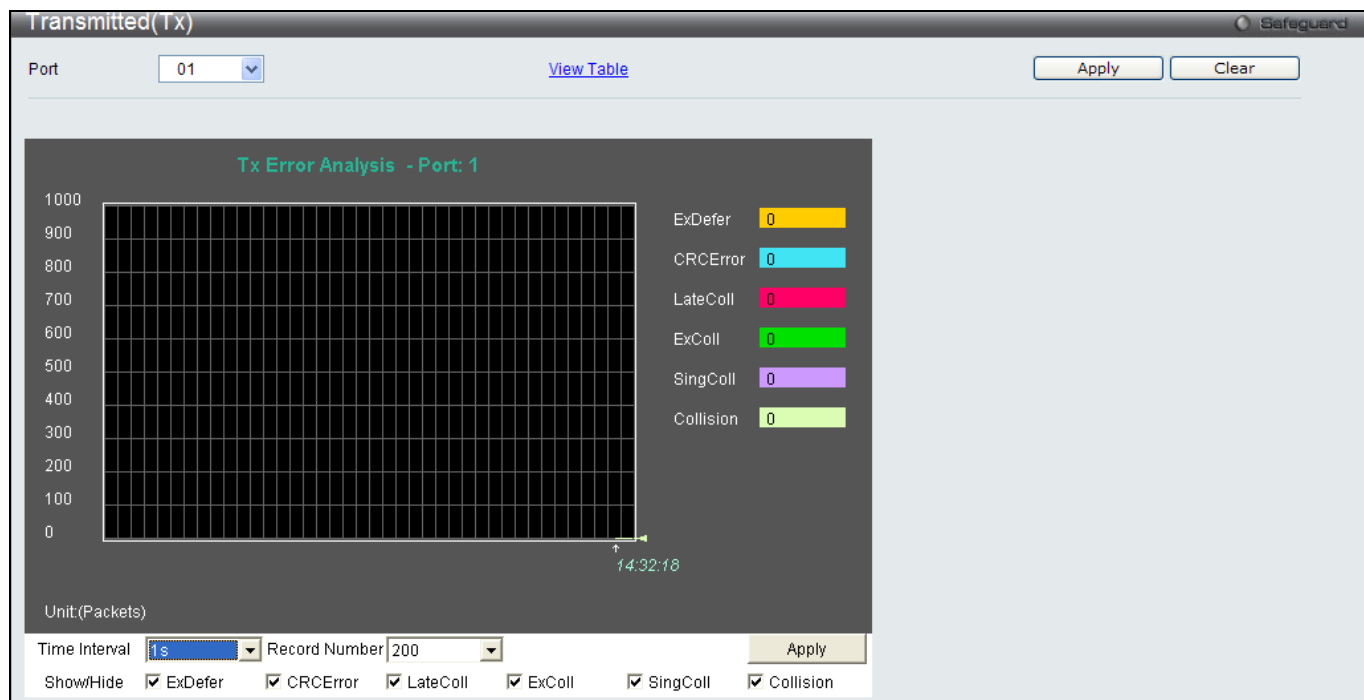


Figure 7 - 15. Transmitted (Tx) window (for errors)

To view the **Transmitted (Tx) Table** window, click the link [View Table](#), which will show the following table:

The screenshot shows the 'Transmitted(Tx) Table' window with a 'Port' dropdown set to '01'. A 'View Graphic' link is visible. The main area contains a table with the following data:

Tx Error	TX Frames
ExDefer	0
CRC Error	0
LateColl	0
ExColl	0
SingColl	0
Collision	0

At the top of the table area, there is a 'Port: 1' label, a '1s' dropdown, and an 'OK' button.

Figure 7 - 16. Transmitted (Tx) Table window (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.

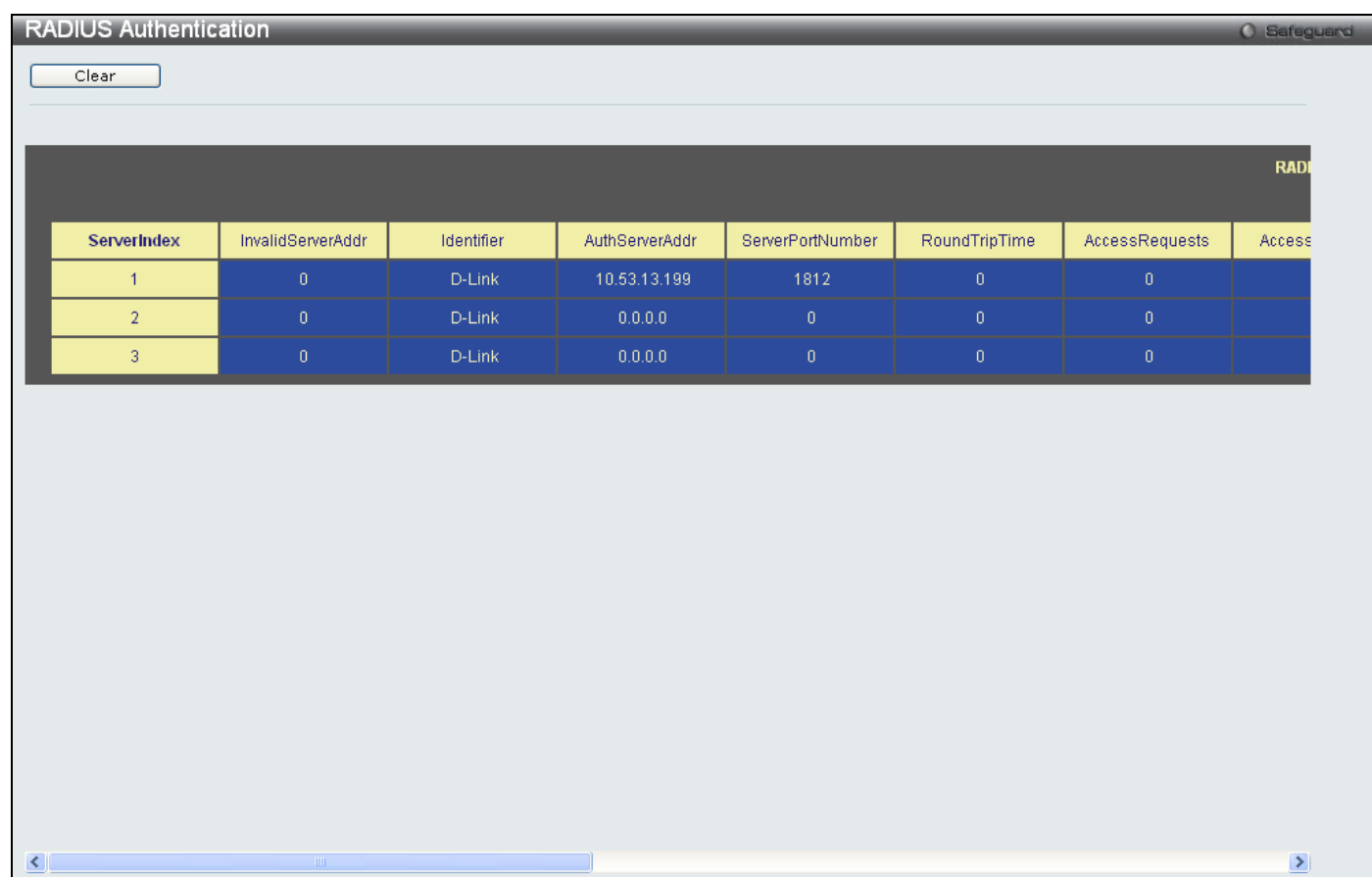
Port Access Control

The following six windows are used to monitor 802.1X statistics of the Switch, on a per port basis.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view the **RADIUS Authentication** window, click **Monitoring > Port Access Control > RADIUS Authentication**:



ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	Access
1	0	D-Link	10.53.13.199	1812	0	0	
2	0	D-Link	0.0.0.0	0	0	0	
3	0	D-Link	0.0.0.0	0	0	0	

Figure 7 - 17. RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following information is displayed:

Parameter	Description
InvalidServerAddresses	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

RADIUS Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view the **RADIUS Account Client** window, click **Monitoring > Port Access Control > RADIUS Account Client**:

ServerIndex	InvalidServerAddr	Identifier	ServerAddr	ServerPortNumber	RoundTripTime	RequestedAuthTime
1	0	D-Link	10.53.13.199	1812	0	0
2	0	D-Link	0.0.0.0	0	0	0
3	0	D-Link	0.0.0.0	0	0	0

Figure 7 - 18. RADIUS Account Client window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following information is displayed:

Parameter	Description
InvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS account. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Accounting server that it shares a secret with.
ServerAddress	The (conceptual) table listing the RADIUS accounting servers with which it shares a secret.
ServerPortNumber	The UDP port it is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout it may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Authenticator State

The following section describes the 802.1X State on the Switch.

To view the Authenticator State, click **Monitoring > Port Access Control > Authenticator State**:

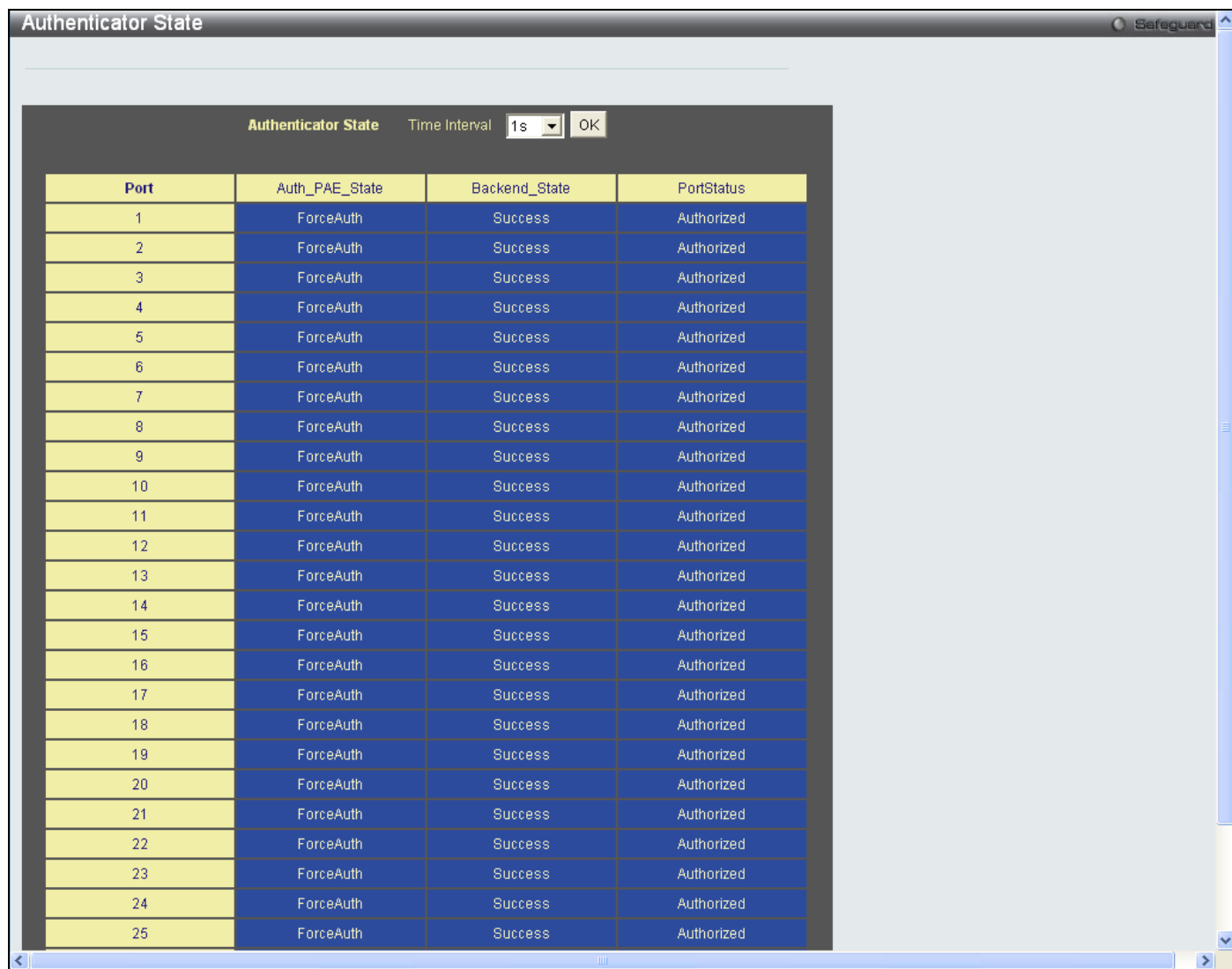


Figure 7 - 19. Authenticator State window

This window displays the Authenticator State for individual ports on a selected device. A polling interval between 1s and 60s seconds can be set using the drop-down menu at the top of the window and clicking **OK**.

The information on this window is described as follows:

Parameter	Description
MAC Address	The MAC Address of the device of the corresponding index number.
Auth PAE State	The Authenticator PAE State value can be: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Backend State	The Backend Authentication State can be Request, Response, Success, Fail, Timeout, Idle, Initialize, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be Authorized, Unauthorized, or N/A.

Authenticator Statistics

This window contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the Authenticator Statistics, click **Monitoring > Port Access Control > Authenticator Statistics**:

The screenshot shows a window titled "Authenticator Statistics" with a "Safeguard" icon in the top right. Below the title bar, there is a sub-header "Authenticator Statistics" and a "Time Interval" dropdown menu set to "1s" with an "OK" button next to it. The main content is a table with the following columns: Port, Frames Rx, Frames Tx, Rx Start, Tx Reqld, Rx LogOff, Tx Req, Rx Respld, and Rx Resp. The table contains 25 rows, each representing a port from 1 to 25. All values in the table are 0.

Port	Frames Rx	Frames Tx	Rx Start	Tx Reqld	Rx LogOff	Tx Req	Rx Respld	Rx Resp
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0

Figure 7 - 20. Authenticator Statistics window

The user may also select the desired time interval to update the statistics, between 1s and 60s, where “s” stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of valid EAPOL frames that have been received by this Authenticator.
Frames Tx	The number of EAPOL frames that have been transmitted by this Authenticator.
Rx Start	The number of EAPOL Start frames that have been received by this Authenticator.
TxReqId	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
RxLogOff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Tx Req	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Rx Respld	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx Resp	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx Error	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Last Version	The protocol version number carried in the most recently received EAPOL frame.
Last Source	The source MAC address carried in the most recently received EAPOL frame.

Authenticator Session Statistics

This window contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Session Statistics** window, click **Monitoring > Port Access Control > Authenticator Session Statistics**:

The screenshot shows a window titled "Authenticator Session Statistics" with a "Safeguard" icon in the top right. The window contains a table with the following data:

Port	Octets Rx	Octets Tx	Frames Rx	Frames Tx
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0

Figure 7 - 21. Authenticator Session Statistics window

The user may select the desired time interval to update the statistics, between 1s and 60s, where “s” stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Octets Rx	The number of octets received in user data frames on this port during the session.
Octets Tx	The number of octets transmitted in user data frames on this port during the session.
Frames Rx	The number of user data frames received on this port during the session.
Frames Tx	The number of user data frames transmitted on this port during the session.
ID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
Authentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server - The Authentication Server is external to the Authenticator's System. (2) Local Authentic Server - The Authentication Server is located within the Authenticator's System.
Time	The duration of the session in seconds.
Terminate Cause	The reason for the session termination. There are eight possible reasons for termination. 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
UserName	The User-Name representing the identity of the Supplicant PAE.

Authenticator Diagnostics

This window contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Diagnostics** window, click **Monitoring > Port Access Control > Authenticator Diagnostics**:

Port	Connect Enter	Connect LogOff	Auth Enter	Auth Success	Auth Timeout	Auth Fail	Au
1	0	0	0	0	0	0	
2	0	0	0	0	0	0	
3	0	0	0	0	0	0	
4	0	0	0	0	0	0	
5	0	0	0	0	0	0	
6	0	0	0	0	0	0	
7	0	0	0	0	0	0	
8	0	0	0	0	0	0	
9	0	0	0	0	0	0	
10	0	0	0	0	0	0	
11	0	0	0	0	0	0	
12	0	0	0	0	0	0	
13	0	0	0	0	0	0	
14	0	0	0	0	0	0	
15	0	0	0	0	0	0	
16	0	0	0	0	0	0	
17	0	0	0	0	0	0	
18	0	0	0	0	0	0	
19	0	0	0	0	0	0	
20	0	0	0	0	0	0	
21	0	0	0	0	0	0	
22	0	0	0	0	0	0	
23	0	0	0	0	0	0	
24	0	0	0	0	0	0	
25	0	0	0	0	0	0	

Figure 7 - 22. Authenticator Diagnostics window

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Connect Enter	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
Connect LogOff	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
Auth Enter	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
Auth Success	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).

Auth Timeout	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
Auth Fail	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).
Auth Reauth	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Auth Start	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
Auth LogOff	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
Authed Reauth	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Authed Start	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
Authed LogOff	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
Responses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
AccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
OtherReqToSupp	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
NonNakRespFromSup	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
Bac Auth Success	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
Bac Auth Fail	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

Browse ARP Table

This window displays current ARP entries on the Switch. To search a specific ARP entry, enter an Interface Name or an IP Address at the top of the window and click **Find**. Click the **Show Static** button to display static ARP table entries. To clear the ARP Table, click **Clear All**.

To view this window, click **Monitoring > Browse ARP Table**:

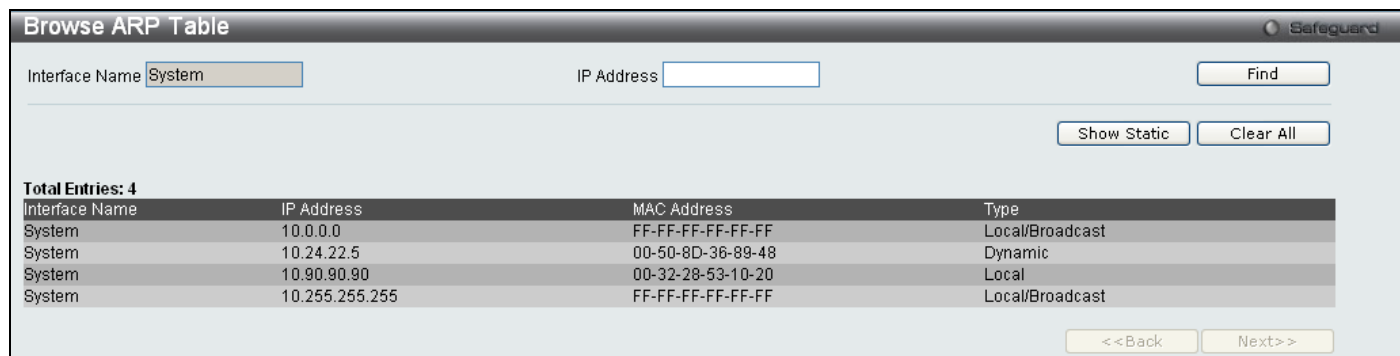


Figure 7 - 23. Browse ARP Table window

Browse VLAN

This window allows the VLAN status for each of the Switch's ports to be viewed by VLAN. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button.

To view this window, click **Monitoring > Browse VLAN**:

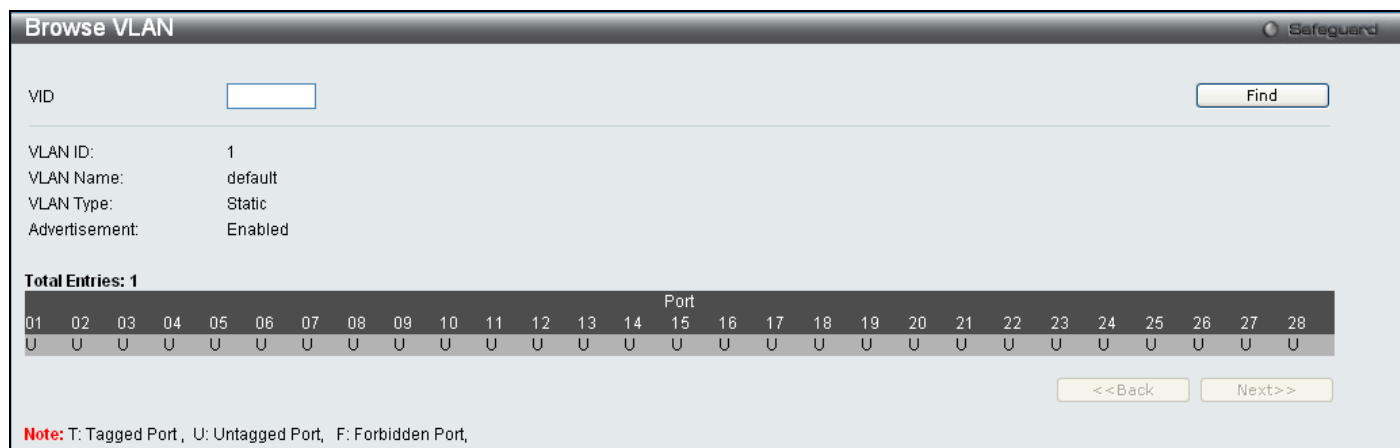


Figure 7 - 24. Browse VLAN window

IGMP Snooping

The following windows are used to configure the IGMP Snooping settings of the Switch.

Browse IGMP Router Port

This window displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button to display the various types of IGMP router ports that belong to the specified VLAN.

To view this window, click **Monitoring > IGMP Snooping > Browse IGMP Router Port**:

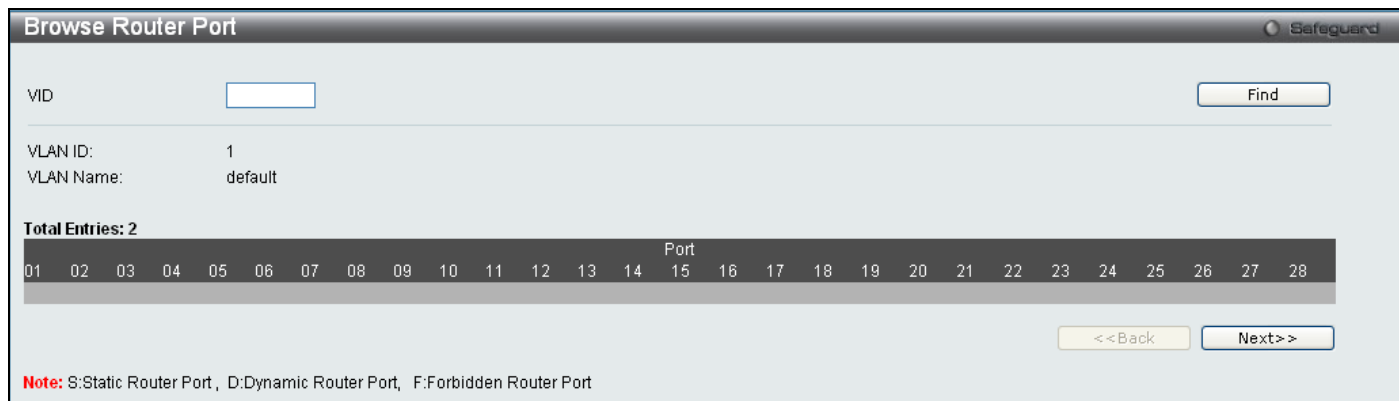


Figure 7 - 25. Browse Router Port window

IGMP Snooping Group

This window allows the Switch’s IGMP Snooping Group Table to be searched. IGMP snooping allows the Switch to read the Multicast Group IP address and source IP address from IGMP packets that pass through the Switch. The number of IGMP reports that are snooped are displayed in the Reports field.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Group**:

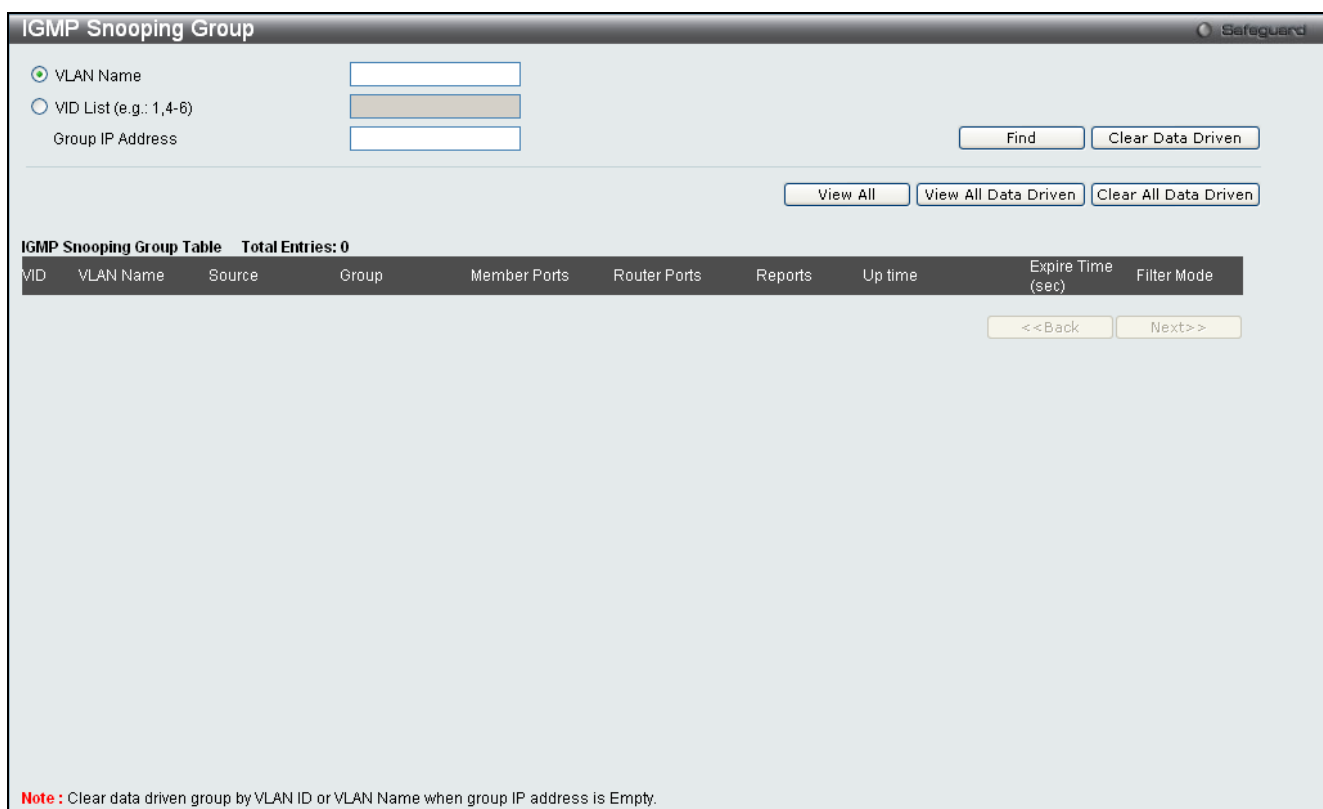


Figure 7 - 26. IGMP Snooping Group window

The following fields can be searched:

Parameter	Description
VLAN Name	The VLAN ID of the multicast group.
VID List (e.g.: 1, 4-6)	The VLAN ports of the multicast group.
Group IP Address	The IP address of the multicast group.

Enter the appropriate information and click **Find**. The searched entries will be shown in the IGMP Snooping Group Table. Click **View All** to see all the entries.

Click **View All Data Driven** to display all the data driven groups learned in the IGMP Snooping Group Table.

Click **Clear Data Driven** to clear the specific data driven groups learned in IGMP Snooping Group Table.

Click **Clear All Data Driven** to clear all data driven groups learned in IGMP Snooping Group Table.



NOTE: To configure IGMP snooping for the Switch, go to the **L2 Features** folder and select **IGMP Snooping > IGMP Snooping Settings**.

IGMP Snooping Host

This window displays current IGMP Snooping host information on the Switch.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Host**:

Figure 7 - 27. IGMP Snooping Host window

Click the corresponding radio button, enter the VLAN Name, VLAN List, Port List, or the Group to view IGMP snooping host information, and click **Find**. The searched entries will be displayed in the lower half of the window.

MLD Snooping

Browse MLD Router Port

This window displays which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch and is designated by D, whereas a Forbidden port is designated by F. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button to display the various types of MLD router ports that belong to the specified VLAN.

To view this window, click **Monitoring > MLD Snooping > Browse MLD Router Port**:

Figure 7 - 28. Browse MLD Router Port window

MLD Snooping Group

The following window allows the user to view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4. The user may browse this table by VLAN present in the Switch by entering that VLAN Name in the empty field shown below, and clicking the **Find** button.

To view this window, click **Monitoring > MLD Snooping > MLD Snooping Group**:

MLD Snooping Group Safeguard

VLAN Name
 VLAN List (e.g.: 1,4-6)
 Group IP Address
Find

View All

MLD Snooping Group Table Total Entries: 0

VID	VLAN Name	Source	Group	Member Port	Filter Mode
<<Back Next>>					

Figure 7 - 29. MLD Snooping Group window

Enter a VLAN Name or VLAN List and Group IP Address in the appropriate field and click the **Find** button.

The searched entries will be shown in the MLD Snooping Group Table. Click **View All** to see all the entries.

LLDP

The Switch offers three LLDP statistic windows.

LLDP Statistics System

To view this window, click **Monitoring > LLDP > LLDP Statistics System**:

LLDP Statistics System Safeguard

LLDP Statistics

Last Change Time	1363
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Ageout	0

Port: Find

LLDP Statistics Ports

Total Tx Frames	0
Total Discarded Rx Frames	0
Rx Errors Frames	0
Total Rx Frames	0
Total Discarded Rx TLVs	0
Total Unrecognized Rx TLVs	0
Total Aged out Neighbor Information	0

Figure 7 - 30. LLDP Statistics System window

LLDP Local Port Information

To view this window, click **Monitoring > LLDP > LLDP Local Port Information**:

The screenshot shows the 'LLDP Local Port Information' window with a 'Show Normal' button. Below the title bar is the 'LLDP Local Port Brief Table' header. The table contains 28 rows of port information.

Port	Port ID Subtype	Port ID	Port Description
1	Local	/1	D-Link DES-3200-28 R1.28 Port 1
2	Local	/2	D-Link DES-3200-28 R1.28 Port 2
3	Local	/3	D-Link DES-3200-28 R1.28 Port 3
4	Local	/4	D-Link DES-3200-28 R1.28 Port 4
5	Local	/5	D-Link DES-3200-28 R1.28 Port 5
6	Local	/6	D-Link DES-3200-28 R1.28 Port 6
7	Local	/7	D-Link DES-3200-28 R1.28 Port 7
8	Local	/8	D-Link DES-3200-28 R1.28 Port 8
9	Local	/9	D-Link DES-3200-28 R1.28 Port 9
10	Local	/10	D-Link DES-3200-28 R1.28 Port 10
11	Local	/11	D-Link DES-3200-28 R1.28 Port 11
12	Local	/12	D-Link DES-3200-28 R1.28 Port 12
13	Local	/13	D-Link DES-3200-28 R1.28 Port 13
14	Local	/14	D-Link DES-3200-28 R1.28 Port 14
15	Local	/15	D-Link DES-3200-28 R1.28 Port 15
16	Local	/16	D-Link DES-3200-28 R1.28 Port 16
17	Local	/17	D-Link DES-3200-28 R1.28 Port 17
18	Local	/18	D-Link DES-3200-28 R1.28 Port 18
19	Local	/19	D-Link DES-3200-28 R1.28 Port 19
20	Local	/20	D-Link DES-3200-28 R1.28 Port 20
21	Local	/21	D-Link DES-3200-28 R1.28 Port 21
22	Local	/22	D-Link DES-3200-28 R1.28 Port 22
23	Local	/23	D-Link DES-3200-28 R1.28 Port 23
24	Local	/24	D-Link DES-3200-28 R1.28 Port 24
25	Local	/25	D-Link DES-3200-28 R1.28 Port 25
26	Local	/26	D-Link DES-3200-28 R1.28 Port 26
27	Local	/27	D-Link DES-3200-28 R1.28 Port 27
28	Local	/28	D-Link DES-3200-28 R1.28 Port 28

Figure 7 - 31. LLDP Local Port Information window

LLDP Remote Port Information

To view this window, click **Monitoring > LLDP > LLDP Remote Port Information**:

The screenshot shows the 'LLDP Remote Port Information' window. It features a search interface with a 'Port' dropdown menu set to '01', a 'Find' button, and a 'Show Normal' button. Below the search area, it displays 'Remote Entities Count : 0' and a table header for remote entities.

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description
Remote Entities Count : 0					

Figure 7 - 32. LLDP Remote Port Information window

Ethernet OAM

This folder contains two windows to view **Ethernet OAM Event Log** information and **Ethernet OAM Statistics**.

Browse Ethernet OAM Event Log

This window allows the user to view the Ethernet OAM event log information. The Switch can buffer up to 1000 event logs. The event log will provide and record detailed information about each OAM event. Specify the port number and port list you wish to view and click **Find**. To remove an entry, enter the appropriate information and click **Clear**.

To view this window, click **Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log** as shown below:

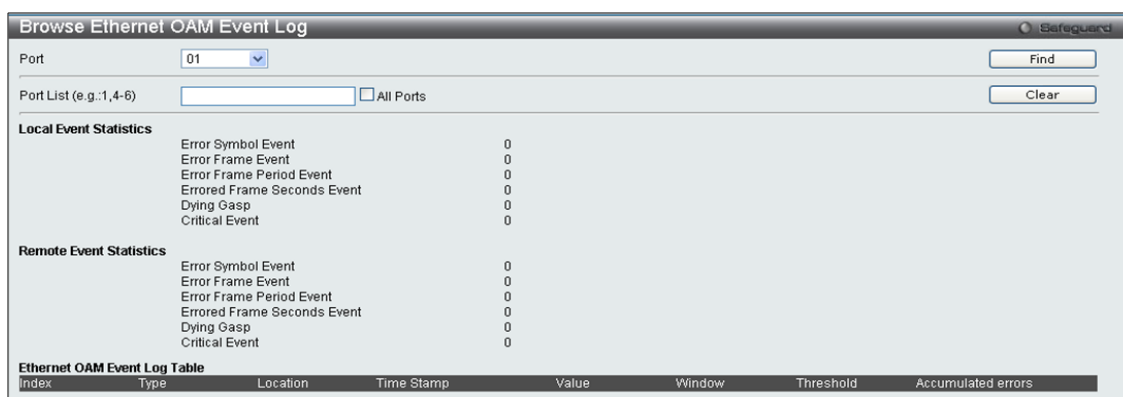


Figure 7 - 33. Browse Ethernet OAM Event Log window

Browse Ethernet OAM Statistics

This window displays the Ethernet OAM Statistic information on each port of the Switch. To clear information for a particular port or list of ports enter the ports and click **Clear**.

To view this window, click **Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics** as shown below:

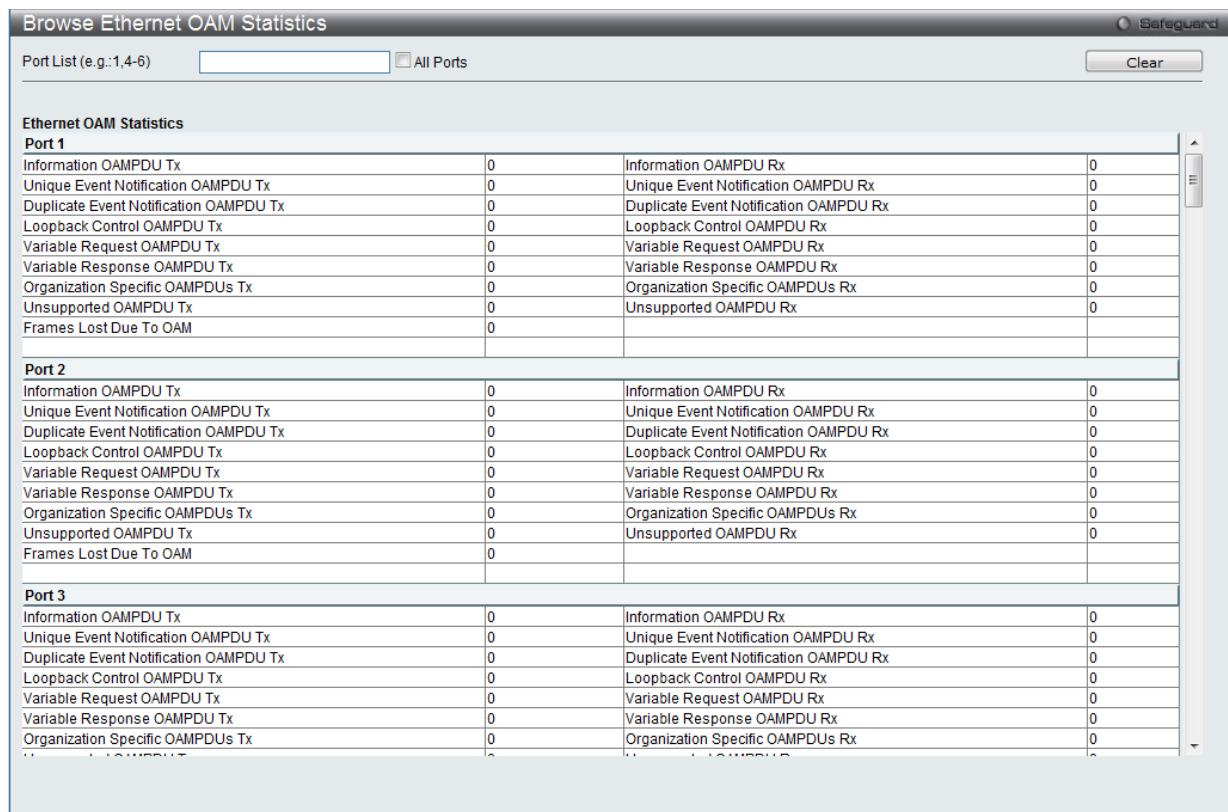


Figure 7 - 34. Browse Ethernet OAM Statistics window

Connectivity Fault Management

CFM Fault Table

This window will display the fault conditions detected by the MEPs on the Switch.

To view this window, click **Monitoring > CFM > CFM Fault Table** as shown below:



Figure 7 - 35. Browse CFM Fault MEP window

Parameter	Description
MD Name:	Enter the maintenance domain name to display.
MA Name:	Enter the maintenance association name to display.

Click **Find** to display connection faults for the specified MD and MA.

CFM MP Table

This window is used to browse the CFM port MP list on the Switch.

To view this window, click **Monitoring > CFM > CFM MP Table** as shown below:

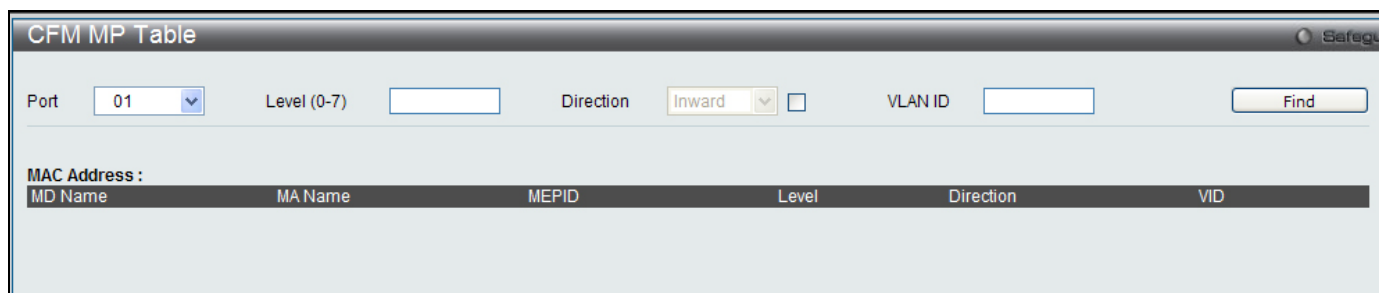


Figure 7 - 36. Browse CFM Port MP List window

The following parameters can be configured:

Parameter	Description
Port	The port to which the MAC address below corresponds.
Level (0-7)	The MD level of the entry you wish to view.
Direction	The direction of the MEP. <i>Inward</i> indicates an inward facing MEP. <i>Outward</i> indicates an outward facing MEP.
VLAN ID	The VLAN identifier of the entry you wish to view.

Click **Find** to see the entry displayed in the table.

CFM Packet Counter

This window displays the CFM packet Rx/Tx counters on the Switch. Enter the ports you wish to view and click **Find**. To view this window, click **Monitoring > CFM > CFM Packet Counter** as shown below:

The screenshot shows the 'CFM Packet Counter' window. At the top, there is a 'Port List (e.g.:1,5-10)' input field, an 'All Ports' checkbox, a 'State' dropdown menu set to 'Transmit', and 'Find' and 'Clear' buttons. Below this is a table titled 'CFM Transmit Statistics' with columns: Port, AIPkt, CCM, LBR, LBM, LTR, and LTM. The table lists ports from 1 to 28, with an 'All' row at the top. All data points in the table are 0.

Port	AIPkt	CCM	LBR	LBM	LTR	LTM
All	0	0	0	0	0	0
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0
25	0	0	0	0	0	0
26	0	0	0	0	0	0
27	0	0	0	0	0	0
28	0	0	0	0	0	0

Figure 7 - 37. CFM Packet Counter List window

Parameter	Description
Port List:	Select the ports to display. If not specified, all ports will be shown.
Type:	<i>Receive</i> – Selecting this option will display all the CFM packets received. <i>Transmit</i> – Selecting this option will display all the CFM packets transmitted. <i>CCM</i> – Selecting this option will display all the CFM packets transmitted and received.

Click **Find** to display the information.

CFM MIPCCM Table

This window displays the CFM MIPCCM entries on the Switch.

To view this window, click **Monitoring > CFM > CFM MIPCCM Table** as shown below:

The screenshot shows the 'CFM MIPCCM List' window. It displays 'Total Entries: 0' and a table with columns: MA, VID, MAC Address, and Port. The table is currently empty.

MA	VID	MAC Address	Port
Total Entries: 0			

Figure 7 - 38. CFM MIPCCM Table

MAC-based Access Control Authentication State

This window allows the user to view the MAC-based Access Control authentication information. Specify the port list to view and click **Find**. To remove an entry, enter the appropriate information and click **Clear By Port**. Click **View All Hosts** to see all the entries. To remove all hosts, click **Clear All Hosts**.

To view this window, click **Monitoring > MAC-based Access Control Authentication State**:

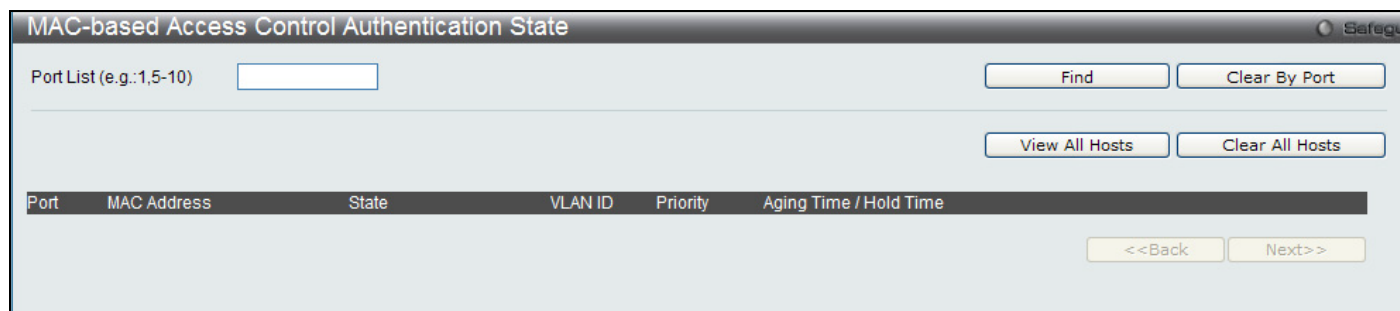


Figure 7 - 39. MAC-based Access Control Authentication State menu

Browse Session Table

This window displays the management sessions since the Switch was last rebooted.

To view the **Browse Session Table** window, click **Monitoring > Browse Session Table**:

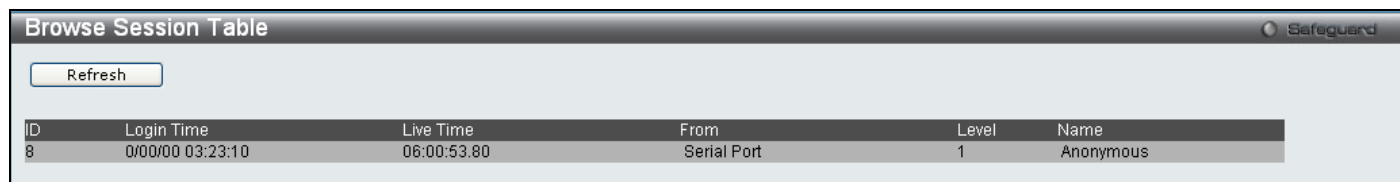


Figure 7 - 40. Browse Session Table window

MAC Address Table

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

To view the **MAC Address Table** window, click **Monitoring > MAC Address Table**

VID	VLAN Name	MAC Address	Port	Type
1	default	00-32-28-53-10-20	CPU	Self
1	default	00-50-8D-36-89-48	17	Dynamic

Figure 7 - 41. MAC Address Table window

The functions used in the MAC address table are described below:

Parameter	Description
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
Clear Dynamic Entries	Click this button will allow the user to delete all dynamic entries of the address table.
View All Entry	Click this button will allow the user to view all entries of the address table.
Clear All Entry	Click this button will allow the user to delete all entries of the address table.

System Log

The web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

To view the Switch history log, click **Monitoring > System Log**:

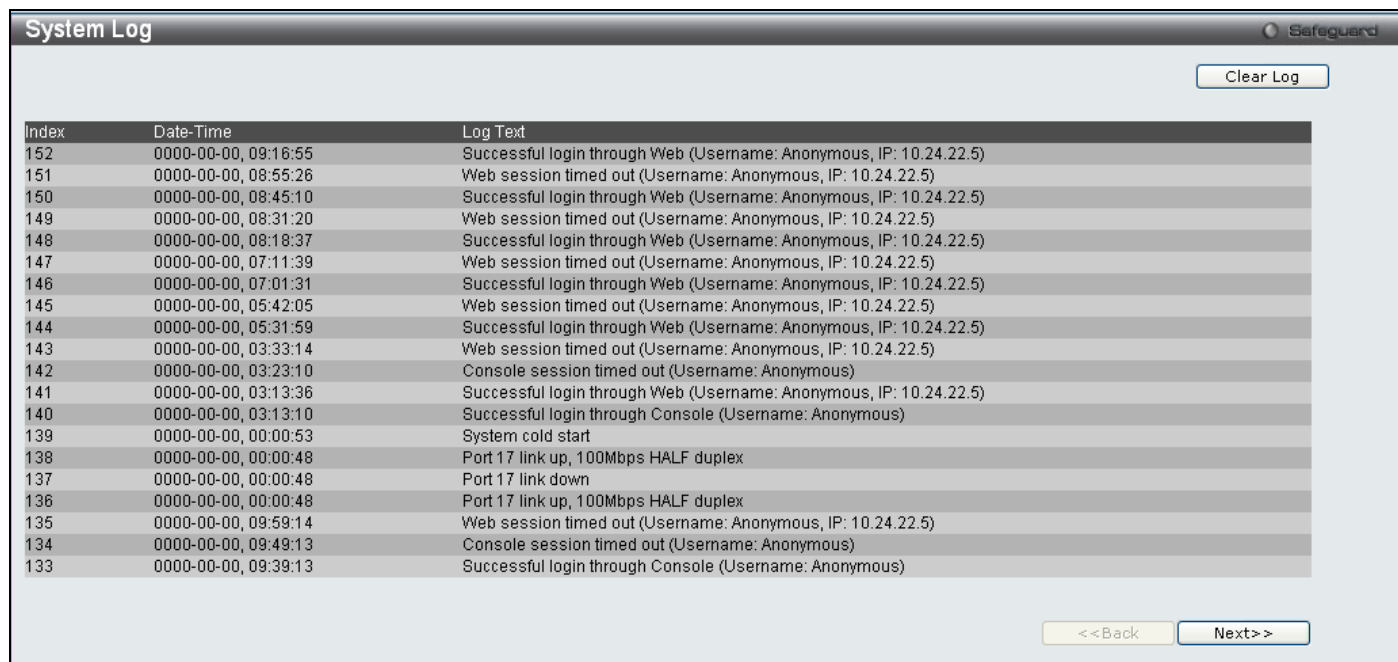


Figure 7 - 42. System Log window

The Switch can record event information in its own logs. Click **Next** to go to the next page of the **System Log** window. Clicking **Clear** will allow the user to clear the Switch History Log.

The information in the table is categorized as:

Parameter	Description
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Date-Time	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

Section 8

Save and Tools

Save Configuration

Save Log

Save All

Configuration File Upload & Download

Upload Log File

Reset

Ping Test

Download Firmware

Reboot System

The three **Save** windows include: **Save Configuration**, **Save Log**, and **Save All**. Each version of the window will aid the user in saving configurations to the Switch's memory.

The options include:

- **Save Configuration** to save the current configuration file.
- **Save Log** to save only the current log.
- **Save All** to save the current configuration file and log.

Save Configuration

Open the **Save** drop-down menu at the top of the Web manager and click **Save Configuration** to open the following window:

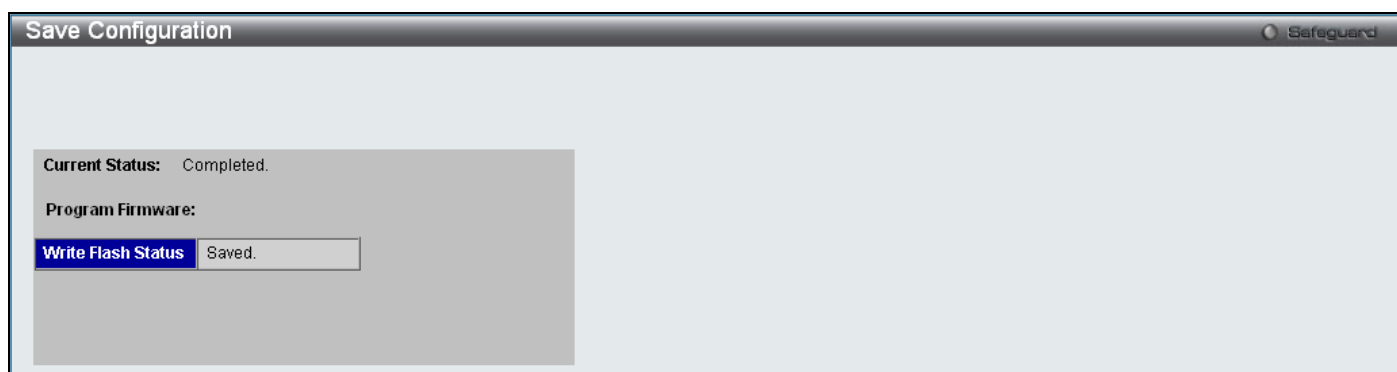
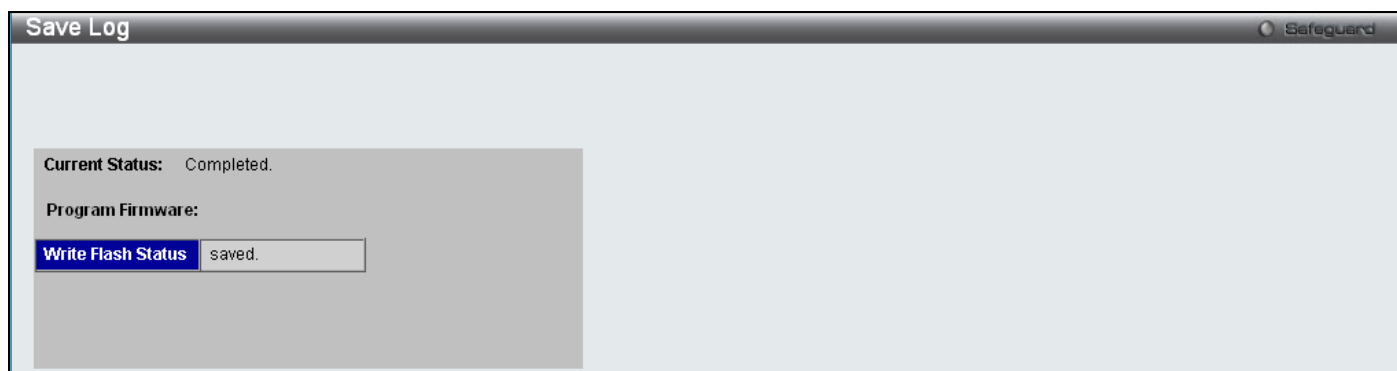


Figure 8 - 1. Save Configuration window

Save Log

Open the **Save** drop-down menu at the top of the Web manager and click **Save Log** to open the following window:

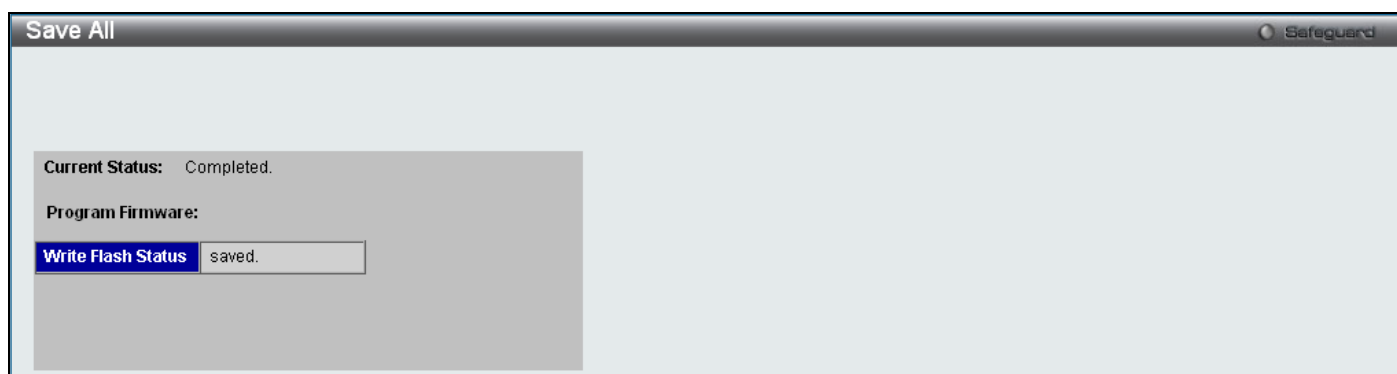


The screenshot shows a window titled "Save Log" with a "Safeguard" icon in the top right corner. The main content area is a light gray box containing the following text: "Current Status: Completed.", "Program Firmware:", and "Write Flash Status" followed by a text input field containing the word "saved".

Figure 8 - 2. Save Log window

Save All

Open the **Save** drop-down menu at the top of the Web manager and click **Save All** to open the following window:



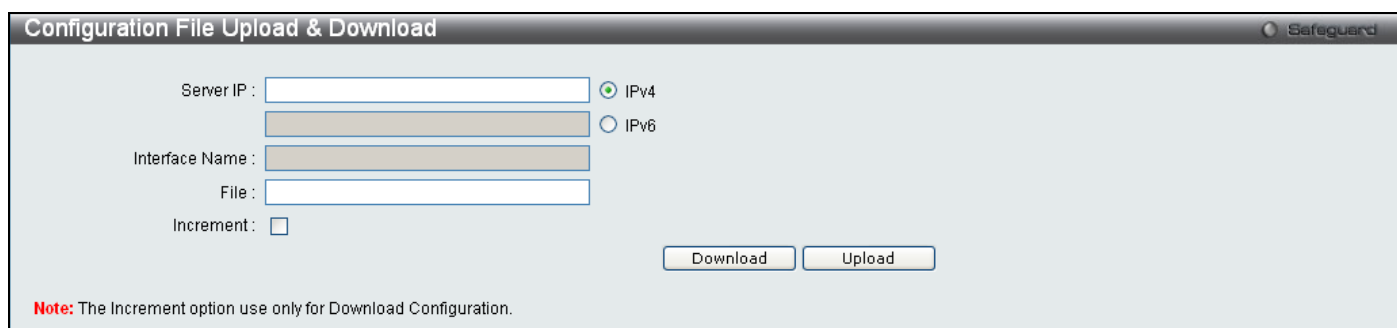
The screenshot shows a window titled "Save All" with a "Safeguard" icon in the top right corner. The main content area is a light gray box containing the following text: "Current Status: Completed.", "Program Firmware:", and "Write Flash Status" followed by a text input field containing the word "saved".

Figure 8 - 3. Save All window

Configuration File Upload & Download

The Switch can upload and download configuration files.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Configuration File Upload & Download** to open the following window:



The screenshot shows a window titled "Configuration File Upload & Download" with a "Safeguard" icon in the top right corner. The form contains the following fields and controls:

- Server IP: IPv4 IPv6
- Interface Name:
- File:
- Increment:
- Buttons: Download, Upload

Note: The Increment option use only for Download Configuration.

Figure 8 - 4. Configuration File Upload & Download window

Use the radio button to select IPv4 and specify File name or use the radio button to select IPv6, enter a Server IP, Interface Name, and File name. Click either **Download** or **Upload** to initiate the file transfer.

Upload Log File

To upload a log file, enter a Server IP address, use the radio button to select IPv4 and then enter a File name, or use the radio button to select IPv6, enter a Server IP, Interface Name, and File name. Click **Upload**.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Upload Log File** to open the following window:

Figure 8 - 5. Upload Log File window

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.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Reset System** to open the following window:

Figure 8 - 6. Reset System window

Ping Test

Users can Ping either an IPv4 address or an IPv6 address. Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Ping Test** to open the following window:

Ping Test Safeguard

IPv4 Ping Test :
Enter the IP address of the device or station you want to ping, then click **Start**.

Target IP Address :

Repeat Pinging for: Infinite times
 (1-255 times)

Timeout : (1-99 sec)

IPv6 Ping Test :
Enter the IP address of the device or station you want to ping, then click **Start**.

Target IP Address :

Interface Name:

Repeat Pinging for: Infinite times
 (1-255 times)

Size: (1-6000)

Timeout : (1-10 sec)

Figure 8 - 7. Ping Test window

The user may click the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between 1 and 255. Click **Start** to initiate the Ping program.

The following parameters may be configured or viewed:

Parameter	Description
Target IP Address	Enter an IP address to be Pinged.
Interface Name	For IPv6 only, enter the name of the interface to be Pinged.
Repeat Pinging for	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between 1 and 255.
Size	For IPv6 only, enter a value between 1 and 6000. The default is 100.
Timeout	For IPv4, select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. For IPv6, select a timeout period between 1 and 10 seconds for this Ping message to reach its destination. In either case, if the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Click **Start** to initialize the Ping program

Download Firmware

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

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Download Firmware** to open the following window:

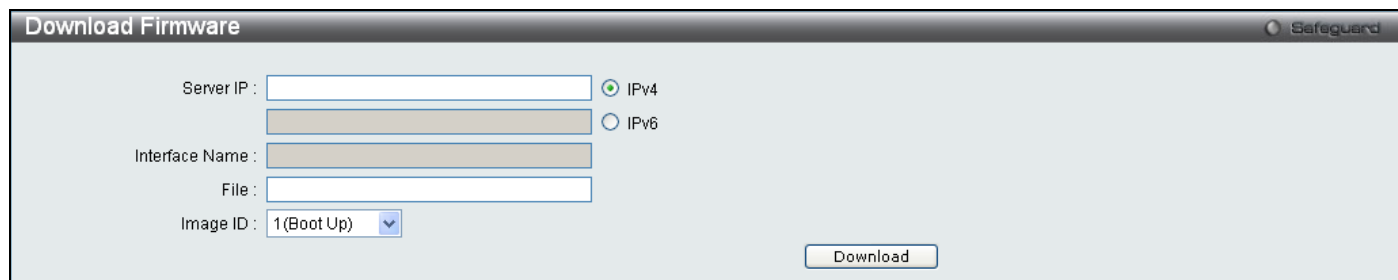


Figure 8 - 8. Download Firmware window

Use the radio button to select either IPv4 or IPv6. Enter the TFTP Server IP address for the type of IP selected. Specify the path/file name of the TFTP File. Select the desired Image ID, *1(Boot Up)* or 2. Click **Download** to initiate the file transfer.

Reboot System

The following window is used to restart the Switch.

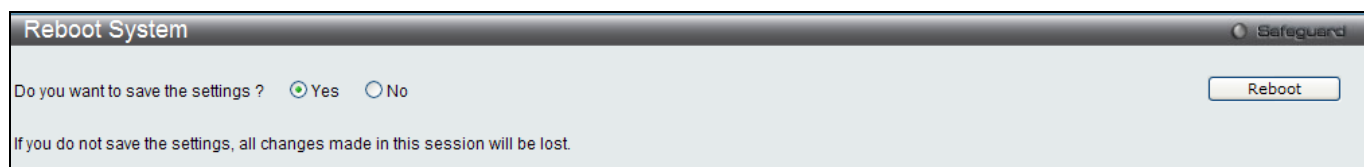


Figure 8 - 9. Reboot System window

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.

Appendix A Password Recovery Procedure

This document describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This document will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

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.

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                                     V1.00.006
-----
Power On Self Test ..... 100%

MAC Address   : 00-63-32-28-01-01
H/W Version   : B1

Please wait, loading V1.28.005 Runtime image ..... 100%

The switch is now entering Password Recovery Mode.
```

```
The switch is currently in Password Recovery Mode.
>
```

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

Appendix B 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 cold start	System cold start	Critical
	System warm start	System warm start	Critical
	Configuration saved to flash	Configuration saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	Configuration saved to flash by console	Configuration saved to flash by console (Username: <username>)	Informational
	System log saved to flash	System log saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	System log saved to flash by console	System log saved to flash by console (Username: <username>)	Informational
	Configuration and log saved to flash	Configuration and log saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	Configuration and log saved to flash by console	Configuration and log saved to flash by console (Username: <username>)	Informational
Upload/Download	Firmware upgraded successfully	Firmware upgraded successfully (Username: <username>, IP: <ipaddr>)	Informational
	Firmware upgraded by console successfully	Firmware upgraded by console successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful	Firmware upgrade was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Firmware upgrade by console was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded (Username: <username>, IP: <ipaddr>)	Informational
	Configuration successfully downloaded by console	Configuration successfully by console downloaded (Username: <username>)	Informational
	Configuration download was unsuccessful	Configuration download was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration download by console was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded (Username: <username>, IP: <ipaddr>)	Informational
	Configuration successfully	Configuration successfully by console uploaded	Informational

	uploaded by console	(Username: <username>)	
	Configuration upload was unsuccessful	Configuration upload was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration upload by console was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>)	Warning
	Log message successfully uploaded	Log message successfully uploaded (Username: <username>, IP: <ipaddr>)	Informational
	Log message successfully uploaded by console	Log message successfully by console uploaded (Username: <username>)	Informational
	Log message upload was unsuccessful	Log message upload was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Log message upload by console was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>)	Warning
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>, IP: <ipaddr>)	Informational
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>)	Informational
	Web session timed out	Web session timed out (Username: <username>, IP: <ipaddr>)	Informational
	Successful login through Web (SSL)	Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Web (SSL)	Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>)	Warning
	Login failed through Web (SSL)	Login failed through Web (SSL) due to AAA server timeout or improper configuration	Informational
	Logout through Web (SSL)	Logout through Web (SSL) (Username: <username>, IP: <ipaddr>)	Informational
	Web (SSL) session timed	Web (SSL) session timed out (Username: <username>,	Informational

	out	IP: <ipaddr>)	
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Warning
STP	Topology changed	Topology changed (Instance:<InstanceID> port<portNum>)	Informational
	New Root selected	[CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>)	Informational
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational
	Root restriction enabled	Port <portNum> STP root restriction is enabled	Informational
	Root restriction disabled	Port <portNum> STP root restriction is disabled	Informational
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>)	Warning
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational
	SSH server is enabled	SSH server is enabled	Informational
	SSH server is disabled	SSH server is disabled	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	Successful login through Console authenticated by AAA	Informational

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

	local_enable method		
	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>)	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>)	Warning
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Web(SSL) authenticated by AAA local_enable method	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	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>)	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>)	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>)	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>)	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>)	Informational
	Successful Enable Admin through Web (SSL) authenticated by AAA none method.	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	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>)	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>)	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
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
Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
Successful Enable Admin through Web(SSL) authenticated by AAA server	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
Enable Admin failed through Web (SSL) authenticated by AAA server	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
Enable Admin failed through Telnet 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>)	Warning
Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational

	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through SSH 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>)	Warning
	AAA server response is wrong	AAA server <serverIP> (Protocol: <protocolname>) response is wrong	Warning
	AAA doesn't support this functionality.	AAA doesn't support this functionality.	Informational
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning
Port security	Port security has exceeded its maximum learning size and will not learn any new addresses	Port security violation (Port: <portNum>, MAC: <macaddr>)	Warning
IP-Mac-port Binding	Unauthenticated IP address discarded by IP mac port binding	Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry is conflicting with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static FDB	Dynamic IMPB entry is conflicting with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry is conflicting with static IMPB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Creating IMPB entry failed due to no ACL rule available	Creating IMPB entry failed due to no ACL rule available(IP:<ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	the number of blocked entries reaches the threshold on a port	Port <portNum> enters stop IMPB learning state.	Warning
	User manually recover from IMPB stop learning state.	Port <portNum> recovers from IMPB stop learning state.	Warning
IP and Password Changed	IP Address change activity	Management IP address was changed into <ipAddr> by (Username: <username>, IP:<ipaddr>)	Informational
	IP Address change activity by console	Management IP address was changed into <ipAddr> by console (Username: <username>)	Informational
	Password change activity	User <username> Password was changed by (Username: <username>, IP:<ipaddr>)	Informational
	Password change activity by console	User <username> Password was changed by console (Username: <username>)	Informational
Safeguard	Safeguard Engine is in	Safeguard Engine enters NORMAL mode	Informational

Engine	normal mode		
	Safeguard Engine is in exhausted mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast storm 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 shutdown due to a packet storm	Port <portNum> is currently shutdown due to a packet storm	Warning
Gratuitous ARP	Conflict IP was detected with this device	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>), Interface: <interface>)	Informational
802.1X	Radius server assigned VID: to port	Radius server <server_ip> assigned VID: <VLAN_ID> to Port <portNum> (Account: <user_account>)	Informational
	Radius server assigned ingress bandwidth: Kbits to port	Radius server <server_ip> assigned ingress bandwidth: <bandwidth_value>Kbits to Port<portNum> (Account: <user_account>)	Informational
	Radius server assigned ingress bandwidth: no limit to port	Radius server <server_ip> assigned ingress bandwidth: no limit to Port <portNum> (Account: <user_account>)	Informational
	Radius server assigned egress bandwidth: Kbits to port	Radius server <server_ip> assigned egress bandwidth: <bandwidth_value> Kbits to Port <portNum> (Account: <user_account>)	Informational
	Radius server assigned egress bandwidth: no limit to Port	Radius server <server_ip> assigned egress bandwidth: no limit to Port<portNum> (Account: <user_account>)	Informational
	Radius server assigned 802.1p default priority: to Port	Radius server <server_ip> assigned 802.1p default priority: <priority 0-7> to Port <portNum> (Account: <user_account>)	Informational
	802.1x Authentication failure	802.1x Authentication failure from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication failure for the radius server	802.1x Authentication failure for the radius server <server_ip> timeout from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication failure for the 802.1X client session timeout	802.1x Authentication failure for the 802.1X client session timeout from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication success	802.1x Authentication success from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Informational
Loopback	Port loop occurred	Port <portNum> LBD loop occurred. Port blocked.	Critical
	Port loop detection	Port <portNum> LBD port recovered. Loop detection	Informational

	restarted after interval time	restarted.	
	Port with VID loop occurred	Port <portNum> VID <vlanID> LBD loop occurred. Packet discard begun.	Critical
	Port with VID Loop detection restarted after interval time	Port <portNum> VID <vlanID> LBD recovered. Loop detection restarted.	Informational
	VLAN LOOP Max Number exceed	Loop VLAN number overflow	Informational
Denial of Service	The DoS attack is blocked	<dos_name> is detected from (IP: <ipaddr> Port: <portNum>)	Critical
MAC-based Access Control	A host fails to pass the authentication	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>)	Informational
	A host passes the authentication	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	A host is aged out.	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	Failed to assign ACL profiles/rules from RADIUS server	RADIUS server <ipAddr> assigns <username> ACL failure at port <portNum> (<string>)	Warning
OAM	Dying gasp event(remote)	OAM dying gasp event received (Port <portNum>)	Warning
	Dying gasp event(local)	Device encountered an OAM dying gasp event.	Warning
	Critical event(remote)	OAM critical event event received (Port <portNum>)	Warning
	Critical event(local)	Device encountered an OAM critical event	Warning
	Errored Symbol Period Event(remote)	Errored symbol period event received (Port <portNum>)	Warning
	Errored Frame Event	Errored frame event received(Port <portNum>)	Warning
	Errored Frame Period Event	Errored frame period event received(Port <portNum>)	Warning
	Errored Frame Seconds Summary Event	Errored frame seconds summary event received (Port <portNum>)	Warning
	Remote loopback start	OAM Remote loopback started (Port <portNum>)	Warning
	Remote loopback stop	OAM Remote loopback terminated (Port <portNum>)	Warning
ERPS	Signal fail detected	Signal fail detected on node (MAC: <macaddr>)	Informational
	Signal fail cleared	Signal fail cleared on node (MAC: <macaddr>)	Informational
	RPL owner conflict	RPL owner conflicted on the ring (MAC: <macaddr>)	Warning
BPDU Protection	BPDU attack happened.	Port <portNum> enter BPDU under protection state (mode: drop / block / shutdown)	Informational

	BPDU attack automatically recover	Port <portNum> recover from BPDU under protection state automatically	Informational
	BPDU attack manually recover	Port <portNum> recover from BPDU under protection state manually	Informational
CFM	Cross-connect is detected	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <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 <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 <portNum>, Direction:<mepdirection>)	Warning
	Remote MEP's MAC reports an error status	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Warning
	Remote MEP detects CFM defects	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Informational
DHCP Server Screening	Detected untrusted DHCP server IP address.	Detected untrusted DHCP server(IP: <ipaddr>,	Informational

Appendix C Trap List

Trap Name/OID	Variable Bind	Format	MIB Name
coldStart 1.3.6.1.6.3.1.1.5.1	None	V2	RFC1907 (SNMPv2-MIB)
warmStart 1.3.6.1.6.3.1.1.5.2	None	V2	RFC1907 (SNMPv2-MIB)
authenticationFailure 1.3.6.1.6.3.1.1.5.5	None	V2	RFC1907 (SNMPv2-MIB)
linkDown 1.3.6.1.6.3.1.1.5.3	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)
linkup 1.3.6.1.6.3.1.1.5.4	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)
newRoot 1.3.6.1.2.1.17.0.1	None	V2	RFC1493 (BRIDGE-MIB)
topologyChange 1.3.6.1.2.1.17.0.2	None	V2	RFC1493 (BRIDGE-MIB)
risingAlarm 1.3.6.1.2.1.16.0.1	alarmIndex alarmVariable alarmSampleType alarmValue alarmRisingThreshold	V2	rfc2819 (RMON-MIB)
fallingAlarm 1.3.6.1.2.1.16.0.2	alarmIndex alarmVariable alarmSampleType alarmValue alarmFallingThreshold	V2	rfc2819 (RMON-MIB)
LldpRemTablesChange 1.0.8802.1.1.2.0.0.1	lldpStatsRemTablesInserts lldpStatsRemTablesDeletes lldpStatsRemTablesDrops lldpStatsRemTablesAgeouts	V2	LLDP-MIB
dot1agCfmFaultAlarm	dot1agCfmMepHighestPrDefect	V2	IEEE8021-CFM-MIB
dot3OamThresholdEvent	dot3OamEventLogTimestamp	V2	DOT3-OAM-MIB

1.3.6.1.2.1.158.0.1	dot3OamEventLogOui dot3OamEventLogType dot3OamEventLogLocation dot3OamEventLogWindowHi dot3OamEventLogWindowLo dot3OamEventLogThresholdHi dot3OamEventLogThresholdLo dot3OamEventLogValue dot3OamEventLogRunningTotal dot3OamEventLogEventTotal		
dot3OamNonThresholdEvent 1.3.6.1.2.1.158.0.2	dot3OamEventLogTimestamp dot3OamEventLogOui dot3OamEventLogType dot3OamEventLogLocation dot3OamEventLogEventTotal	V2	DOT3-OAM-MIB

Proprietary Trap List

Trap Name/OID	Variable Bind	Format	MIB Name
SwIpMacBindingViolationTrap 1.3.6.1.4.1.171.12.23.5.0.1	swIpMacBindingPortIndex swIpMacBindingViolationIP swIpMacBindingViolationMac	V2	IPMacBind-MIB
swIpMacBindingStopLearningTrap 1.3.6.1.4.1.171.12.23.5.0.2	swIpMacBindingPortIndex	V2	IPMacBind-MIB
swIpMacBindingRecoverLearningTrap 1.3.6.1.4.1.171.12.23.5.0.3	swIpMacBindingPortIndex	V2	IPMacBind-MIB
swMacBasedAuthLoggedSuccess 1.3.6.1.4.1.171.12.35.11.1.0.1	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
SwMacBasedAuthLoggedFail 1.3.6.1.4.1.171.12.35.11.1.0.2	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
SwMacBasedAuthAgesOut 1.3.6.1.4.1.171.12.35.11.1.0.3	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
swPktStormOccurred 1.3.6.1.4.1.171.12.25.5.0.1	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB

swPktStormCleared 1.3.6.1.4.1.171.12.25.5.0.2	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB
agentGratuitousARPTrap 1.3.6.1.4.1.171.12.1.7.2.0.5	agentGratuitousARPIpAddr agentGratuitousARPMacAddr agentGratuitousARPPortNumber agentGratuitousARPInterfaceName	V2	Genmgmt-MIB
swSafeGuardChgToExhausted 1.3.6.1.4.1.171.12.19.4.1.0.1	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB
swSafeGuardChgToNormal 1.3.6.1.4.1.171.12.19.4.1.0.2	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB
swDoSAttackDetected 1.3.6.1.4.1.171.12.59.4.0.1	swDoSCtrlType swDoSNotifyVarIpAddr swDoSNotifyVarPortNumber	V2	DoSPrev-MIB
swSingleIPMSColdStart 1.3.6.1.4.1.171.12.8.6.0.11	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSWarmStart 1.3.6.1.4.1.171.12.8.6.0.12	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSLinkDown 1.3.6.1.4.1.171.12.8.6.0.13	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SINGLE-IP-MIB
swSingleIPMSLinkUp 1.3.6.1.4.1.171.12.8.6.0.14	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SINGLE-IP-MIB
swSingleIPMSAuthFail 1.3.6.1.4.1.171.12.8.6.0.15	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSnewRoot 1.3.6.1.4.1.171.12.8.6.0.16	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSTopologyChange 1.3.6.1.4.1.171.12.8.6.0.17	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSrisingAlarm 1.3.6.1.4.1.171.12.8.6.0.18	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSfallingAlarm 1.3.6.1.4.1.171.12.8.6.0.19	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSmacNotification 1.3.6.1.4.1.171.12.8.6.0.20	swSingleIPMSID swSingleIPMSMacAddr swSingleIPMSTrapMessage	V2	SINGLE-IP-MIB
swERPSSFDetectedTrap 1.3.6.1.4.1.171.12.78.4.0.1	swERPSSNodeId	V2	ERPS-MIB

swERPSSFClearedTrap 1.3.6.1.4.1.171.12.78.4.0.2	swERPSNodeId	V2	ERPS-MIB
swERPSPLOwnerConflictTrap 1.3.6.1.4.1.171.12.78.4.0.3	swERPSNodeId	V2	ERPS-MIB
swBpduProtectionUnderAttackingTrap 1.3.6.1.4.1.171.12.76.4.0.1	swBpduProtectionPortIndex swBpduProtectionPortMode	V2	BPDU- PROTECTION-MIB
swBpduProtectionRecoveryTrap 1.3.6.1.4.1.171.12.76.4.0.2	swBpduProtectionPortIndex swBpduProtectionRecoveryMethod	V2	BPDU- PROTECTION-MIB
swFilterDetectedTrap 1.3.6.1.4.1.171.12.37.100.0.1	swFilterDetectedIP swFilterDetectedport	V2	FILTER-MIB
swL2PortSecurityViolationTrap 1.3.6.1.4.1.171.11.113.1.1.2.20.0.1 1.3.6.1.4.1.171.11.113.1.2.2.20.0.1 1.3.6.1.4.1.171.11.113.1.3.2.20.0.1 1.3.6.1.4.1.171.11.113.1.4.2.20.0.1	swL2PortSecurityPortIndex swL2PortSecurityViolationMac	V2	des3200-10- L2mgmt.mib des3200-18- L2mgmt.mib des3200-26- L2mgmt.mib des3200-28- L2mgmt.mib des3200-28f- L2mgmt.mib
swL2macNotification 1.3.6.1.4.1.171.11.113.1.1.2.20.0.2 1.3.6.1.4.1.171.11.113.1.2.2.20.0.2 1.3.6.1.4.1.171.11.113.1.3.2.20.0.2 1.3.6.1.4.1.171.11.113.1.4.2.20.0.2	swL2macNotifyInfo	V2	des3200-10- L2mgmt.mib des3200-18- L2mgmt.mib des3200-26- L2mgmt.mib des3200-28- L2mgmt.mib des3200-28f- L2mgmt.mib
swL2PortLoopOccurred 1.3.6.1.4.1.171.11.113.1.1.2.20.0.3 1.3.6.1.4.1.171.11.113.1.2.2.20.0.3 1.3.6.1.4.1.171.11.113.1.3.2.20.0.3 1.3.6.1.4.1.171.11.113.1.4.2.20.0.3	swL2LoopDetectPortIndex	V2	des3200-10- L2mgmt.mib des3200-18- L2mgmt.mib des3200-26- L2mgmt.mib des3200-28- L2mgmt.mib des3200-28f- L2mgmt.mib
swL2PortLoopRestart 1.3.6.1.4.1.171.11.113.1.1.2.20.0.4 1.3.6.1.4.1.171.11.113.1.2.2.20.0.4 1.3.6.1.4.1.171.11.113.1.3.2.20.0.4 1.3.6.1.4.1.171.11.113.1.4.2.20.0.4	swL2LoopDetectPortIndex	V2	des3200-10- L2mgmt.mib des3200-18- L2mgmt.mib des3200-26- L2mgmt.mib des3200-28- L2mgmt.mib

			des3200-28f-L2mgmt.mib
swL2VlanLoopOccurred 1.3.6.1.4.1.171.11.113.1.1.2.20.0.5 1.3.6.1.4.1.171.11.113.1.2.2.20.0.5 1.3.6.1.4.1.171.11.113.1.3.2.20.0.5 1.3.6.1.4.1.171.11.113.1.4.2.20.0.5	swL2LoopDetectPortIndex swL2VlanLoopDetectVID	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2VlanLoopRestart 1.3.6.1.4.1.171.11.113.1.1.2.20.0.6 1.3.6.1.4.1.171.11.113.1.2.2.20.0.6 1.3.6.1.4.1.171.11.113.1.3.2.20.0.6 1.3.6.1.4.1.171.11.113.1.4.2.20.0.6	swL2LoopDetectPortIndex swL2VlanLoopDetectVID	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib

Appendix D RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DES-3200 is used in the following modules: 802.1X (Port-based and Host-based), and MAC-based Access Control.

The description that follows explains the following RADIUS Attributes Assignment types:

- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign **Ingress/Egress bandwidth by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of "0" or more, than the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to *no_limited*.

To assign **802.1p default priority by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or Host-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign **VLAN by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC-based Access Control authentication is successful, the port will be added to VLAN 3. However, if the user does not configure the VLAN attribute and authenticates successfully, the port will be kept in its original VLAN. If the VLAN attribute configured on the RADIUS server does not exist, the port will not be assigned to the requested VLAN.

To assign **ACL by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for an ACL. The RADIUS ACL assignment is only used in MAC-based Access Control.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	12 (for ACL profile) 13 (for ACL rule)	Required
Attribute-Specific Field	Used to assign the ACL profile or rule.	ACL Command For example: ACL profile: create access_profile ethernet vlan 0xFFF profile_id 100; ACL rule: config access_profile profile_id 100 add access_id auto_assign ethernet vlan_id default port all deny;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile ethernet vlan 0xFFF profile_id 100**; ACL rule: **config access_profile profile_id 100 add access_id auto_assign ethernet**), and the MAC-based Access Control authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to Chapter 22 Access Control List (ACL) Commands.