



# User Manual

Product Model: **DGS-3700 Series**

Layer 2 Managed Gigabit Ethernet Switch

Release 1.00

Information in this document is subject to change without notice.

© 2009 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.

July 2009 P/N 651370012005G

# Table of Contents

Preface.....	xi
Intended Readers .....	1
Typographical Conventions.....	1
Notes, Notices, and Cautions .....	1
<b>Web-based Switch Configuration .....</b>	<b>2</b>
Introduction .....	2
Login to Web Manager.....	2
Web-based User Interface .....	3
Web Pages .....	4
<b>Configuration .....</b>	<b>6</b>
Device Information.....	7
System Information.....	7
Serial Port Settings.....	8
IP Address .....	9
Setting the Switch's IP Address using the Console Interface .....	11
Interface Settings.....	11
IPv6 Route Settings.....	13
IPv6 Neighbor Settings.....	13
Port Configuration.....	14
Port Settings .....	14
Port Description .....	15
Port Error Disabled .....	16
Static ARP Settings .....	16
User Accounts .....	17
System Log Configuration .....	20
System Log Settings.....	20
System Log Server .....	20
System Severity Settings.....	22
DHCP Relay.....	23
DHCP Relay Global Settings .....	23
DHCP Relay Interface Settings.....	26
DHCP Relay Option 60 Default Settings.....	26
DHCP Relay Option 60 Settings .....	27
DHCP Relay Option 61 Default Settings.....	27
DHCP Relay Option 61 Settings .....	28
Out of Band Management Settings .....	28
External Alarm Settings .....	29
DHCP Auto Configuration Settings.....	29
MAC Address Aging Time .....	30
Web Settings .....	30

Telnet Settings .....	30
Password Encryption .....	31
Clipaging Settings .....	31
Firmware Information .....	31
Dual Configuration Settings .....	32
Ping Test .....	33
Local Loopback Ports Settings .....	34
VLAN Counter Settings .....	35
SNTP Settings .....	36
Time Settings .....	36
TimeZone Settings .....	37
MAC Notification Settings .....	38
MAC Notification Global Settings .....	38
MAC Notification Port Settings .....	39
SNMP Settings .....	40
SNMP Global State Settings .....	41
SNMP View Table .....	41
SNMP Group Table .....	42
SNMP User Table .....	43
SNMP Community Table .....	44
SNMP Host Table .....	45
SNMP v6Host Table .....	45
SNMP Engine ID .....	46
SNMP Trap Configuration .....	47
Time Range Settings .....	47
sFlow .....	48
sFlow Global State Settings .....	48
sFlow Analyzer Server Settings .....	48
sFlow Flow Sampler Settings .....	49
sFlow Counter Poller Settings .....	50
Single IP Management .....	51
Single IP Settings .....	52
Topology .....	53
Tool Tips .....	56
Right-Click .....	57
Menu Bar .....	59
Firmware Upgrade .....	60
Configuration File Backup/Restore .....	60
Upload Log File .....	61
DDM .....	61
Browse DDM Status List .....	61
DDM Settings .....	61
DDM Temperature Threshold Settings .....	62
DDM Voltage Threshold Settings .....	63

DDM Bias Current Threshold Settings .....	63
DDM Tx Power Threshold Settings .....	64
DDM Rx Power Threshold Settings .....	64
<b>L2 Features .....</b>	<b>66</b>
Jumbo Frame .....	66
VLANs .....	67
Understanding IEEE 802.1p Priority .....	67
VLAN Description .....	67
IEEE 802.1Q VLANs .....	68
Double VLANs .....	72
802.1Q VLAN .....	74
Subnet VLAN .....	78
Subnet VLAN Settings .....	78
VLAN Precedence Settings .....	78
Q-in-Q .....	79
Q-in-Q Settings .....	79
VLAN Translation Settings .....	80
Q-in-Q and VLAN Translation Rules .....	81
802.1v Protocol VLAN .....	82
802.1v Protocol Group Settings .....	82
802.1v Protocol VLAN Settings .....	83
RSPAN Settings .....	84
GVRP Settings .....	84
GVRP Global Settings .....	85
MAC-based VLAN Settings .....	86
PVID Auto Assign Settings .....	86
Port Trunking .....	87
LACP Port Settings .....	89
Traffic Segmentation .....	90
BPDU Tunneling Settings .....	91
IGMP Snooping .....	92
IGMP Snooping Settings .....	92
IGMP Snooping Rate Limit Settings .....	94
IGMP Snooping Static Group Settings .....	94
IGMP Multicast Group Profile Settings .....	95
IGMP Snooping Multicast VLAN Settings .....	95
IPv4 Multicast Profile Settings .....	96
IPv4 Limited Multicast Range Settings .....	97
IPv4 Max Multicast Group Settings .....	97
MLD Snooping .....	98
MLD Snooping Settings .....	98
MLD Snooping Rate Limit Settings .....	100
MLD Snooping Static Group Settings .....	101
MLD Multicast Group Profile Settings .....	101

MLD Snooping Multicast VLAN Settings .....	102
IPv6 Multicast Profile Settings.....	103
IPv6 Limited Multicast Range Settings.....	104
IPv6 Max Multicast Group Settings .....	104
Port Mirror .....	105
Loopback Detection Settings .....	106
Spanning Tree .....	107
STP Bridge Global Settings .....	109
STP Port Settings .....	111
MST Configuration Identification .....	112
STP Instance Settings .....	113
MSTP Port Information .....	114
Forwarding & Filtering.....	115
Unicast Forwarding .....	115
Multicast Forwarding.....	115
Multicast Filtering Mode .....	116
LLDP .....	116
LLDP Global Settings.....	117
LLDP Port Settings .....	118
LLDP Management Address List .....	119
LLDP Basic TLVs Settings.....	119
LLDP Dot1 TLVs Settings .....	120
LLDP Dot3 TLVs Settings .....	121
LLDP Statistics System.....	121
LLDP Local Port Information.....	122
LLDP Remote Port Information.....	123
CFM .....	123
CFM Port Settings.....	123
CFM CCM PDUs Forwarding Mode.....	124
CFM MPs Reply LTRs .....	124
CFM MIPCCM List.....	124
Connectivity Fault Management Settings.....	125
CFM Loopback Settings.....	126
CFM Linktrace Settings.....	127
Ethernet OAM .....	128
Ethernet OAM Settings .....	128
Ethernet OAM Configuration Settings.....	129
<b>QoS .....</b>	<b>130</b>
Advantages of QoS.....	130
Understanding QoS .....	131
HOL Blocking Pevention.....	133
Bandwidth Control .....	133
Traffic Control .....	134
802.1p Default Priority .....	136

802.1p User Priority .....	137
QoS Scheduling Mechanism .....	137
QoS Scheduling .....	138
In Band Manage Settings .....	139
SRED .....	140
SRED Settings .....	140
SRED Drop Counter .....	142
DSCP Trust Settings .....	142
DSCP Map Settings .....	142
802.1p Map Settings .....	144
<b>Security .....</b>	<b>145</b>
Safeguard Engine .....	145
Trusted Host .....	147
IP-MAC-Port Binding .....	147
IMP Binding Global Settings .....	147
IMP Binding Port Settings .....	148
IMP Binding Entry Settings .....	150
DHCP Snooping Entries .....	151
MAC Block List .....	151
Port Security .....	151
Port Security Port Settings .....	151
Port Security VLAN Settings .....	152
Port Security Entries .....	153
DHCP Server Screening Settings .....	153
DHCP Screening Port Settings .....	154
DHCP Offer Filtering .....	154
802.1X .....	155
802.1X Port-Based and Host-Based Access Control .....	155
Understanding 802.1X Port-based and Host-based Network Access Control .....	158
Port-Based Network Access Control .....	158
Host-Based Network Access Control .....	159
802.1X Global Settings .....	160
802.1X Port Settings .....	160
802.1X User .....	162
Authentication RADIUS Server .....	162
Initialize Port(s) .....	163
Reauthenticate Port(s) .....	163
Guest VLAN Configuration .....	164
Guest VLAN .....	165
SSL Settings .....	165
Download Certificate .....	166
Ciphersuite .....	166
SSH .....	168
SSH Settings .....	168

SSH Authmode and Algorithm Settings .....	169
SSH User Authentication Lists .....	170
<b>Access Authentication Control</b> .....	<b>171</b>
Authentication Policy Settings.....	173
Application Authentication Settings.....	173
Authentication Server Group.....	174
Authentication Server.....	175
Login Method Lists.....	176
Enable Method Lists .....	177
Local Enable Password Settings.....	178
RADIUS Accounting Settings.....	179
<b>MAC-based Access Control</b> .....	<b>180</b>
Notes About MAC-based Access Control .....	180
MAC-based Access Control Settings .....	180
MAC-based Access Control Local Settings.....	182
<b>Web Authentication</b> .....	<b>183</b>
Conditions and Limitations.....	184
Web-based Access Control Settings.....	184
Web-based Access Control User Settings.....	185
<b>NetBIOS Filtering</b> .....	<b>186</b>
NetBIOS Filtering Settings .....	186
<b>ACL</b> .....	<b>187</b>
ACL Configuration Wizard .....	187
Access Profile List .....	188
CPU Interface Filtering .....	205
CPU Access Profile List.....	206
ACL Finder.....	217
ACL Flow Meter .....	217
<b>Monitoring</b> .....	<b>220</b>
Device Status.....	220
Cable Diagnostic.....	220
CPU Utilization.....	221
Port Utilization.....	222
Packet Size .....	222
Memory Utilization .....	224
Packets .....	224
Received (RX).....	224
UMB_cast (RX).....	226
Transmitted (TX) .....	227
Errors .....	230
Received (RX).....	230
Transmitted (TX) .....	231
Port Access Control .....	233



RADIUS Authentication.....	233
RADIUS Account Client .....	234
Authenticator State .....	236
Authenticator Statistics .....	237
Authenticator Session Statistics.....	238
Authenticator Diagnostics .....	239
Browse ARP Table .....	241
VLAN.....	242
Browse VLAN.....	242
Show VLAN Ports .....	243
IGMP Snooping .....	243
Browse IGMP Router Port.....	243
IGMP Snooping Group.....	243
IGMP Snooping Forwarding Table.....	244
Browse IGMP Snooping Counter .....	244
MLD Snooping .....	245
Browse MLD Router Port.....	245
MLD Snooping Group .....	245
MLD Snooping Forwarding Table .....	246
Browse MLD Snooping Counter.....	247
Browse Session Table .....	247
CFM .....	247
CFM Packet Counter List.....	247
CFM Packet Counter CCM List.....	248
Browse CFM Fault MEP.....	248
Browse CFM Port MP List.....	248
MAC Address Table.....	249
Browse VLAN Counter Statistics .....	249
Ethernet OAM .....	250
Browse Ethernet OAM Event Log .....	250
Browse Ethernet OAM Statistics.....	250
Historical Counter & Utilization .....	252
Browse Historical Counter.....	252
Browse Historical Utilization.....	253
System Log .....	253
<b>Save Services and Tools.....</b>	<b>255</b>
Save Configuration ID 1.....	255
Save Configuration ID 2.....	256
Save Log.....	256
Save All.....	256
Configuration File Backup & Restore .....	257
Upload Log File.....	257
Reset.....	257

Download Firmware .....	258
Reboot System .....	258
<b>Mitigating ARP Spoofing Attacks Using Packet Content ACL.....</b>	<b>259</b>
<b>System Log Entries .....</b>	<b>267</b>
<b>Glossary.....</b>	<b>278</b>
<b>Password Recovery Procedure .....</b>	<b>280</b>

## Preface

The **DGS-3700 Series User Manual** is divided into sections that describe the system installation and operating instructions with examples.

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

**Section 2, Configuration** – A detailed discussion about configuring some of the basic functions of the Switch, including accessing the System information, Serial Port Settings, IP Address, Interface Settings, IPv6 Route Settings, IPv6 Neighbor Settings, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, System Severity Settings, DHCP Relay, Out of Band Management Settings, External Alarm Settings, DHCP Auto Configuration Settings, MAC Address Aging Time, Web Settings, Telnet Settings, Password Encryption, Clipaging Settings, Firmware Information, Dual Configuration Settings, Ping Test, Local Loopback Port Settings, VLAN Counter Settings, SNMP Settings, MAC Notification Settings, SNMP Settings, Time Range Settings, sFlow, Single IP Management and DDM.

**Section 3, L2 Features** – A discussion of the Layer 2 features on the Switch, including Jumbo Frame, 802.1Q VLAN, Subnet VLAN, QinQ, 802.1v Protocol VLAN, RSPAN Settings, GVRP Settings, GVRP Global Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, BPDU Tunneling Settings, IGMP Snooping, MLD Snooping, Port Mirror, Loopback Detection Settings, Spanning Tree, Forwarding & Filtering, LLDP, CFM and Ethernet OAM.

**Section 4, QoS** – Features information on Switch QoS functions, including HOL Blocking Prevention, Bandwidth Control, Traffic Control, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Mechanism, QoS Scheduling, In Band Manage Settings and SRED.

**Section 5, Security** – Features information on Switch security functions, including Safeguard Engine, Trusted Host, IP-MAC-Port Binding, Port Security, DHCP Server Screening, 802.1X, SSL Settings, SSH, Access Authentication Control, MAC-based Access Control, Web Authentication, and NetBIOS Filtering Settings.

**Section 6, ACL** – Discussion on the ACL functions of the Switch, including ACL Configuration Wizard, Access Profile List, CPU Access Profile List, ACL Finder, and ACL Flow Meter.

**Section 7, Monitoring** – Features information about the monitoring functions on the Switch including, Cable Diagnostic, CPU Utilization, Port Utilization, Packet Size, Memory Utilization, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, IGMP Snooping, MLD Snooping, Browse Session Table, CFM, MAC Address Table, Browse VLAN Counter Statistics, Ethernet OAM and Historical Counter & Utilization.

**Section 8, Save Services and Tools** – Save Configuration ID 1, Save Configuration ID 2, Save Log, Save All, Configuration File Backup and Restore, Upload Log File, Reset, Download Firmware, and Reboot System.

**Appendix A, Mitigating ARP Spoofing Attacks Using Packet Content ACL** – This section introduces ARP protocol, ARP spoofing attacks, and the counter measure brought by D-Link's switches to counter ARP spoofing attacks.

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

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

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

## Intended Readers

The *DGS-3700 Series Manual* contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

## Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
<b>Bold font</b>	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the <b>File</b> menu and choose <b>Cancel</b> . 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.
<b>Boldface Typewriter Font</b>	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.
<b>Menu Name &gt; Menu Option</b>	<b>Menu Name &gt; Menu Option</b> Indicates the menu structure. <b>Device &gt; Port &gt; Port Properties</b> 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 Opera, Netscape Navigator/Communicator, or Microsoft Internet Explorer. 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.

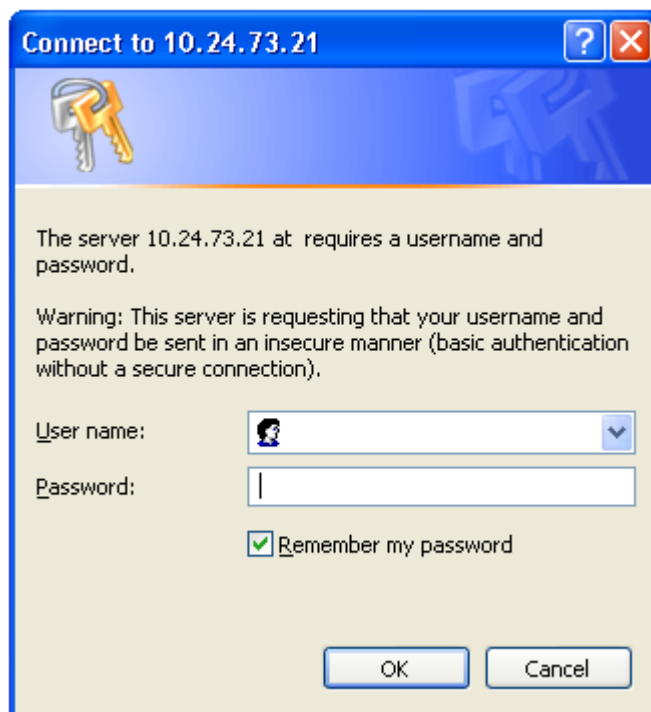
## Login to Web Manager

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.



**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.

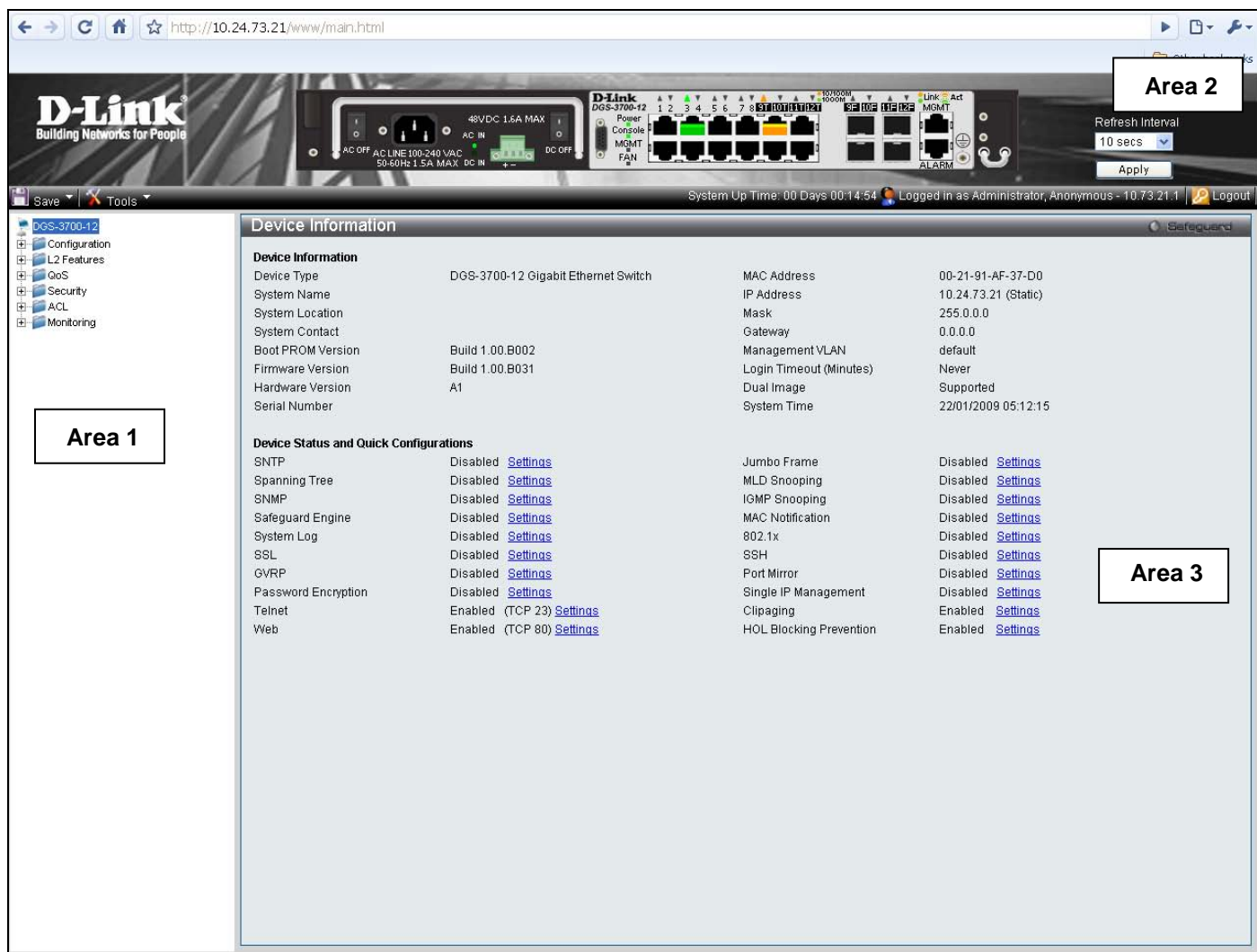


Figure 1 - 2 Main Web-Manager page

Area	Function
Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyper-linked window buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, 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 Changes web menu (explained below) or use the command line interface (CLI) command save.

## 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** – A detailed discussion about configuring some of the basic functions of the Switch, accessing the System information, Serial Port Settings, IP Address, Interface Settings, IPv6 Route Settings, IPv6 Neighbor Settings, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, System Severity Settings, DHCP Relay, Out of Band Management Settings, External Alarm Settings, DHCP Auto Configuration Settings, MAC Address Aging Time, Web Settings, Telnet Settings, Password Encryption, Clipping Settings, Firmware Information, Dual Configuration Settings, Ping Test, Local Loopback Port Settings, VLAN Counter Settings, SNMP Settings, MAC Notification Settings, SNMP Settings, Time Range Settings, sFlow, Single IP Management and DDM.

**L2 Features** – A discussion of the Layer 2 features on the Switch, including Jumbo Frame, 802.1Q VLAN, Subnet VLAN, QinQ, 802.1v Protocol VLAN, RSPAN Settings, GVRP Settings, GVRP Global Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, BPDU Tunneling Settings, IGMP Snooping, MLD Snooping, Port Mirror, Loopback Detection Settings, Spanning Tree, Forwarding & Filtering, LLDP, CFM and Ethernet OAM.

**QoS** – Features information on Switch QoS functions, including HOL Blocking Prevention, Bandwidth Control, Traffic Control, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Mechanism, QoS Scheduling, In Band Manage Settings and SRED.

**Security** – Features information on Switch security functions, including Safeguard Engine, Trusted Host, IP-MAC-Port Binding, Port Security, DHCP Server Screening, 802.1X, SSL Settings, SSH, Access Authentication Control, MAC-based Access Control, Web Authentication, and NetBIOS Filtering Settings.

**ACL** – Discussion on the ACL functions of the Switch, including ACL Configuration Wizard, Access Profile List, CPU Access Profile List, ACL Finder, and ACL Flow Meter.

**Monitoring** – Features information about the monitoring functions on the Switch including, Cable Diagnostic, CPU Utilization, Port Utilization, Packet Size, Memory Utilization, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, IGMP Snooping, MLD Snooping, Browse Session Table, CFM, MAC Address Table, Browse VLAN Counter Statistics, Ethernet OAM and Historical Counter & Utilization and System Log.



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



## Section 2

# Configuration

*Device Information*

*System Information*

*Serial Port Settings*

*IP Address*

*Interface Settings*

*IPv6 Route Settings*

*IPv6 Neighbor Settings*

*Port Configuration*

*Static ARP Settings*

*User Accounts*

*System Log Configuration*

*System Severity Settings*

*DHCP Relay*

*Out of Band Management Settings*

*External Alarm Settings*

*DHCP Auto Configuration Settings*

*MAC Address Aging Time*

*Web Settings*

*Telnet Settings*

*Password Encryption*

*Clipaging Settings*

*Firmware Information*

*Dual Configuration Settings*

*Ping Test*

*Local Loopback Ports Settings*

*VLAN Counter Settings*

*SNTP Settings*

*MAC Notification Settings*

*SNMP Settings*

*Time Range Settings*

*sFlow*

*Single IP Management*

*DDM*

## 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 **DGS-3700-12/DGS-3700-12G Web Management Tool** folder. The **Device Information** window shows the Switch's **MAC Address** (assigned by the factory and unchangeable), the **Boot PROM Version**, **Firmware Version**, **Hardware Version** and **Serial Number** as well as other information about different settings on the Switch. This information is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status. Some functions are hyper-linked to their configuration window for easy access from the **Device Information** window.

Device Information			
<b>Device Information</b>			
Device Type	DGS-3700-12 Gigabit Ethernet Switch	MAC Address	00-21-91-AF-37-D0
System Name		IP Address	10.24.73.21 (Static)
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	Build 1.00.B002	Management VLAN	default
Firmware Version	Build 1.00.B031	Login Timeout (Minutes)	Never
Hardware Version	A1	Dual Image	Supported
Serial Number		System Time	22/01/2009 05:12:15
<b>Device Status and Quick Configurations</b>			
SNTP	Disabled <a href="#">Settings</a>	Jumbo Frame	Disabled <a href="#">Settings</a>
Spanning Tree	Disabled <a href="#">Settings</a>	MLD Snooping	Disabled <a href="#">Settings</a>
SNMP	Disabled <a href="#">Settings</a>	IGMP Snooping	Disabled <a href="#">Settings</a>
Safeguard Engine	Disabled <a href="#">Settings</a>	MAC Notification	Disabled <a href="#">Settings</a>
System Log	Disabled <a href="#">Settings</a>	802.1x	Disabled <a href="#">Settings</a>
SSL	Disabled <a href="#">Settings</a>	SSH	Disabled <a href="#">Settings</a>
GVRP	Disabled <a href="#">Settings</a>	Port Mirror	Disabled <a href="#">Settings</a>
Password Encryption	Disabled <a href="#">Settings</a>	Single IP Management	Disabled <a href="#">Settings</a>
Telnet	Enabled (TCP 23) <a href="#">Settings</a>	Clipaging	Enabled <a href="#">Settings</a>
Web	Enabled (TCP 80) <a href="#">Settings</a>	HOL Blocking Prevention	Enabled <a href="#">Settings</a>

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**.

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

**Figure 2 - 2 System Information window**

The fields that can be configured are described below:

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

Click **Apply** to implement changes made.

## Serial Port Settings

The following window contains information about the Serial Port Settings including the Baud Rate and the Auto Logout settings.

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

**Figure 2 - 3 Serial Port Settings window**

The fields that can be configured are described below:

Parameter	Description
<b>Baud Rate</b>	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>115200</i> , which is the default setting.
<b>Auto Logout</b>	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.

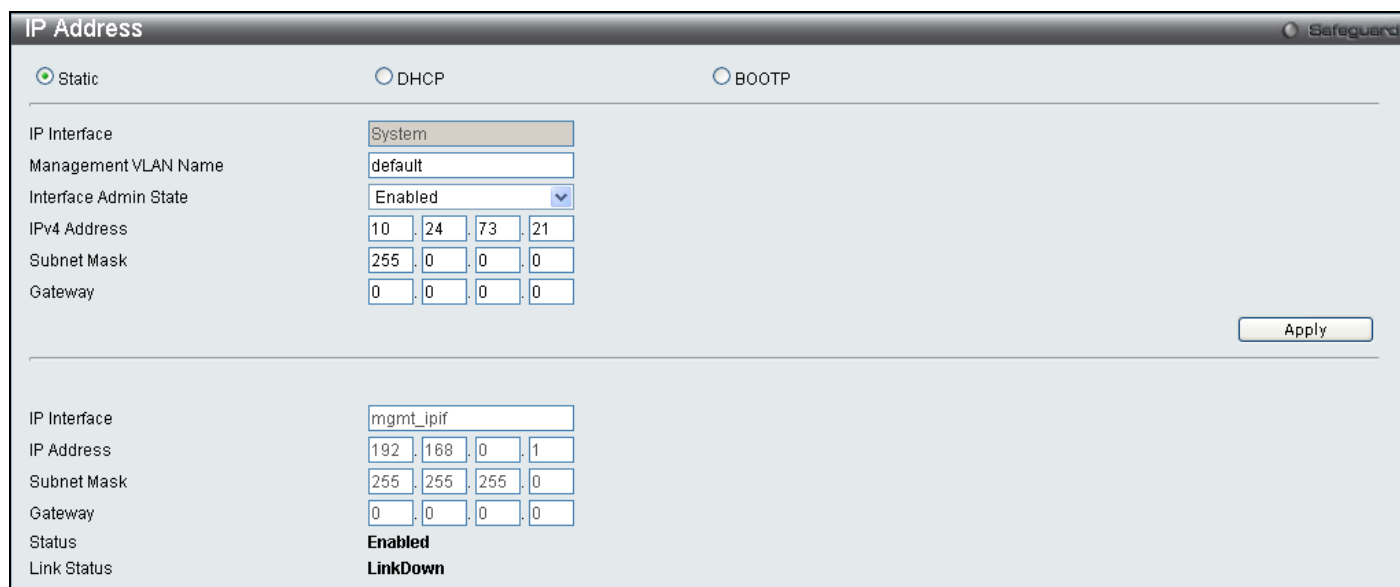


**NOTE:** If a user configures the serial port's baud rate, the baud rate will take effect and save immediately. Baud rate settings will not change even if the user resets or reboots the Switch. The Baud rate will only change when the user configures it again. The serial port's baud rate setting is not stored in the Switch's configuration file. Resetting the Switch will not restore the baud rate to the default setting.

## IP Address

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 *DGS-3700 Series CLI Manual* for more information.

To view this window, click **Configuration > IP Address** as shown below:



The screenshot shows the 'IP Address' configuration window. At the top, there are three radio buttons: 'Static' (selected), 'DHCP', and 'BOOTP'. Below the radio buttons, there are two sections. The first section, under 'Static', has the following fields: 'IP Interface' (System), 'Management VLAN Name' (default), 'Interface Admin State' (Enabled), 'IPv4 Address' (10.24.73.21), 'Subnet Mask' (255.0.0.0), and 'Gateway' (0.0.0.0). An 'Apply' button is located at the bottom right of this section. The second section, under 'DHCP', has the following fields: 'IP Interface' (mgmt\_ipif), 'IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), and 'Gateway' (0.0.0.0). Below these fields, there are two status indicators: 'Status' (Enabled) and 'Link Status' (LinkDown).

**Figure 2 - 4 IP Address Settings window**

The upper part of the page allows you to manually assign the Switch's IP address, subnet mask, and default gateway address:

1. Select *Static* at the top of the screen.
2. Enter the appropriate IP Address and Subnet Mask.
3. If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the Gateway. If you will manage the Switch from the subnet on which it is installed, you can 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* VLAN Name. The *default* VLAN contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the *Management VLAN Name* of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.



**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 *BOOTP* or *DHCP*, this will determine how the Switch will be assigned an IP address.

The lower part of the page is to display the Out-of-band management information that has been configured in **Configuration > Out of Band Management Settings** window.

The IP Address Settings options are:

Parameter	Description
<b>Static</b>	Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator.
<b>DHCP</b>	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.
<b>BOOTP</b>	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.
<b>IP Interface</b>	This field displays the IP Interface that is currently being used on the Switch.
<b>Management VLAN Name</b>	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 <b>Security IP Management</b> 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.
<b>Interface Admin State</b>	This field enables or disables the Interface Admin State. When the state is enabled, the IPv4 processing will be started when the IPv4 address is configured on the IPIF. The IPv6 processing will be started when the IPv6 address is explicitly configured on the IPIF.
<b>IPv4 Address</b>	The address should specify a host address and length of the network prefix. There can be multiple IPv4 addresses defined on an interface. Thus, as a new address is defined, it is added on this IP Interface.
<b>Subnet Mask</b>	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.
<b>Gateway</b>	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an Intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Click **Apply** to implement changes made.

## 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 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 indicated 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.

## Interface Settings

This window allows the user to create and configure interfaces on the Switch.

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

The screenshot shows the 'Interface Settings' window. At the top, there are input fields for 'Interface Name' and 'VLAN Name', and a dropdown for 'Interface Admin. State' set to 'Enabled'. There are 'Create' and 'Delete All' buttons. Below this is a table with the following data:

Interface	VLAN Name	Admin State	
System	default	Enabled	[Edit] [IPv4 Edit] [IPv6 Edit] [Delete]

Figure 2 - 5 Interface Settings window

The following parameters can be configured:

Parameter	Description
<b>Interface Name</b>	Enter the name you wish to give the IP Interface.
<b>VLAN Name</b>	Enter the name of the VLAN corresponding to the System interface.
<b>Interface Admin. State</b>	Allows the user to enable or disable the interface administration state.

Click **Create** to create the entry or **Delete All** to delete all the current IP Interface entries.

To edit the *VLAN Name* or *Admin. State* click the **IPv4 Edit** or **IPv6 Edit** button as shown below.

The screenshot shows the 'Interface Settings Edit' window. It has the same configuration fields as Figure 2-5. The table below has an 'Apply' button instead of 'Edit' for the 'System' entry:

Interface	VLAN Name	Admin.State	
System	default	Enabled	[Apply] [IPv4 Edit] [IPv6 Edit] [Delete]

Figure 2 - 6 Interface Settings Edit window

Enter the new **VLAN Name** and **Admin. State** and click **Apply**. To edit an entry for IPv4 features click the corresponding **IPv4 Edit** button.

**Figure 2 - 7 IPv4 Interface Settings Edit window**

The following parameters can be configured:

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

Click **Apply** to implement changes made.

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

**Figure 2 - 8 IPv6 Interface Settings Edit window**

The following parameters can be configured:

Parameter	Description
<b>Interface Name</b>	Displays the interface being edited.
<b>VLAN Name</b>	Enter the name of the VLAN corresponding to the interface.
<b>IPv6 Network Address</b>	Enter the IPv6 Network Address to be configured. The interface can have multiple IPv6 addresses defined. Configuration of IPv6 addresses must be done through the command config ipif.
<b>IPv6 State</b>	Allows the user to enable or disable the IPv6 state on the interface.
<b>NS Retransmit time (0-4294967295)</b>	This field is used to set the interval, in milliseconds that the Switch will produce neighbor solicitation packets to be sent out over the local network. This is used to discover IPv6 neighbors on the local network. The user may select a time between 0 and 4294967295 milliseconds. The default is 0.

<b>Automatic Link Local Address</b>	Enables or disables the automatic configuration of link local addresses when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.
-------------------------------------	---

Click **Apply** to implement changes made.

## IPv6 Route Settings

This window allows the user to create and configure IPv6 Route interfaces to the Switch's IP routing table.

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

**Figure 2 - 9 IPv6 Route Settings window**

The following parameters can be configured:

Parameter	Description
<b>Interface Name</b>	Enter the name you wish to give the IPv6 Route Interface.
<b>Nexthop Address</b>	Enter the IPv6 address for the next hop router.
<b>Metric (1-65535)</b>	Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
<b>Backup State</b>	The user may choose between Primary and Backup. If the Primary Static/Default Route fails, the Backup Route will support the entry.

Click **Apply** to implement changes made. To remove any entry, click the **Delete All** button.

## IPv6 Neighbor Settings

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

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

**Figure 2 - 10 IPv6 Neighbor Settings window**

The following parameters can be configured:



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

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

## Port Configuration

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

### Port Settings

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

#### To configure switch ports:

Choose the port or sequential range of ports using the **From Port / To Port** port pull-down menus.

Use the remaining pull-down menus to configure the parameters described below:

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

- From Port: 01
- To Port: 01
- State: Enabled
- Speed/Duplex: Auto
- Flow Control: Disabled
- Address Learning: Enabled
- Medium Type: Copper

The table below shows the status of ports 01 through 12:

Port	State	Speed/Duplex	Flow Control	Connection	Address Learning
01	Enabled	Auto	Disabled	Link Down	Enabled
02	Enabled	Auto	Disabled	Link Down	Enabled
03	Enabled	Auto	Disabled	100M/Full/None	Enabled
04	Enabled	Auto	Disabled	Link Down	Enabled
05	Enabled	Auto	Disabled	Link Down	Enabled
06	Enabled	Auto	Disabled	Link Down	Enabled
07	Enabled	Auto	Disabled	1000M/Full/None	Enabled
08	Enabled	Auto	Disabled	Link Down	Enabled
09 (C)	Enabled	Auto	Disabled	Link Down	Enabled
09 (F)	Enabled	Auto	Disabled	Link Down	Enabled
10 (C)	Enabled	Auto	Disabled	Link Down	Enabled
10 (F)	Enabled	Auto	Disabled	Link Down	Enabled
11 (C)	Enabled	Auto	Disabled	Link Down	Enabled
11 (F)	Enabled	Auto	Disabled	Link Down	Enabled
12 (C)	Enabled	Auto	Disabled	Link Down	Enabled
12 (F)	Enabled	Auto	Disabled	Link Down	Enabled

Figure 2 - 11 Port Settings window

The following parameters can be configured:

Parameter	Description
<b>From Port / To Port</b>	Use the pull-down menus to select the port or range of ports to be configured.
<b>State</b>	Toggle this field to either enable or disable a given port or group of ports.
<b>Speed/Duplex</b>	<p>Toggle the <b>Speed/Duplex</b> 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_M</i>, <i>1000M/Full_S</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_M</i> (master) and <i>1000M/Full_S</i> (slave) parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (<i>1000M/Full_M</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_S</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_M</i>, the other side of the connection must be set for <i>1000M/Full_S</i>. Any other configuration will result in a link down status for both ports.</p>
<b>Flow Control</b>	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> .
<b>Address Learning</b>	When <i>Enabled</i> , destination and source MAC addresses are automatically listed in the forwarding table. The default setting is <i>Enabled</i> .
<b>Medium Type</b>	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> .

Click **Apply** to implement the new settings on the Switch. Click **Refresh** to reload the page.

## Port Description

The Switch supports a port description feature where the user may assign names to various ports on the Switch.

Use the **From Port / To Port** pull-down menu to choose a port or range of ports to describe, and then enter a description of the port(s). Click **Apply** to set the descriptions in the **Port Description Table**.

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).

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

From Port	To Port	Medium Type	Description
01	01	Copper	

Port	Description
01	
02	
03	
04	
05	
06	
07	
08	
09 (C)	
09 (F)	
10 (C)	
10 (F)	
11 (C)	
11 (F)	
12 (C)	
12 (F)	

Figure 2 - 12 Port Description window

## Port Error Disabled

The following window will display the information about ports that have had their connection status disabled, for reasons such as Loopback Detection or link down status.

To view this window, click **Configuration > Port Configuration > Port Error Disabled** as shown below.

Port	Port State	Connection Status	Reason
------	------------	-------------------	--------

Figure 2 - 13 Port Error Disabled window

The following parameters are displayed:

Parameter	Description
<b>Port</b>	Displays the port that has been error disabled.
<b>Port State</b>	Describes the current running state of the port, whether <i>Enabled</i> or <i>Disabled</i> .
<b>Connection Status</b>	This field will read the uplink status of the individual ports, whether enabled or Disabled.
<b>Reason</b>	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** as shown below:

**Static ARP Settings** Safeguard

**Global Settings**  
 ARP Aging Time (0-65535)  min

**Add Static ARP Entry**  
 IP Address  MAC Address

**Total Entries: 3**

Interface	IP Address	MAC Address	Type		
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
System	10.24.73.21	00-01-02-03-04-00	Local	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Figure 2 - 14 Static ARP Settings window

The following fields can be set:

Parameter	Description
<b>ARP Aging Time (0-65535)</b>	The user may globally set the maximum amount of time, in minutes, 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 0-65535 minutes with a default setting of 20 minutes.
<b>IP Address</b>	The IP address of the ARP entry.
<b>MAC Address</b>	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.



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

## User Accounts

Use the **User Account Management** window to control user privileges, create new users and view existing User Accounts.

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

**User Accounts** Safeguard

**Add User Accounts**  
 User Name  Password   
 Access Right  Confirm Password

**Note:** Password/User Name should be less than 15 characters.

**Total Entries : 0**

User Name	Access Right	Old Password	New Password	Confirm Password	Encryption
-----------	--------------	--------------	--------------	------------------	------------

Figure 2 - 15 User Accounts window

The following fields can be set:

Parameter	Description
<b>User Name</b>	The name of the user, an alphanumeric string of up to 15 characters.
<b>Access Right</b>	There are three levels of user privileges, <b>Admin</b> , <b>Operator</b> and <b>User</b> . Some menu selections available to users with <b>Admin</b> privileges may not be available to those with <b>User</b> or <b>Operator</b>

	<p>level privileges.</p> <p>There are 3 levels of security offered on the Switch, the <b>Operator</b> level privilege will allow users to configure and view configurations on the Switch, except for those involving security features, which are still left to the <b>Admin</b> level privilege. <b>Operator</b> level users can be authenticated through either the local authentication method of the Switch, or through the Access Authentication Control feature, discussed later in this document. Once the user has logged in to the Switch in the <b>Operator</b> level, certain security screens and windows will not be made available to view, or to configure. Only <b>Admin</b> level users have access to these features.</p> <p>(Table 2 - 1 below summarizes <b>Admin</b>, <b>Operator</b> and <b>User</b> level privileges)</p>
<b>New Password</b>	Enter a password for the new user.
<b>Confirm New Password</b>	Retype the new password.

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

**Figure 2 - 16 User Accounts window**

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



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

## Admin, Operator and User Privileges

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

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

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

Management	Admin	Operator	User
Configuration	Yes	Yes	Read-only
Network Monitoring	Yes	Yes	Read-only

Community Strings and Trap Stations	Yes	Yes	Read-only
Update Firmware and Configuration Files	Yes	No	No
System Utilities	Yes	Yes	No
Factory Reset	Yes	No	No
<b>User Account Management</b>			
Add/Update/Delete User Accounts	Yes	No	No
View User Accounts	Yes	No	No

**Table 2 - 1 Admin, Operator and User Privileges**

## System Log Configuration

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

### System Log Settings

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

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

Figure 2 - 17 System Log Settings window

The following parameters can be set:

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

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

### System Log Server

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

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

Figure 2 - 18 System Log Server window

The following parameters can be set:

Parameter	Description																																																				
<b>Server ID</b>	Syslog server settings index (1-4).																																																				
<b>Server IP Address</b>	The IP address of the Syslog server.																																																				
<b>UDP Port (514 or 6000-65535)</b>	Type the UDP port number used for sending Syslog messages. The default is 514.																																																				
<b>Severity</b>	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> .																																																				
<b>Facility</b>	<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: <b>Bold</b> 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><b>16</b></td> <td><b>local use 0 (local0)</b></td> </tr> <tr> <td>5</td> <td>messages generated internally by syslog line printer subsystem</td> <td><b>17</b></td> <td><b>local use 1 (local1)</b></td> </tr> <tr> <td>7</td> <td>network news subsystem</td> <td><b>18</b></td> <td><b>local use 2 (local2)</b></td> </tr> <tr> <td>8</td> <td>UUCP subsystem</td> <td><b>19</b></td> <td><b>local use 3 (local3)</b></td> </tr> <tr> <td>9</td> <td>clock daemon</td> <td><b>20</b></td> <td><b>local use 4 (local4)</b></td> </tr> <tr> <td>10</td> <td>security/authorization messages</td> <td><b>21</b></td> <td><b>local use 5 (local5)</b></td> </tr> <tr> <td>11</td> <td>FTP daemon</td> <td><b>22</b></td> <td><b>local use 6 (local6)</b></td> </tr> <tr> <td></td> <td></td> <td><b>23</b></td> <td><b>local use 7 (local7)</b></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	<b>16</b>	<b>local use 0 (local0)</b>	5	messages generated internally by syslog line printer subsystem	<b>17</b>	<b>local use 1 (local1)</b>	7	network news subsystem	<b>18</b>	<b>local use 2 (local2)</b>	8	UUCP subsystem	<b>19</b>	<b>local use 3 (local3)</b>	9	clock daemon	<b>20</b>	<b>local use 4 (local4)</b>	10	security/authorization messages	<b>21</b>	<b>local use 5 (local5)</b>	11	FTP daemon	<b>22</b>	<b>local use 6 (local6)</b>			<b>23</b>	<b>local use 7 (local7)</b>
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	<b>16</b>	<b>local use 0 (local0)</b>																																																		
5	messages generated internally by syslog line printer subsystem	<b>17</b>	<b>local use 1 (local1)</b>																																																		
7	network news subsystem	<b>18</b>	<b>local use 2 (local2)</b>																																																		
8	UUCP subsystem	<b>19</b>	<b>local use 3 (local3)</b>																																																		
9	clock daemon	<b>20</b>	<b>local use 4 (local4)</b>																																																		
10	security/authorization messages	<b>21</b>	<b>local use 5 (local5)</b>																																																		
11	FTP daemon	<b>22</b>	<b>local use 6 (local6)</b>																																																		
		<b>23</b>	<b>local use 7 (local7)</b>																																																		
<b>Status</b>	Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate.																																																				

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



## System Severity Settings

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

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

System Severity	Severity Level
Trap	Information
Log	Information

**Figure 2 - 19 System Severity Settings**

Use the drop-down menus to configure the parameters described below.

Parameter	Description
<b>System Severity</b>	Choose how the alerts are used from the drop-down menu. Select <i>log</i> to send the alert of the Severity Type configured to the Switch's log for analysis. Choose <i>trap</i> to send it to an SNMP agent for analysis. Select <i>all</i> to send the chosen alert type to an SNMP agent and the Switch's log for analysis.
<b>Severity Level</b>	Choose what level of alert will trigger sending the log entry or trap message as defined by the Severity Name. Select <i>critical</i> to send only critical events to the Switch's log or SNMP agent. Choose <i>warning</i> to send critical and warning events to the Switch's log or SNMP agent. Select <i>information</i> to send informational, warning and critical events to the Switch's log or SNMP agent.

Click **Apply** to implement the new System Severity Settings.

## DHCP Relay

The DHCP Relay folder contains six windows regarding the DHCP relay functions on the Switch. The DHCP windows include **DHCP Relay Global Settings**, **DHCP Relay Interface Settings**, **DHCP Relay Option 60 Default Settings**, **DHCP Relay Option 60 Settings**, **DHCP Relay Option 61 Default Settings** and **DHCP Relay Option 61 Settings**.

### DHCP Relay Global Settings

This window is used to enable and configure **DHCP Relay Global Settings** on the Switch. The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1 and 16 hops, with a default value of 4. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a DHCP REQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 0 and 65,536 seconds, with a default value of 0 seconds.

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

Figure 2 - 20 DHCP Relay Global Settings window

The following fields can be set:

Parameter	Description
<b>DHCP Relay State</b>	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> .
<b>DHCP Relay Hops Count Limit (1-16)</b>	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.
<b>DHCP Relay Time Threshold (0-65535)</b>	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 <b>seconds</b> field of the DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given DHCP packet.
<b>DHCP Relay Option 82 State</b>	<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</p>

	DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
<b>DHCP Relay Agent Information Option 82 Check</b>	<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>
<b>DHCP Relay Agent Information Option 82 Policy</b>	<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 <b>DHCP Agent Information Option 82 Check</b> 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>
<b>DHCP Relay Option 60 State</b>	<p>This function enables or disables the DHCP option 60 state. When option 60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 60 or per IPIF configured servers. If the relay servers are determined based on option 60, then the IPIF configured servers will be ignored. If the relay servers are not determined by option 60 then the IPIF configured servers will be used to determine the relay servers.</p>
<b>DHCP Relay Option 61 State</b>	<p>This function enables or disables the DHCP option 61 state. When option 61 is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61. The relay servers will be determined based on option 61 and the IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then IPIF configured servers will be used to determine the relay servers.</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:

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

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

### Remote ID sub-option format:

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

- Sub-option type
- Length
- Remote ID type
- Length
- MAC address: The Switch's system MAC address.

**Figure 2 - 21 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 information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **DHCP Relay Interface Table** at the bottom of the following window. The user may add up to four server IP's per IP interface on the Switch.

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

**Figure 2 - 22 DHCP Relay Interface Settings and DHCP Relay Interface Table window**

The following parameters may be configured or viewed:

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

Click **Apply** to implement changes made.

## DHCP Relay Option 60 Default Settings

This window allows the user to configure the DHCP Relay Option 60 Default servers. When there are no matching servers found for the packet based on option 60, the relay servers will be determined by the default relay server setting. Similarly when there is no match found for the packet, the relay servers will be determined based on the default relay servers.

To view this window, click **Configuration > DHCP Relay > DHCP Relay Option 60 Default Settings** as shown below:

**Figure 2 - 23 DHCP Relay Option 60 Default Settings window**

The following parameters may be configured:

Parameter	Description
<b>Relay IP Address</b>	Enter the specified IP address for the DHCP relay forward.
<b>Mode</b>	Use the pull down menu to choose either <i>Relay</i> or <i>Drop</i> . When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules.

Click **Add** to add a new Relay IP Address entry. Click **Apply** to implement changes made. To remove any entries click the corresponding **Delete** button.

## DHCP Relay Option 60 Settings

This window is used to configure option 60 relay rules on the Switch. Different strings can be specified for the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.

To view this window, click **Configuration > DHCP Relay > DHCP Relay Option 60 Settings** as shown below:

**Figure 2 - 24 DHCP Relay Option 60 Settings window**

The following parameters may be configured:

Parameter	Description
<b>String</b>	Enter the specified string, up to a maximum of 255 alphanumeric characters.
<b>Server IP</b>	Enter the relay server IP address.
<b>Match Type</b>	Use the drop down menu to select either <i>Exact Match</i> or <i>Partial Match</i> . <i>Exact Match</i> – The option 60 string in the packet must fully match the specified string. <i>Partial Match</i> – The option 60 string in the packet only needs to partially match the specified string.

Click **Add** to add a new entry. To search for a particular entry enter the correct *IP Address* or *String* and click **Find**. To delete an entry select it and click **Delete**.

## DHCP Relay Option 61 Default Settings

This window is used to configure the DHCP Relay Option 61 Default Settings. These settings are used to determine the rule to process those packets that have no option 61 matching rules.

To view this window, click **Configuration > DHCP Relay > DHCP Relay Option 61 Default Settings** as shown below:

**Figure 2 - 25 DHCP Relay Option 61 Default Settings window**

The following parameters may be configured:

Parameter	Description
<b>DHCP Relay Option 61 Default</b>	Use the pull down menu to choose either <i>Relay</i> or <i>Drop</i> . When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules. Enter the IP Address of the entry you wish to configure.

Click **Apply** to implement changes made.

## DHCP Relay Option 61 Settings

This command is used to add a rule to the relay server based on option 61. The matching rule can be based on either the MAC address or by using a user-specified string. Only one relay server can be specified for a MAC-address or a string. If the existing relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of servers.

To view this window, click **Configuration > DHCP Relay > DHCP Relay Option 61 Settings** as shown below:

Figure 2 - 26 DHCP Relay Option 61 Settings window

The following parameters may be configured:

Parameter	Description
<b>Client ID</b>	Use the drop down menu to select the method of identification for the Client ID either <i>MAC Address</i> or <i>String</i> . The <i>MAC Address</i> will specify the hardware address of the client and the <i>String</i> will specify the client ID. Choose a method and enter the appropriate information into the box provided.
<b>Relay Rule</b>	Use the pull down menu to choose either <i>Relay</i> or <i>Drop</i> . When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules. Choose a method and enter the appropriate information into the box provided.

Click **Add** to create a new entry. To remove an entry, enter the appropriate *Client ID* information and click **Delete**. To delete all entries click **Delete All**.

## Out of Band Management Settings

This window is used to configure the RJ-45 Out-of-band (OOB) management port on the Switch. The OOB port is physically isolated from the data channels of the Switch. This port allows administrators manage the device remotely without the impact data channel congestion. The OOB management is a method to manage devices while sharing the network bandwidth with other management traffic. The OOB port allows Management packets and ARP requests to pass while other packets will be dropped.

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

Figure 2 - 27 Out of Band Management Settings window

The following parameters may be configured:

Parameter	Description
IP Address	Enter the IP address of the interface.
Subnet Mask	Enter the Subnet mask of the interface.
Gateway	Enter the default gateway of the out of band management networks.
Status	Allows the user to <i>Enable</i> or <i>Disable</i> the IP interface.
Link Status	Displays the current configurations of the out of band management interface.

Click **Apply** to implement changes.

## External Alarm Settings

This window is used to display and configure the messages receiving from the RJ-45 alarm port when external alarm occurs. The alarm port is designed to collect the alarm message generated by the 3-party alarm generator. While receiving the alarm messages, the Switch will send out alarm traps to the NMS according to the message you configured.

To view this window, click **Configuration > External Alarm Settings** as shown below:

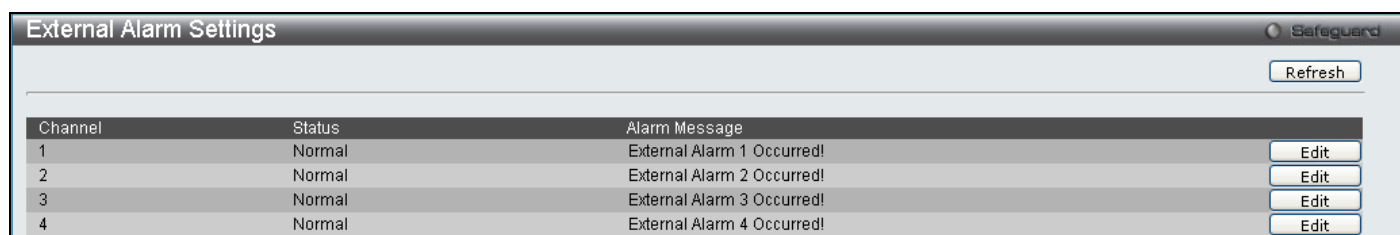


Figure 2 - 28 External Alarm Settings window

To modify an existing message click the corresponding **Edit** button and retype the new *Alarm Message* as shown below.

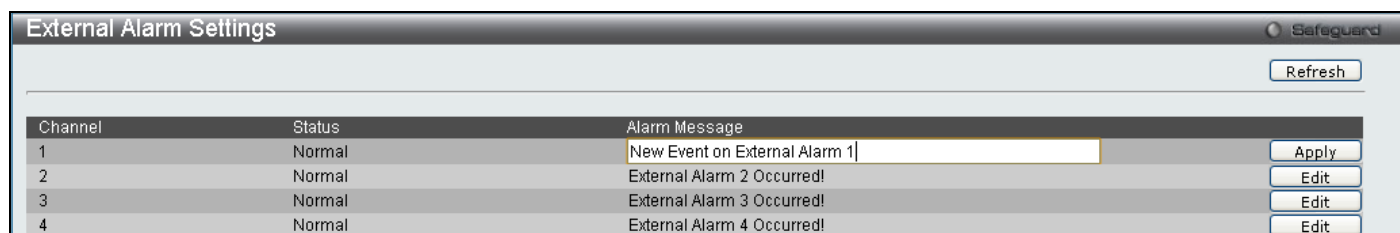


Figure 2 - 29 External Alarm Settings window – Edit

Enter the new information and click **Apply** to implement changes made.

## DHCP Auto Configuration Settings

The DHCP auto 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** as shown below:

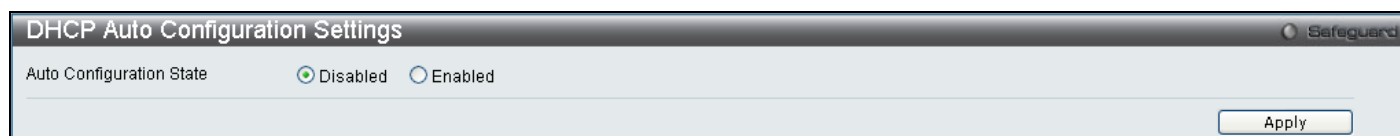


Figure 2 - 30 DHCP Auto Configuration Settings window



When DHCP autoconfiguration 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 autoconfiguration 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 view this window, click **Configuration > MAC Address Aging Time** as shown below:

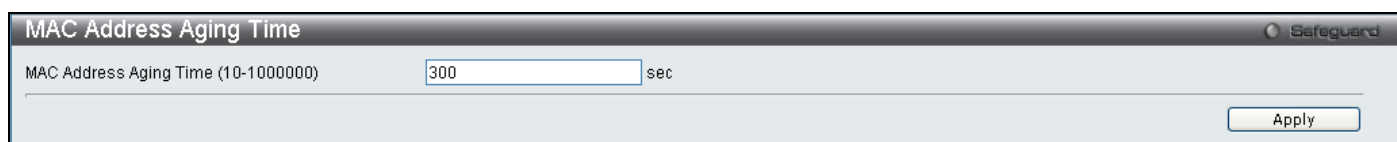


Figure 2 - 31 MAC Address Aging Time window

## 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.

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



Figure 2 - 32 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 view this window, click **Configuration > Telnet Settings** as shown below:



Figure 2 - 33 Telnet Settings window

## Password Encryption

Password Encryption Status can be *Enabled* or *Disabled* in this window, it is *Disabled* by default. Password encryption allows the user to encrypt a password in the configuration file 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 plaintext form.

To view this window, click **Configuration > Password Encryption** as shown below:

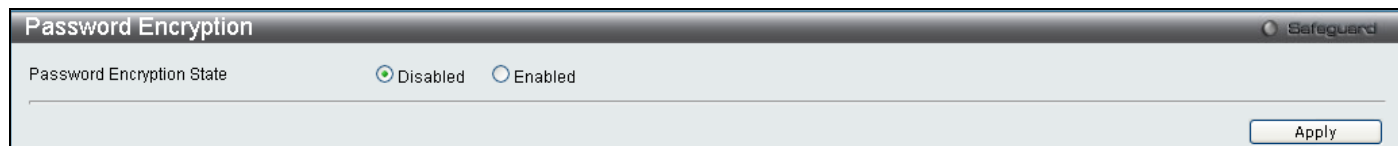


Figure 2 - 34 Password Encryption window

## Clipaging Settings

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

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

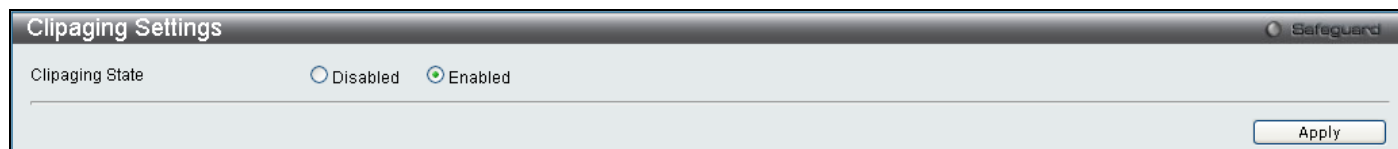


Figure 2 - 35 Clipaging Settings window

## Firmware Information

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

To view this window, click **Configuration > Firmware Information** as shown below:

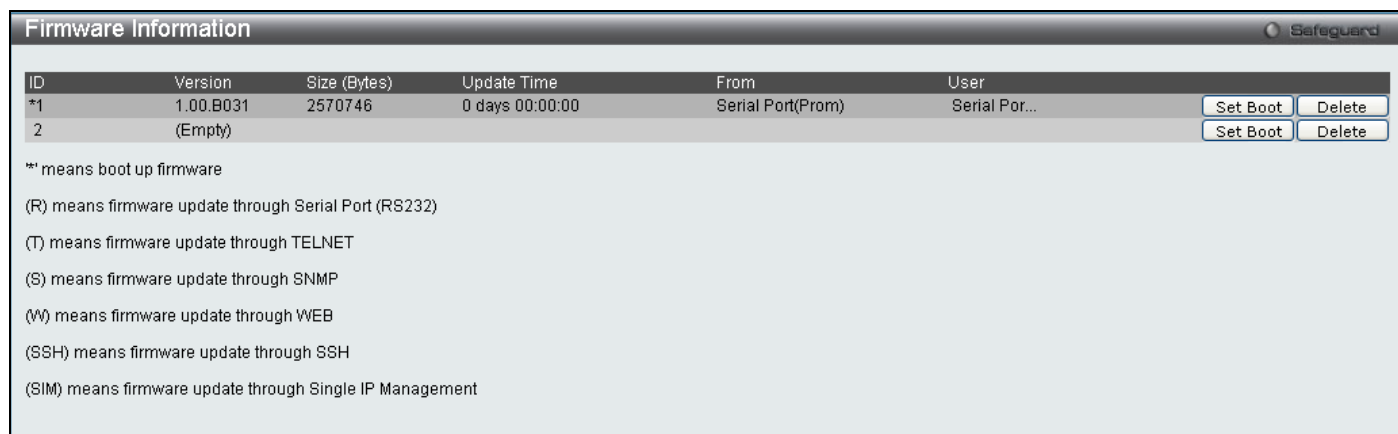


Figure 2 - 36 Firmware Information window

This window holds the following information:

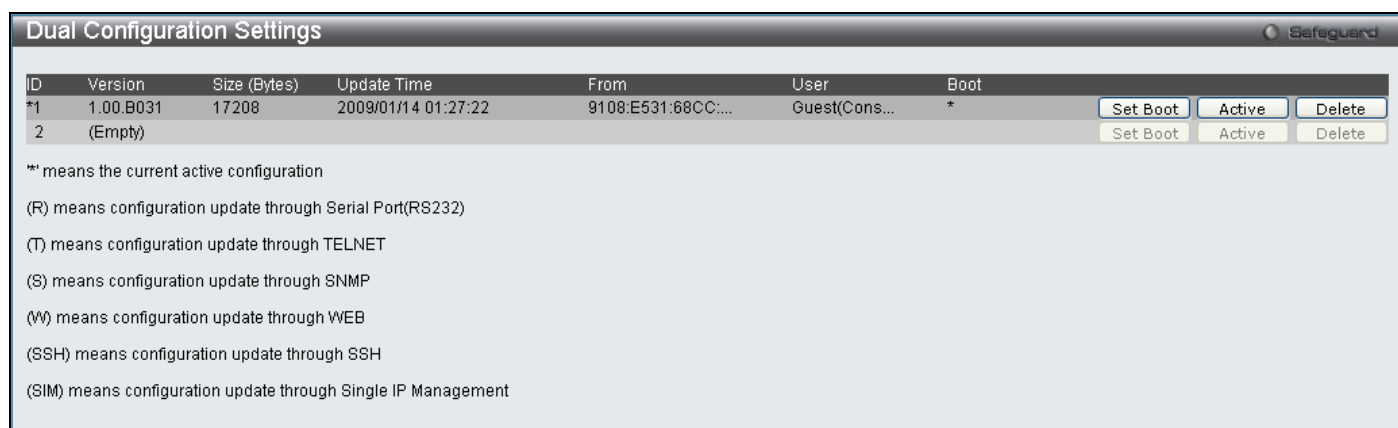
Parameter	Description
ID	States the image ID number of the firmware in the Switch's memory. The Switch can store two firmware images for use. Image ID 1 will be the default boot up firmware for the Switch unless

	otherwise configured by the user.
<b>Version</b>	States the firmware version.
<b>Size (Bytes)</b>	States the size of the corresponding firmware, in bytes.
<b>Update Time</b>	States the specific time the firmware version was downloaded to the Switch.
<b>From</b>	<p>States the IP address of the origin of the firmware. There are five ways firmware may be downloaded to the Switch.</p> <p><b>R</b> – If the IP address has this letter attached, it denotes a firmware upgrade through the serial port RS232.</p> <p><b>T</b> – If the IP address has this letter attached to it, it denotes a firmware upgrade through Telnet.</p> <p><b>S</b> – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Simple Network Management Protocol (SNMP).</p> <p><b>W</b> – If the IP address has this letter attached to it, it denotes a firmware upgrade through the web-based management interface.</p> <p><b>SSH</b> – If the IP address has these three letters attached, it denotes a firmware update through SSH.</p> <p><b>SIM</b> – If the IP address has these letters attached, it denotes a firmware upgrade through the Single IP Management feature.</p>
<b>User</b>	States the user who downloaded the firmware. This field may read “Anonymous” or “Unknown” for users that are unidentified.

## Dual Configuration Settings

The following window is used to configure firmware information set in the Switch. The DGS-3700 Series has the capability to store two firmware images in its memory.

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



**Figure 2 - 37 Dual Configuration Settings**

This window displays the following information:

Parameter	Description
<b>ID</b>	States the ID number of the configuration file located in the Switch's memory. The Switch can store two configuration files for use. ID 1 will be the default boot up configuration file for the Switch unless otherwise configured by the user.
<b>Version</b>	Displays the firmware version set in the Switch.

<b>Size(bytes)</b>	Displays the size of the configuration file, in bytes.
<b>Update time</b>	Displays the time that the configuration file was updated to the Switch.
<b>From</b>	Displays the location from which the configuration file was uploaded.
<b>User</b>	Displays the name of the user (device) that updated this configuration file. Unknown users will be displayed as Anonymous.
<b>Boot</b>	Click the <b>Boot</b> button under this heading to use this configuration file as the boot up firmware for the Switch. This will apply upon the next reboot of the Switch.
<b>Active</b>	Click the <b>Active</b> button to enable the configuration file settings.
<b>Delete</b>	Click the <b>Delete</b> button under this heading to delete this configuration file from the Switch's memory.

## Ping Test

Ping is a small program that sends ICMP Echo packets to the IPv6 or IPv4 address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view this window, click **Configuration > Ping Test** as shown below:

**Figure 2 - 38 Ping Test window**

The following parameters may be configured:

Parameter	Description
<b>IPv4 Ping Test</b>	
<b>Target IP Address</b>	Enter the Target IPv4 Address of the host.
<b>Repeat Pinging for</b>	Check the Infinite times radio button, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. Or the user may opt to

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

Click **Start** to initiate the Ping program

## Local Loopback Ports Settings

The Local Loopback Ports Settings are used to start or stop the internal loopback test on selected ports, or set to/recover external loopback mode. When internal loopback is enabled, the device starts to send test packets to the port, and keeps monitoring the packets received. When internal loopback is disabled, the loopback test is terminated and the result is displayed. A port can only operate in one loopback mode at a time. When external loopback is enabled, the MAC/PHY is set to external loopback mode. When external loopback is disabled, the MAC/PHY resumes normal operation.

To view this window, click **Configuration > Local Loopback Ports Settings** as shown below:

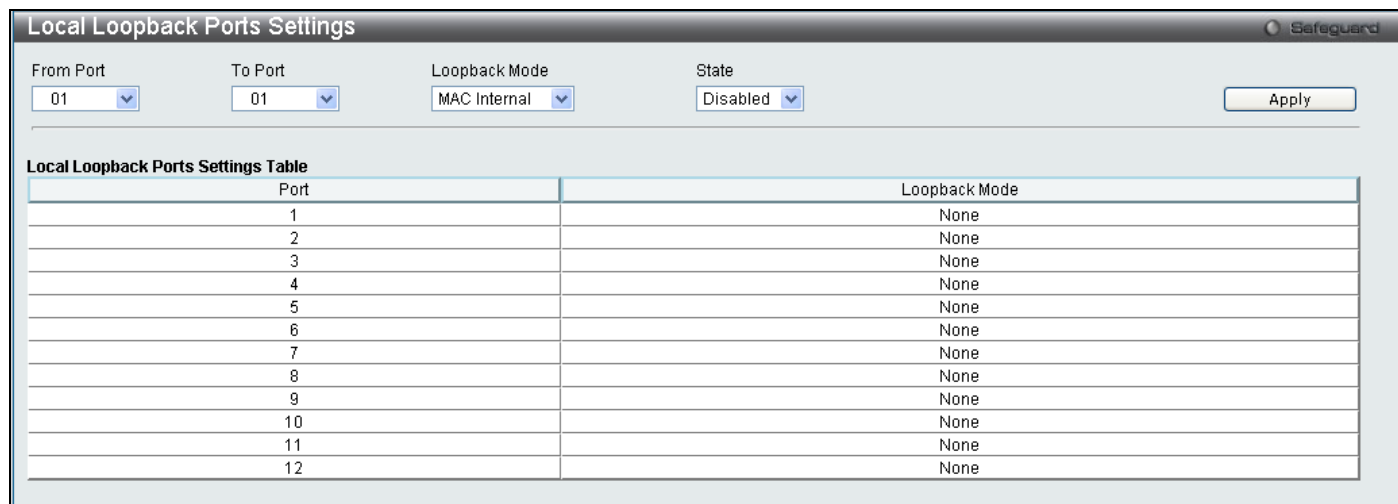


Figure 2 - 39 Local Loopback Ports Settings window

The following parameters may be configured:

Parameter	Description
<b>From Port / To Port</b>	Select a port or group of ports to <i>Enable</i> or <i>Disable</i> the Local Loopback Ports Settings using

	the pull-down menus.
<b>Loopback Mode</b>	This function allows the user to select MAC Internal/MAC External or PHY Internal/PHY External. MAC and PHY represent the layer on which the loopback is performed while the Internal or External represents the local loopback mode.
<b>State</b>	Select <i>Enable</i> to start internal loopback test; for external loopback, set port(s) to external loopback mode. Select <i>Disable</i> to stop internal loopback test; for external loopback, recover port(s) from external loopback mode.

Click **Apply** to implement changes.

## VLAN Counter Settings

The VLAN Counter Settings table is used to create the control entry for VLAN traffic flow statistics. The user can create control entries to count statistics for specific VLANs, or to count statistics for specific ports on specific VLANs. The statistics can be either byte count or packet count and can be counted for different frame types.

To view this window, click **Configuration > VLAN Counter Settings** as shown below:

**Figure 2 - 40 VLAN Counter Settings window**

The following parameters may be configured:

Parameter	Description
<b>VID List</b>	Check the radius button to identify the VLAN by its VLAN ID. Enter the VID or VID list you wish to configure.
<b>VLAN Name</b>	Check the radius button to identify the VLANs by their VLAN name.
<b>Ports (e.g.:1-5)</b>	Enter a list of ports, or check the <b>All Ports</b> check box to specify all the ports.
<b>Packet Type</b>	Use the drop down menu to select the packet type. <i>broadcast</i> – Specifies to count broadcast packets. <i>unicast</i> – Specifies to count unicast packets. <i>multicast</i> – Specifies to count multicast packets. <i>all</i> – Specifies to count all packets.
<b>Counter Type</b>	Use the drop down menu to select the counter type. To count at the packet level select <i>Packet</i> , to count at the byte level specify <i>Byte</i> .
<b>VID (1-4094)</b>	To search for a particular VLAN, enter the VID and click <b>Find</b> .

Click **Add** to create a new entry. To remove an entry click **Delete** to delete all entries click **Delete All**.

## SNTP Settings

The Simple Network Time Protocol Settings can be configured in the next two windows.

### Time Settings

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

To view this window, click **Configuration > SNTP Settings > Time Settings** as shown below:

**Figure 2 - 41 Time Settings window**

The following parameters can be set or are displayed:

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

Click **Apply** to implement changes made.

## TimeZone Settings

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

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

The screenshot shows the 'TimeZone Settings' window with the following configuration:

- Daylight Saving Time State:** Disabled
- Daylight Saving Time Offset In Minutes:** 60
- Time Zone Offset from GMT In +/-HH:MM:** + 00:00

**DST Repeating Settings:**

- From: Which Week Of The Month: First
- From: Day Of Week: Sun
- From: Month: Apr
- From: Time In HH MM: 00:00
- To: Which Week Of The Month: Last
- To: Day Of Week: Sun
- To: Month: Oct
- To: Time In HH MM: 00:00

**DST Annual Settings:**

- From: Month: Apr
- From: Day: 29
- From: Time In HH MM: 00:00
- To: Month: Oct
- To: Day: 12
- To: Time In HH MM: 00:00

An 'Apply' button is located at the bottom right of the window.

Figure 2 - 42 Time Zone and DST Settings window

The following parameters can be set:

Parameter	Description
<b>Time Zone and DST</b>	
<b>Daylight Saving Time State</b>	Use this pull-down menu to enable or disable the DST Settings.
<b>Daylight Saving Time Offset in Minutes</b>	Use this pull-down menu to specify the amount of time that will constitute your local DST offset 30, 60, 90, or 120 minutes.
<b>Time Zone Offset from GMT in +/-HH:MM</b>	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
<b>DST Repeating Settings</b>	
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.	



<b>From :Which Week of the Month</b>	Enter the week of the month that DST will start.
<b>From: Day of the Week</b>	Enter the day of the week that DST will start on.
<b>From: Month</b>	Enter the month DST will start on.
<b>From: Time in HH:MM</b>	Enter the time of day that DST will start on.
<b>To: Which Week of the Month</b>	Enter the week of the month the DST will end.
<b>To: Day of the Week</b>	Enter the day of the week that DST will end.
<b>To: Month</b>	Enter the month that DST will end.
<b>To:Time in HH:MM</b>	Enter the time DST will end.
<b>DST Annual Settings</b>	
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.	
<b>From: Month</b>	Enter the month DST will start on, each year.
<b>From: Day</b>	Enter the day of the week DST will start on, each year.
<b>From: Time in HH:MM</b>	Enter the time of day DST will start on, each year.
<b>To: Month</b>	Enter the month DST will end on, each year.
<b>To: Day</b>	Enter the date DST will end on, each year.
<b>To: Time in HH:MM</b>	Enter the time of day that DST will end on, each year.

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

## 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

This window is used to configure the MAC Notification Global Settings for the Switch.

To view this window, click **Configuration > MAC Notification Settings > MAC Notification Global Settings** as shown below:

**Figure 2 - 43 MAC Notification Global Settings window**

The following parameters may be viewed and modified:

Parameter	Description
<b>State</b>	Enable or disable MAC notification globally on the Switch.
<b>Interval (1-2147483647 sec)</b>	The time in seconds between notifications.
<b>History Size (1-500)</b>	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

This window is used to configure the MAC Notification Port Settings for the Switch.

To view this window, click **Configuration > MAC Notification Settings > MAC Notification Port Settings** as shown below:

Port	MAC Address Notification State
01	Disabled
02	Disabled
03	Disabled
04	Disabled
05	Disabled
06	Disabled
07	Disabled
08	Disabled
09	Disabled
10	Disabled
11	Disabled
12	Disabled

**Figure 2 - 44 MAC Notification Port Settings window**

The following parameters may be modified:

Parameter	Description
<b>From Port / To Port</b>	Select a port or group of ports to enable for MAC notification using the pull-down menus.
<b>State</b>	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 DGS-3700 Series supports the SNMP versions 1, 2c, and 3. The default SNMP setting is disabled. You must enable SNMP. Once SNMP is enabled you can choose which version you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

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

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

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

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

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

## Traps

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

## MIBs

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

The DGS-3700 Series incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The DGS-3700 Series supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

## SNMP Global State Settings

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

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

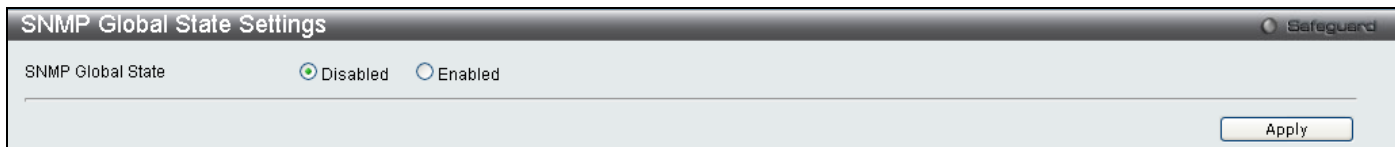


Figure 2 - 45 SNMP Global State Settings window

## SNMP View Table

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

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

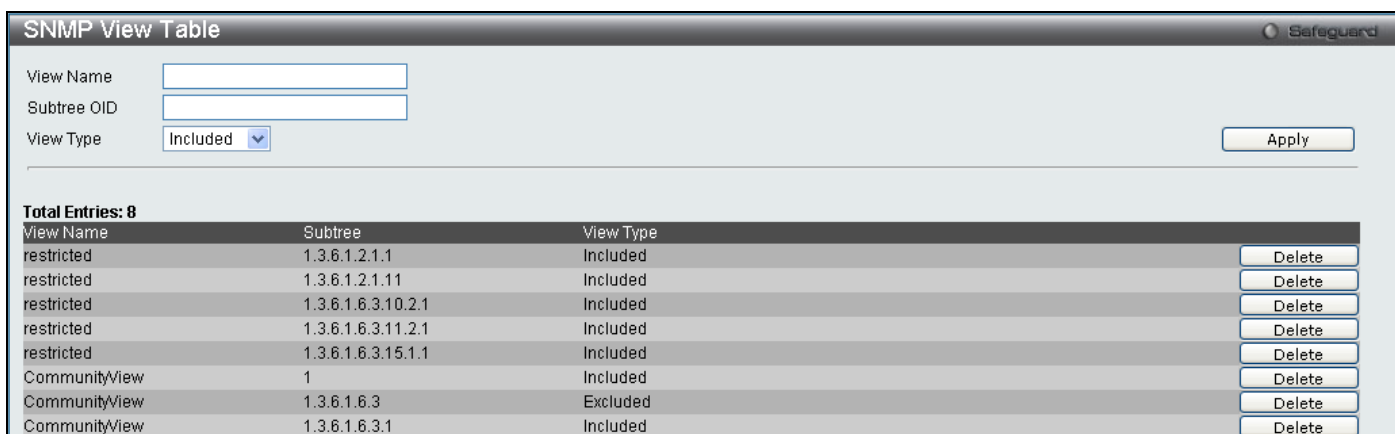


Figure 2 - 46 SNMP View Table window

The following parameters can be set:

Parameter	Description
<b>View Name</b>	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
<b>Subtree OID</b>	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.
<b>View Type</b>	Select <b>Included</b> to include this object in the list of objects that an SNMP manager can access. Select <b>Excluded</b> to exclude this object from the list of objects that an SNMP manager can access.

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

## SNMP Group Table

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

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

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 - 47 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
<b>Group Name</b>	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
<b>Read View Name</b>	This name is used to specify the SNMP group created can request SNMP messages.
<b>Write View Name</b>	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
<b>Notify View Name</b>	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
<b>User-based Security Model</b>	<p><i>SNMPv1</i> – Specifies that SNMP version 1 will be used.</p> <p><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.</p> <p><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.</p>
<b>Security Level</b>	<p>The Security Level settings only apply to SNMPv3.</p> <p><i>NoAuthNoPriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><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.</p> <p><i>AuthPriv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p>

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** as shown below:

**Figure 2 - 48 SNMP User Table window**

The following parameters may be set:

Parameter	Description
<b>User Name</b>	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
<b>Group Name</b>	This name is used to specify the SNMP group created can request SNMP messages.
<b>SNMP Version</b>	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.
<b>SNMP V3 Encryption</b>	None – Indicates that there is no SNMP V3 Encryption Password – Indicates that there is SNMP V3 Encryption through a password Key – Indicates that there is SNMP V3 Encryption through a key.
<b>Auth-Protocol by Password</b>	MD5 – Indicates that the HMAC-MD5-96 authentication level will be used. SHA – Indicates that the HMAC-SHA authentication protocol will be used.
<b>Priv-Protocol by Password</b>	None – Indicates that no authorization protocol is in use. DES – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
<b>Auth-Protocol by Key</b>	MD5 – Indicates that the HMAC-MD5-96 authentication level will be used. SHA – Indicates that the HMAC-SHA authentication protocol will be used.
<b>Priv-Protocol by password</b>	None – Indicates that no authorization protocol is in use. DES – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

<b>Password</b>	Enter a Password when SNMP V3 Encryption is enabled for Password mode.
<b>Key</b>	Enter a Key when SNMP V3 Encryption is enabled for Key mode.

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

## SNMP Community Table

Use this table to view existing SNMP Community Table configurations and to create a SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

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

Community Name	View Name	Access Right	
private	CommunityView	read_write	Delete
public	CommunityView	read_only	Delete

**Figure 2 - 49 SNMP Community Table window**

The following parameters can set:

Parameter	Description
<b>Community Name</b>	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.
<b>View Name</b>	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.
<b>Access Right</b>	<p><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.</p> <p><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.</p>

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

## SNMP Host Table

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

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

**Figure 2 - 50 SNMP Host Table window**

The following parameters can set:

Parameter	Description
<b>Host IP Address</b>	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
<b>User-based Security Model</b>	<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.
<b>Security Level</b>	<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.
<b>Community String/ SNMP V3 User Name</b>	Type in the community string or SNMP V3 user name as appropriate.

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

## SNMP v6Host Table

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

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

**Figure 2 - 51 SNMP V6Host Table window**

The following parameters can be configured:

Parameter	Description
<b>Host Ipv6 Address</b>	Enter the IPv6 host IP address to which the trap packet will be sent.
<b>User-based Security Model</b>	Used the drop down menu to select the user-based security model. <i>SNMPv1</i> – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP) version 1, is a network management protocol that provides a means to



	<p>monitor and control network devices.</p> <p><b>SNMPv2</b> – Specifies that SNMP version 2 will be used. The SNMP v2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><b>SNMPv3</b> – Specifies that SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> <li>• Message integrity – ensures that packets have not been tampered with during transit.</li> <li>• Authentication – determines if an SNMP message is from a valid source.</li> <li>• Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.</li> </ul>
<b>Security Level</b>	<p>When SNMPv3 is in use, it is necessary to choose the security level. Use the drop down menu to select from the following:</p> <p><i>noauth_nopriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.</p>
<b>Community String/SNMPv3 User Name</b>	<p>Enter an alphanumeric string that will be used to authorize a remote SNMP manager to access the Switch's SNMP agent. Alternatively enter the SNMPv3 user name.</p>

Click **Apply** to implement changes made.

## SNMP Engine ID

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

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

The screenshot shows a configuration window titled "SNMP Engine ID" with a "Safeguard" icon in the top right corner. The "Engine ID" field contains the alphanumeric string "800000ab03002191af37d0". Below the field, a red note states: "Note: Engine ID length is 10-64, the accepted character is from 0 to F." An "Apply" button is located in the bottom right corner of the window.

**Figure 2 - 52 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, click **Configuration > SNMP Settings > SNMP Trap Configuration** as shown below:

The screenshot shows the 'SNMP Trap Configuration' window. It has a title bar with 'Safeguard' on the right. Inside, there are two rows of settings: 'SNMP Traps' and 'SNMP Authentication Trap'. Each row has a dropdown menu currently set to 'Enabled'. At the bottom right, there is an 'Apply' button.

**Figure 2 - 53 SNMP Trap Configuration window**

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

## Time Range Settings

The Time Range 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 view this window, click **Configuration > Time Range Settings** as shown below:

The screenshot shows the 'Time Range Settings' window. It has a title bar with 'Safeguard' on the right. The main area contains:
 

- 'Range Name': A text input field with '(Max Support 32 Characters)' to its right.
- 'Hours(HH MM SS)': Two sets of dropdown menus for 'Start Time' and 'End Time', each with fields for hours, minutes, and seconds.
- 'Weekdays': Checkboxes for 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun', followed by a 'Select All Days' checkbox.

 An 'Apply' button is located at the bottom right. Below the main settings, there is a section titled 'Total Entries: 0' and a table header with columns: 'Range Name', 'Days', 'Start Time', and 'End Time'.

**Figure 2 - 54 Time Range Settings window**

Parameter	Description
<b>Range Name</b>	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the Access Profile table to identify the access profile and associated rule to be enabled during this time range.
<b>Hours</b>	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: <ul style="list-style-type: none"> <li><i>Start Time</i> - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system.</li> <li><i>End Time</i> - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.</li> </ul>
<b>Weekdays</b>	Use the check boxes to select the corresponding days of the week that this time range is to be enabled. Tick the Select All Days check box to configure this time range for every day of the week.

Click **Apply** to implement changes made. Currently configured entries will be displayed in the Time Range Information table in the bottom half of the window shown above.

## sFlow

The sFlow folder contains four windows to enable and configure the sFlow settings on the Switch.

### sFlow Global State Settings

This table is used to enable or disable the sFlow Global State Settings on the Switch. The sFlow version, address and state configurations can also be viewed in this table.

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

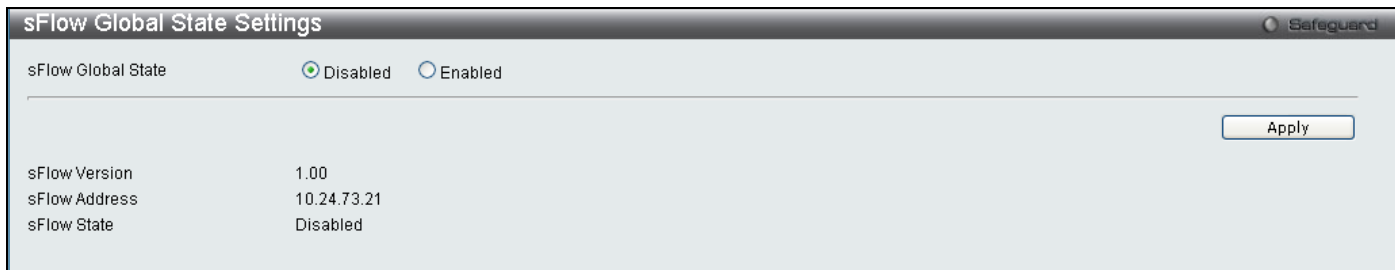


Figure 2 - 55 Time Range Settings window

Select *Disabled* or *Enabled* and click **Apply**.

### sFlow Analyzer Server Settings

This window is used to configure the sFlow analyzer server settings. You can specify more than one analyzer server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP address and UDP port numbers.

To view this window, click **Configuration > sFlow > sFlow Analyzer Server Settings** as shown below:

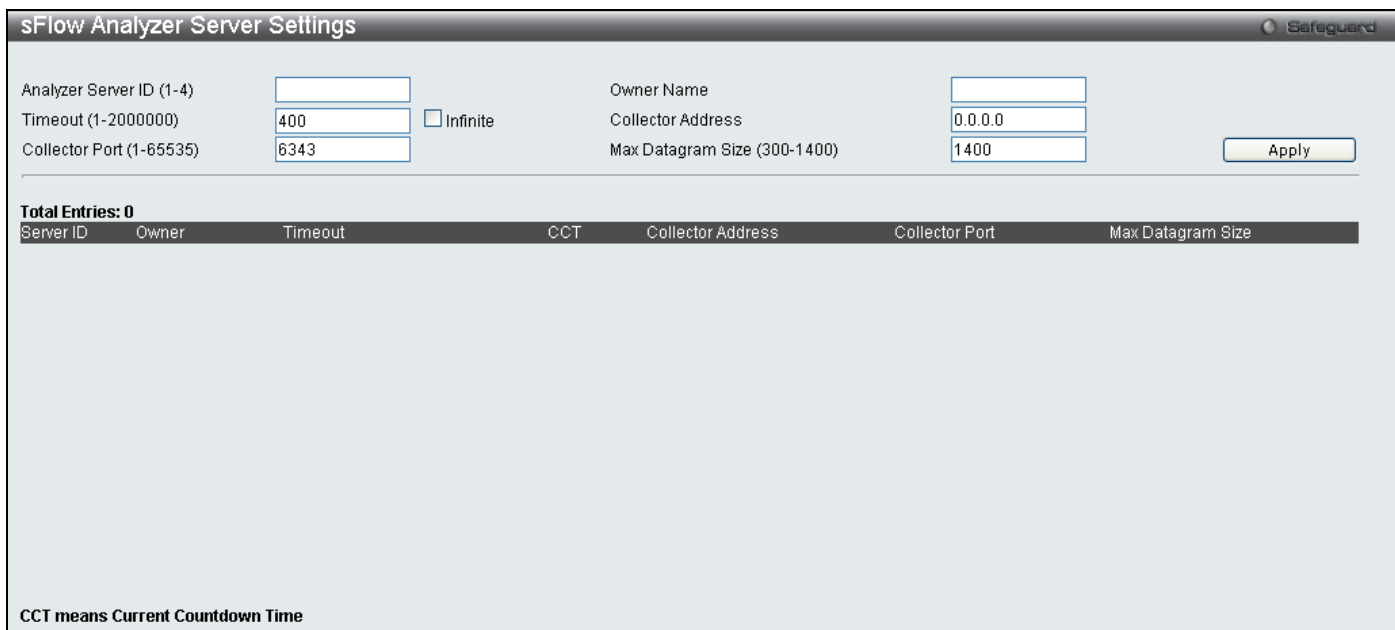


Figure 2 - 56 sFlow Analyzer Server Settings window

The following parameters can be configured:

Parameter	Description
<b>Analyzer Server ID (1-4)</b>	Up to four sFlow Analyzer Servers can be configured.
<b>Owner Name</b>	The entity making use of this sflow analyzer server. When owner is set or modified, the

	timeout value will become 400 automatically.
<b>Timeout (1-2000000)</b>	The length of time before the server is timed out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. "Infinite" indicates that the analyzer server will never time out. If not specified, the default value is 400.
<b>Collector Address</b>	The IP address of the analyzer server. If not specified, the address will be 0.0.0.0 which means that the entry will be inactive.
<b>Collector Port (1-65535)</b>	The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6364.
<b>Max Datagram size (300-1400)</b>	The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.

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

## sFlow Flow Sampler Settings

This table is used to create sFlow flow sampler settings on the Switch. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.

To view this window, click **Configuration > sFlow > sFlow Flow Sampler Settings** as shown below:

**Figure 2 - 57 sFlow Flow Sampler Settings window**

The following parameters can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies the port or list of ports to be configured.
<b>Analyzer Server ID (1-4)</b>	The analyzer server id specifies the ID of a server analyzer where the packet will be forwarded.
<b>Rate (0-65535)</b>	The sampling rate for packet sampling. The actual rate is the configured rate value multiplied by 256. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from about 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.
<b>MAX Header Size (18-256)</b>	The maximum number of leading bytes in the packet which will be sampled, encapsulated and forwarded to the server. If not specified, the default value is 128.

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

## sFlow Counter Poller Settings

This window is used to create the sflow counter poller settings on the Switch. Within the sflow counter poller function, the port statistics counter information will be forwarded to the server at the configured interval. These counters are RFC 2233 counters.

To view this window, click **Configuration > sFlow > sFlow Counter Poller Settings** as shown below:

**Figure 2 - 58 sFlow Counter Poller Settings window**

The following parameters can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies the port or list of ports to be configured.
<b>Analyzer Server ID (1-4)</b>	The analyzer server id specifies the ID of a server analyzer where the packet will be forwarded.
<b>Interval (20-120)</b>	Specifies the maximum number of seconds between successive statistic counter information. To disable the interval check the <b>Disabled</b> box.

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

## 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, 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 CS becomes a MS, it automatically becomes a member of the first SNMP community (include 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.

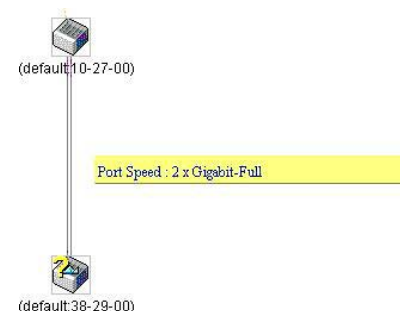
## The Upgrade to v1.6

To better improve SIM management, the DGS-3700 Series 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, as shown in the adjacent picture.



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. This window is used to enable the SIM for the Switch using the Web interface.

To view this window, click **Configuration > Single IP Management > Single IP Settings** as shown below:

**Figure 2 - 59 Single IP Settings window (disabled)**

Change the **SIM State** to *Enabled*, and the **Role State** to *Commander* using the pull-down menu and click **Apply**.

Single IP Settings	
SIM State	Enabled
Role State	Commander
Group Name	
Discovery Interval (30 - 90)	30 sec
Hold Time Count (100-255)	100 sec
Apply	

**Figure 2 - 60 Single IP Settings window (enabled)**

The following parameters can be set:

Parameters	Description
<b>SIM State</b>	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.
<b>Role State</b>	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.
<b>Group Name</b>	The user may enter a name for the group.
<b>Discovery Interval (30-90)</b>	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 <b>Discovery Interval</b> from 30 to 90 seconds.
<b>Hold Time Count (100-255)</b>	This parameter may be set for the time, in seconds the Switch will hold information sent to it from other switches, utilizing the <b>Discovery Interval</b> . The user may set the hold time from 100 to 255 seconds.

Click **Apply** to implement the settings.

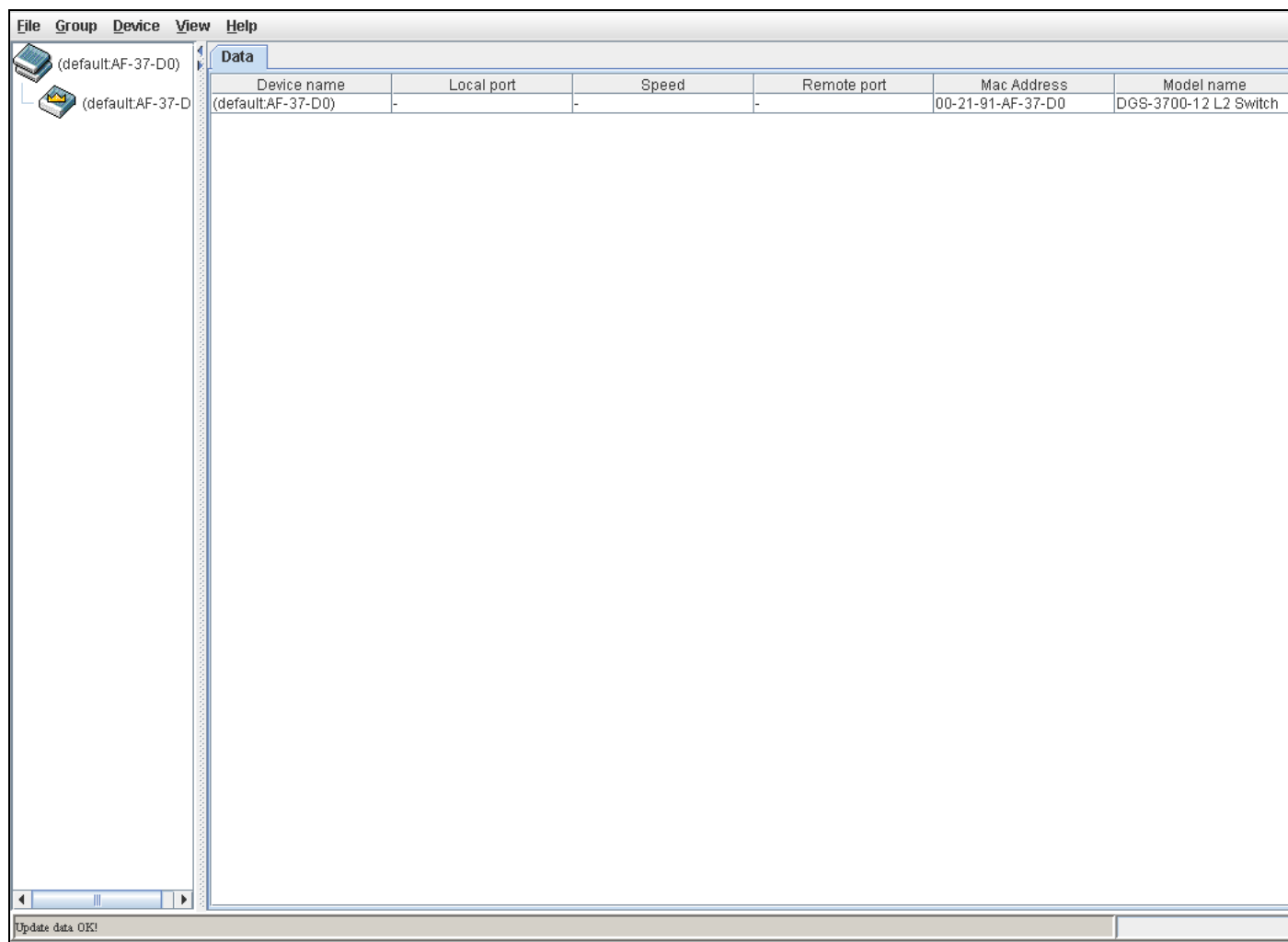
After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade** and **Configuration Backup/Restore** and **Upload Log File**.

## 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, as seen below.



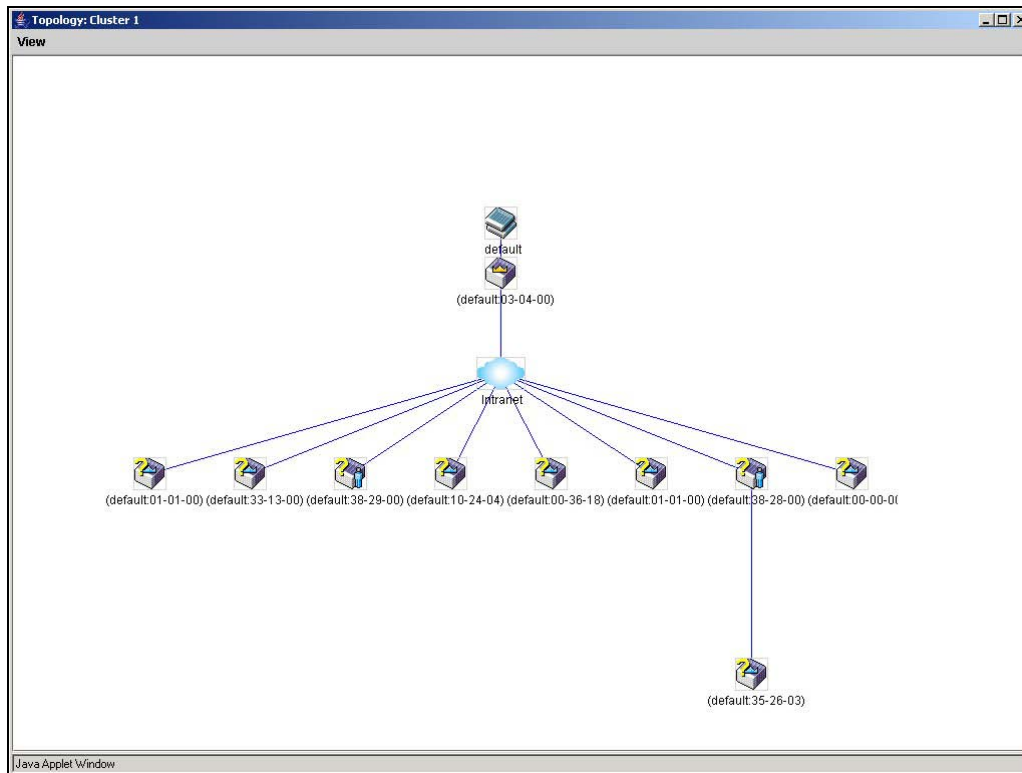


**Figure 2 - 61 Single IP Management window – Tree View**

The Tree View window holds the following information under the **Data** tab:

Parameter	Description
<b>Device Name</b>	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.
<b>Remote Port</b>	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.
<b>Speed</b>	Displays the connection speed between the CS and the MS or CaS.
<b>Local Port</b>	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.
<b>MAC Address</b>	Displays the MAC address of the corresponding Switch.
<b>Model Name</b>	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 - 62 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 screen 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 - 63 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.

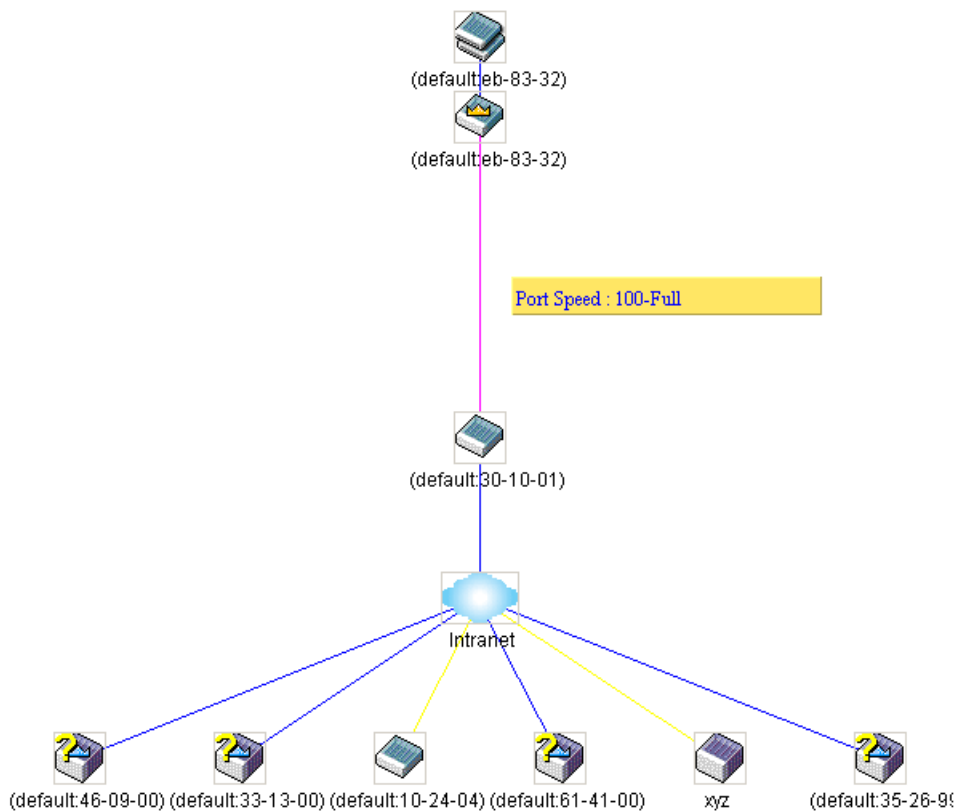


Figure 2 - 64 Port Speed Utilizing the Tool Tip

## 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

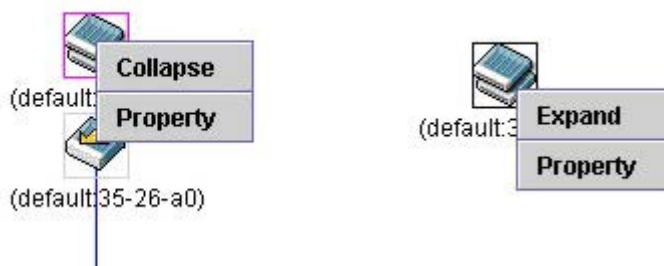


Figure 2 - 65 Right-Clicking a Group Icon

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.

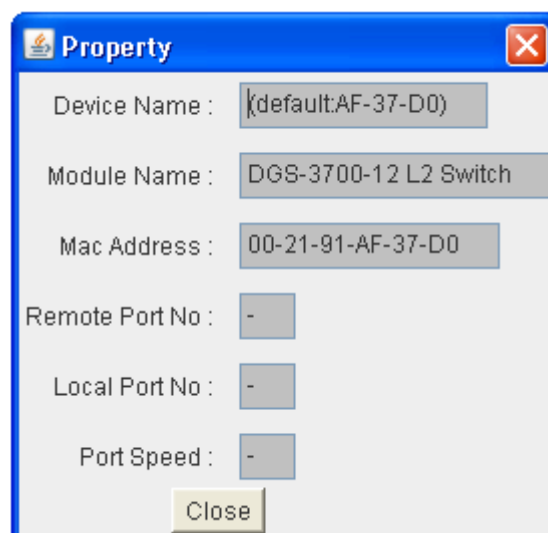


Figure 2 - 66 Property window

This window holds the following information:

Parameter	Description
<b>Device Name</b>	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.
<b>Module Name</b>	Displays the full module name of the switch that was right-clicked.
<b>MAC Address</b>	Displays the MAC Address of the corresponding Switch.
<b>Local Port No.</b>	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.
<b>Remote Port No.</b>	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.
<b>Port Speed</b>	Displays the connection speed between the CS and the MS or CaS

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

## Commander Switch Icon

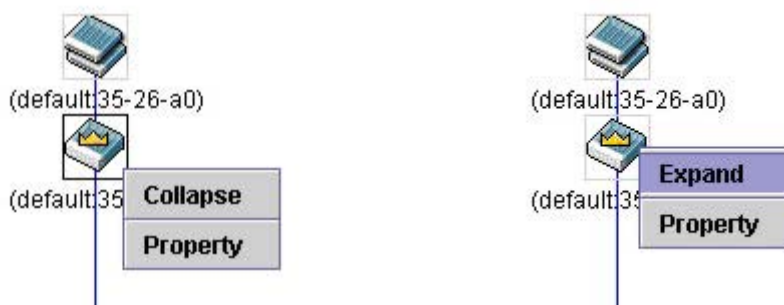


Figure 2 - 67 Right-Clicking a Commander Icon

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 - 68 Right-Clicking a Member icon

The following options may appear for the user to configure:

**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 - 69 Right-Clicking a Candidate icon

The following options may appear for the user to configure:

**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.

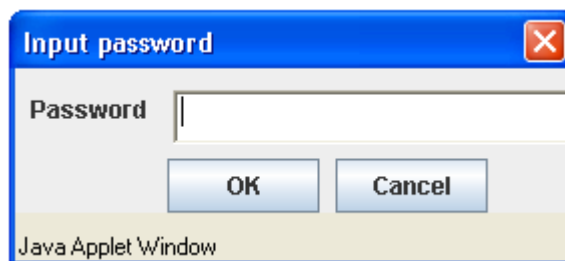


Figure 2 - 70 Input password window

**Property** – To pop up a window to display the device information, as shown below.

## Menu Bar

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



Figure 2 - 71 Menu Bar of the Topology View

The five menus on the menu bar are as follows.

### File

**Print Setup** – Will view the image to be printed.

**Print Topology** – Will print the topology map.

**Preference** – Will set display properties, such as polling interval, and the views to open at SIM startup.

### Group

**Add to group** – Add a candidate to a group. Clicking this option will reveal the following dialog 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.

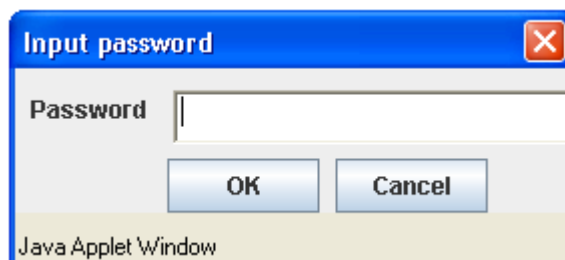


Figure 2 - 72 Input password window

**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 - 73 About window

## Firmware Upgrade

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

To view this window, click **Configuration > Single IP Management > Firmware Upgrade** as shown below:

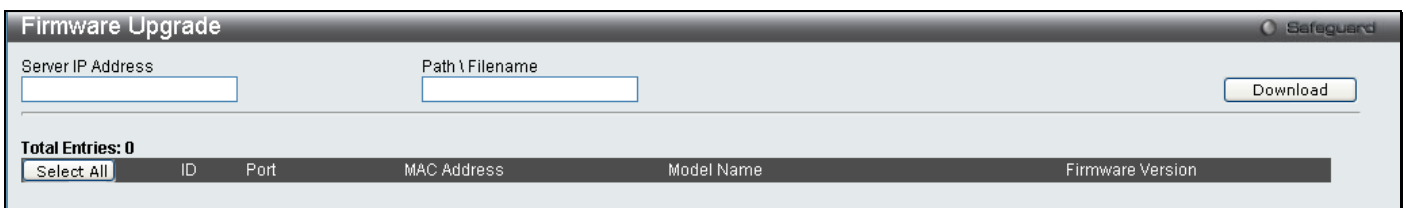


Figure 2 - 74 Firmware Upgrade window

## Configuration File Backup/Restore

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

To view this window, click **Configuration > Single IP Management > Configuration File Backup/Restore** as shown below:

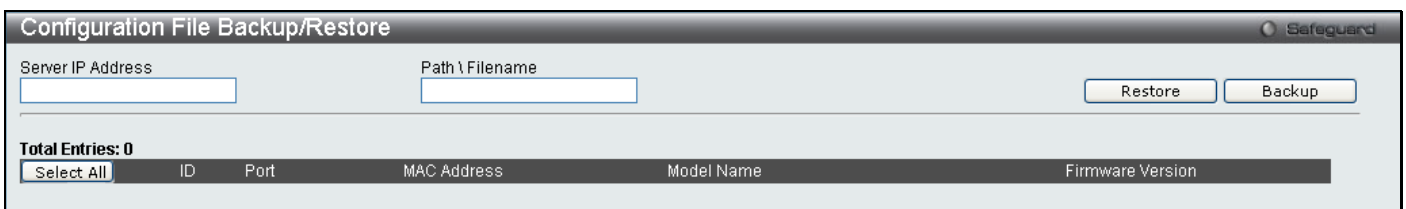


Figure 2 - 75 Configuration File Backup/Restore window

## 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** as shown below:

Figure 2 - 76 Upload Log File window

## DDM

This folder contains windows that perform Digital Diagnostic Monitoring functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP modules inserting to the Switch and to configure alarm settings, warning settings, temperature threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

## Browse DDM Status List

This window displays the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view this window, click **Configuration > DDM > Browse DDM Status List** as shown below:

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	Tx Power (mW)	Rx Power (mW)
1	-	-	-	-	-
2	-	-	-	-	-
3	-	-	-	-	-
4	-	-	-	-	-
5	-	-	-	-	-
6	-	-	-	-	-
7	-	-	-	-	-
8	-	-	-	-	-
9	-	-	-	-	-
10	-	-	-	-	-
11	-	-	-	-	-
12	-	-	-	-	-

Figure 2 - 77 Browse DDM Status List window

To view the status for a specific port or list of ports, enter the port list and click **Find**. To display the status for all ports, check the **All Ports** box and click **Find**.

## DDM Settings

The DDM settings window allows the user to configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

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



Port	DDM State	Shutdown
9	Enabled	Alarm
10	Enabled	Alarm
11	Enabled	Alarm
12	Enabled	Alarm

Note: The Port(s) 1,2,3,4,5,6,7,8 is(are) not SFP Port(s).

Figure 2 - 78 DDM Settings window

The following fields can be configured:

Parameter	Description
<b>Trap Log</b>	Specifies whether or not to send the trap and log, when the operating parameter exceeds the alarm or warning threshold.
<b>From Port / To Port</b>	Specifies a port or range of ports to be configured.
<b>State</b>	Specifies to <i>Enable</i> or <i>Disable</i> the DDM settings state.
<b>Shutdown</b>	Specifies whether or not to shutdown the port, when the operating parameter exceeds the <i>Alarm</i> or <i>Warning</i> threshold.

Click **Apply** to implement changes made.

## DDM Temperature Threshold Settings

This table is used to configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view this window, click **Configuration > DDM > DDM Temperature Threshold Settings** as shown below:

Port	High Alarm (Celsius)	Low Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)
9	-	-	-	-
10	-	-	-	-
11	-	-	-	-
12	-	-	-	-

Figure 2 - 79 DDM Temperature Threshold Settings window

The following fields can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies a port or range of ports to be configured.
<b>High Alarm</b>	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
<b>Low Alarm</b>	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm is taken.
<b>High Warning</b>	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning is taken.
<b>Low Warning</b>	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning is taken.

Click **Apply** to implement changes made.

## DDM Voltage Threshold Settings

This table is used to configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view this window, click **Configuration > DDM > DDM Voltage Threshold Settings** as shown below:

Port	High Alarm (Volt)	Low Alarm (Volt)	High Warning (Volt)	Low Warning (Volt)
9	-	-	-	-
10	-	-	-	-
11	-	-	-	-
12	-	-	-	-

**Figure 2 - 80 DDM Voltage Threshold Settings window**

The following fields can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies a port or range of ports to be configured.
<b>High Alarm</b>	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
<b>Low Alarm</b>	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm is taken.
<b>High Warning</b>	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning is taken.
<b>Low Warning</b>	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning is taken.

Click **Apply** to implement changes made.

## DDM Bias Current Threshold Settings

This table is used to configure the threshold of the bias current for specific ports on the Switch.

To view this window, click **Configuration > DDM > DDM Bias Current Threshold Settings** as shown below:

Port	High Alarm (mA)	Low Alarm (mA)	High Warning (mA)	Low Warning (mA)
9	-	-	-	-
10	-	-	-	-
11	-	-	-	-
12	-	-	-	-

**Figure 2 - 81 DDM Bias Current Threshold Settings window**

The following fields can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies a port or range of ports to be configured.
<b>High Alarm</b>	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
<b>Low Alarm</b>	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm is taken.

<b>High Warning</b>	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning is taken.
<b>Low Warning</b>	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning is taken.

Click **Apply** to implement changes made.

## DDM Tx Power Threshold Settings

This table is used to configure the threshold of Tx power for specific ports on the Switch.

To view this window, click **Configuration > DDM > DDM Tx Power Threshold Settings** as shown below:

Port	High Alarm (mW)	Low Alarm (mW)	High Warning (mW)	Low Warning (mW)
9	-	-	-	-
10	-	-	-	-
11	-	-	-	-
12	-	-	-	-

**Figure 2 - 82 DDM Tx Power Threshold Settings window**

The following fields can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies a port or range of ports to be configured.
<b>High Alarm</b>	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
<b>Low Alarm</b>	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm is taken.
<b>High Warning</b>	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning is taken.
<b>Low Warning</b>	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning is taken.

Click **Apply** to implement changes made.

## DDM Rx Power Threshold Settings

This table is used to configure the threshold of Rx power for specific ports on the Switch.

To view this window, click **Configuration > DDM > DDM Rx Power Threshold Settings** as shown below:

Port	High Alarm (mW)	Low Alarm (mW)	High Warning (mW)	Low Warning (mW)
9	-	-	-	-
10	-	-	-	-
11	-	-	-	-
12	-	-	-	-

**Figure 2 - 83 DDM Rx Power Threshold Settings window**

The following fields can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specifies a port or range of ports to be configured.
<b>High Alarm</b>	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
<b>Low Alarm</b>	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm is taken.
<b>High Warning</b>	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning is taken.
<b>Low Warning</b>	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning is taken.

Click **Apply** to implement changes made.

## Section 3

# L2 Features

**Jumbo Frame**

**802.1Q VLAN**

**Subnet VLAN**

**QinQ**

**802.1v Protocol VLAN**

**RSPAN Settings**

**GVRP Settings**

**GVRP Global Settings**

**MAC-based VLAN Settings**

**PVID Auto Assign Settings**

**Port Trunking**

**LACP Port Settings**

**Traffic Segmentation**

**BPDU Tunneling Settings**

**IGMP Snooping**

**MLD Snooping**

**Port Mirror**

**Loopback Detection Settings**

**Spanning Tree**

**Forwarding & Filtering**

**LLDP**

**CFM**

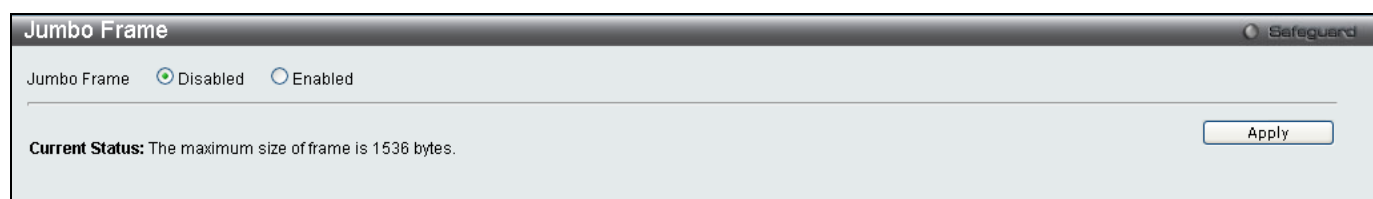
**Ethernet OAM**

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 *Disabled*. When enabled, jumbo frame (frames larger than the standard Ethernet frame size of 1536 bytes) of up to 13K (and 13312 bytes tagged) can be transmitted by the Switch.

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



**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.

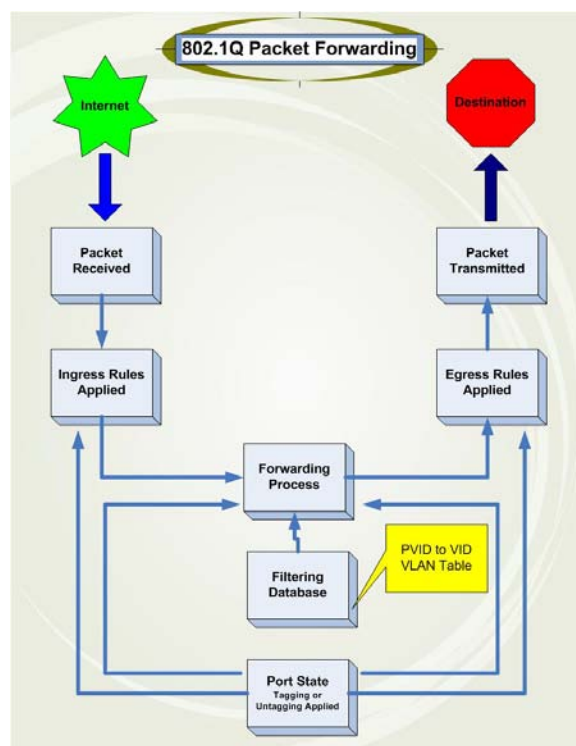


Figure 3 - 2 IEEE 802.1Q Packet Forwarding

## 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 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

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

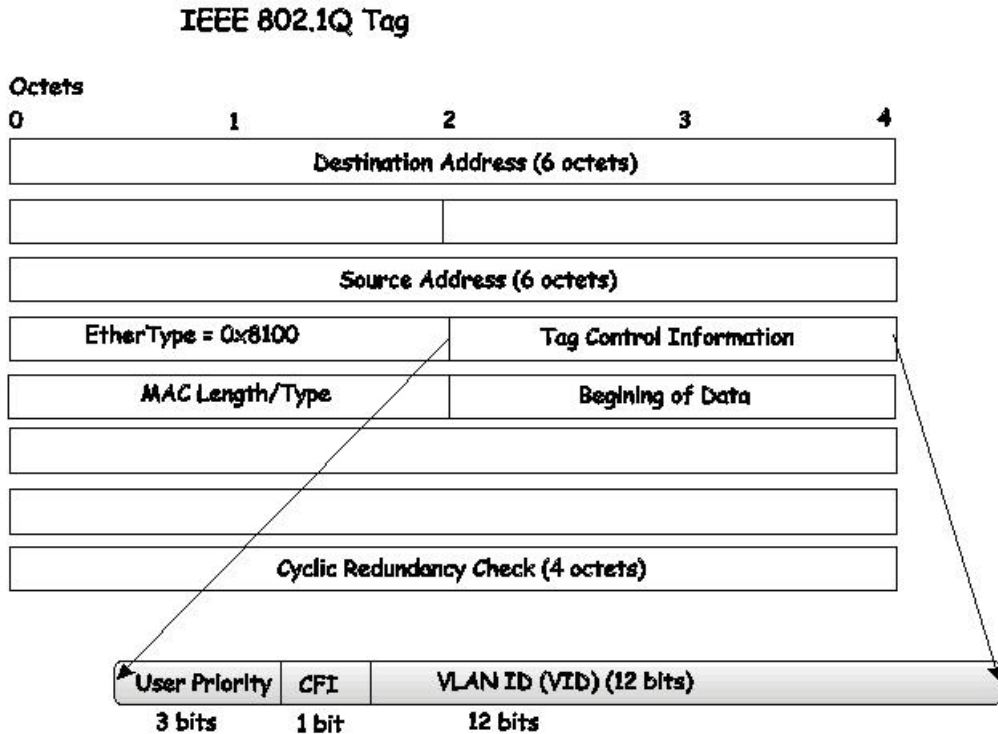


Figure 3 - 3 IEEE 802.1Q Tag

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.

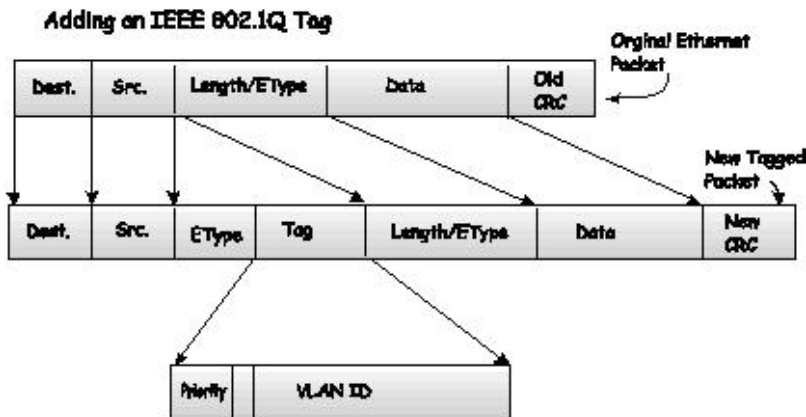


Figure 3 - 4 Adding an IEEE 802.1Q Tag



## 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.

## Double VLANs

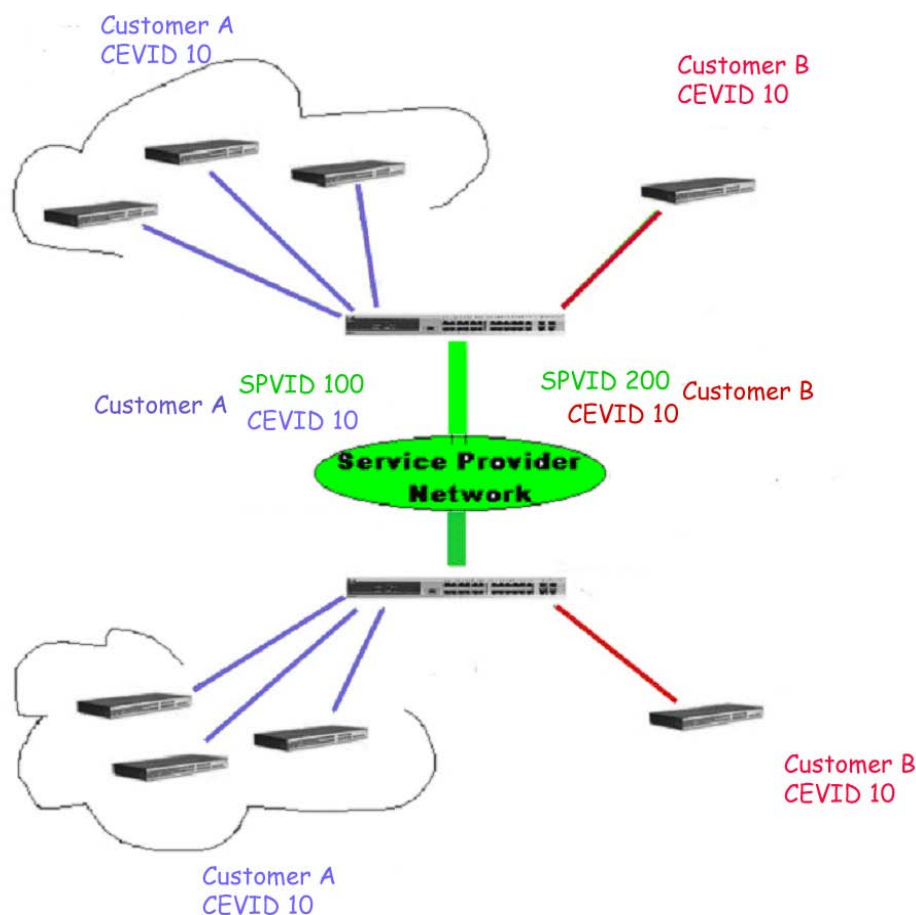
Double or Q-in-Q VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers,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

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

Here is an example Double VLAN tagged packet.

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

Consider the example below:



**Figure 3 - 5 Double VLAN Example**

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double 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) and 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 Double VLANs

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

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

- Web-based Access Control
- IP Multicast Routing
- GVRP
- All Regular 802.1Q VLAN functions

## 802.1Q VLAN

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

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

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

**Figure 3 - 6 Current 802.1Q Static VLANs Entries window**

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



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

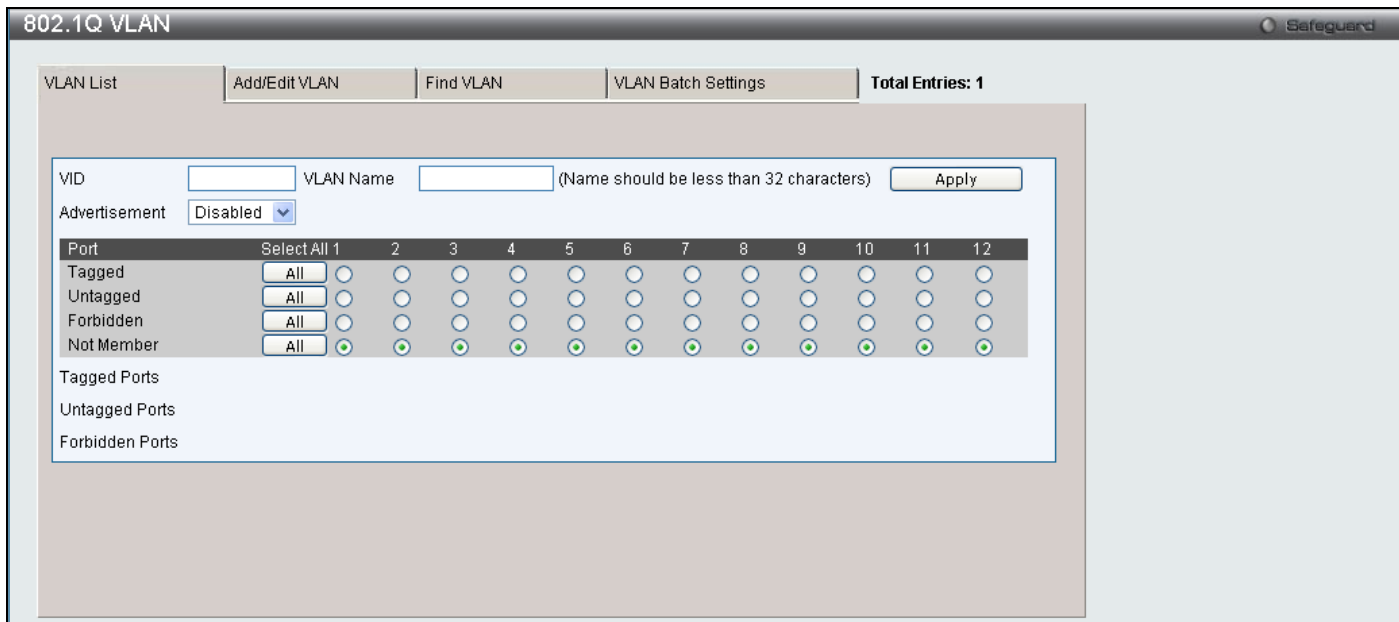


Figure 3 - 7 802.1Q VLAN window – Add/Edit VLAN Tab

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



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

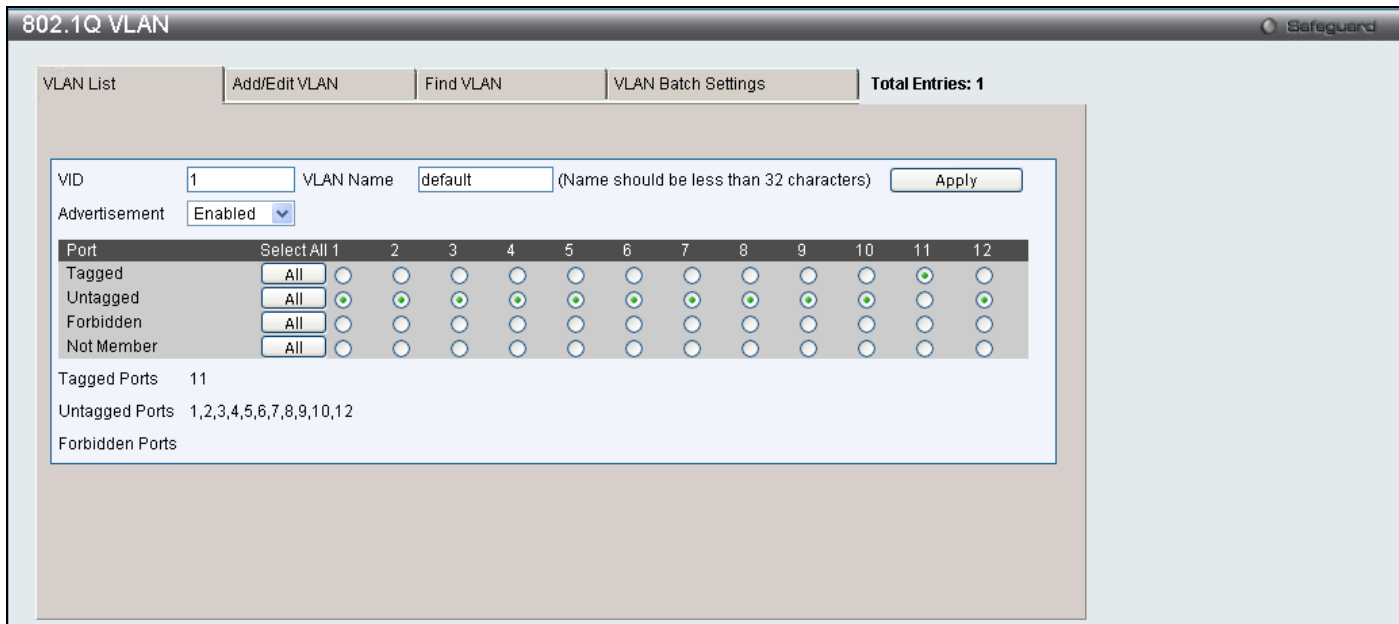


Figure 3 - 8 802.1Q VLAN window – Edit window

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

Parameter	Description
<b>VID</b>	Allows the entry of a VLAN ID, or displays the VLAN ID of an existing VLAN in the <b>Edit</b> window. VLANs can be identified by either the VID or the VLAN name.
<b>VLAN Name</b>	Allows the entry of a name for a new VLAN, or modifying the VLAN name in the <b>Edit</b> window. VLAN Name should be no more than 32 characters in length.

<b>Advertisement</b>	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
<b>Port Settings</b>	Allows an individual port to be specified as member of a VLAN.
<b>Tagged</b>	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
<b>Untagged</b>	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
<b>Forbidden</b>	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.
<b>Not Member</b>	Allows an individual port to be specified as a non-VLAN member.

Click **Apply** to implement changes made.

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

**Figure 3 - 9 802.1Q VLAN window – Find VLAN window**

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

**Figure 3 - 10 802.1Q VLAN window – VLAN Batch Settings window**

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

Parameter	Description
<b>VID List (e.g 2-5)</b>	Enter a VLAN ID List that can be added, deleted or configured.
<b>Advertisement</b>	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
<b>Port List (e.g. 1-5)</b>	Allows an individual port list to be added or deleted as a member of the VLAN.
<b>Tagged</b>	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
<b>Untagged</b>	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
<b>Forbidden</b>	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.



## Subnet VLAN

### Subnet VLAN Settings

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

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

**Figure 3 - 11 Subnet VLAN Settings window**

The following parameters can be configured:

Parameter	Description
<b>VLAN Name</b>	The VLAN Name to be associated with the subnet.
<b>VLAN ID</b>	The VLAN ID to be associated with the subnet.
<b>IPv4 Network Address</b>	Is used to specify an IPv4 network address. The format is ipaddress/prefix length. The prefix length of the IPv4 network address cannot be greater than 64.
<b>IPv6 Network Address</b>	Is used to specify an IPv6 network address. The format is ipaddress/prefix length. The prefix length of the IPv6 network address cannot be greater than 64.
<b>Priority</b>	The priority to be associated with the subnet. Its range is 0-7.

Enter the appropriate information and click Add to create a new entry. To search for a particular entry enter the appropriate information and click Find. To remove an entry click Delete. To view all entries on the Switch click Show All to remove all entries click Delete All.

### VLAN Precedence Settings

The VLAN precedence settings are used to configure VLAN classification precedence on each port. You can specify the order of MAC-based VLAN classifications and subnet VLAN classifications. If a port's VLAN classification is a MAC-based precedence, MAC-based VLAN classification will process first. If MAC-based VLAN classification fails, the subnet VLAN classification will be executed. If a port's VLAN classification is subnet VLAN precedence, the subnet VLAN classification will process first. If subnet VLAN classification fails, the MAC-based VLAN classification will be executed.

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

Port	VLAN Precedence
1	MAC-Based VLAN
2	MAC-Based VLAN
3	MAC-Based VLAN
4	MAC-Based VLAN
5	MAC-Based VLAN
6	MAC-Based VLAN
7	MAC-Based VLAN
8	MAC-Based VLAN
9	MAC-Based VLAN
10	MAC-Based VLAN
11	MAC-Based VLAN
12	MAC-Based VLAN

**Figure 3 - 12 VLAN Precedence Settings window**

The following parameters can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specify the port or range of ports you wish to configure.
<b>VLAN Precedence</b>	Use the drop down menu to select the VLAN precedence, choose either <i>MAC Based VLAN</i> or <i>Subnet VLAN</i> . MAC Based VLAN – Specifies that the MAC-based VLAN classification is given precedence over the subnet VLAN classification. Subnet VLAN – Specifies that the subnet VLAN classification is given precedence over the MAC-based VLAN classification.

Click **Apply** to implement changes made.

## Q-in-Q

### Q-in-Q Settings

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

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

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

Port	Role	Missdrop	Outer TPID	Use Inner Priority	Add Inner Tag
1	NNI	Disabled	0x88A8	Disabled	Disabled
2	NNI	Disabled	0x88A8	Disabled	Disabled
3	NNI	Disabled	0x88A8	Disabled	Disabled
4	NNI	Disabled	0x88A8	Disabled	Disabled
5	NNI	Disabled	0x88A8	Disabled	Disabled
6	NNI	Disabled	0x88A8	Disabled	Disabled
7	NNI	Disabled	0x88A8	Disabled	Disabled
8	NNI	Disabled	0x88A8	Disabled	Disabled
9	UNI	Disabled	0x88A8	Disabled	Disabled
10	NNI	Disabled	0x88A8	Disabled	Disabled
11	NNI	Disabled	0x88A8	Disabled	Disabled
12	NNI	Disabled	0x88A8	Disabled	Disabled

Figure 3 - 13 QinQ Settings window

The following fields can be set:

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

Click **Apply** to implement changes.

## 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 > QinQ > VLAN Translation Settings** as shown below:

**Figure 3 - 14 VLAN Translation Settings window**

The following fields can be set:

Parameter	Description
<b>From Port / To Port</b>	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
<b>CVID (1-4094)</b>	The customer VLAN ID List to which the tagged packets will be added.
<b>Action</b>	Specify if you want SPVID packets to be added or replaced.
<b>SPVID (1-4094)</b>	This configures the VLAN to join the Service Providers VLAN as a tagged member.
<b>Priority (0-7)</b>	Select a priority for the VLAN ranging from 0-7. With 7 having the highest priority.

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

## Q-in-Q and VLAN Translation Rules

### For ingress untagged packets at UNI ports:

1. The switch does not reference the VLAN translation table.
2. Check switch VLAN tables. The sequence: *mac-based VLAN* -> *subnet-based VLAN* -> *protocol-based VLAN* -> *port-based VLAN*. If matched, the matched VLAN will become this packet's 'SPVLAN'.

### For ingress tagged packets at UNI ports

1. The switch will look up the VLAN translation table. If matched, the VLAN tag will be translated (replace CEVLAN with SVLAN, or add SPVLAN).
2. Otherwise, check switch VLAN tables. The sequence is the same as above. The matched VLAN will become this packet's 'SPVLAN'.

## 802.1v Protocol VLAN

### 802.1v Protocol Group Settings

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

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

Figure 3 - 15 802.1v Protocol Group Settings window

The following fields can be set:

Parameter	Description
<b>Group ID</b>	Select an ID number for the group, between 1 and 16.
<b>Group Name</b>	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 characters.
<b>Protocol</b>	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> , <i>IEEE802.3_LLC</i> and <i>IEEE802.3_SNAP</i> .
<b>Protocol Value (0-FFFF)</b>	Enter a value for the Group.

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

## 802.1v Protocol VLAN Settings

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

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

Figure 3 - 16 Protocol VLAN Settings window

The following fields can be set:

Parameter	Description
<b>Group ID</b>	Click the corresponding radio button to select a previously configured Group ID from the drop-down menu.
<b>Group Name</b>	Click the corresponding radio button to select a previously configured Group Name from the drop-down menu.
<b>VID (1-4094)</b>	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.
<b>VLAN Name</b>	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.
<b>802.1p Priority</b>	<p>This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.</p> <p>Click the corresponding box if you want to set the 802.1p default priority of a packet to the value entered in the Priority (0-7) field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
<b>Port List (e.g.: 1-6)</b>	Select the specified ports you wish to configure by entering the port number in this field, or check the <b>Select All Ports</b> box.
<b>Search Port List</b>	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 <b>Find</b> . To display all previously configured port lists on the bottom half of the screen click the <b>Show All</b> button, to clear all previously configured lists click the <b>Delete All</b> button.

## RSPAN Settings

This table controls the RSPAN function. The purpose of the RSPAN function is to mirror the packets to a remote switch. The packet travels from the switch where the monitored packet is received, through the intermediate switch, then to the switch where the sniffer is attached. The first switch is also named the source switch. RSPAN VLAN mirroring will only work when RSPAN Global Settings are enabled. RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

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

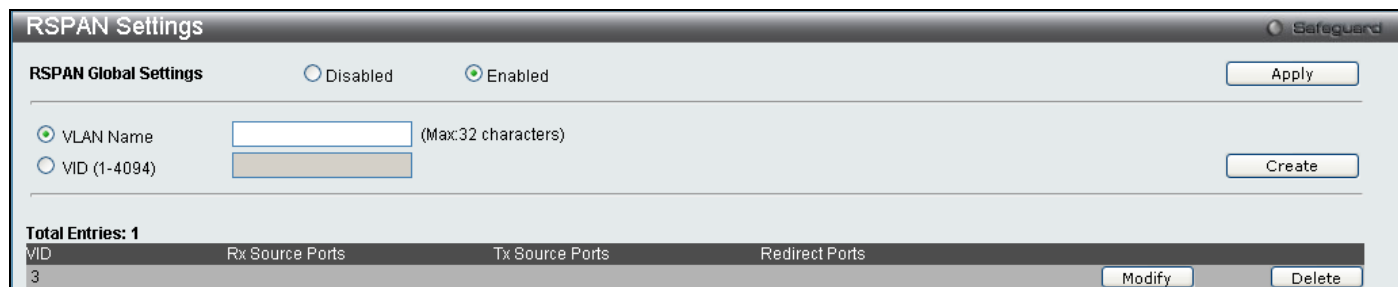


Figure 3 - 17 RSPAN Settings window

Enter the *VLAN Name* or *VID* and click **Create**. To remove an entry click **Delete**, to modify an entry click the corresponding **Modify** button.

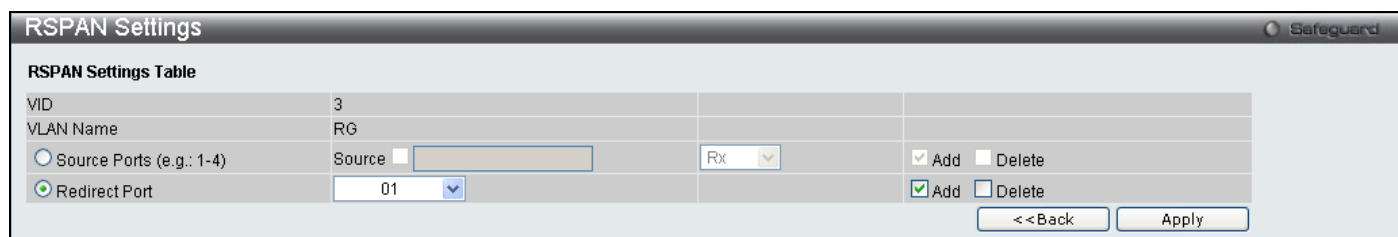


Figure 3 - 18 RSPAN Settings window – Edit

Enter the *Source Ports* or *Redirect Ports* you wish to **Add** or **Delete** and click **Apply**. To return to the RSPAN Settings window click **<<Back**.

## GVRP Settings

The table allows the user to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID do not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

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

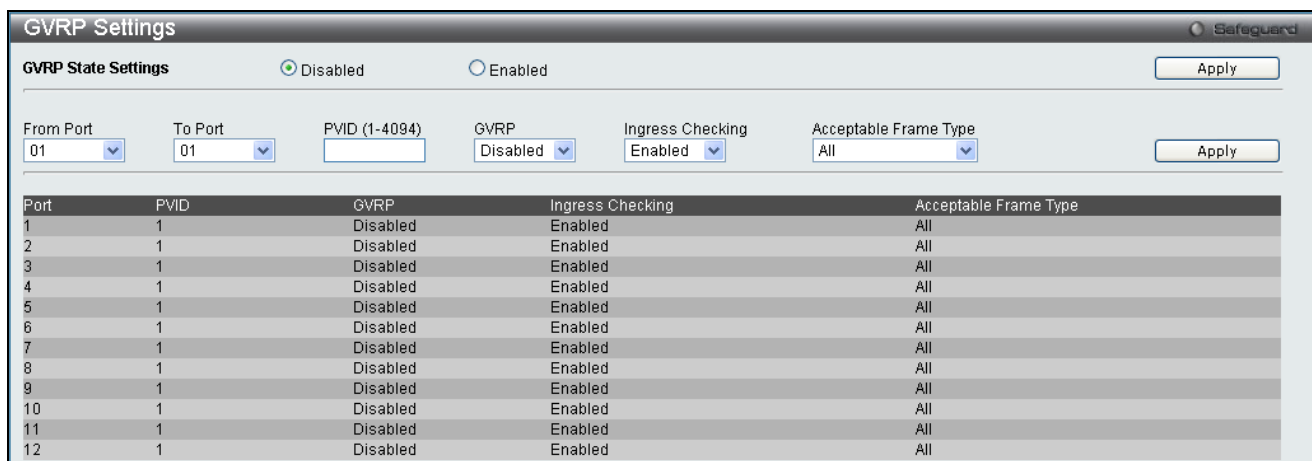


Figure 3 - 19 GVRP Settings window

The following fields can be set:

Parameter	Description
<b>From Port / To Port</b>	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 <b>802.1Q Port Settings</b> window.
<b>GVRP</b>	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is <i>Disabled</i> by default.
<b>PVID</b>	The read-only field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
<b>Ingress Check</b>	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>Disabled</i> by default.
<b>Acceptable Frame Type</b>	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>Admit_All</i> , which mean both tagged and untagged frames will be accepted. <i>Admit_All</i> is enabled by default.

Click **Apply** to implement changes made.

## GVRP Global Settings

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

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

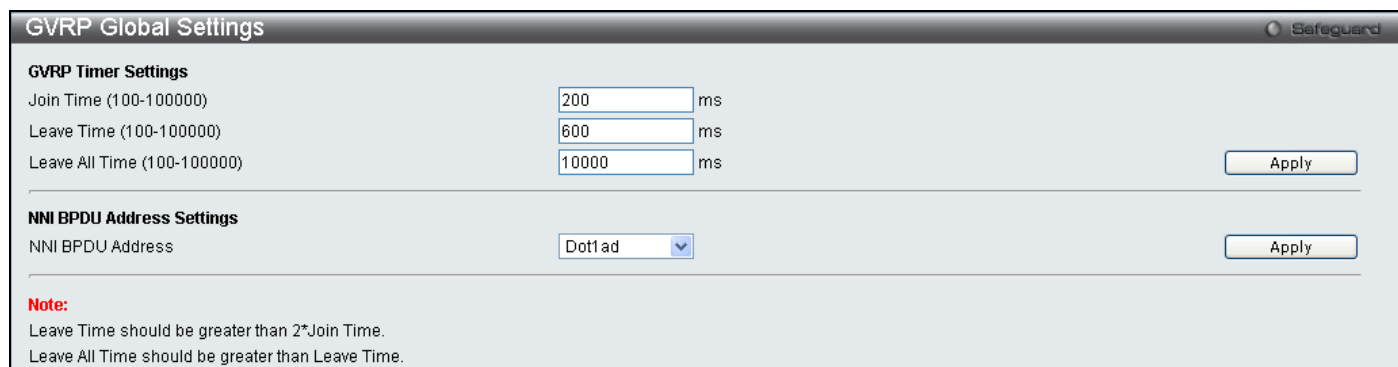


Figure 3 - 20 GVRP Timer Settings window

The following fields can be set:

Parameter	Description
<b>Join Time (100-100000)</b>	The time in milliseconds that specifies the amount of time between the Switch receiving the information about becoming a member of the group and actually joining the group. The default is 200.
<b>Leave Time (100-100000)</b>	The time in milliseconds that specifies the maximum amount of time between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. The default is 600. The <b>Leave Time</b> must be greater than 2 join times.



<b>Leave All Time (100-100000)</b>	The time in milliseconds that specifies the amount of time the Switch will take to Leave All groups. The default is 10000. The <b>Leave All Time</b> must be greater than the <b>Leave Time</b> .
<b>NNI BPDU Address</b>	This specifies the GVRP's pdu MAC address of the NNI port. <i>Dot1d</i> – Specifies GVRP's pdu MAC address of NNI port using 802.1d. <i>Dot1ad</i> – Specifies GVRP's pdu MAC address of NNI port using 802.1ad.

Click **Apply** to implement changes made.

## MAC-based VLAN Settings

This table 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 regardless of the authentication function operated on the port. 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** as shown below:

Figure 3 - 21 MAC-based VLAN Settings window

The following fields can be set

Parameter	Description
<b>MAC Address</b>	Specify the MAC address to be reauthenticated by entering it into the <b>MAC Address</b> field.
<b>VLAN Name</b>	Enter the VLAN name of a previously configured VLAN.

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

## PVID Auto Assign Settings

This commands *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*.

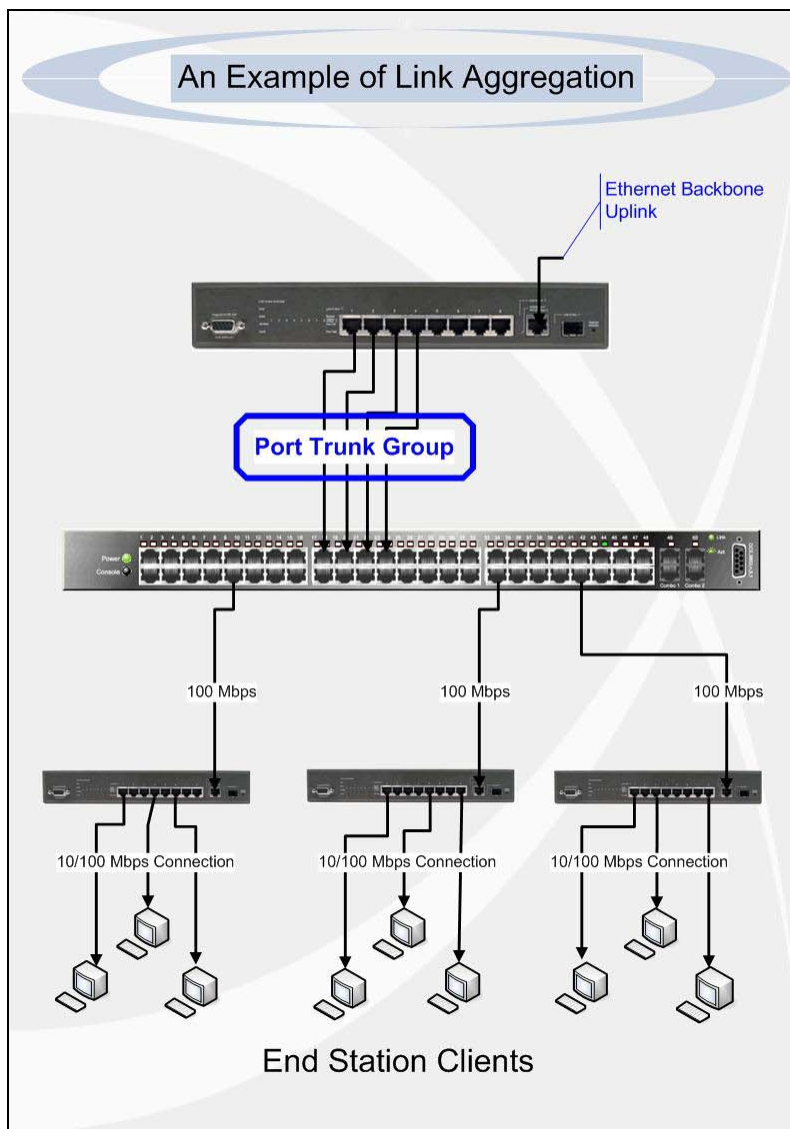
To view this window, click **L2 Features > PVID Auto Assign Settings** as shown below:

Figure 3 - 22 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. DGS-3700 Series supports up to 6 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.



**Figure 3 - 23 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 ports 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 6 link aggregation groups, each group consisting of 2 to 8 links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the four (optional) Gigabit ports, which can only belong to a single link aggregation group. All of the ports in the group must be members of the

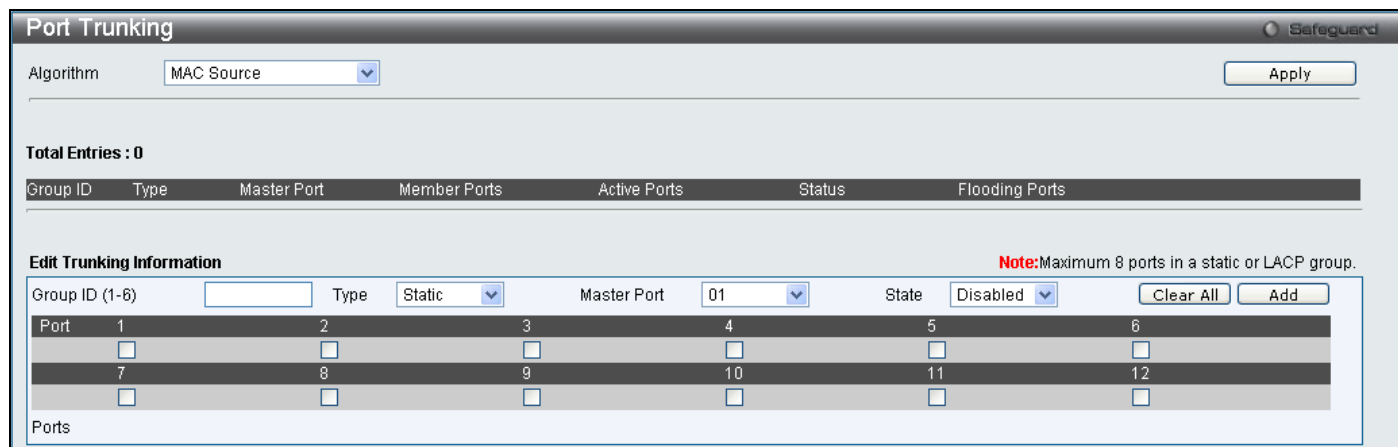
same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should 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** as shown below:



**Figure 3 - 24Port Trunking window**

The following fields can be set

Parameter	Description
<b>Algorithm</b>	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).
<b>Group ID</b>	Select an ID number for the group, between 1 and 6.
<b>Type</b>	This pull-down menu allows you to select between Static and LACP (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group.
<b>Master Port</b>	Choose the Master Port for the trunk group using the pull-down menu.
<b>State</b>	Trunk groups can be toggled between Enabled and Disabled. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
<b>Active Port</b>	Shows the port that is currently forwarding packets.
<b>Member Ports</b>	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
<b>Flooding Port</b>	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.

Click **Apply** to implement changes made.

## LACP Port Settings

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

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

Port	Activity
1	Passive
2	Passive
3	Passive
4	Passive
5	Passive
6	Passive
7	Passive
8	Passive
9	Passive
10	Passive
11	Passive
12	Passive

**Figure 3 - 25 LACP Port Settings window**

The following fields can be set

Parameter	Description
<b>From Port / To Port</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Activity</b>	<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 either a single switch or a group of ports on another switch in a switch stack. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Master switch CPU. This page allows you to view which port on a given switch will be allowed to forward packets to other ports on that switch. Select a port number from the drop down menu to display the forwarding ports. To configure new forwarding ports for a particular port, select a port from the menu and click **Apply**.

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

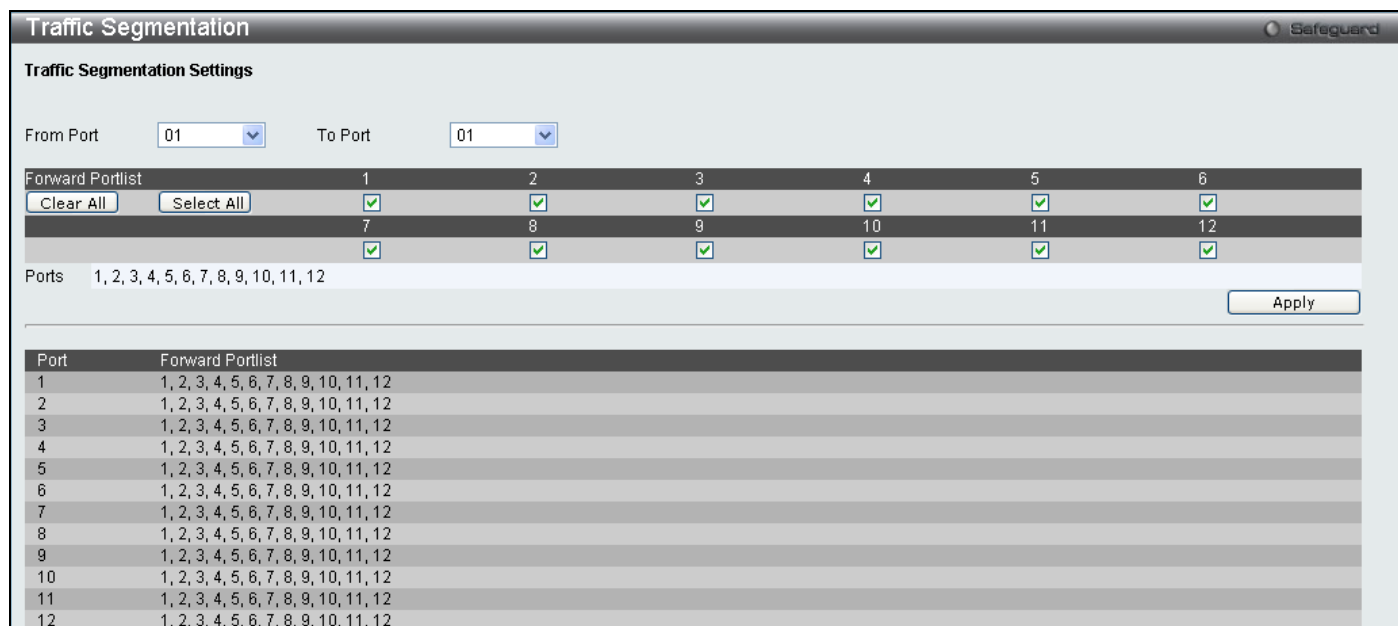


Figure 3 - 26 Traffic Segmentation window

The following fields can be set

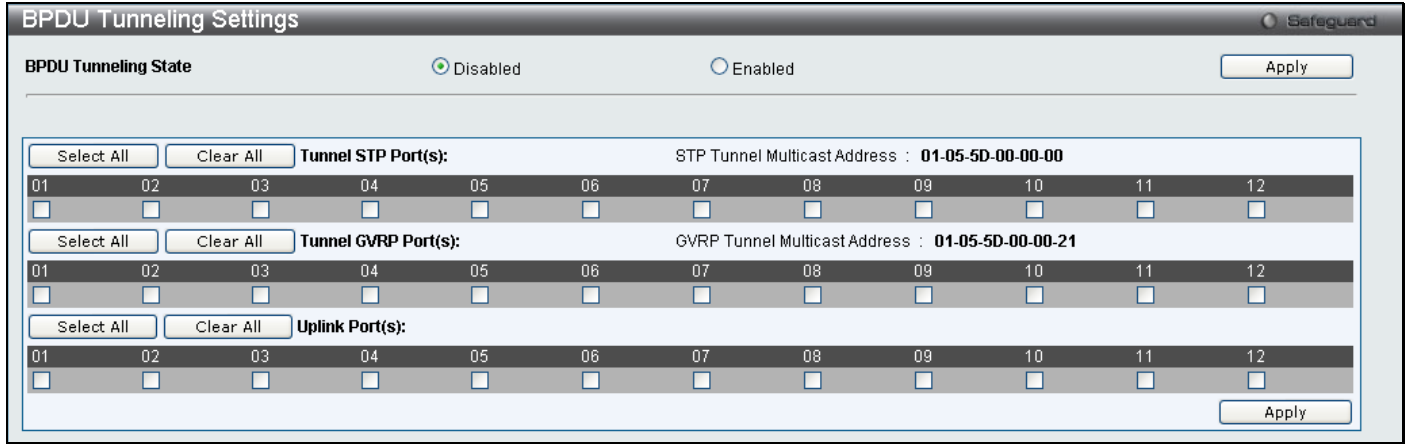
Parameter	Description
<b>From Port / To Port</b>	Check the corresponding boxes for the port(s) to transmit packets.
<b>Forward Portlist</b>	Check the boxes to select which of the ports on the Switch will be able to forward packets. These ports will be allowed to receive packets from the port specified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

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

# BPDU Tunneling Settings

This table is used to configure the BPDU Tunneling port types. When the device is operated with Q-in-Q enabled, DA will be replaced by the tunnel multicast address, and the BPDU will be tagged with the tunnel VLAN based on the Q-in-Q VLAN configuration and the tunnel/uplink setting. When the device is operated without Q-in-Q enabled, the BPDU will have its DA replaced by the tunnel multicast address and be transmitted out based on the VLAN configuration and the tunnel/uplink setting. The tunnel multicast address for STP BPDU is 01-05-5d-00-00-00. The tunnel multicast address for GVRP BPDU is 01-05-5d-00-00-21.

To view this window, click **L2 Features > BPDU Tunneling Settings** as shown below:



**Figure 3 - 27 BPDU Tunneling window**

Select the ports and port types on which the BPDU tunneling will be enabled or disabled and click **Apply**.

## IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

In order to use IGMP Snooping it must first be enabled for the entire Switch (see the **DGS-3700-12/DGS-3700-12G Switch Series Web Management Tool**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link 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 the **IGMP Snooping Settings** window to enable or disable IGMP Snooping on the Switch. To modify the settings, click the **Edit** button under Parameter Settings and a new table will appear for the user to configure.

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

Figure 3 - 28 IGMP Snooping Settings window

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

Figure 3 - 29 IGMP Snooping Parameters Settings - Edit window

The following fields can be set:

Parameter	Description
<b>VLAN ID</b>	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.
<b>VLAN Name</b>	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.
<b>Rate Limit</b>	Displays the rate limitation.
<b>Querier IP</b>	The querier IP address to send IGMP queries.
<b>Querier Expiry</b>	Displays the querier expiry time.

<b>Time</b>	
<b>Query Interval (1-65535)</b>	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 65535 seconds are allowed. Default = 125.
<b>Max Response Time (1-25)</b>	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
<b>Robustness Value (1-255)</b>	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 1 to 255. Default = 2.
<b>Last Member Query Interval (1-25 Sec)</b>	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1.
<b>Data Driven Group Expiry Time (1-65535)</b>	Allows the user to set the time that an IGMP Snooping data driven learning group will expire for the specified VLAN.
<b>Querier State</b>	Choose Enabled to enable transmitting IGMP Query packets or Disabled to disable. The default is Disabled.
<b>Fast Leave</b>	This parameter allows the user to enable the Fast Leave function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch. The default is Disabled.
<b>State</b>	Select Enabled to implement IGMP Snooping. This field is Disabled by default.
<b>Report Suppression</b>	Select Enable or Disable for IGMP Snooping report suppression for specified VLANs.
<b>Data Driven Learning State</b>	Allows users to enable or disable IGMP snooping data driven learning for the specified VLAN.
<b>Data Driven Learning Aged Out</b>	Allows users to enable or disable aged_out of IGMP Snooping data driven learning for the specified VLAN.
<b>Version</b>	Allows the user to configure the IGMP version used on the Switch. The default value is 3.
<b>Querier Role</b>	This read-only field describes the behavior of the router for sending query packets. Querier will denote that the router is sending out IGMP query packets. Non-Querier will denote that the router is not sending out IGMP query packets. This field will only read Querier when the Querier State and the State fields have been Enabled.

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

Figure 3 - 30 IGMP Snooping Router IP Settings – Edit window



## IGMP Snooping Rate Limit Settings

This table allows the user to configure the rate of IGMP snooping control packets that are allowed per port or VLAN. To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Rate Limit Settings** as shown below:

Figure 3 - 31 IGMP Snooping Rate Limit Settings window

The following parameters can be configured:

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

Click **Apply** to implement changes made.

## IGMP Snooping Static Group Settings

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

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Static Group Settings** as shown below:

Figure 3 - 32 IGMP Snooping Static Group Settings window

The following parameters can be configured:

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

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

## IGMP Multicast Group Profile Settings

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

To view this window, click **L2 Features > IGMP Snooping > IGMP Multicast Group Profile Settings** as shown below:

The screenshot shows the 'IGMP Multicast Group Profile Settings' window. At the top, there is a 'Profile Name' input field with a '(Max 32 characters)' label and an 'Add' button. Below this is a 'Delete All' button. A section titled 'Total Entries: 1' contains a table with one row: 'Profile Name' | 'dg'. To the right of this row is a 'Delete' button. A 'Group List' link is also visible at the bottom right.

**Figure 3 - 33 IGMP Multicast Group Profile Settings window**

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

The screenshot shows the 'Multicast Group Profile Multicast Address Settings' window. It features a 'Profile Name' field with the value 'dg' and a 'Multicast Address List' input field with the example '235.2.2.1-235.2.2.2'. There are 'Add', '<<Back', and 'Delete' buttons. Below is a table titled 'Multicast Address Group List: 1' with one entry: 'NO.' | '1' | 'Multicast Address List' | '236.3.3.1-236.3.3.2'.

**Figure 3 - 34 IGMP Multicast Group Profile Settings window – Group List**

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

## IGMP Snooping Multicast VLAN Settings

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

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Multicast VLAN Settings** as shown below:

The screenshot shows the 'IGMP Snooping Multicast VLAN Settings' window. It has two sections for 'Multicast VLAN(v4) Global State' and 'Multicast VLAN(v4) Forward Unmatched', both with 'Disabled' selected. Below are input fields for 'VLAN Name', 'VID (2-4094)', 'State' (a dropdown menu), 'Member Port', 'Tagged Member Port', 'Replace Source IP', and 'Source Port'. There are 'Clear All' and 'Add' buttons. At the bottom, a table titled 'Total Entries: 0' has columns: 'VID', 'VLAN Name', 'Replace Source IP', 'State', 'Member Port', 'Tagged Port', and 'Source Port'.

**Figure 3 - 35 IGMP Snooping Multicast VLAN Settings window**

The following fields can be set

Parameter	Description
<b>VLAN Name</b>	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
<b>VID (2-4094)</b>	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.

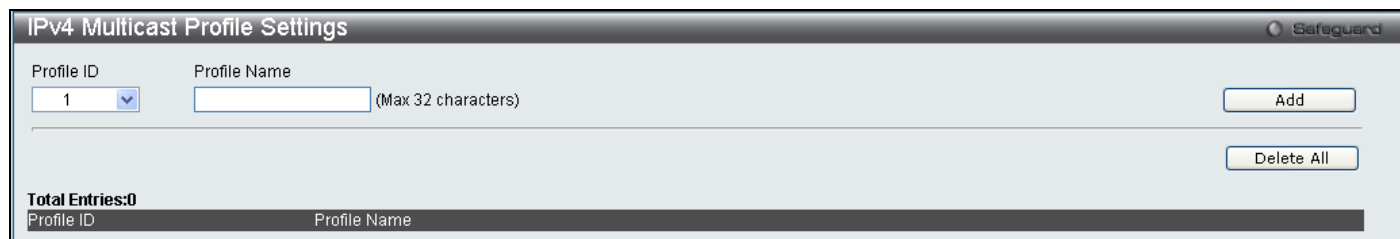
<b>State</b>	Use the drop-down menu to toggle between <i>Enabled</i> and <i>Disabled</i> .
<b>Replace Source IP</b>	Enter an IP address that new IP address to be used.
<b>Member Port (e.g.:1-4,6)</b>	Select the ports that will be members of the Multicast VLAN. (Eg. Ports 1 to 4 and port 6)
<b>Source Port (e.g.:1-4,6)</b>	Select the source Port for the Multicast VLAN.
<b>Tagged Member Port (e.g.:1-4,6)</b>	Select the ports that will be tagged as members of the VLAN.

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

## IPv4 Multicast Profile Settings

The **IPv4 Multicast Profile Settings** window allows the user to add a profile to which multicast IPv4 address(es) reports are to be received on specified ports or VLANs on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP Multicast address or range of IPv4 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports or VLANs.

To view this window, click **L2 Features > IGMP Snooping > IPv4 Multicast Profile Settings** as shown below:

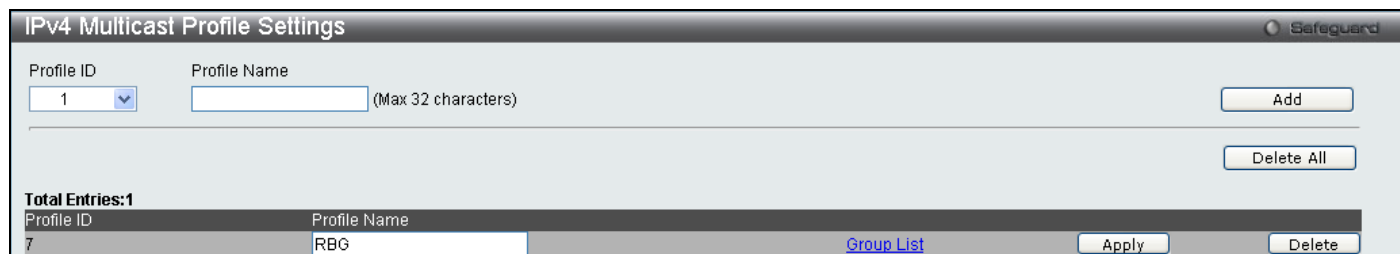


**Figure 3 - 36 IPv4 Multicast Profile Settings window**

The following fields can be set

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

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



**Figure 3 - 37 IPv4 Multicast Profile Settings – Edit window**

To configure the Group List Settings click the hyperlinked [Group List](#).

Figure 3 - 38 IP Multicast Address Group List Settings – Group List 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.

## IPv4 Limited Multicast Range Settings

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

To configure these settings, click **L2 Features > IGMP Snooping > IPv4 Limited Multicast Range Settings**.

Figure 3 - 39 IPv4 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**.

## IPv4 Max Multicast Group Settings

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

To view this window, click **L2 Features > IGMP Snooping > IPv4 Max Multicast Group Settings** as shown below:

VLAN ID	Max Multicast Group Number
1	Infinite
6	Infinite

Figure 3 - 40 IPv4 Max Multicast Group Settings window

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

## MLD Snooping

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

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID and the associated multicast IPv6 multicast group address and then considers this port to be a active listening port. The active listening ports are the only ones to receive multicast group data.

## MLD Control Messages

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

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

## MLD Snooping Settings

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

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

**MLD Snooping Settings**

**MLD Global Settings**

MLD Snooping State  Disabled  Enabled Apply

---

**MLD Data Driven Learning Settings**

Max Learned Entry Value (1-1024)  Apply

---

**Total Entries: 2**

VID	VLAN Name	State		
1	default	Disabled	<a href="#">Modify Router Port</a>	<span>Edit</span>
6	VLAN6	Disabled	<a href="#">Modify Router Port</a>	<span>Edit</span>

<<Back Next>>

**Figure 3 - 41 MLD Snooping Settings window**

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

MLD Snooping Parameters Settings			
VLAN ID	1	VLAN Name	default
Rate Limit	No Limitation	Querier IP	0
Querier Expiry Time	0 secs	Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec	Robustness Value (1-255)	2
Last Member Query Interval (1-25)	1 sec	Data Driven Group Expiry Time (1-65535)	260 sec
Querier State	Disabled	Fast Done	Disabled
State	Disabled	Report Suppression	Enabled
Data Driven Learning State	Enabled	Data Driven Learning Aged Out	Disabled
Version	2	Querier Role	Non-Querier

**Figure 3 - 42 MLD Snooping Parameters Settings – Edit window**

The following parameters may be viewed or modified:

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

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

Figure 3 - 43 MLD Snooping Router IP Settings – Modify window

## MLD Snooping Rate Limit Settings

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

To view this window, click **L2 Features > MLD Snooping > MLD Snooping Rate Limit Settings**, as shown below:

Figure 3 - 44 MLD Snooping Rate Limit Settings window

The following parameters may be viewed or modified:

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

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

Figure 3 - 45 MLD Snooping Rate Limit Settings – Edit window

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

## MLD Snooping Static Group Settings

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

To view this window, click **L2 Features > MLD Snooping > MLD Snooping Static Group Settings**, as shown below

Figure 3 - 46 MLD Snooping Static Group Settings window

The following parameters may be viewed or modified:

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

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

## MLD Multicast Group Profile Settings

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

To view this window, click **L2 Features > MLD Snooping > MLD Multicast Group Profile Settings** as shown below:



**Figure 3 - 47 MLD Multicast Group Profile Settings window**

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

**Figure 3 - 48 Multicast Group Profile Multicast Address Settings window – Group List**

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

## MLD Snooping Multicast VLAN Settings

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

To view this window, click **L2 Features > MLD Snooping > MLD Snooping Multicast VLAN Settings** as shown below:

**Figure 3 - 49 MLD Snooping Multicast VLAN Settings window**

The following fields can be set:

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

<b>Tagged Member Port (e.g.:1-4,6)</b>	Select the ports that will be tagged as members of the VLAN.
--	--

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

## IPv6 Multicast Profile Settings

The **IPv6 Multicast Profile Settings** window allows the user to add a profile to which multicast IPv6 address(es) reports are to be received on specified ports or VLANs on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP Multicast address or range of IPv6 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports or VLANs.

To view this window, click **L2 Features > MLD Snooping > IPv6 Multicast Profile Settings** as shown below:

**Figure 3 - 50 IPv6 Multicast Profile Settings window**

The following fields can be set:

Parameter	Description
<b>Profile ID</b>	Use the drop-down menu to choose a Profile ID.
<b>Profile Name</b>	Enter a name for the IPv6 Multicast Profile.

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

**Figure 3 - 51 IPv6 Multicast Profile Settings – Edit window**

To configure the Group List Settings click the hyperlinked [Group List](#).

**Figure 3 - 52 Multicast Address Group List Settings – Group List 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.

## IPv6 Limited Multicast Range Settings

The **IPv6 Limited Multicast Range Settings** enables the user to configure the ports or VLANs on the switch that will be involved in the Limited IPv6 Multicast Range. The user can configure the range of IPv6 multicast addresses that will be accepted on the ports or VLANs.

To view this window, click **L2 Features > MLD Snooping > IPv6 Limited Multicast Range Settings** as shown below:

Figure 3 - 53 IPv6 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**.

## IPv6 Max Multicast Group Settings

The **IPv6 Max Multicast Group Settings** allows users to configure the ports or VLANs on the switch that will be apart of the max number of multicast groups that can be learned.

To view this window, click **L2 Features > MLD Snooping > IPv6 Max Multicast Group Settings** as shown below:

VLAN ID	Max Multicast Group Number
1	Infinite
6	Infinite

Figure 3 - 54 IPv6 Max Multicast Group Settings window

To add a new IPv6 Max Multicast Group enter the information and click **Apply**, to search for an entry enter the information and click **Find**.

## 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 **L2 Features > Port Mirror** as shown below:

**Port Mirror** Safeguard

**Target Port Settings**

State  Disabled  Enabled

Target Port 1

Source Port 1

Sniffer Mode	Ports
Tx	
Rx	

**Source Port Settings**

Sniffer Mode	1	2	3	4	5	6	7	8	9	10	11	12
Tx		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rx		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Tx												
Rx												

Apply

Figure 3 - 55 Port Mirror window

### To configure a mirror port:

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



**NOTE:** You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

## Loopback Detection Settings

The Loopback Detection function is used to detect the loop created by a specific port. This feature is used to temporarily shutdown a port on the Switch when a loop detecting packet has been looped back to the switch. When the Switch detects that these packets are received from a port or a VLAN, it signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to discarding state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the pull-down menu.

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

Port	Loopdetect State	Loop Status
1	Disabled	Normal
2	Disabled	Normal
3	Disabled	Normal
4	Disabled	Normal
5	Disabled	Normal
6	Disabled	Normal
7	Disabled	Normal
8	Disabled	Normal
9	Disabled	Normal
10	Disabled	Normal
11	Disabled	Normal
12	Disabled	Normal

Figure 3 - 56 Loopback Detection Settings window

The following parameters can be configured:

Parameter	Description
<b>LBD State</b>	Used to <i>Enable</i> or <i>Disable</i> loopback detection. The default is <i>Disabled</i> .
<b>Mode</b>	Use the drop-down menu to toggle between <i>Port Based</i> and <i>VLAN Based</i> .
<b>Interval (1-32767)</b>	Set a Loopdetect Interval between 1 and 32767 seconds. The default is 10 seconds.
<b>Trap Status</b>	Select the trap status, choose <i>None</i> , <i>Loop Detected</i> , <i>Loop Cleared</i> or <i>Both</i> .
<b>Recover Time (0 or 60-1000000)</b>	Time allowed (in seconds) for recovery when a Loopback is detected. The Loopdetect Recover Time can be set at 0 seconds, or 60 to 1000000 seconds. Entering 0 will disable the Loopdetect Recover Time. The default is 60 seconds.
<b>From Port / To Port</b>	Use the drop-down menu to select a beginning and ending port number.
<b>State</b>	Use the drop-down menu to toggle between <i>Enabled</i> and <i>Disabled</i> .

Click **Apply** to implement changes made.

## Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol; 802.1D-2004 STP compatible, 802.11d-2004 Rapid STP and 802.1q-2005 MSTP. 802.1D STP will be familiar to most networking professionals. However, since 802.1w RSTP has been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D STP and 802.1w RSTP.

### 802.1w Rapid Spanning Tree

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

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

### Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking and listening used in 802.1D and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 6-2 below compares how the two protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1D is this absence of immediate feedback from adjacent bridges.

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

**Table 3 - 2 Comparing Port States**

RSTP is capable of a more rapid transition to a forwarding state – it no longer relies on timer configurations – RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

### Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

## **P2P Port**

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

## **802.1D and 802.1w Compatibility**

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D format when necessary. However, any segment using 802.1D STP will not benefit from the rapid transition and rapid topology change detection of RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP.

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

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

## STP Bridge Global Settings

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

To view this window, click **L2 features > Spanning Tree > STP Bridge Global Settings** as shown below:

**Figure 3 - 57 STP Bridge Global Settings window**

The following parameters can be set:

Parameter	Description
<b>STP State</b>	Use the radio buttons to enable or disable the STP Status.
<b>STP Version</b>	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices:  <i>STPCompatibility</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.
<b>Forwarding BPDU</b>	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 Disabled.
<b>Bridge Max Age (6-40 Sec)</b>	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.
<b>Bridge Hello Time (1-10 Sec)</b>	The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge.
<b>Bridge Forward Delay (4-30 Sec)</b>	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.
<b>TX Hold Count (1-10)</b>	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.



<b>Max Hops (1-20)</b>	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 1 to 20. The default is 20.
<b>NNI BPDU Address</b>	Configure NNI port address. <i>dot1d</i> – Specifies GVRP's bpdu MAC address of NNI port using the definition of 802.1d. <i>dot1ad</i> – Specifies GVRP's pdu MAC address of NNI port using the definition of 802.1ad.

Click **Apply** to implement changes made.



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

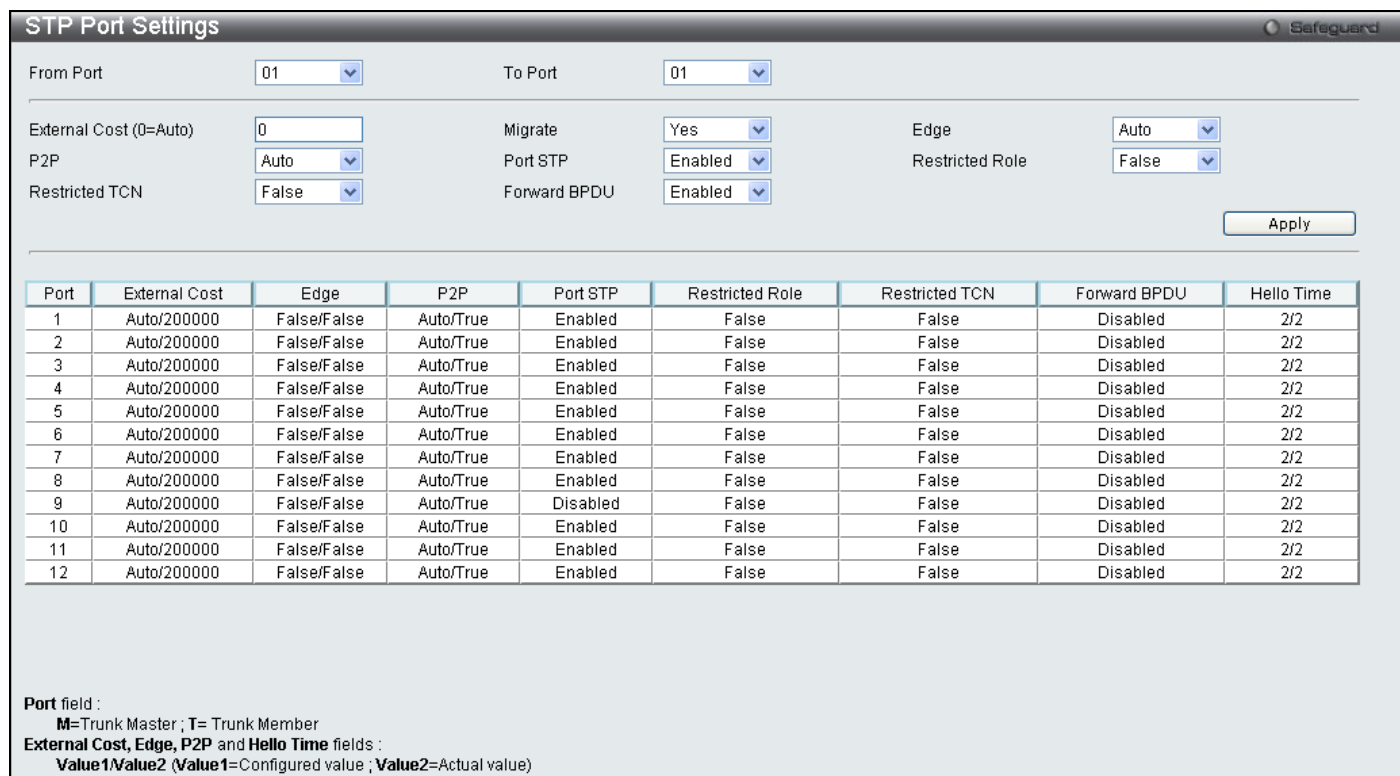
Max. Age  $\leq$  2 x (Forward Delay - 1 second)

Max. Age  $\geq$  2 x (Hello Time + 1 second)

## STP Port Settings

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

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



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

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 - 58 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
<b>From Port / To Port</b>	A consecutive group of ports may be configured starting with the selected port.
<b>External Cost (0=Auto)</b>	<p>The external cost defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</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>

<b>Migrate</b>	Setting this parameter as <i>Yes</i> 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 <i>yes</i> 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.
<b>Edge</b>	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.
<b>P2P</b>	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 <i>p2p</i> 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.
<b>Port STP</b>	Allows STP to be <i>Enabled</i> or <i>Disabled</i> for the ports.
<b>Restricted Role</b>	Toggle between <i>True</i> and <i>False</i> to set whether this port is restricted to be selected as a root port. The default value is <i>False</i> .
<b>Restricted TCN</b>	Toggle between <i>True</i> and <i>False</i> to set whether this port is restricted to be selected as a propagate topology change. The default value is <i>False</i> .
<b>Forward BPDU</b>	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> .

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** as shown below:

The screenshot shows the 'MST Configuration Identification' window with the following details:

- MST Configuration Identification Settings:**
  - Configuration Name: 00:21:91:AF:37:D0
  - Revision Level (0-65535): 0
  - Apply button
- Instance ID Settings:**
  - MSTI ID (1-15): [Empty field]
  - Type: Add VID (dropdown menu)
  - VID List (1-4094): [Empty field]
  - Apply button
- Total Entries: 1**

MSTI ID	VID List
CIST	1-4094

Figure 3 - 59 MST Configuration Identification window

The window above contains the following information:

Parameter	Description
<b>Configuration Name</b>	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 <b>STP Bridge Global Settings</b> window.
<b>Revision Level (0-65535)</b>	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.
<b>MSTI ID</b>	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.
<b>Type</b>	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.
<b>VID List (1-4094)</b>	This field displays the VLAN IDs associated with the specific MSTI.

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

## STP Instance Settings

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

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

The screenshot shows the 'STP Instance Settings' window. At the top, there's a title bar with 'STP Instance Settings' and a 'Safeguard' icon. Below the title bar, there's a section for 'STP Priority Settings' with two input fields: 'MSTI ID' and 'Priority' (set to 0). An 'Apply' button is to the right. Below this is a table with 'Total Entries: 1'. The table has three columns: 'Instance Type', 'Instance Status', and 'Instance Priority'. The entry is 'CIST', 'Disabled', and '32768(Bridge Priority: 32768, SYS ID Ext: 0)'. There are 'Edit' and 'View' buttons next to the entry. At the bottom, there's a section for 'STP Instance Operational Status' with a list of parameters and their values, such as 'MSTP ID' (--), 'Designated Root Bridge' (--), 'External Root Cost' (--), 'Regional Root Bridge' (--), etc.

**Figure 3 - 60 STP Instance Settings window**

The following information can be set:

Parameter	Description
<b>MSTI ID</b>	Displays the MSTI ID of the instance being modified. An entry of 0 in this field denotes the CIST (default MSTI).
<b>Priority</b>	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.

**STP Instance Settings**

STP Priority Settings

MSTI ID: 0      Priority: 0     

---

Total Entries: 1

Instance Type	Instance Status	Instance Priority	
CIST	Disabled	4096(Bridge Priority: 4096, SYS ID Ext: 0)	<input type="button" value="Edit"/> <input type="button" value="View"/>

---

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 - 61 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 this window, click **L2 Features > Spanning Tree > MSTP Port Information** as shown below:

**MSTP Port Information**

Port: 01     

---

MSTP Port Setting

Instance ID:      Internal Path Cost (1-200000000):      Priority: 0     

---

Port 1 Settings

MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role	
0	N/A	200000	128	Forwarding	NonStp	<input type="button" value="Edit"/>

Figure 3 - 62 MSTP Port Information window

The following parameters can be viewed or set:

Parameter	Description
<b>Port</b>	Use the drop-down menu to select a port.
<b>Instance ID</b>	Displays the MSTI ID of the instance being configured. The range is from 0 to 15. An entry of 0 in this field denotes the CIST (default MSTI).
<b>Internal Path cost (1-200000000)</b>	<p>This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto). There are two options:</p> <p><i>0 (auto)</i> – Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.</p> <p><i>value 1-200000000</i> – Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.</p>
<b>Priority</b>	Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

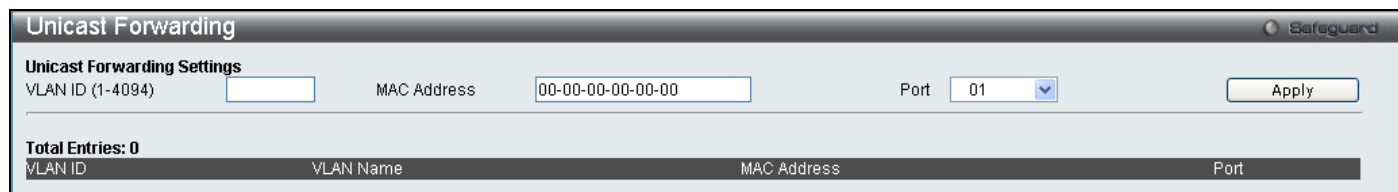
Click **Apply** to implement changes made.

## Forwarding & Filtering

This folder contains windows for Unicast Forwarding, Multicast Forwarding and Multicast Filtering Mode.

### Unicast Forwarding

To view this window, click **L2 Features > Forwarding & Filtering > Unicast Forwarding** as shown below:



**Figure 3 - 63 Unicast Forwarding window**

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

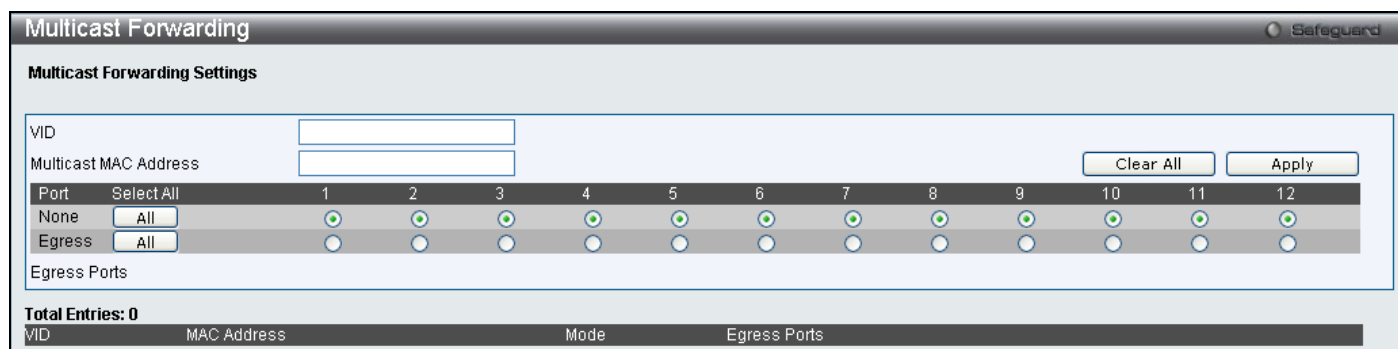
Parameter	Description
<b>VLAN ID (1-4094)</b>	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
<b>MAC Address</b>	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
<b>Port</b>	Allows the selection of the port number on which the MAC address entered above resides.

Click **Apply** to implement the changes made. The new entries will be displayed on the Unicast Forwarding Table on the bottom half of the screen.

### Multicast Forwarding

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

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Forwarding** as shown below:



**Figure 3 - 64 Multicast Forwarding window**

The following parameters can be set:

Parameter	Description
<b>VID</b>	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
<b>Multicast MAC Address</b>	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
<b>Port Settings</b>	Allows the selection of ports that will be members of the static multicast group and ports either that are forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are:  <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.  <i>Egress</i> – The port is a static member of the multicast group.

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

## Multicast Filtering Mode

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

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

**Multicast Filtering Mode** Safeguard

VLAN Name  VID List

All  Multicast Filter Mode: Forward All Groups

VID List:

**Total Entries: 2**

VID	VLAN Name	Multicast Filter Mode
1	default	Forward Unregistered Groups
6	VLAN6	Forward Unregistered Groups

Figure 3 - 65 Multicast Filtering Mode window

## LLDP

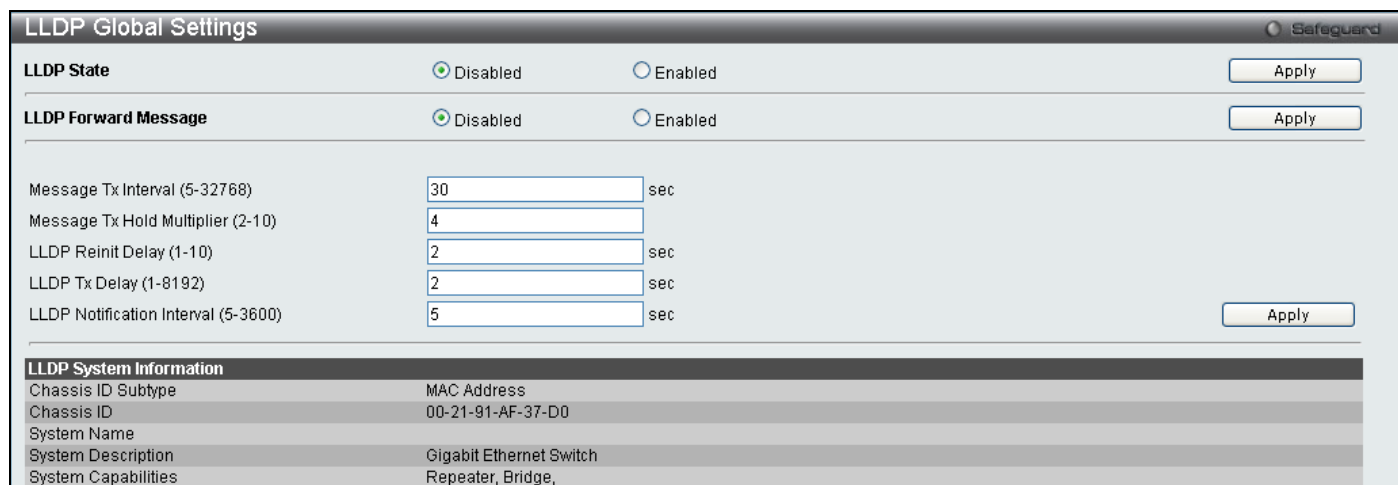
The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that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

This window is used to configure the LLDP Global Settings on the Switch. When LLDP is enabled the Switch can start to transmit, receive and process LLDP packets. The specific function of each port will depend on the per port LLDP settings. LLDP Global State is *Disabled* by default.

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



**Figure 3 - 66 LLDP Global Settings window**

The following parameters can be set:

Parameter	Description
<b>LLDP State</b>	Used to Enable or Disable LLDP on the Switch.
<b>LLDP Forward Message</b>	When LLDP is disabled, this function controls the LLDP packet forwarding. It will flood the received LLDP packet to all ports that have the same VLAN and will advertise to other stations attached to the same IEEE 802 LAN. When LLDP is enabled, this function does not take effect.
<b>Message TX Interval (5-32768)</b>	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).
<b>Message TX Hold Multiplier (2-10)</b>	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.
<b>LLDP Reinit Delay (1-10)</b>	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).
<b>LLDP TX Delay (1-8192)</b>	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).
<b>LLDP Notification Interval (5-3600)</b>	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

This window is used to display the LLDP port settings on the Switch. The ports can be individually configured to send notifications to configured SNMP trap receivers.

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

Port ID	Notification	Admin Status	IPv4(IPv6) Address
1	Disabled	Tx and Rx	
2	Disabled	Tx and Rx	
3	Disabled	Tx and Rx	
4	Disabled	Tx and Rx	
5	Disabled	Tx and Rx	
6	Disabled	Tx and Rx	
7	Disabled	Tx and Rx	
8	Disabled	Tx and Rx	
9	Disabled	Tx and Rx	
10	Disabled	Tx and Rx	
11	Disabled	Tx and Rx	
12	Disabled	Tx and Rx	

**Figure 3 - 67 LLDP Port Settings window**

The following parameters can be set:

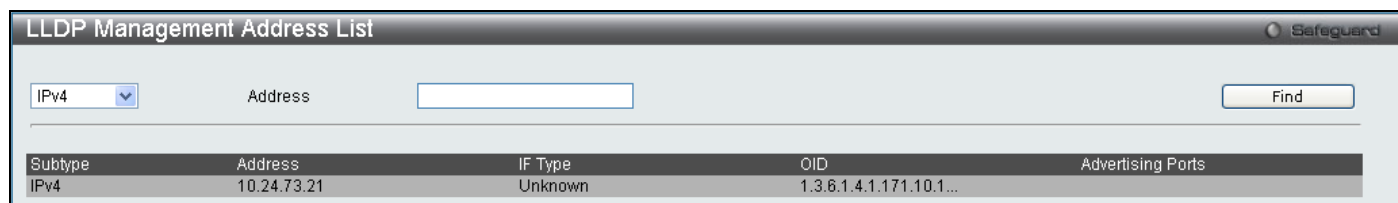
Parameter	Description
<b>From Port /To Port</b>	Use the pull-down menu to select a range of ports to be configured.
<b>Notification</b>	Use the pull-down menu to <i>Enable</i> or <i>Disable</i> each port for sending change notifications to the configured SNMP trap receiver(s) when an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The notification will include new available information, information timeout and information updates. The changing type includes any data update/insert/remove.
<b>Admin Status</b>	This functions controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains <b>TX</b> , <b>RX</b> , <b>TX And RX</b> or <b>Disabled</b> . <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 TX And RX.
<b>Subtype</b>	Used to specify the type of address that will be used either <i>IPv4</i> or <i>IPv6</i> .
<b>Action</b>	Used to <i>Enable</i> or <i>Disable</i> the advertise management address function based on port.
<b>Address</b>	Enter the <i>IPv4</i> or <i>IPv6</i> address as previously specified. 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 Management Address List

This window is used to find the LLDP management address information on the Switch.

To view this window, click **L2 Features > LLDP > LLDP Management Address List** as shown below:



Subtype	Address	IF Type	OID	Advertising Ports
IPv4	10.24.73.21	Unknown	1.3.6.1.4.1.171.10.1...	

**Figure 3 - 68 LLDP Management Address List window**

The following parameters can be set:

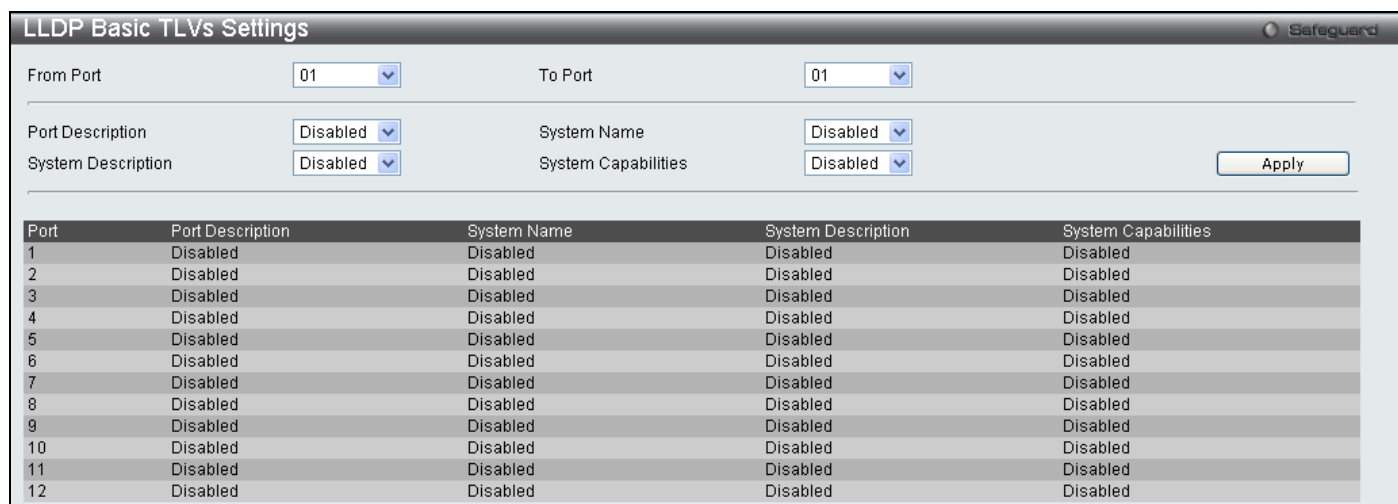
Parameter	Description
<b>Address</b>	Use the drop down menu to select either the <i>IPv4</i> or <i>IPv6</i> Address. Enter the management ip address or the ip address of the entity you wish to advertise to. IPv4/IPv6 is a management IP so the IP information will be sent with the frame when the mgt_addr config is enabled.

Click **Find** to implement changes made.

## LLDP Basic TLVs Settings

This window is used to enable the settings for the Basic TLVs Settings. An active LLDP port on the Switch always includes mandatory data in its outbound advertisements. There are four optional data types that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory data types cannot be disabled. There are also four data types which can be optionally selected. These include Port Description, System Name, System Description and System Capability.

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



Port	Port Description	System Name	System Description	System Capabilities
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled

**Figure 3 - 69 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
<b>From Port /To Port</b>	Use the pull-down menu to select a range of ports to be configured.

<b>Port Description</b>	Use the drop-down menu to enable or disable port description.
<b>System Name</b>	Use the drop-down menu to enable or disable system name.
<b>System Description</b>	Use the drop-down menu to enable or disable system description.
<b>System Capabilities</b>	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** as shown below:

Port	PVID State	Port and Protocol VID State	VID	VLAN Name State	VID	Protocol Identity State	Protocol Identity
1	Disabled	Disabled		Disabled		Disabled	
2	Disabled	Disabled		Disabled		Disabled	
3	Disabled	Disabled		Disabled		Disabled	
4	Disabled	Disabled		Disabled		Disabled	
5	Disabled	Disabled		Disabled		Disabled	
6	Disabled	Disabled		Disabled		Disabled	
7	Disabled	Disabled		Disabled		Disabled	
8	Disabled	Disabled		Disabled		Disabled	
9	Disabled	Disabled		Disabled		Disabled	
10	Disabled	Disabled		Disabled		Disabled	
11	Disabled	Disabled		Disabled		Disabled	
12	Disabled	Disabled		Disabled		Disabled	

**Figure 3 - 70 LLDP Dot1 TLVs Settings window**

The following parameters can be set:

Parameter	Description
<b>From Port / To Port</b>	Use the pull-down menu to select a range of ports to be configured.
<b>Dot1 TLV PVID</b>	Use the drop-down menu to enable or disable the advertised PVID. This TLV optional datatype determines whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
<b>Dot1 TLV Protocol VLAN</b>	Use the drop-down menu to enable or disable the advertised Protocol VLAN ID. This TLV optional data type indicates whether the corresponding Local System's port and protocol VLAN ID instance will be transmitted on the port. If a port is associated with multiple protocol VLANs, those enabled ports and protocol VLAN IDs will be advertised.
<b>Dot1 TLV VLAN</b>	Use the drop-down menu to enable or disable the advertised VLAN Name. This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN name will be advertised. Those enabled VLAN name will be advertised. If the numbers of VLANs are larger, it will only bring limited numbers of VLANs due to restrictions of the package length.
<b>Dot1 TLV Protocol Identity</b>	Use the drop-down menu to enable or disable the advertised Protocol Identity. This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning

Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.

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** as shown below:

Port	MAC/PHY Configuration Status	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled
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

**Figure 3 - 71 LLDP Dot3 TLVs Settings window**

The following parameters can be set:

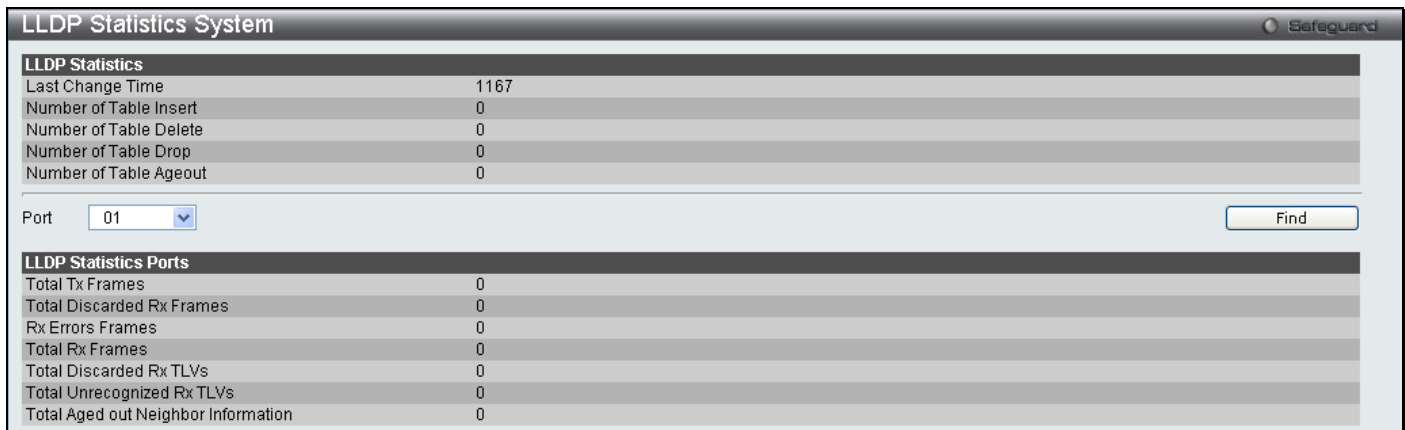
Parameter	Description
<b>From Port / To Port</b>	Use the drop-down menu to select a range of ports to be configured.
<b>MAC/PHY Configuration Status</b>	This TLV optional data type indicates that the LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This indicates it is possible for two 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> .
<b>Link Aggregation</b>	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> .
<b>Maximum Frame Size</b>	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.

## LLDP Statistics System

LLDP Statistics System allows you an overview of neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch. Use the drop-down menu to check a specific port and click **Find** the information will be displayed in the lower half of the table.

To view this window, click **L2 Features > LLDP > LLDP Statistics System** as shown below:



LLDP Statistics	
Last Change Time	1167
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Ageout	0

Port: 01 Find

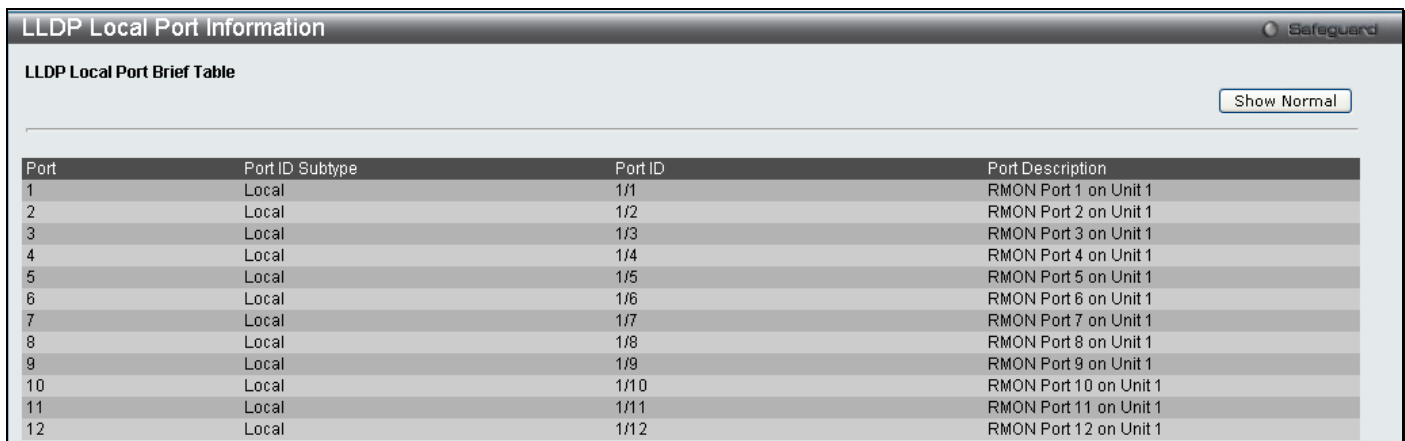
LLDP Statistics Ports	
Total Tx Frames	0
Total Discarded Rx Frames	0
Rx Errors Frames	0
Total Rx Frames	0
Total Discarded Rx TLVs	0
Total Unrecognized Rx TLVs	0
Total Aged out Neighbor Information	0

Figure 3 - 72 LLDP Statistics System window

## LLDP Local Port Information

LLDP Local Port Information window displays the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

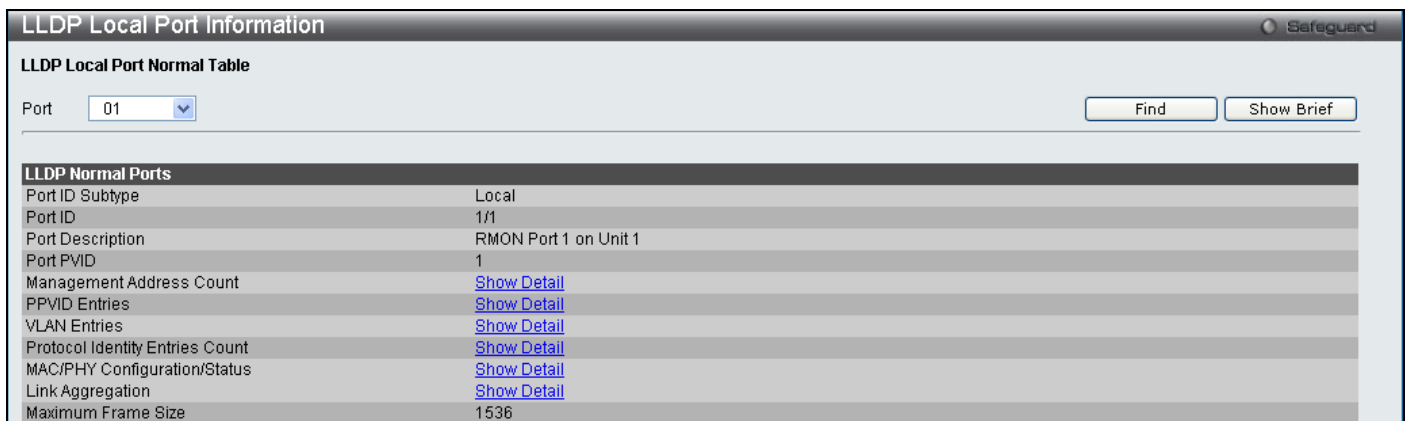
To view this window, click **L2 Features > LLDP > LLDP Local Port Information** as shown below:



Port	Port ID Subtype	Port ID	Port Description
1	Local	1/1	RMON Port 1 on Unit 1
2	Local	1/2	RMON Port 2 on Unit 1
3	Local	1/3	RMON Port 3 on Unit 1
4	Local	1/4	RMON Port 4 on Unit 1
5	Local	1/5	RMON Port 5 on Unit 1
6	Local	1/6	RMON Port 6 on Unit 1
7	Local	1/7	RMON Port 7 on Unit 1
8	Local	1/8	RMON Port 8 on Unit 1
9	Local	1/9	RMON Port 9 on Unit 1
10	Local	1/10	RMON Port 10 on Unit 1
11	Local	1/11	RMON Port 11 on Unit 1
12	Local	1/12	RMON Port 12 on Unit 1

Figure 3 - 73 LLDP Local Port Information window

To view the information on a per port basis click the **Show Normal** button, which will display the following window:



LLDP Local Port Normal Table	
Port	01
Find Show Brief	
LLDP Normal Ports	
Port ID Subtype	Local
Port ID	1/1
Port Description	RMON Port 1 on Unit 1
Port PVID	1
Management Address Count	<a href="#">Show Detail</a>
PPVID Entries	<a href="#">Show Detail</a>
VLAN Entries	<a href="#">Show Detail</a>
Protocol Identity Entries Count	<a href="#">Show Detail</a>
MAC/PHY Configuration/Status	<a href="#">Show Detail</a>
Link Aggregation	<a href="#">Show Detail</a>
Maximum Frame Size	1536

Figure 3 - 74 LLDP Local Port Information (Show Normal) window

Use the drop-down menu to select a port and click **Find** the information will be displayed on the lower half of the window. To return to the previous window click the **Show Brief** button. To view details of individual parameters click the hyperlinked [Show Detail](#), which will reveal the following window.

Port	Subtype	Address	IF Type	OID
1	IPv4	10.24.73.21	Unknown	1.3.6.1.4.1.171.10.1...

Figure 3 - 75 LLDP Local Port Information (Show Detail) window

To return to the **LLDP Local Port Information** window click the **<<Back** button.

## LLDP Remote Port Information

This window displays port information learned from the neighbor. The switch receives packets from a remote station but is able to store the information as local.

To view this window, click **L2 Features > LLDP > LLDP Remote Port Information** as shown below:

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

Figure 3 - 76 LLDP Remote Port Information window

Select the port you wish to view by using the drop-down menu and click **Find** the information will be displayed in the lower half of the table. To view the settings for an individual port select the port and click **Show Normal** which will display the following window.

Entity	Information
--------	-------------

Figure 3 - 77 LLDP Remote Port Information (Show Normal) window

## CFM

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

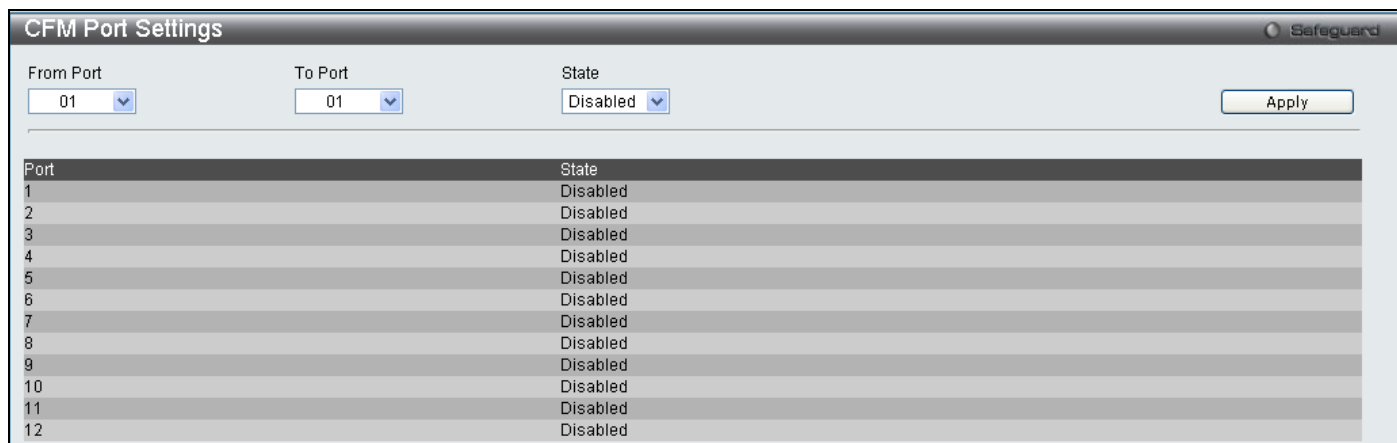
Ethernet CFM frames have a special Ether Type (0x8902). All CFM messages are confined to a maintenance domain per VLAN basis. There are different message types which are identified by unique Opcode of the CFM frame payload.

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

## CFM Port Settings

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

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



The CFM Port Settings window displays configuration options for CFM ports. It includes fields for 'From Port', 'To Port', and 'State', each with a dropdown menu. Below these fields is a table listing ports 1 through 12 and their current 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

Figure 3 - 78 CFM Port Settings window

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

## CFM CCM PDUs Forwarding Mode

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

To view this window, click **L2 Features > CFM > CFM CCM PDUs Forwarding Mode** as shown below:



The CFM CCM PDUs Forwarding Mode window shows a dropdown menu for 'PDUs Forwarding Mode' set to 'Software'. A note at the bottom states: 'Note:CCM:Continuity Check Message'.

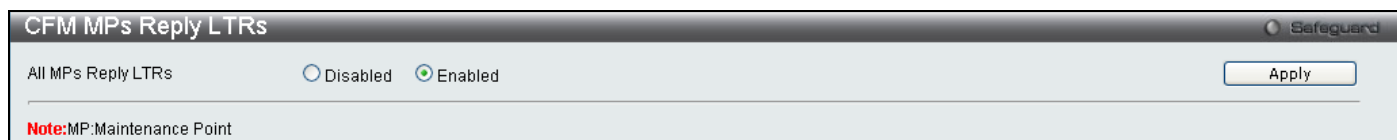
Figure 3 - 79 CFM CCM PDUs Forwarding Mode window

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

## CFM MPs Reply LTRs

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

To view this window, click **L2 Features > CFM > CFM MPs Reply LTRs** as shown below:



The CFM MPs Reply LTRs window features radio buttons for 'All MPs Reply LTRs', with 'Disabled' selected and 'Enabled' unselected. A note at the bottom states: 'Note:MP:Maintenance Point'.

Figure 3 - 80 CFM MPs Reply LTRs window

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

## CFM MIPCCM List

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

To view this window, click **L2 Features > CFM > CFM MIPCCM List** as shown below:



Figure 3 - 81 CFM MIPCCM List window

## Connectivity Fault Management Settings

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

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

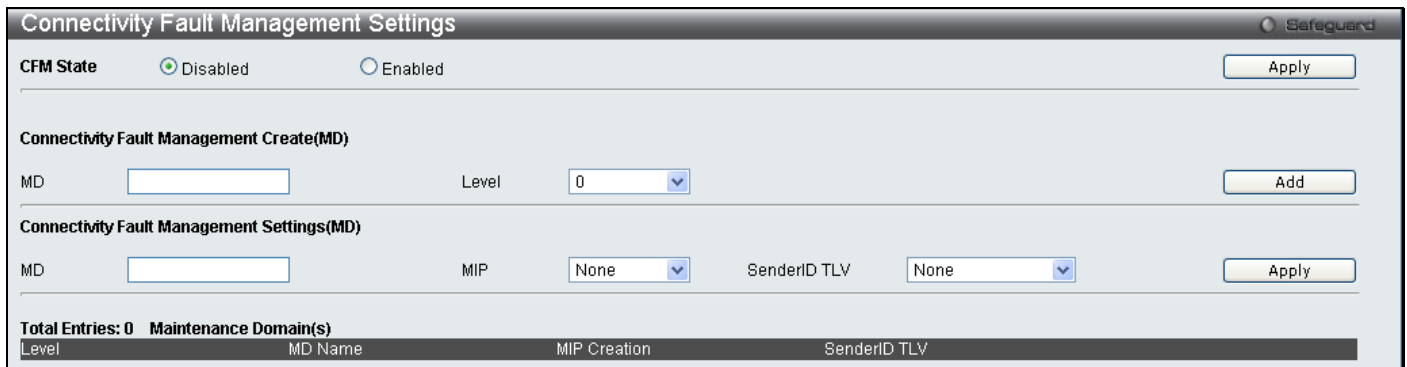


Figure 3 - 82 Connectivity Fault Management Settings window

The following parameters can be set or are displayed:

Parameter	Description
<b>CFM State</b>	Used to <i>Enable</i> or <i>Disable</i> the CFM State.
<b>Connectivity Fault Management Create(MD)</b>	
<b>MD</b>	Enter the maintenance domain name you wish to create.
<b>Level</b>	Enter the maintenance domain level.
<b>Connectivity Fault Management Settings(MD)</b>	
<b>MD</b>	Enter the maintenance domain name you wish to configure.



<b>MIP</b>	<p>This setting controls the creation of MIPs.</p> <p><i>None</i> – Means that no MIPs will be created. This is the default value.</p> <p><i>Auto</i> – MIPs are created when the next lower active MD-level on the port is reached or there are no lower active MD levels.</p> <p><i>Explicit</i> – MIPs are created when the next lower active MD-level on the port is reached.</p>
<b>SenderID TLV</b>	Used to define the TLV data types of the maintenance domain. The user can choose between <i>None</i> , <i>Chassis</i> , <i>Manage</i> or <i>Chassis Manage</i> .

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

## CFM Loopback Settings

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

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

**Figure 3 - 83 CFM Loopback Settings window**

The following parameters can be configured:

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

<b>LBM's Priority</b>	The 802.1p priority to be set in the transmitted LBMs. If not specified it uses the same priority as CCMs and LTMs sent by the MEP.
-----------------------	---

Click **Apply** to implement changes made.

## CFM Linktrace Settings

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

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

**Figure 3 - 84 CFM Linktrace Settings window**

The following parameters can be configured:

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

Click **Apply** to implement changes made.

# Ethernet OAM

## Ethernet OAM Settings

This window is used to configure the ports Ethernet OAM mode. In Active mode the ports can initiate OAM discovery and start or stop remote loopback. When a port in OAM enabled, any change to the OAM mode will cause the OAM discovery to be restarted.

To view this window, click **L2 Features > Ethernet OAM > Ethernet OAM Settings** as shown below:

**Ethernet OAM Settings**

Ethernet OAM Settings

From Port: 01 To Port: 01 Mode: Active State: Disabled Remote Loopback: Start Received Remote Loopback: Ignore Apply

**Ethernet OAM Table**

**Port 1**

Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Support
Unidirection	Not Supported
Link Monitoring	Support
Variable Request	Not Supported
PDU Revision	0
Operation Status	Disable
Loopback Status	No Loopback

**Port 2**

Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Support
Unidirection	Not Supported
Link Monitoring	Support
Variable Request	Not Supported
PDU Revision	0
Operation Status	Disable
Loopback Status	No Loopback

**Port 3**

Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Support
Unidirection	Not Supported
Link Monitoring	Support

Figure 3 - 85 Ethernet OAM Settings window

The following parameters can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specify a range of ports to be configured.
<b>Mode</b>	Specify to operate in either <i>Active</i> mode or <i>Passive</i> mode. The default mode is <i>Active</i> .
<b>State</b>	Specify that the OAM function state is <i>Enabled</i> or <i>Disabled</i> . The default state is <i>Disabled</i> .
<b>Remote Loopback</b>	Specify to <i>Start</i> or <i>Stop</i> the OAM remote loopback function.
<b>Received Remote Loopback</b>	Specify whether to <i>Process</i> or to <i>Ignore</i> the received Ethernet OAM remote loopback function. The default method is <i>Ignore</i> .

Click **Apply** to implement changes.

## Ethernet OAM Configuration Settings

This window is used to configure and display the primary controls and status information for Ethernet OAM on the Switch.

To view this window, click **L2 Features > Ethernet OAM > Ethernet OAM Configuration Settings** as shown below:

**Figure 3 - 86 Ethernet OAM Configuration Settings window**

The following parameters can be configured:

Parameter	Description
<b>From Port / To Port</b>	Specify a range of ports to be configured.
<b>Link Event</b>	Configures the Ethernet OAM critical link event. Specify <i>Link Monitor</i> or <i>Critical Link Event</i> .
<b>Link Monitor</b>	Indicates that the OAM entity can send and receive Event Notification OAMPDU.
<b>Threshold (0-4294967295)</b>	Specify the number of error frame seconds in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 error frame second.
<b>Window (1000-60000)</b>	Specify the period of error frame summary events. The range is 1000ms-60000ms and the default value is 1000 ms.
<b>Notify</b>	Specify to <i>Enable</i> or <i>Disable</i> the event notification. The default state is <i>Enabled</i> .

Click **Apply** to implement changes.

## Section 4

# QoS

*HOL Blocking Prevention*

*Bandwidth Control*

*Traffic Control*

*802.1p Default Priority*

*802.1p User Priority*

*QoS Scheduling Mechanism*

*QoS Scheduling*

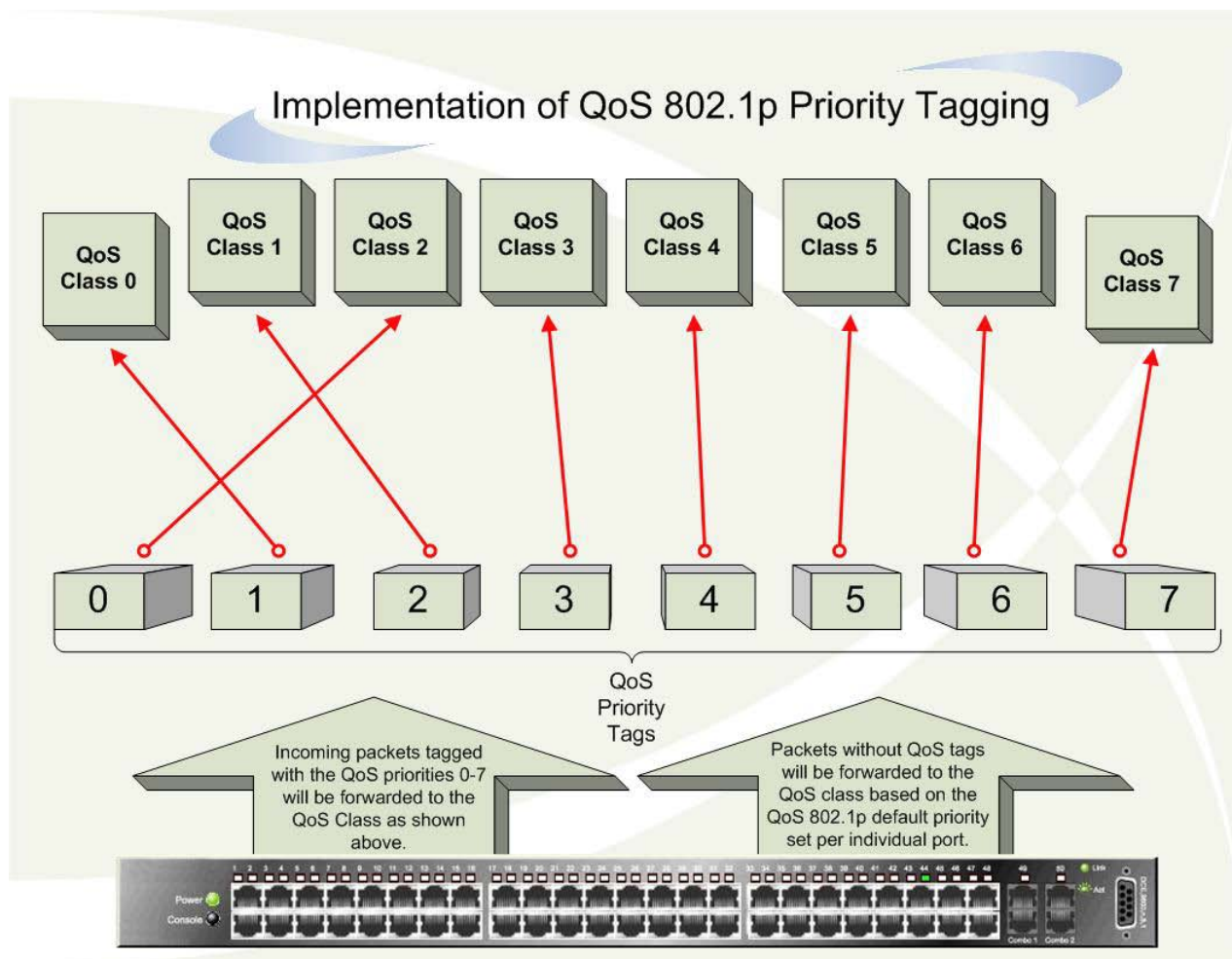
*In Band Manage Settings*

*SRED*

The DGS-3700 Series 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 bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements 802.1P priority queuing.



**Figure 4 - 1 Mapping QoS on the Switch**

The picture above shows the default priority setting for the Switch. Class-7 has the highest priority of the eight 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, let's say 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 it will be emptied before any other packet is forwarded. This results in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

## Understanding QoS

The Switch has eight priority queues. These priority queues are labeled from 0-7, with 7 being the highest priority and 0 the lowest priority queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A-H, with their respective weight value: 8-1. When each queue has 10 outbound packets, they are sent in the following sequence:

A1, B1, C1, D1, E1, F1, G1, H1,

A2, B2, C2, D2, E2, F2, G2,

A3, B3, C3, D3, E3, F3,

A4, B4, C4, D4, E4,

A5, B5, C5, D5,

A6, B6, C6,

A7, B7,

A8,

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

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

B10, C9, D8, E7, F6,

C10, D9, E8,

D10,

E9, F7, G5, H3,

E10, F8, G6,

F9,

F10, G7, H4,

G8,

G9, H5,

G10, H6 ~ H10

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

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the DGS-3700 Series has eight priority queues (and eight Classes of Service) for each port on the Switch.

## HOL Blocking Prevention

This window is used to enable HOL Prevention Settings on the Switch.

To view this window, click **QoS > HOL Blocking Prevention Settings** as shown below:

Figure 4 - 2 HOL Prevention Settings window

## Bandwidth Control

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

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

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

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 - 3 Bandwidth Control window

The following parameters can be set or are displayed:

Parameter	Description
<b>From port / To port</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Type</b>	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.
<b>No Limit</b>	This drop-down menu allows you to select <i>Enabled</i> or <i>Disabled</i> to specify whether the selected port have unlimited bandwidth.



<b>Rate (64-1024000)</b>	This field allows you to enter the data rate, in Kbits per second, that will be the limit for the selected port. The value must be a multiple of 64, between 64 and 1024000.
--------------------------	--

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

## 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 Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recover it using the **Port Configuration** window in the **Configuration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the Shutdown option of the Action field in the window below.

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

**Traffic Control** Safeguard

**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 (0-255000)	131072 pkt/s
Storm Control Type	None		

**Traffic Trap Settings**

None

Port	Storm Control Type	Action	Threshold	Count Down	Interval
1	None	Drop	131072	0	5
2	None	Drop	131072	0	5
3	None	Drop	131072	0	5
4	None	Drop	131072	0	5
5	None	Drop	131072	0	5
6	None	Drop	131072	0	5
7	None	Drop	131072	0	5
8	None	Drop	131072	0	5
9	None	Drop	131072	0	5
10	None	Drop	131072	0	5
11	None	Drop	131072	0	5
12	None	Drop	131072	0	5

**Note:** For unicast storm traffic, the violated action is always 'drop'.

**Figure 4 - 4 Traffic Control window**

The following parameters can be configured:

Parameter	Description
<b>Traffic Control Settings</b>	
<b>From Port / To Port</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Action</b>	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 BPDUs packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the <b>Port Configuration</b> window in the <b>Administration</b> 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.
<b>Count Down (0 or 5-30)</b>	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, 5-30 minutes. 0 is disable forever state, port will not enter shutdown forever mode.
<b>Time Interval (5-30)</b>	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.
<b>Threshold (0-255000)</b>	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from 0 to 255000 with a default setting of 131072.
<b>Storm Control Type</b>	Select the type of Storm Type to detect, either Broadcast Multicast or Unicast. Once selected, use the pull-down menu to enable or disable this storm detection.
<b>Traffic Trap Setting</b>	
<b>Traffic Trap Settings</b>	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: <ul style="list-style-type: none"> <li>• <i>None</i> – Will not send any Storm trap warning messages regardless of action taken by the Traffic Control mechanism.</li> <li>• <i>Storm Occurred</i> – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only.</li> <li>• <i>Storm Cleared</i> – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only.</li> <li>• <i>Both</i> – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch.</li> </ul> <p>This function cannot be implemented in the Hardware mode. (When Drop is chosen in the Action field.)</p>

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



**NOTE:** Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).



**NOTE:** Ports that are in the Shutdown forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.



**NOTE:** Ports that are in Shutdown Forever mode will be seen as link down in all windows and screens until the user recovers these ports.

## 802.1p Default Priority

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

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

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

**Figure 4 - 5 802.1p Default Priority window**

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

## 802.1p User Priority

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

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

Port	Priority	Class ID
1	0	Class-2
1	1	Class-0
1	2	Class-1
1	3	Class-3
1	4	Class-4
1	5	Class-5
1	6	Class-6
1	7	Class-7
2	0	Class-2
2	1	Class-0
2	2	Class-1
2	3	Class-3
2	4	Class-4
2	5	Class-5
2	6	Class-6
2	7	Class-7
3	0	Class-2
3	1	Class-0
3	2	Class-1
3	3	Class-3
3	4	Class-4
3	5	Class-5
3	6	Class-6
3	7	Class-7
4	0	Class-2
4	1	Class-0
4	2	Class-1
4	3	Class-3
4	4	Class-4
4	5	Class-5
4	6	Class-6
4	7	Class-7
5	0	Class-2
5	1	Class-0
5	2	Class-1

Figure 4 - 6 802.1p User Priority window

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

## QoS Scheduling Mechanism

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

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

Port	Mode
1	Strict
2	Strict
3	Strict
4	Strict
5	Strict
6	Strict
7	Strict
8	Strict
9	Strict
10	Strict
11	Strict
12	Strict

Figure 4 - 7 QoS Scheduling Mechanism

The following parameters can be configured.

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

Click **Apply** to implement changes made.

## QoS Scheduling

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

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

**QoS Scheduling** Safeguard

**QoS Scheduling Settings**

From Port:  To Port:  Class ID:  Scheduling Mechanism:  Apply

---

**QoS Scheduling Table**

Port	Class ID	Weight
1	Class-0	1
1	Class-1	2
1	Class-2	3
1	Class-3	4
1	Class-4	5
1	Class-5	6
1	Class-6	7
1	Class-7	8
2	Class-0	1
2	Class-1	2
2	Class-2	3
2	Class-3	4
2	Class-4	5
2	Class-5	6
2	Class-6	7
2	Class-7	8
3	Class-0	1
3	Class-1	2
3	Class-2	3
3	Class-3	4
3	Class-4	5
3	Class-5	6
3	Class-6	7
3	Class-7	8
4	Class-0	1
4	Class-1	2
4	Class-2	3
4	Class-3	4
4	Class-4	5
4	Class-5	6
4	Class-6	7
4	Class-7	8
5	Class-0	1
5	Class-1	2

Figure 4 - 8 QoS Scheduling

The following parameters can be configured:

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

Click **Apply** to implement changes made.

## In Band Manage Settings

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

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



Figure 4 - 9 In Band Manage Settings

Select the priority and click **Apply**.

## SRED

Simple random early detection (sRED) is a simplified RED mechanism based on ASIC capability. Random Early Detection (RED) is a congestion avoidance mechanism at the gateway in packet switched networks. RED gateways keep the average queue size low while allowing occasional bursts of packets in the queue. The switch provides support for sRED through active queue management by probabilistic dropping of incoming colored packets.

Active queue management is a class of algorithms that attempt to proactively drop or mark frames before congestion becomes excessive. The goal is to detect the onset of persistent congestion and take proactive action so that TCP sources contributing to the congestion back off gracefully, insuring good network utilization while minimizing frame loss.

This proactive approach starts discarding specific colored packets before the packet buffer becomes full. If this queue depth is less than the threshold, there is minimal (or no) congestion and the packet is enqueued. If congestion is detected the packet is dropped or queued based on the DSCP.

## SRED Settings

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

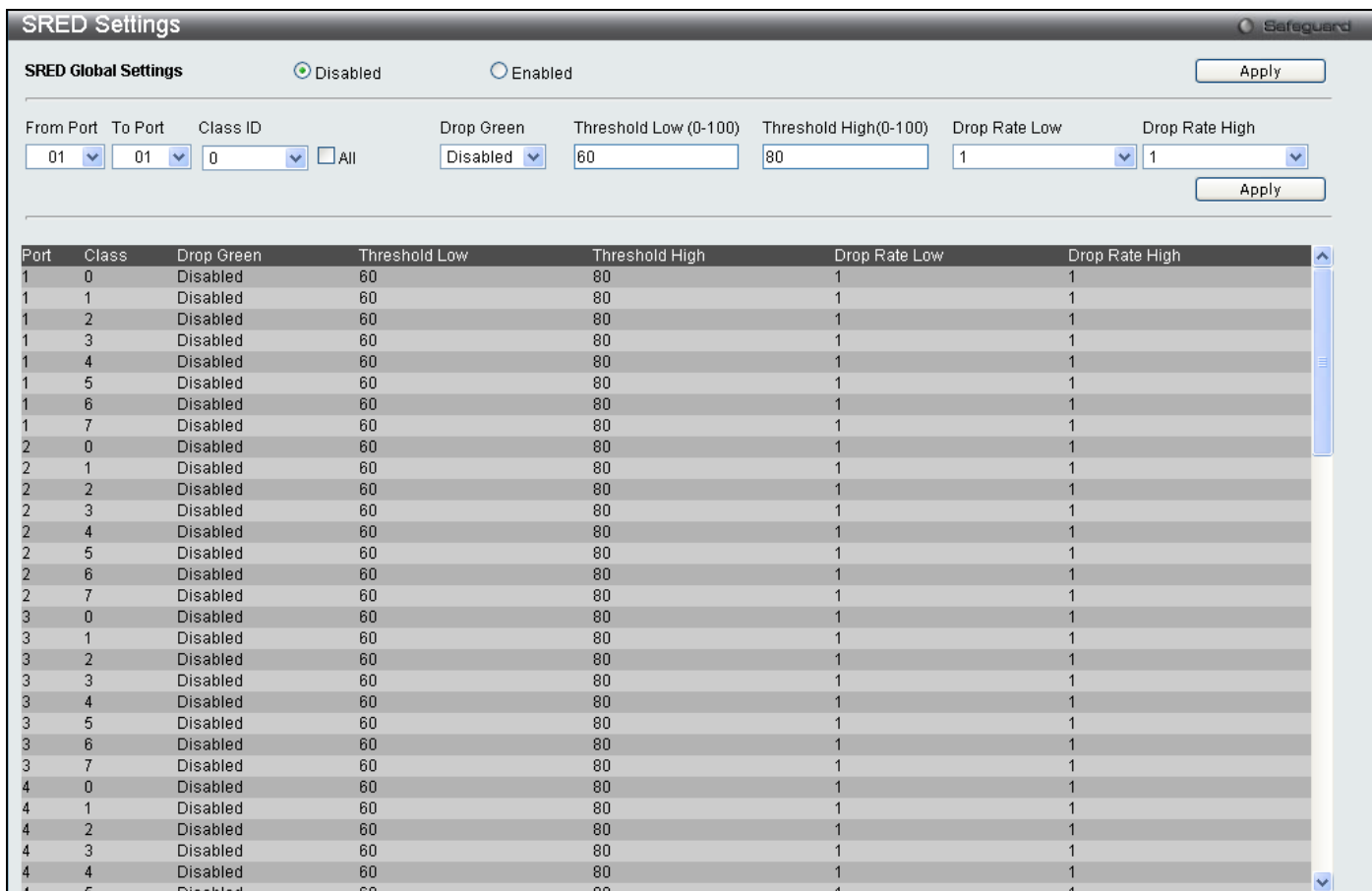


Figure 4 - 10 SRED Settings window

The following parameters may be set:

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

<b>From port / To port</b>	A consecutive group of ports may be configured starting with the selected port.																			
<b>Class ID</b>	Select the Class ID, from 0-7, to configure for the SRED parameters. Selecting <i>all</i> will set the parameters configured here for all CoS queues.																			
<b>Drop Green</b>	<p><i>Enabled:</i> Probabilistic drop yellow and red colored packets if the queue depth is above the lower threshold, and probabilistic drop green colored packets if the queue depth is above the upper threshold.</p> <p><i>Disabled:</i> Probabilistic drop red colored packets if the queue depth is above the lower threshold, and probabilistic drop yellow colored packets if the queue depth is above the upper threshold. Green packets will not be dropped even it reach the threshold.</p>																			
<b>Threshold Low (0-100)</b>	Threshold Low refers to the drop red packets it might also include yellow packets.																			
<b>Threshold High (0-100)</b>	Threshold High refers to the drop yellow or green packets depending on the drop mode.																			
<b>Drop Rate Low</b>	<p>There are eight drop rates as shown below, the user may determine the drop rate for the expected packet.</p> <table border="1"> <thead> <tr> <th><b>Configure Value</b></th> <th><b>Drop rate for expected packet</b></th> </tr> </thead> <tbody> <tr> <td><b>1</b></td> <td><b>100%</b></td> </tr> <tr> <td><b>2</b></td> <td><b>6.25%</b></td> </tr> <tr> <td><b>3</b></td> <td><b>3.125%</b></td> </tr> <tr> <td><b>4</b></td> <td><b>1.5625%</b></td> </tr> <tr> <td><b>5</b></td> <td><b>0.78125%</b></td> </tr> <tr> <td><b>6</b></td> <td><b>0.390625%</b></td> </tr> <tr> <td><b>7</b></td> <td><b>0.1953125%</b></td> </tr> <tr> <td><b>8</b></td> <td><b>0.09765625%</b></td> </tr> </tbody> </table>		<b>Configure Value</b>	<b>Drop rate for expected packet</b>	<b>1</b>	<b>100%</b>	<b>2</b>	<b>6.25%</b>	<b>3</b>	<b>3.125%</b>	<b>4</b>	<b>1.5625%</b>	<b>5</b>	<b>0.78125%</b>	<b>6</b>	<b>0.390625%</b>	<b>7</b>	<b>0.1953125%</b>	<b>8</b>	<b>0.09765625%</b>
<b>Configure Value</b>			<b>Drop rate for expected packet</b>																	
<b>1</b>	<b>100%</b>																			
<b>2</b>	<b>6.25%</b>																			
<b>3</b>	<b>3.125%</b>																			
<b>4</b>	<b>1.5625%</b>																			
<b>5</b>	<b>0.78125%</b>																			
<b>6</b>	<b>0.390625%</b>																			
<b>7</b>	<b>0.1953125%</b>																			
<b>8</b>	<b>0.09765625%</b>																			
<b>Drop Rate High</b>																				

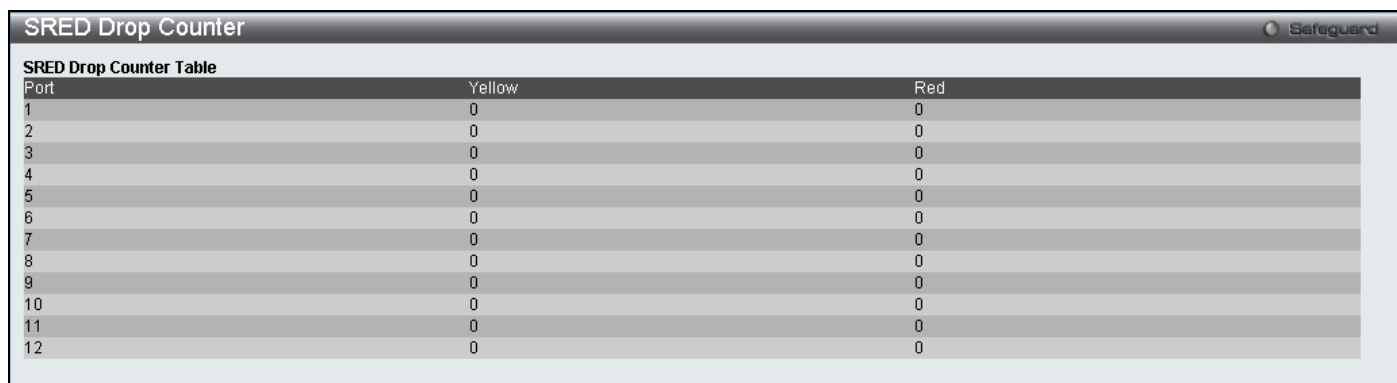
Click **Apply** to implement changes.



## SRED Drop Counter

This window is used to view the SRED Drop Counter settings on the Switch.

To view this window, click **QoS > SRED > SRED Drop Counter** as shown below:



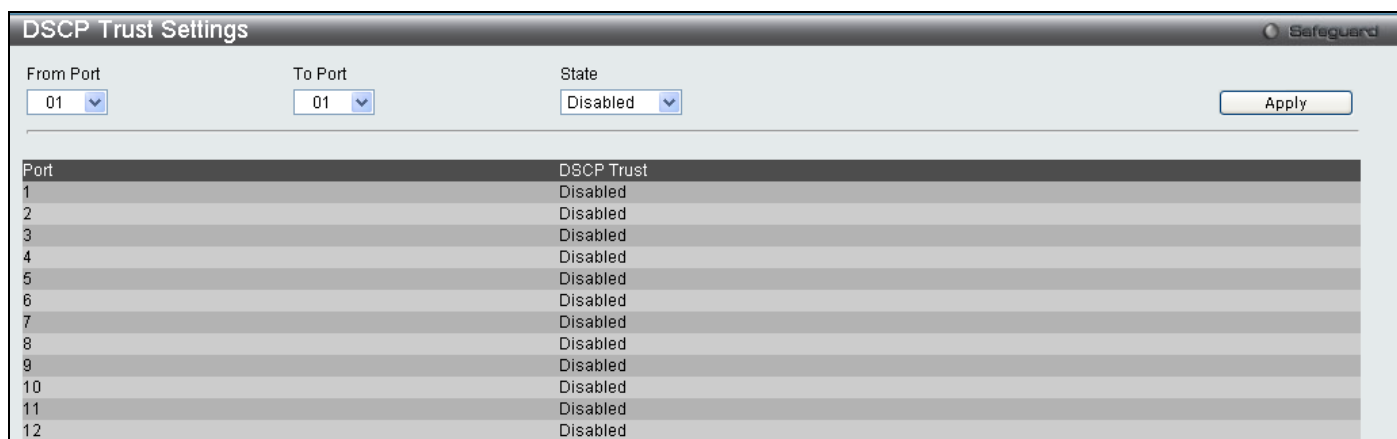
Port	Yellow	Red
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0

Figure 4 - 11 SRED Drop Counter window

## DSCP Trust Settings

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

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



From Port	To Port	State
01	01	Disabled

Port	DSCP Trust
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled

Figure 4 - 12 DSCP Trust Settings window

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

## DSCP Map Settings

This window is used to enable DSCP Map Settings.

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

DSCP Map Settings								
From Port	To Port	DSCP Map		DSCP List(0-63)		Priority		Apply
01	01	DSCP Priority				0		
Port	0	1	2	3	4	5	6	7
1	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
2	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
3	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
4	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
5	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
6	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
7	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
8	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
9	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
10	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
11	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
12	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Figure 4 - 13 DSCP Map Settings window

The following parameters may be set:

Parameter	Description
<b>From port / To port</b>	A consecutive group of ports may be configured starting with the selected port.
<b>DSCP Map</b>	Use the drop-down menu to choose a DSCP Map, you can choose between <i>DSCP Priority</i> , <i>DSCP DSCP</i> and <i>DSCP Color</i> .
<b>DSCP List(0-63)</b>	This field allows the user to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between 0 and 63.
<b>Priority</b>	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.

Click **Apply** to implement changes.

## 802.1p Map Settings

This window is used to enable 802.1p Map Settings.

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

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

**Figure 4 - 14 DSCP Map Settings window**

The following parameters may be set:

Parameter	Description
<b>From port / To port</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Priority List(0-7)</b>	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
<b>Color</b>	Specify the color <i>Red</i> , <i>Yellow</i> or <i>Green</i> .

Click **Apply** to implement changes.

## Section 5

# Security

***Safeguard Engine***

***Trusted Host***

***IP-MAC-Port Binding***

***Port Security***

***DHCP Server Screening Settings***

***802.1X***

***SSL Settings***

***SSH***

***Access Authentication Control***

***MAC-based Access Control***

***Web Authentication***

***NetBIOS Filtering***

## Safeguard Engine

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

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an *Exhausted* mode. When in this mode, the Switch only receives a small amount of ARP or IP broadcast packets for a calculated time interval. Every five seconds, the Switch will check to see if there are too many packets flooding the Switch. If the threshold has been crossed, the Switch will do a rate limit and only allow a small amount of ARP and IP broadcast packets for five seconds. After another five-second checking interval arrives, the Switch will again check the ingress flow of packets. If the flooding has stopped, the Switch will again begin accepting all packets. Yet, if the checking shows that there continues to be too many packets flooding the Switch, it will still only accept a small amount of ARP and IP broadcast packets for double the time of the previous stop period. This doubling of time for stopping ingress ARP and IP broadcast packets will continue until the maximum time has been reached, which is 320 seconds and every stop from this point until a return to normal ingress flow would be 320 seconds. For a better understanding, examine the following example of the Safeguard Engine.

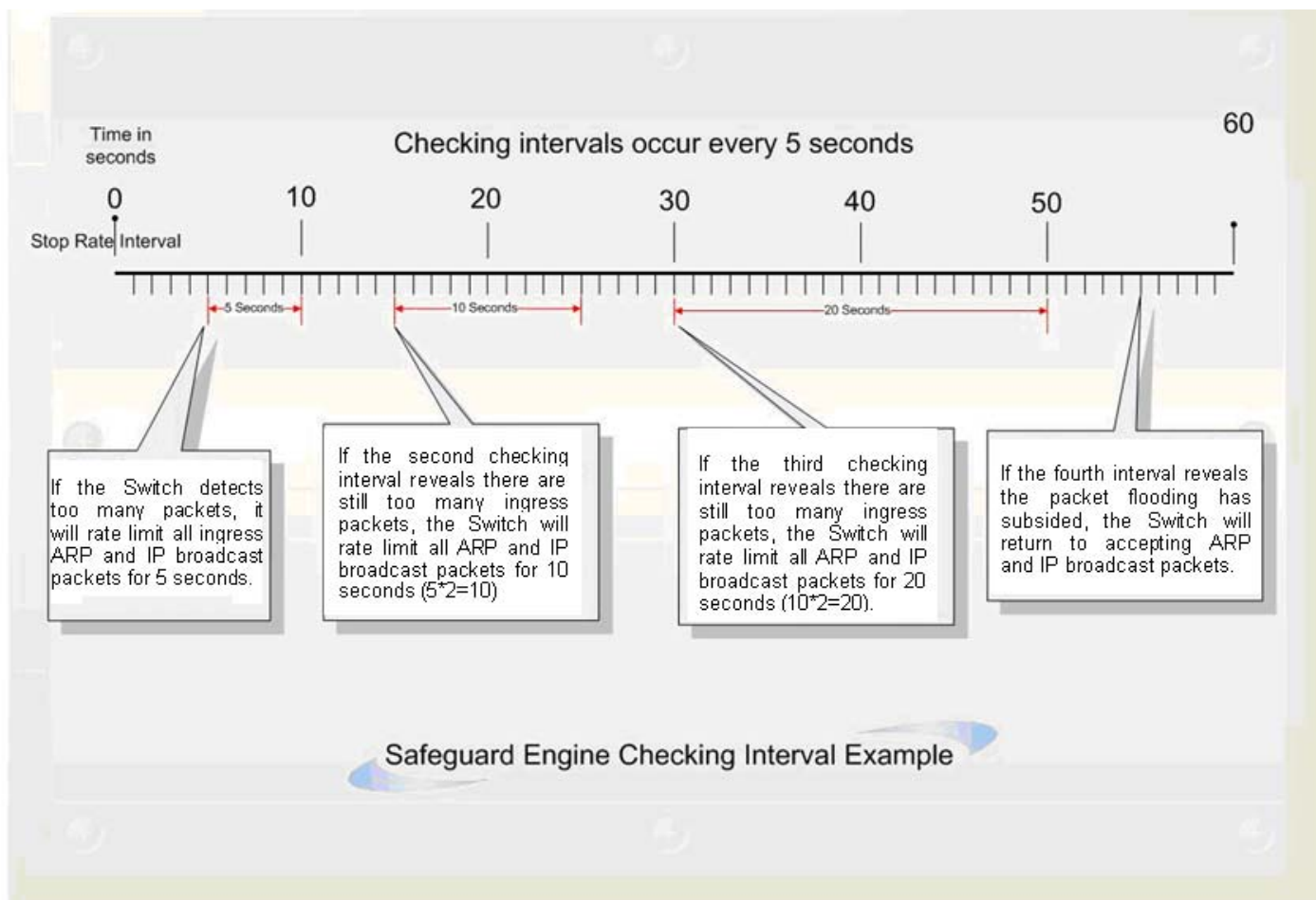


Figure 5 - 1 Mapping QoS on the Switch

For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will accept a few ingress ARP and IP broadcast packets. In the example above, the Switch doubled the time for dropping ARP and IP broadcast packets when consecutive flooding issues were detected at 5-second intervals. (First stop = 5 seconds, second stop = 10 seconds, third stop = 20 seconds) Once the flooding is no longer detected, the wait period for limiting ARP and IP broadcast packets will return to 5 seconds and the process will resume.

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

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

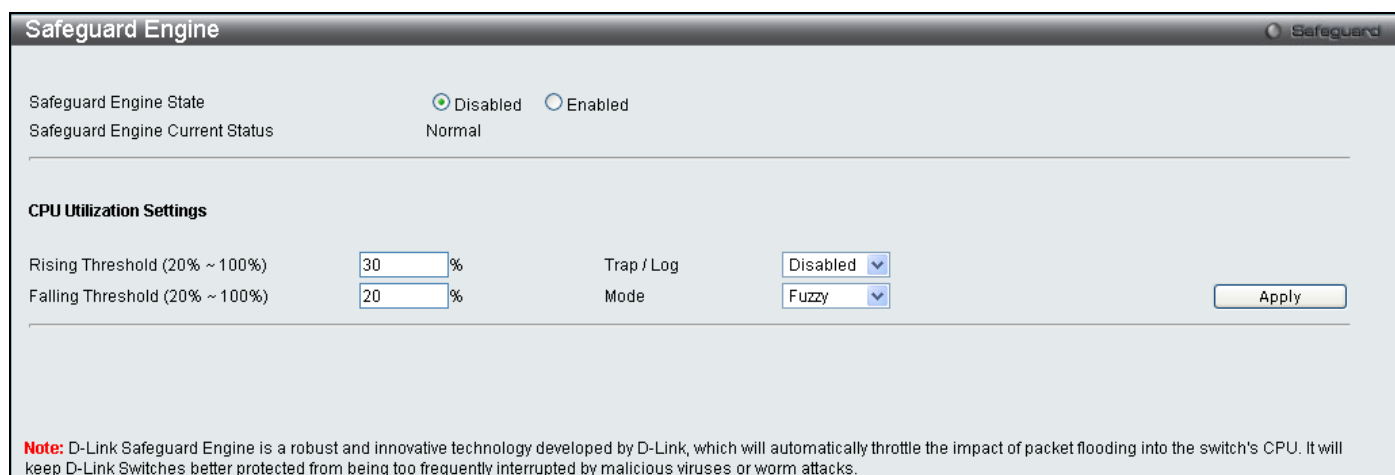


Figure 5 - 2 Safeguard Engine window

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:

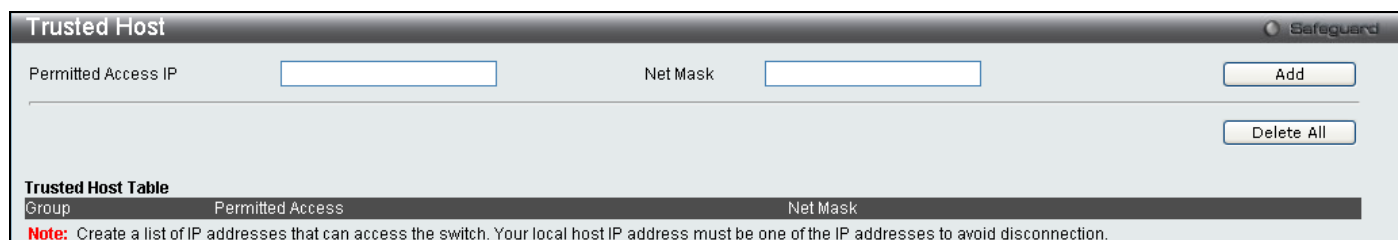
Parameter	Description
<b>Rising Threshold</b>	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into the Exhausted state.
<b>Falling Threshold</b>	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Exhausted state and returns to normal mode.
<b>Trap/log</b>	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.
<b>Mode</b>	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 you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address with a proper subnet mask and click the **Add** button.

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



**Figure 5 - 3 Trusted Host window**

To delete an entry click the corresponding **Delete** 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 binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database, or when DHCP snooping is enabled, the switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. For the DGS-3700 Series, active and inactive entries use the same database. The maximum entry number is 511. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

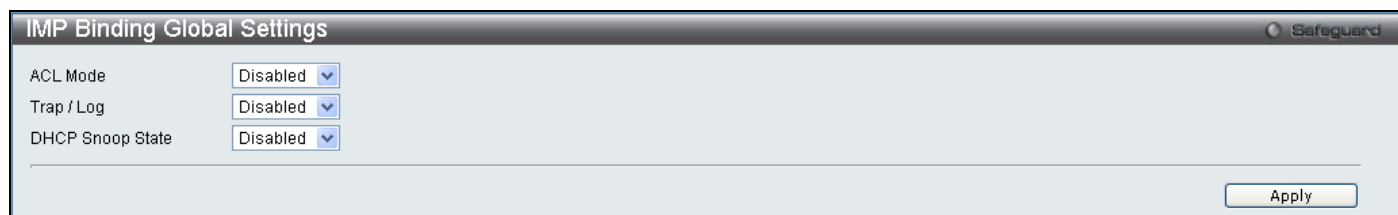
The IP-MAC-Port Binding folder contains five windows: IMP Binding Global Settings, IMP Binding Port Settings, IMP Binding Entry Settings, DHCP Snooping Entries, and MAC Block List.

### IMP Binding Global Settings

This window is used to enable or disable the ACL mode, Trap Log State and DHCP Snoop state on the switch. When the user enables the ACL Mode for IP-MAC Binding it will create two Access Profile Entries on the Switch. The Trap/Log field will enable and disable the sending of trap log messages for IP-MAC 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 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:

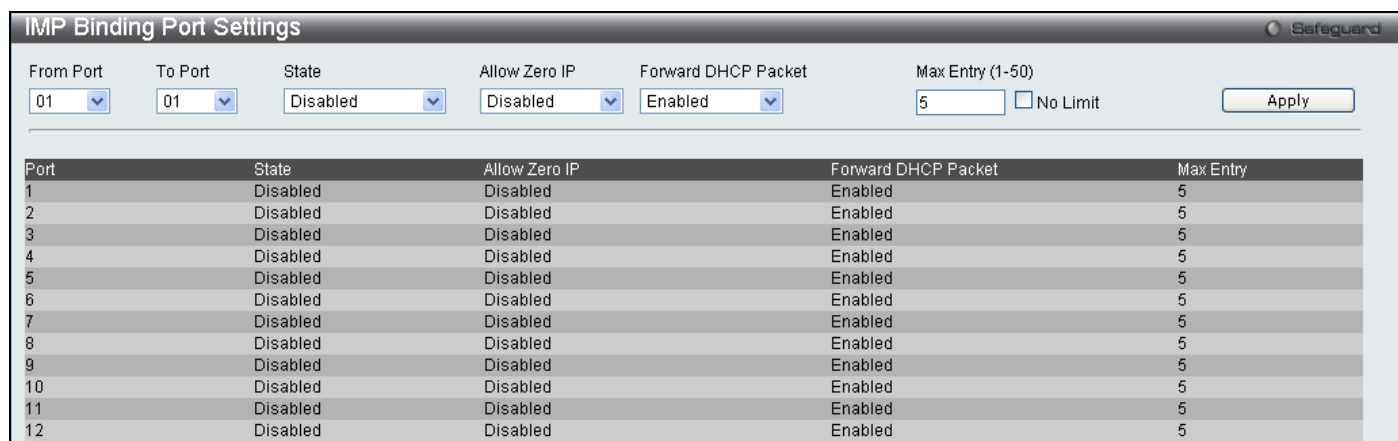
Parameter	Description
<b>ACL Mode</b>	This field will enable and disable the ACL mode for IP-MAC binding on the Switch, without altering previously set configurations. When enabled, the Switch will automatically create two ACL packet content mask entries which will aid the user in processing certain IP-MAC binding entries created. The ACL entries created when this command is <i>Enabled</i> can only be automatically installed if the Access Profile table has two entries available of the possible six entries allowed.
<b>Trap / Log</b>	This field will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, 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 binding configuration set on the Switch.
<b>DHCP Snoop State</b>	Use the pull-down menu to enable or disable the DHCP Snoop State for IP-MAC Binding.

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 and Forward DHCP packet field, and configure the port's Max entry.

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



**Figure 5 - 5 IMP Binding Port Settings window**

The following fields can be set or modified:

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

<b>From Port / To Port</b>	Select a port or range of ports to set for IP-MAC Binding.
<b>State</b>	<p>Use the pull-down menu to Enable or Disable these ports for IP-MAC Binding.</p> <p><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 state. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is strict if not specified. The ports with strict mode will capture unicast DHCP packets through the ACL module. If configuring IP-MAC binding port enable in strict mode when IP-MAC binding DHCP_snoop is enabled, it will create an ACL profile and the rules according to the ports. If there is not enough profile or rule space for ACL profile or rule table, it will return a warning message and will not create ACL profile and rules to capture unicast DHCP packets.</p> <p><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 state. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.</p>
<b>Allow Zero IP</b>	Use the pull-down menu to enable or disable this feature. Allow zero IP configures the state which allows ARP packets with 0.0.0.0 source IP to bypass.
<b>Forward DHCP Packet</b>	By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP snooping is enabled, under the case that DHCP packet which has been trapped by the CPU needs to be forwarded by the software. This setting controls the forwarding behavior in this situation.
<b>Max Entry (1-50)</b>	Specifies the maximum number of IP-MAC-Port Binding entries. By default, per port max entry is 5.

Click **Apply** to implement changes.



## IMP Binding Entry Settings

This table is used to create Static IP MAC Binding Port entries on the switch.

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

**Figure 5 - 6 IMP Binding Entry Settings window**

The following fields can be set or modified:

Parameter	Description
<b>IP Address</b>	Enter the IP address to bind to the MAC address set below.
<b>MAC Address</b>	Enter the MAC address to bind to the IP Address set above.
<b>Ports</b>	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click the All Ports check box to configure this entry for all ports on the Switch.
<b>Mode</b>	<p>The user may set the IP-MAC Binding Mode here by using the pull-down menu. The choices are:</p> <p><i>ARP</i> – Choosing this selection will set a normal IP-Mac Binding entry for the IP address and MAC address entered. If the system is in ARP mode, the arp mode entries and acl mode entries will be effective. If the system is in the acl mode, only the acl mode entries will be active.</p> <p><i>ACL</i> – Choosing this entry will allow only packets from the source IP-MAC binding entry created here. All other packets with a different IP address will be discarded by the Switch. This mode can only be used if the ACL Mode has been enabled in the IMP Global Settings window as seen previously.</p>

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 All** to remove an entry.

## DHCP Snooping Entries

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

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

Figure 5 - 7 DHCP Snooping Entries window

## MAC Block List

This table 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 delete all the entries in the **Blocked Address Browser** window, click **Clear All**.

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

Figure 5 - 8 MAC Block List window

## Port Security

### Port Security Port Settings

A given ports' (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port lock is enabled. Setting the **Admin State** pull-down menu to *Enabled*, and clicking **Apply** can lock the port.

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

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

Figure 5 - 9 Port Security Port Settings window

The following parameters can be set:

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

Click **Apply** to implement changes made.

## Port Security VLAN Settings

This table is used to set the maximum port-security entries that can be learned on a specific VLAN.

To view this window, click **Security > Port Security > Port Security FDB Entries** as shown below:

Figure 5 - 10 Port Security VLAN Settings window

The following parameters can be set:

Parameter	Description
<b>VLAN Name</b>	Specifies a VLAN or list of VLANs by VLAN Name.
<b>VLAN ID (e.g.:1,4-6)</b>	Specifies a VLAN or list of VLANs by VLAN ID.
<b>Max Learning Address</b>	Specifies the maximum number of port-security entries that can be learned by this VLAN. If this parameter is set to 0, no user can get authorization on this VLAN. If the setting is smaller than the number of current learned entries on the VLAN, the command will be rejected. The default value is <i>No Limit</i> .

Click **Apply** to implement changes.

## Port Security Entries

This window is used to configure port security entries by MAC address, port number and VLAN ID.

To view this window, click **Security > Port Security > Port Security Entries** as shown below:

**Figure 5 - 11 Port Security Entries window**

The following parameters can be set:

Parameter	Description
<b>VLAN Name</b>	Specifies a VLAN or list of VLANs by VLAN Name.
<b>VLAN ID (e.g.:1,4-6)</b>	Specifies a VLAN or list of VLANs by VLAN ID.
<b>Port List</b>	Specifies a port or list of ports to be configured.

Click **Apply** to implement changes.

## 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 first time the DHCP filter is enabled it will create both an access profile entry and an access rule per port entry, it will also create other access rules. These rules are used to block all DHCP server packets. In addition to a permit DHCP entry it will also create one access profile and one access rule entry the first time the DHCP client MAC address is used as the client MAC address. The Source IP address is the same as the DHCP server's IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fileds, which the user has configured.

When DHCP Server filter function is enabled all DHCP Server packets will be filtered from a specific port.

The DHCP Server Screening folder contains two windows: DHCP Screening Port Settings and DHCP Offer Filtering.

## DHCP Screening Port Settings

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers.

When the DHCP server filter function is enabled, all DHCP server packets will be filtered from a specific port.

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

From Port	To Port	State
01	01	Disabled

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

Figure 5 - 12 DHCP Screening Port Settings window

The following parameters can be set:

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

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 Server Screening.

## DHCP Offer Filtering

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. The first time the DHCP filter is enabled it will create both an access profile entry and an access rule per port entry, it will also create other access rules. These rules are used to block all DHCP server packets. In addition to a permit DHCP entry, it will also create one access profile and one access rule entry the first time the DHCP client MAC address is used as the client MAC address. The Source IP address is the same as the DHCP server's IP address (UDP source port number 67). These rules are used to permit the DHCP server packets with specific fields, which the user has configured.

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

Figure 5 - 13 DHCP Offer Filtering window

The user may set the following parameters:

Parameter	Description
<b>Server IP Address</b>	The IP address of the DHCP server.

<b>Client's MAC Address</b>	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.
<b>Ports</b>	Choose the range of ports that you want to use as the DHCP server, or check the <i>All Ports</i> box if you wish to use all the ports on the switch.

Click **Apply** to implement changes.

## 802.1X

### 802.1X Port-Based and Host-Based Access Control

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

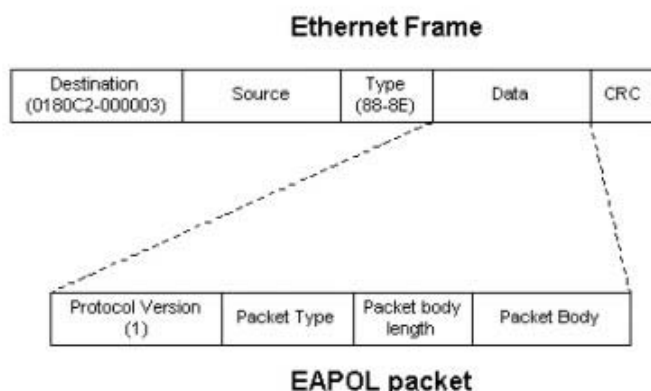


Figure 5 - 14 The EAPOL Packet

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 upkeeping a stable and working Access Control security method.

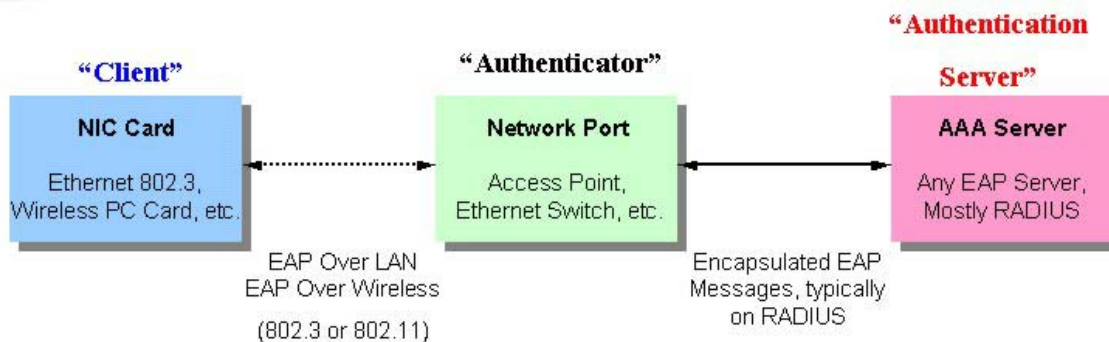


Figure 5 - 15 The three roles of 802.1X

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.

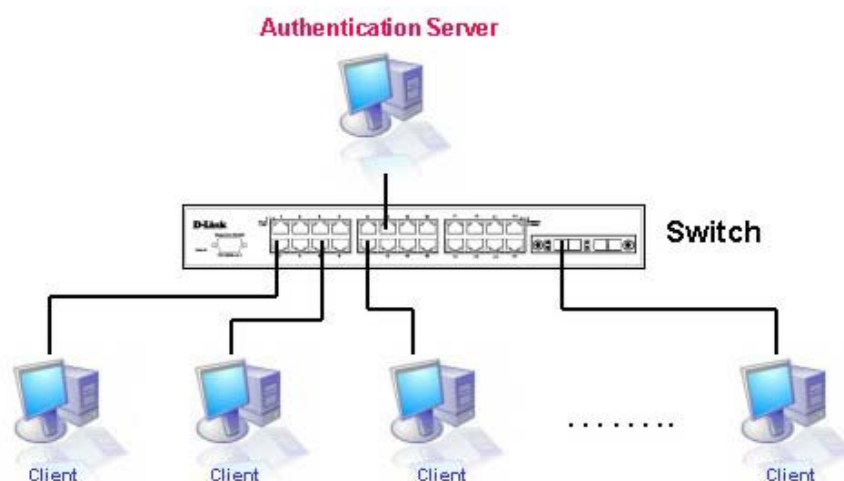


Figure 5 - 16 The Authentication Server

## 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 Global settings**)
2. The 802.1X settings must be implemented by port (**Security / 802.1X / 802.1X Port Settings**)
3. A RADIUS server must be configured on the Switch. (**Security / 802.1X / Authentication RADIUS Server**)

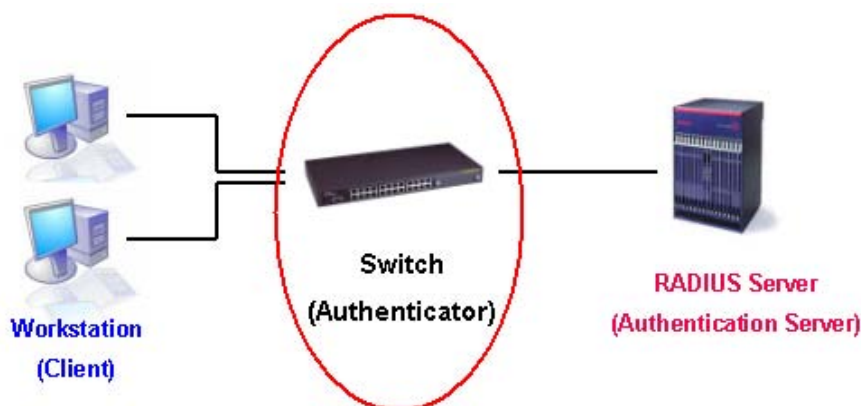


Figure 5 - 17 The Authenticator



## Client

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

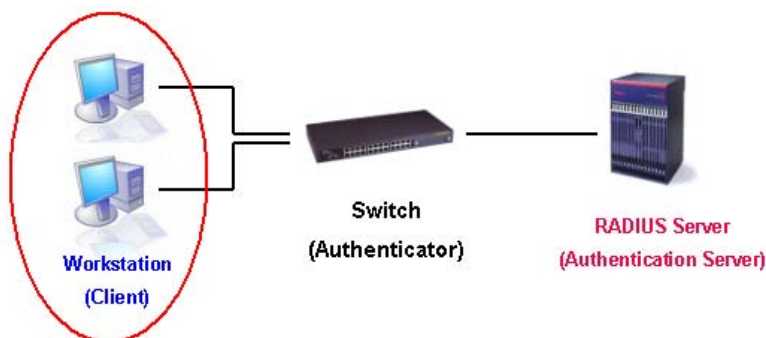


Figure 5 - 18 The Client

## 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 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

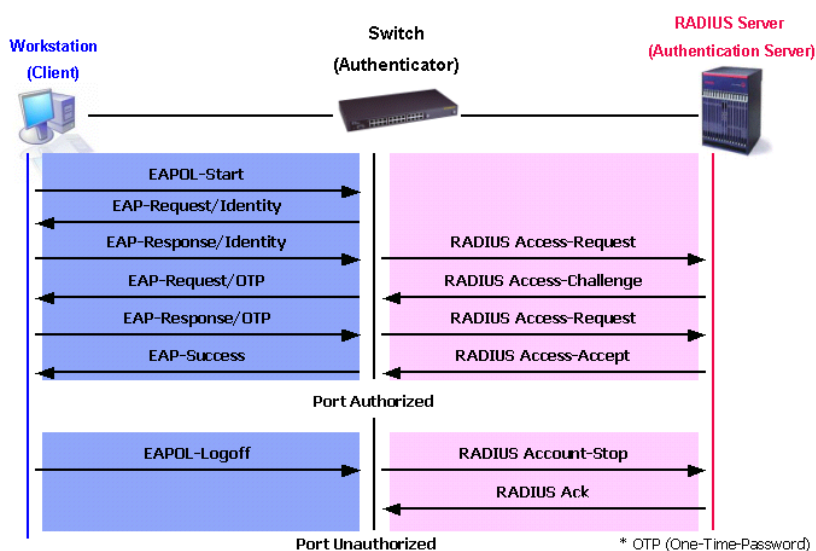


Figure 5 - 19 The 802.1X Authentication Process

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

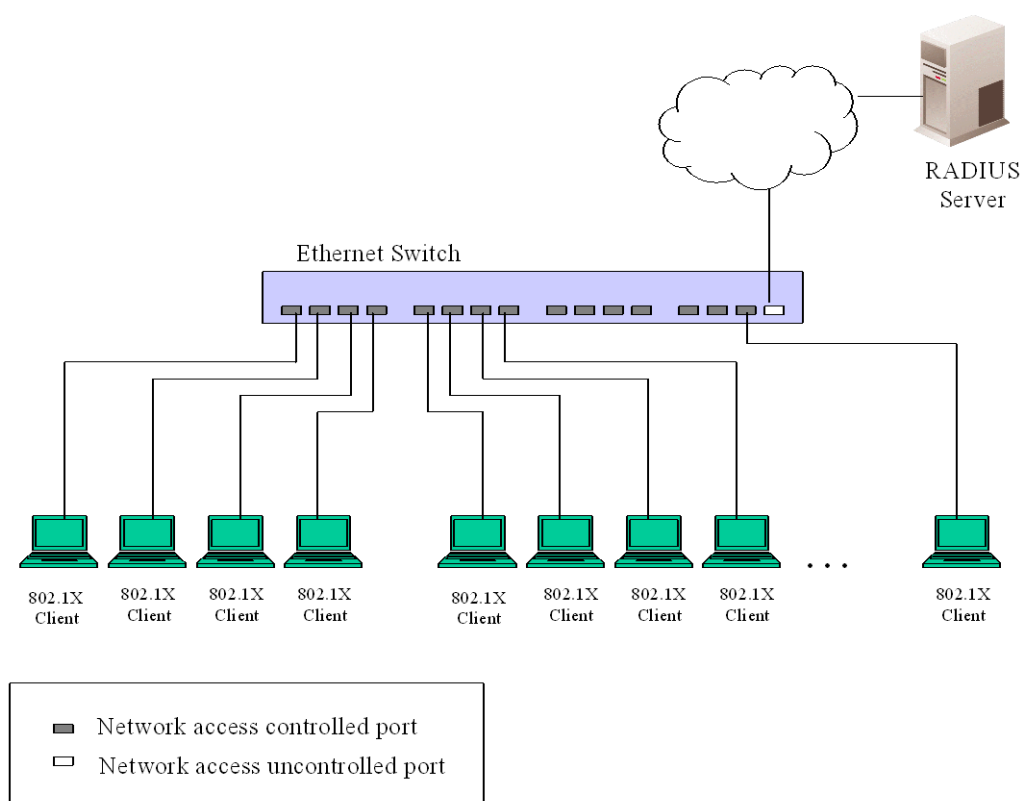
1. Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. Host-Based Access Control – Using this method, the Switch will automatically learn up to sixteen MAC addresses 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.

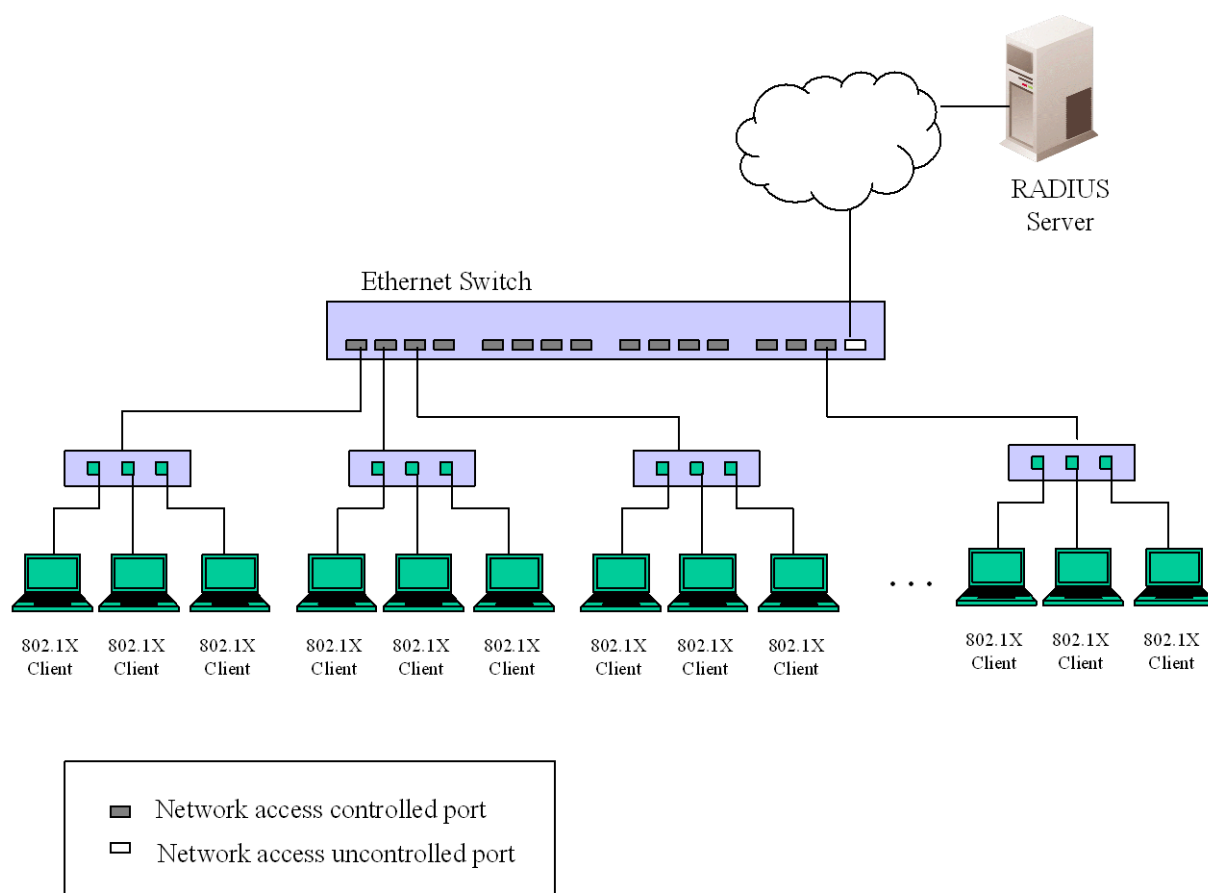
### Port-Based Network Access Control



**Figure 5 - 20 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 - 21 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 Global Settings

This window is used to configure the 802.1X Global Settings on the Switch.

To view this window, click **Security > 802.1X > 802.1X Global Settings** as shown below:

**Figure 5 - 22 802.1X Global Settings window**

This window allows you to set the following features:

Parameter	Description
<b>Authentication Mode</b>	The Authentication Mode allows the user to choose among, <i>Disabled</i> , <i>Port Based</i> or <i>MAC Based</i> Authentication Mode. When choosing <i>MAC Based</i> , Host-based Network Access Control will be enabled on the port.
<b>Authentication Protocol</b>	Choose the Authentication Protocol either <i>RADIUS EAP</i> or <i>Local</i> .
<b>Forward EAPOL PDU</b>	This enables or disables the Switch retransmit EAPOL PDU Request.
<b>Max User (1-1536)</b>	Specify the maximum number of users that can be learned via 802.1X authentication.

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

## 802.1X Port Settings

This window is used to configure the 802.1X Port Settings.

To view this window, click **Security > 802.1X > 802.1X Port Settings** as shown below:

Port	AdmDir	OpenCrDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth	Capability	Forward EAPOL PDU On Port	Max Users On Port
1	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
2	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
3	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
4	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
5	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
6	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
7	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
8	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
9	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
10	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
11	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128
12	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	128

**Figure 5 - 23 802.1X Port Settings window**

This window allows you to set the following features:

Parameter	Description
<b>From Port / To Port</b>	Enter the port or ports to be set.
<b>QuietPeriod (0-65535)</b>	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.
<b>SuppTimeout (1-65535)</b>	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
<b>ServerTimeout (1-65535)</b>	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is 30 seconds.
<b>MaxReq (1-10)</b>	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.
<b>TxPeriod (1-65535)</b>	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is 30 seconds.
<b>ReAuthPeriod (1-65535)</b>	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.
<b>ReAuthentication</b>	Determines whether regular reauthentication will take place on this port. The default setting is <i>Disabled</i> .
<b>PortControl</b>	<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>
<b>Capability</b>	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.
<b>Direction</b>	<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>
<b>Forward EAPOL PDU On Port</b>	This enables or disables the Switch retransmit EAPOL PDU Request on a per port basis.
<b>Max User On Port (1-128)</b>	Specify the maximum number of users that can be learned via 802.1X authentication.

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 view this window, click **Security > 802.1X > 802.1X User** as shown below:

Figure 5 - 24 802.1X 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 view this window, click **Security > 802.1X > Authentication RADIUS Server** as shown below:

Figure 5 - 25 Authentication RADIUS Server window

This window displays the following information:

Parameter	Description
<b>Index</b>	Choose the desired RADIUS server to configure: 1, 2 or 3.
<b>IPv4 Address / IPv6 Address</b>	Select either IPv4 Address or IPv6 Address to set the RADIUS Server IP.
<b>Authentication Port (1-65535)</b>	Set the RADIUS authentication server(s) UDP port. The default port is 1812.
<b>Accounting Port (1-65535)</b>	Set the RADIUS account server(s) UDP port. The default port is 1813.
<b>Timeout (1-255)</b>	Enter the timeout value in seconds (1 to 255) the default value is 5.
<b>Retransmit (1-255)</b>	Set the retransmit value in seconds (1 to 255) the default value is 2.
<b>Key (Max:32 characters)</b>	Set the key the same as that of the RADIUS server. Maximum length of the entry is 32 bytes.

<b>Confirm Key</b>	Re-enter the previously entered <b>Key</b> .
--------------------	--

Click **Apply** to implement changes.

## Initialize Port(s)

This window allows you to initialize ports for the 802.1X Settings. This window will appear in the folder when the “enable 802.1x” command is entered into the command line interface or when the authentication mode is changed to **Port Based** or **MAC Based** in the 802.1X Global Settings window.

To view this window, click **Security > 802.1X > Initialize Port(s)** as shown below:

Port	Auth PAE State	Backend_State	Port Status
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized

**Figure 5 - 26 Initialize Port(s) window**

To initialize port(s), use the drop down menu to select the port(s) and click **Apply**.

## Reauthenticate Port(s)

This window allows you to reauthenticate ports for the 802.1X Settings. This window will appear in the folder when the “enable 802.1x” command is entered into the command line interface or when the authentication mode is changed to **Port Based** or **MAC Based** in the 802.1X Global Settings window.

To view this window, click **Security > 802.1X > Reauthenticate Port(s)** as shown below:

Port	Auth PAE State	Backend_State	Port Status
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized

**Figure 5 - 27 Reauthenticate Port(s) window**

To reauthenticate port(s), use the drop down menu to select the port(s) and click **Apply**.

## 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.

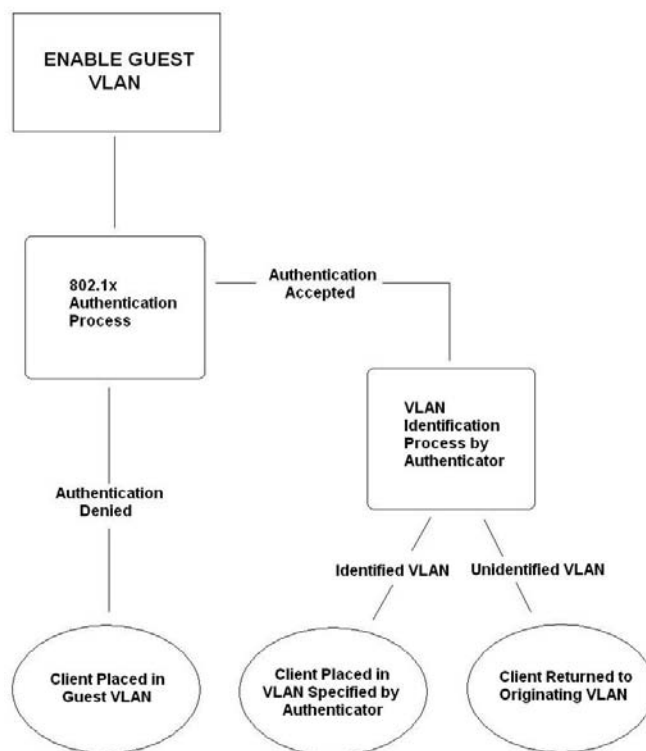


Figure 5 - 28 Guest VLAN Authentication Process

### Limitations Using the Guest VLAN

1. Guest VLANs are only supported for port-based VLANs. MAC-based VLANs cannot undergo this procedure.
2. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
3. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
4. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.

## Guest VLAN

This window is used to configure the Guest VLAN on the Switch.

To view this window, click **Security > 802.1X > Guest VLAN** as shown below:

**Figure 5 - 29 Guest VLAN window**

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

Parameter	Description
<b>VLAN Name</b>	Enter the pre-configured VLAN name to create as an 802.1X Guest VLAN.
<b>Port List</b>	Set the port list of ports to be enabled for the 802.1X Guest VLAN.

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.

## 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:

1. **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.
2. **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.
3. **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** as shown below:

**Figure 5 - 30 SSL Settings**

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

Parameter	Description
<b>SSL Settings</b>	
<b>SSL Status</b>	<i>Enable or Disable</i> the SSL status on the switch. The default is disabled.
<b>Cache Timeout (60-86400)</b>	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.

<b>SSL Ciphersuite Settings</b>	
<b>RSA with RC4_128_MD5</b>	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.
<b>RSA with 3DES EDE CBC SHA</b>	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.
<b>DHE DSS with 3DES EDE CBC SHA</b>	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.
<b>RSA EXPORT with RC4 40 MD5</b>	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.
<b>SSL Certificate Download</b>	
<b>Server IP Address</b>	Enter the IP address of the TFTP server where the certificate files are located.
<b>Certificate File Name</b>	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
<b>Key File Name</b>	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 Lists** 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** as shown below:

Figure 5 - 31 SSH Settings window

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

Parameter	Description
<b>SSH Server State</b>	Enable or disable SSH on the Switch. The default is <i>Disabled</i> .
<b>Max Session (1-8)</b>	Enter a value between 1 and 8 to set the number of users that may simultaneously access the Switch. The default setting is 8.
<b>Connection Timeout (120-600)</b>	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.
<b>Authfail Attempts (2-20)</b>	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.
<b>Rekey Timeout</b>	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 *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.

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** as shown below:

The screenshot shows the following settings:

- SSH Authentication Mode Settings:** Password, Public Key, Host Based (all checked).
- Encryption Algorithm:** 3DES-CBC, AES128-CBC, AES192-CBC, AES256-CBC, Cast128-CBC, ARC4, Blow-fish-CBC, Twofish128, Twofish192, Twofish256 (all checked).
- Data Integrity Algorithm:** HMAC-MD5, HMAC-SHA1 (both checked).
- Public Key Algorithm:** HMAC-RSA, HMAC-DSA (both checked).

**Figure 5 - 32 SSH Authmode and Algorithm Settings window**

The following algorithms may be set:

Parameter	Description
<b>SSH Authentication Mode Settings</b>	
<b>Password</b>	This parameter may be enabled if the administrator wishes to use a locally configured password for authentication on the Switch. The default is enabled.
<b>Public Key</b>	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.
<b>Host-based</b>	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.
<b>Encryption Algorithm</b>	
<b>3DES-CBC</b>	Check the box to enable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
<b>Blow-fish CBC</b>	Check the box to enable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
<b>AES128-CBC</b>	Check the box to enable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
<b>AES192-CBC</b>	Check the box to enable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
<b>AES256-CBC</b>	Check the box to enable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
<b>ARC4</b>	Check the box to enable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.

<b>Cast128-CBC</b>	Check the box to enable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
<b>Twofish128</b>	Check the box to enable the twofish128 encryption algorithm. The default is enabled.
<b>Twofish192</b>	Check the box to enable the twofish192 encryption algorithm. The default is enabled.
<b>Twofish256</b>	Check the box to enable the twofish256 encryption algorithm. The default is enabled.
<b>Data Integrity Algorithm</b>	
<b>HMAC-SHA1</b>	Check the box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.
<b>HMAC-MD5</b>	Check the box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.
<b>Public Key Algorithm</b>	
<b>HMAC-RSA</b>	Check the box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
<b>HMAC-DSA</b>	Check the 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

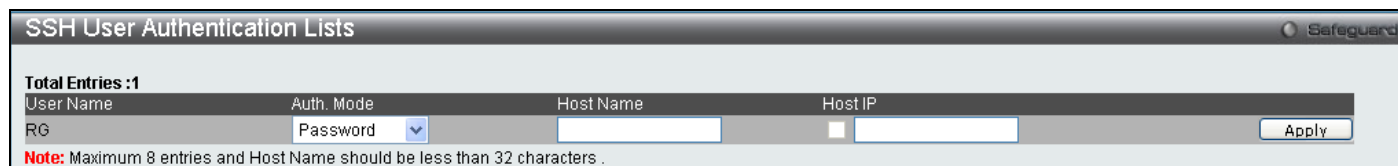
The following windows are used to configure parameters for users attempting to access the Switch through SSH.

To view this window, click **Security > SSH > SSH User Authentication Lists** as shown below:



**Figure 5 - 33 SSH User Authentication Lists window**

In the example above, the User Account “RG” has been previously set using the User Accounts window in the **Configuratrion** 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 - 34 SSH User Authentication Lists - Edit window**

The user may set the following parameters:

Parameter	Description
<b>User Name</b>	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.
<b>Auth. Mode</b>	The administrator may choose one of the following to set the authorization for users attempting to access the Switch.  <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><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 publickey on a SSH server for authentication.</p>
<b>Host Name</b>	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.
<b>Host IP</b>	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 cannot use the “enable admin” command to promote to the admin privilege level.



**NOTE:** TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)



## Authentication Policy Settings

This command will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

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

**Figure 5 - 35 Authentication Policy Settings window**

The following parameters can be set:

Parameters	Description
<b>Authentication Policy</b>	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
<b>Response Timeout (0-255)</b>	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.
<b>User Attempts (1-255)</b>	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 3.

Click **Apply** to implement changes made.

## Application Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list.

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

**Figure 5 - 36 Application's Authentication Settings window**

The following parameters can be set:

Parameter	Description
<b>Application</b>	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.
<b>Login Method List</b>	Using the pull-down menu, configure an application for normal login on the user level, utilizing



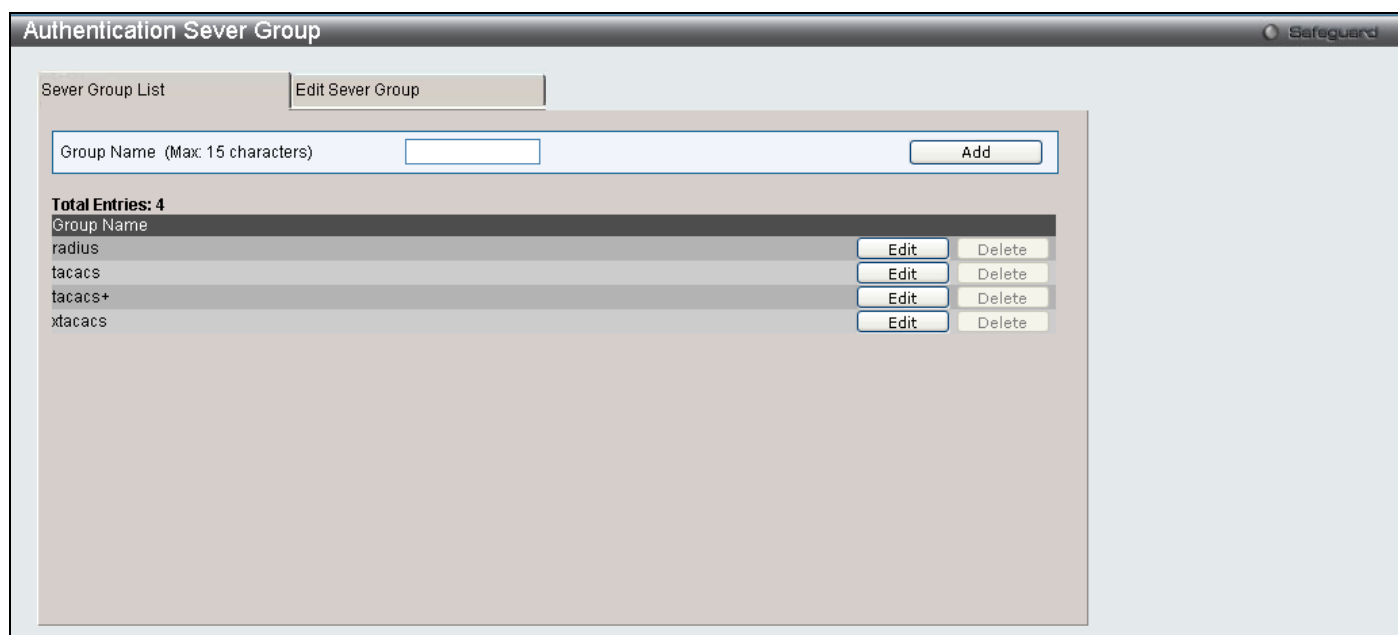
	a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the <b>Login Method Lists</b> window, in this section, for more information.
<b>Enable Method List</b>	Using the pull-down menu, configure an application for normal login on 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 <b>Enable Method Lists</b> window, in this section, for more information

Click **Apply** to implement changes made.

## Authentication Server Group

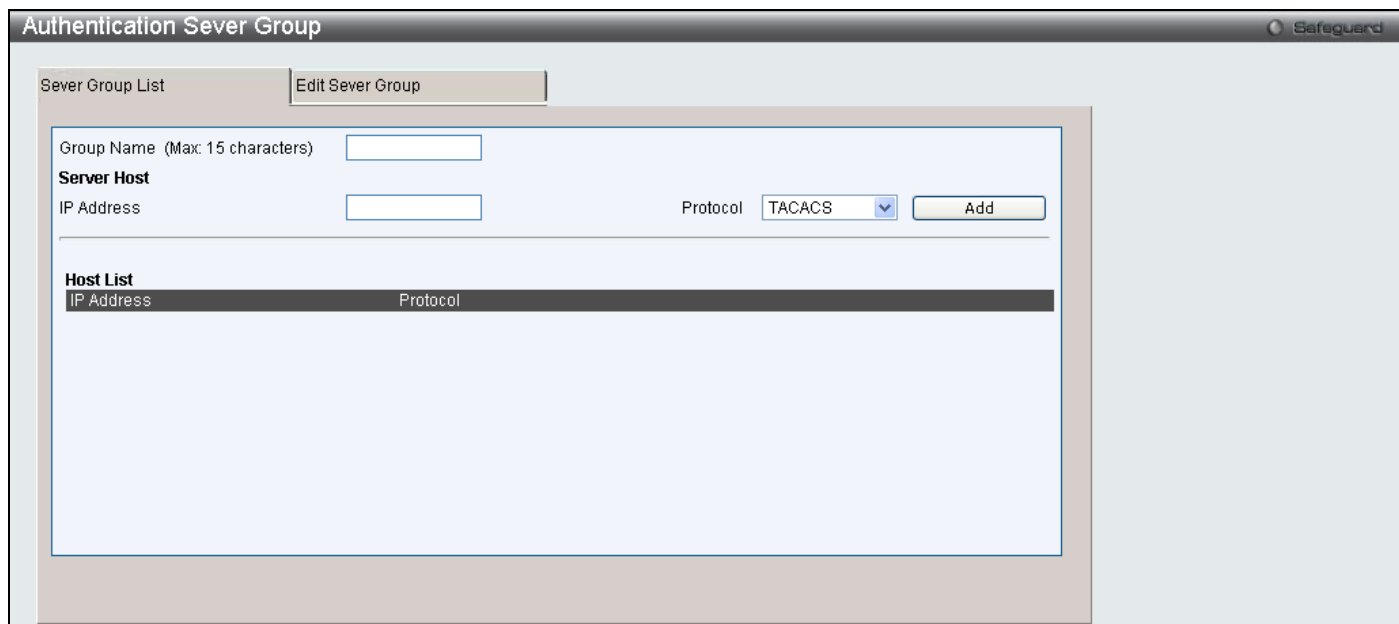
This window will allow users to set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view this window, click **Security > Access Authentication Control > Authentication Server Group** as shown below:



**Figure 5 - 37 Authentication Server Group Settings window**

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



**Figure 5 - 38 Authentication Server Group Settings Edit window**

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



**NOTE:** The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

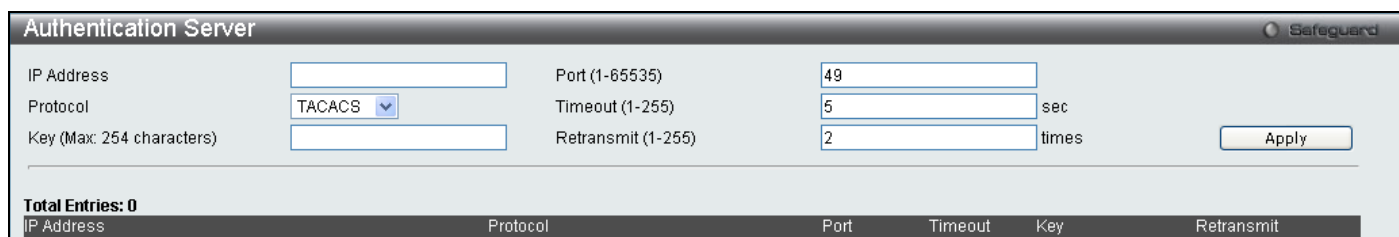


**NOTE:** The four built in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

## Authentication Server

This window will set user-defined Authentication Server Hosts for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

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



**Figure 5 - 39 Authentication Server Settings window**

Configure the following parameters to add an Authentication Server Host:

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

<b>IP Address</b>	The IP address of the remote server host the user wishes to add.
<b>Port (1-65535)</b>	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.
<b>Protocol</b>	The protocol used by the server host. The user may choose one of the following: <i>TACACS</i> – Enter this parameter if the server host utilizes the TACACS protocol. <i>XTACACS</i> – Enter this parameter if the server host utilizes the XTACACS protocol. <i>TACACS+</i> – Enter this parameter if the server host utilizes the TACACS+ protocol. <i>RADIUS</i> – Enter this parameter if the server host utilizes the RADIUS protocol.
<b>Timeout (1-255)</b>	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.
<b>Key</b>	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
<b>Retransmit (1-255)</b>	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.

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



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

## Login Method Lists

This command will configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS – XTACACS - local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

When the user 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, 3 kinds of privilege levels can be assigned to the user and the user cannot use the **Enable Admin** window to promote to admin privilege level.

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

Method List Name (Max: 15 characters)

Priority 1:  Priority 2:

Priority 3:  Priority 4:

---

**Total Entries: 1**

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4
default	local	----	----	----

**Figure 5 - 40 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
<b>Method List Name</b>	Enter a method list name defined by the user of up to 15 characters.
<b>Priority 1, 2, 3, 4</b>	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p> <p><i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.</p> <p><i>radius</i> – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><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.</p> <p><i>local</i> – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.</p> <p><i>none</i> – Adding this parameter will require no authentication to access the Switch.</p>

## Enable Method Lists

The **Enable Method List Settings** window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.



**NOTE:** To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following table, click **Security > Access Authentication Control > Enable Method Lists** as shown below:

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4	Edit	Delete
default	local	-----	-----	-----		

**Figure 5 - 41 Enable Method List window**

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

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

Parameter	Description
<b>Method List Name</b>	Enter a method list name defined by the user of up to 15 characters.
<b>Priority 1, 2, 3, 4</b>	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><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.</p> <p><i>none</i> – Adding this parameter will require no authentication to access the Switch.</p> <p><i>radius</i> – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p> <p><i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><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.</p>

## Local Enable Password Settings

This window will configure the locally enabled password for the Enable Admin command. When a user chooses the "local\_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view this window, click **Security > Access Authentication Control > Local Enable Password Settings** as shown below:

**Figure 5 - 42 Local Enable Password window**

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

Parameter	Description
<b>Old Local Enable Password</b>	If a password was previously configured for this entry, enter it here in order to change it to a new password
<b>New Local Enable Password</b>	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.
<b>Confirm Local Enable Password</b>	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

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

## RADIUS Accounting Settings

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

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

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

**Network** – When enabled, the Switch will send informational packets to a remote RADIUS server when network events occur on the Switch.

**Shell** – When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet, or SSH.

**System** - When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot.

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

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

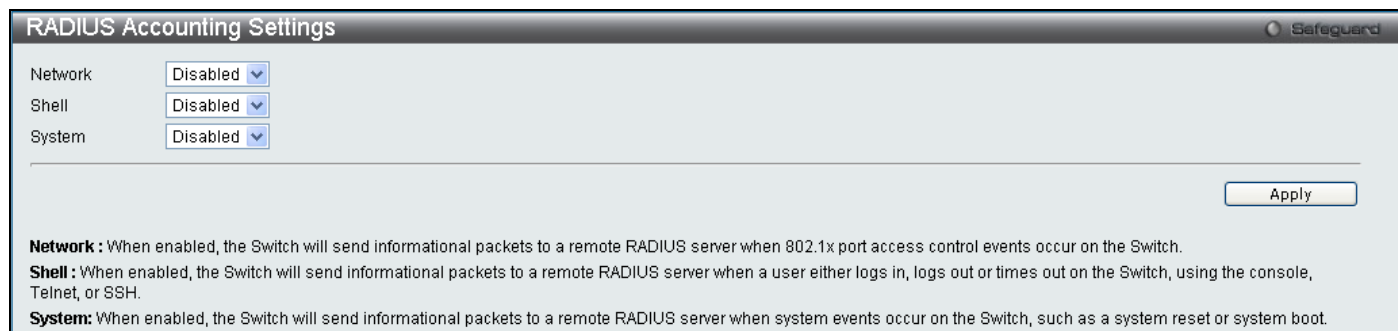


Figure 5 - 43 RADIUS Accounting Settings window

## 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. A port accepts a maximum of sixteen authenticated MAC addresses per physical port of a VLAN that is not a Guest VLAN. Other MAC addresses attempting authentication on a port with the maximum number of authenticated MAC addresses will be blocked.
4. Ports that have been enabled for Link Aggregation, stacking, 802.1X authentication, 802.1X Guest VLAN, Port Security, GVRP or Web-based authentication cannot be enabled for the 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. MAC-based Access Control Global Settings

To view this window, click **Security > MAC-based Access Control > MAC-based Access Control Settings** as shown below:

Figure 5 - 44 MAC-based Access Control Settings window

The following parameters may be viewed or set:

Parameter	Description
<b>Settings</b>	
<b>MBA Global State</b>	Click the radio buttons to globally enable or disable the MAC-based Access Control function on the Switch.
<b>Method</b>	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.
<b>Password</b>	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
<b>Guest VLAN Name / Guest VLAN ID</b>	Click the radio button to configure the Guest VLAN Name or Guest VLAN ID. Enter the name of the previously configured Guest VLAN being used for this function.
<b>Guest VLAN Member Ports</b>	Enter the list of ports that have been configured for the Guest VLAN.
<b>Port Settings</b>	
<b>From Port / To Port</b>	Enter the Port range.
<b>State</b>	Use the pull-down menu to enable or disable the MAC-based Access Control function on individual ports.
<b>Mode</b>	Select <i>Host Based</i> or <i>Mac Based</i> mode.
<b>Aging Time (1-1440)</b>	The time period during which an authenticated host will be kept in an authenticated state. When the aging time is timed out, the host will be moved back to an



	unauthenticated state. The range is between 1 and 1440 minutes. The default is 1440.
<b>Hold Time (1-300)</b>	If a host fails to pass authentication, the next authentication will not started within hold time unless the user clears the entry state manually. The default is 300.

Click **Apply** to implement changes.

## 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 view this window, click **Security > MAC-based Access Control > MAC-based Access Control Local Settings** as shown below:

**Figure 5 - 45 MAC-based Access Control Local MAC Settings**

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 **Apply**. To change a MAC address or a VLAN in the list, click the corresponding **Edit** 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**.

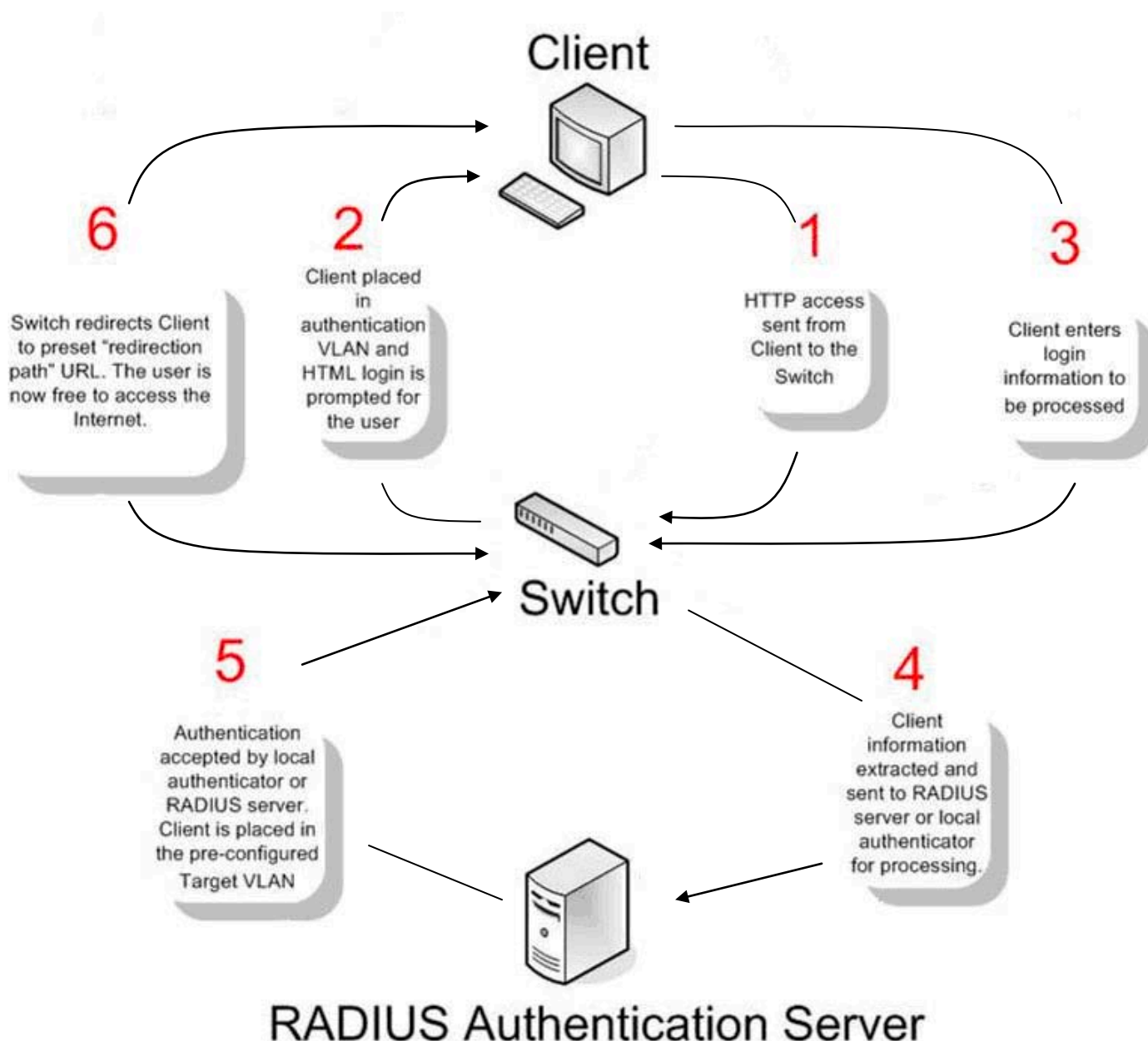
## Web Authentication

Web authentication, also known as Web-based Access Control, is another port based access control method implemented similarly to the 802.1X port based access control method previously stated. This function will allow user authentication through a RADIUS server or through the local authentication set on the Switch when a user is trying to access the network via the switch, if the port connected to the user is enabled for this feature.

The user attempting to gain web access will be prompted for a username and password before being allowed to accept HTTP packets from the Switch. When a client attempts to access a website, that port is placed in the authentication VLAN set by the user. All clients in this authentication VLAN will be queried for authentication by the local method or through a RADIUS server. Once accepted, the user will be placed in a target VLAN on the Switch where it will have rights and privileges to openly access the Internet. If denied access, no packets will pass through to the user and thus, that user will be returned to the authentication VLAN from where it came and the authentication procedure will have to be reattempted by the user.

Once a client has been authenticated on a particular port, that port will be placed in the pre-configured VLAN and any other clients on that port will be automatically authenticated to access the specified Redirection Path URL, as well as the authenticated client.

Here is an example of the basic six step process all parties of the authentication go through for a successful Web-based Access Control process.



## Conditions and Limitations

1. The subnet of the authentication VLAN's IP interface must be the same as that of the client. If not configured properly, the authentication will be permanently denied by the authenticator.
2. If the client is utilizing DHCP to attain an IP address, the authentication VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.
3. The authentication VLAN of this function must be configured to access a DNS server to improve CPU performance, and allow the processing of DNS, UDP and HTTP packets.
4. Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
5. The Redirection Path must be set before the Web-based Access Control can be enabled. If not, the user will be prompted with an error message and the Web-based Access Control will not be enabled.
6. If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling the Web-based Access Control on the Switch.

## Web-based Access Control Settings

This window is used to configure the Switch for Web-based Access Control Settings on the Switch.

To view this window, click **Security > Web Authentication > Web-based Access Control Settings** as shown below:

Port	State	User Name	Auth State	Assigned Vlan
1	Disabled	N/A	N/A	N/A
2	Disabled	N/A	N/A	N/A
3	Disabled	N/A	N/A	N/A
4	Disabled	N/A	N/A	N/A
5	Disabled	N/A	N/A	N/A
6	Disabled	N/A	N/A	N/A
7	Disabled	N/A	N/A	N/A
8	Disabled	N/A	N/A	N/A
9	Disabled	N/A	N/A	N/A
10	Disabled	N/A	N/A	N/A
11	Disabled	N/A	N/A	N/A
12	Disabled	N/A	N/A	N/A

**Figure 5 - 46 Web-based Access Control Settings**

To set the Web-based Access Control for the Switch, complete the following fields:

Parameter	Description
<b>State</b>	Toggle the State field to either <i>Enable</i> or <i>Disable</i> for the Web-based Access Control settings of the Switch.
<b>Method</b>	Use the pull-down menu to choose the authenticator for Web-based Access Control. The user may choose:  <i>local</i> – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch configured using the User Account Creation screen seen below.  <i>radius</i> – Choose this parameter to use a remote RADIUS server as the authenticating method

	for users trying to access the network via the switch. This RADIUS server must have already been pre-assigned by the administrator using the RADIUS Server window located in the 802.1X section.
<b>Logout Timer (1-1440)</b>	The logout time is displayed in minutes, enter a value between 1 and 1440.
<b>Authentication VLAN</b>	Enter the VLAN name which users will be placed while authenticated by the Switch or a RADIUS server. This VLAN should be pre-configured to have limited access rights to web based authenticated users.
<b>Redirection Page</b>	Enter the URL of the website that authenticated users placed in the VLAN are directed to once authenticated. This path must be entered into this field before the Web-based Access Control can be enabled.
<b>Port List</b>	Specify the ports to be enabled as Web-based Access Control ports. Only these ports will accept authentication parameters from the user wishing limited access rights through the Switch. When one client on a port has been authenticated for Web-based Access Control, all clients on this port are authenticated as well.  Use the State pull-down menu to enable these configured ports as Web-based Access Control ports.

Click **Apply** to implement changes made.



**NOTE:** To enable the Web-based Access Control function, the redirection path field must have the URL of the website that users will be directed to once they enter the limited resource, pre-configured VLAN. Users who attempt to Apply settings without the Redirection Page field set will be prompted with an error message and Web-based Access Control will not be enabled. The URL should follow the form `http(s)://www.dlink.com`



**NOTE:** The subnet of the IP address of the authentication VLAN must be the same as that of the client, or the client will always be denied authentication.



**NOTE:** A successful authentication should direct the client to the stated web page. If the client does not reach this web page, yet does not receive a **Fail!** message, the client will already be authenticated and therefore should refresh the current browser window or attempt to open a different web page.

## Web-based Access Control User Settings

This window is used to configure the Switch for Web Authentication Settings.

To view this window, click **Security > Web Authentication > Web-based Access Control User Settings** as shown below:

**Figure 5 - 47 Web-based Access Control User Settings window**

The following parameters may be configured:

Parameter	Description
	<b>Create User</b>

<b>User Name</b>	Enter the username of up to 15 alphanumeric characters of the guest wishing to access the web through this process. This field is for administrators who have selected <i>local</i> as their web based authenticator.
<b>VLAN Name</b>	Enter the VLAN name of a previously configured VLAN to which the successfully authenticated web user will be mapped.
<b>Password</b>	Enter the password the administrator has chosen for the selected user. This field is case sensitive and must be a complete alphanumeric string. This field is for administrators who have selected <i>local</i> as their web based authenticator.
<b>Confirmation</b>	Re-enter the password.

Click **Apply** to implement changes.

## NetBIOS Filtering

NetBIOS is an application programming interface, providing a set of functions that applications use to communicate across networks. NetBEUI, the NetBIOS Enhanced User Interface, was created as a data-link-layer frame structure for NetBIOS. A simple mechanism to carry NetBIOS traffic, NetBEUI has been the protocol of choice for small MS-DOS- and Windows-based workgroups. NetBIOS no longer lives strictly inside of the NetBEUI protocol. Microsoft worked to create the international standards described in RFC 1001 and RFC 1002, NetBIOS over TCP/IP (NBT).

If the network administrator wants to block the network communication on more than two computers which use NETBUEI protocol, it can use NETBIOS filtering to filter these kinds of packets.

If the user enables the NETBIOS filter, the switch will create one access profile and three access rules automatically. If the user enables the extensive NETBIOS filter, the switch will create one more access profile and one more access rule.

## NetBIOS Filtering Settings

This window is used to configure the NetBIOS Filtering Setting.

To view this window, click **Security > NetBIOS Filtering Settings** as shown below:

The screenshot shows the 'NetBIOS Filtering Settings' window. It is divided into two main sections. The first section is titled 'NetBIOS Filtering (Filter NetBIOS over TCP/IP)'. It contains two buttons: 'Select All' and 'Clear All'. Below these is a 'Ports:' label followed by a row of 12 checkboxes, each labeled with a number from 01 to 12. An 'Apply' button is positioned at the bottom right of this section. The second section is titled 'Extensive NetBIOS Filtering (Filter NetBIOS over 802.2)'. It also contains 'Select All' and 'Clear All' buttons, a 'Ports:' label, and a row of 12 checkboxes labeled 01 through 12. An 'Apply' button is at the bottom right of this section as well.

**Figure 5 - 48 NetBIOS Filtering Settings window**

Enter the ports you wish to configure to filter NetBIOS packets from specified ports and click **Apply**.

## Section 6

# ACL

***ACL Configuration Wizard***

***Access Profile List***

***CPU Access Profile List***

***ACL Finder***

***ACL Flow Meter***

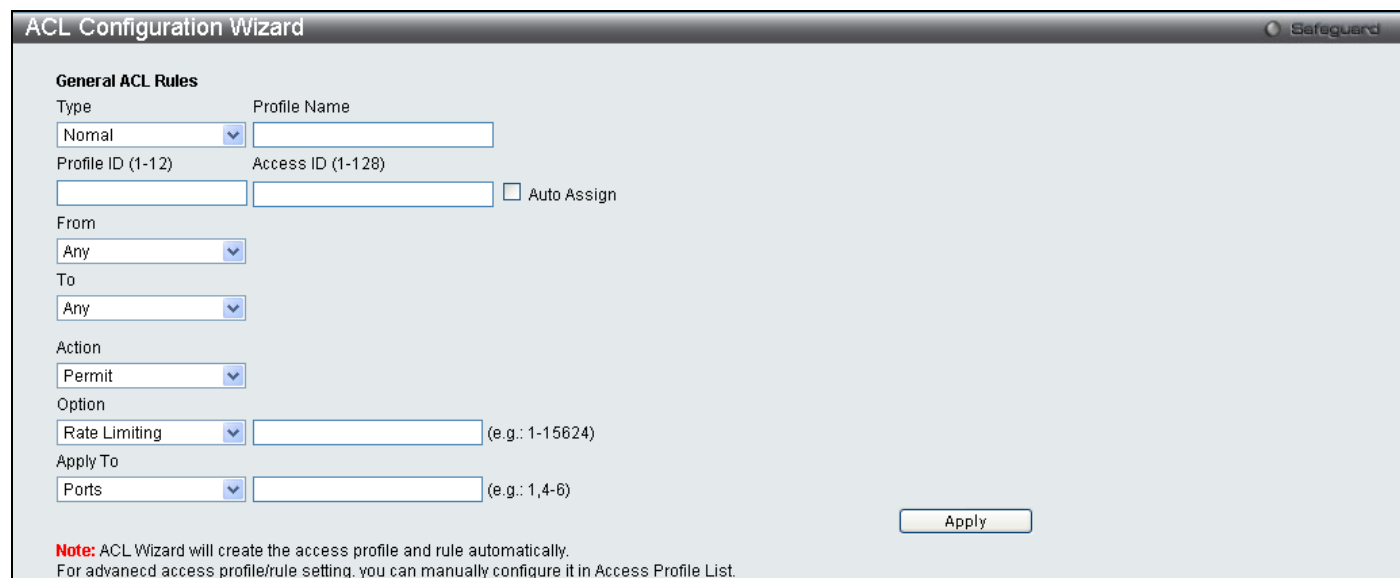
Access profiles allow you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of Packet Content, MAC address, or IP address.

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

## ACL Configuration Wizard

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

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



**Figure 6 - 1 ACL Configuration Wizard window**

The following parameters can be configured.

Parameter	Description
<b>Type</b>	Select the type of ACL you wish to create, either normal or CPU.
<b>Profile Name</b>	Select a unique Profile Name for this profile set.
<b>Profile ID (1-12)</b>	Enter a unique identifier number for this profile set. This value can be set from 1 to 12.
<b>Access ID (1-128)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 128.

<b>From</b>	Use the drop-down menu to select from MAC Address, IPv4 Address or IPv6.
<b>To</b>	Use the drop-down menu to select from MAC Address, IPv4 Address or IPv6. When IPv6 is selected the user can only enter the IPv6 source address or the IPv6 destination address at any one time.
<b>Action</b>	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 to 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.
<b>Option</b>	Use the pull down menu to select an option, the user can choose between <i>Rate Limiting</i> , <i>Change 1P Priority</i> , <i>Replace DSCP</i> and <i>Replace ToS Precedence</i> .
<b>Apply To</b>	Use the pull down menu to select an option, the user can choose between <i>Ports</i> , <i>VLAN Name</i> or <i>VLAN ID</i> and enter the appropriate information.

Click **Apply** to implement changes made.

## Access Profile List

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

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



**Figure 6 - 2 Access Profile Lists**

To add an ACL Profile, click the **Add ACL Profile** button, which, will display the window below. There are four **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IPv4** address-based profile configuration, one for the **Packet Content** and one for **IPv6**. You can explore the four **Access Profile Configuration** options by entering a Profile ID and Profile Name and using the radio button to select an ACL Type and click **Select**. The user may remove all Access Profiles by clicking the **Delete All** button (This button will not clear Address Binding ACL entries, which can only be deleted through the **IP-MAC Binding** window). The page shown below is the **Ethernet Access Profile Configuration** page.

**Add ACL Profile** Safeguard

Select Profile ID: 1

Select ACL Type:  Ethernet ACL  IPv6 ACL

Tagged

Profile Name: [Empty]

IPv4 ACL  Packet Content ACL

Select

<< Back Create

**Figure 6 - 3 Add Access Profile (Ethernet)**

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



**Figure 6 - 4 Add Ethernet ACL Profile window**

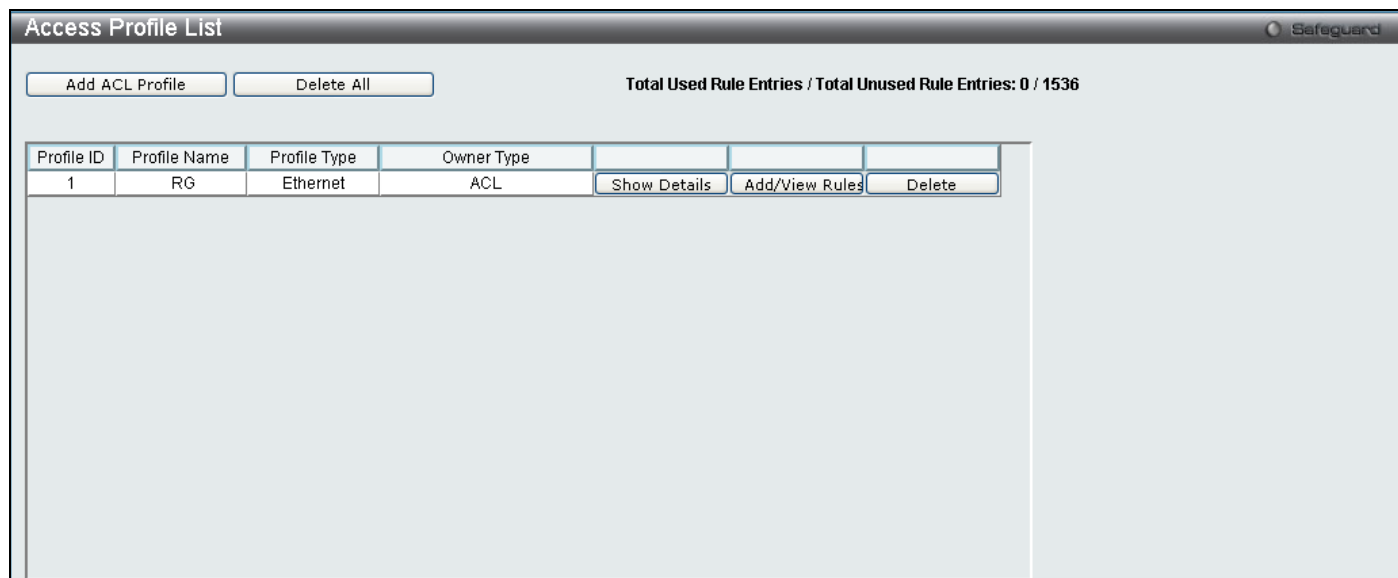
Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the Access Profile List page click **Back**.

The following parameters can be configured.

Parameter	Description
<b>Ethernet ACL</b>	To configure this profile select the Ethernet ACL, and use the drop down menu to choose between <i>tagged</i> or <i>untagged</i> .
<b>Source MAC Mask</b>	Enter a MAC address mask for the source MAC address.
<b>Destination MAC Mask</b>	Enter a MAC address mask for the destination MAC address.
<b>Select ACL Type</b>	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 <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IPv4</i> to instruct the Switch to examine the IPv4 address in each frame's header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to check the content of the packet header.
<b>802.1Q VLAN</b>	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.
<b>802.1P</b>	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.

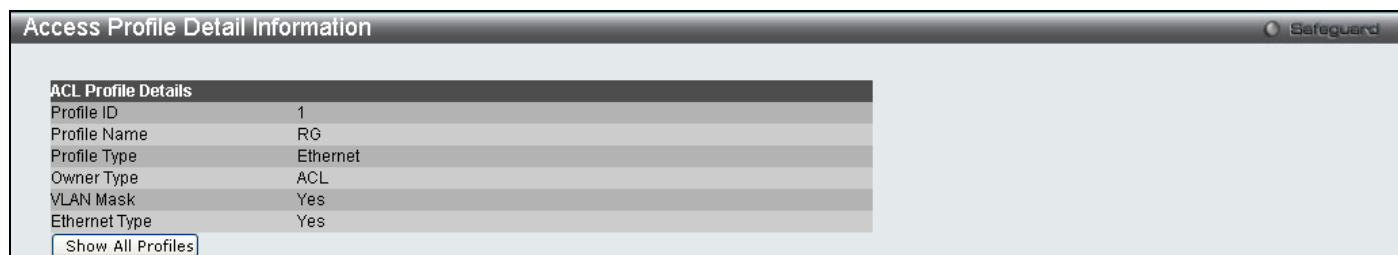
<b>Ethernet Type</b>	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.
----------------------	---

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



**Figure 6 - 5 Access Profile List (Ethernet)**

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



**Figure 6 - 6 Access Profile Details (Ethernet)**

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

Add Access Rule			
<b>Profile Information</b>			
Profile ID	1	Profile Name	RG
Profile Type	Ethernet	Owner Type	ACL
VLAN Mask	Yes	Ethernet Type	Yes
<hr/>			
<b>Rule Detail</b> (Keep an input field as blank to treat the corresponding option as do not care)			
Access ID (1-128)	1	<input type="checkbox"/> Auto Assign	
VLAN Mask			
VLAN ID			
Ethernet Type (0-FFFF)			
<b>Rule Action</b>			
Action	Permit		
Priority (0-7)		<input type="checkbox"/>	
Replace Priority		<input type="checkbox"/>	
Replace DSCP (0-63)		<input type="checkbox"/>	
Replace ToS Precedence (0-7)		<input type="checkbox"/>	
Time Range Name			<input type="checkbox"/>
Rx Rate (1-15624)		No Limit <input checked="" type="checkbox"/>	
Counter	Disabled		
Ports			(e.g.:1,4-6,9)
Ports			
VLAN Name			
VLAN ID			
		<input type="button" value=" &lt;&lt;Back"/> <input type="button" value=" Apply"/>	

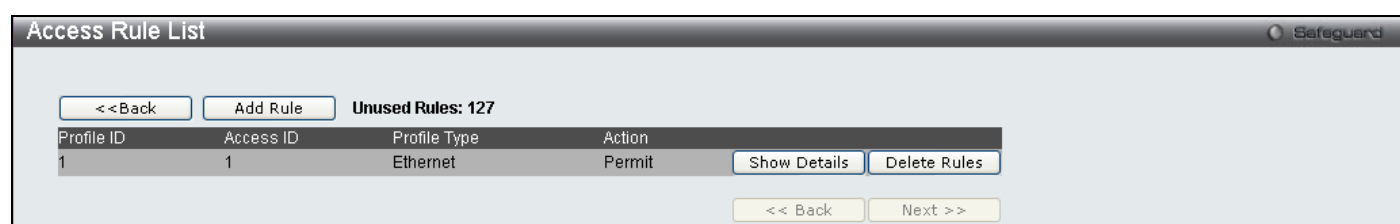
Figure 6 - 7 Access Profile Ethernet

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

Parameter	Description
<b>Access ID (1-128)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 128. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
<b>VLAN Mask</b>	Allows the entry of a VLAN Mask for a previously configured VLAN.
<b>VLAN ID</b>	Allows the entry of a VLAN ID for a previously configured VLAN.
<b>802.1p (0-7)</b>	Enter a value from 0 to 7 to specify that the access profile will apply only to packets with this 802.1p priority value.
<b>Action</b>	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.
<b>Priority</b>	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
<b>Replace Priority</b>	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
<b>Replace DSCP (0-63)</b>	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.
<b>Replace ToS</b>	Select this option to instruct the Switch to replace the Type of Service as part of the packet

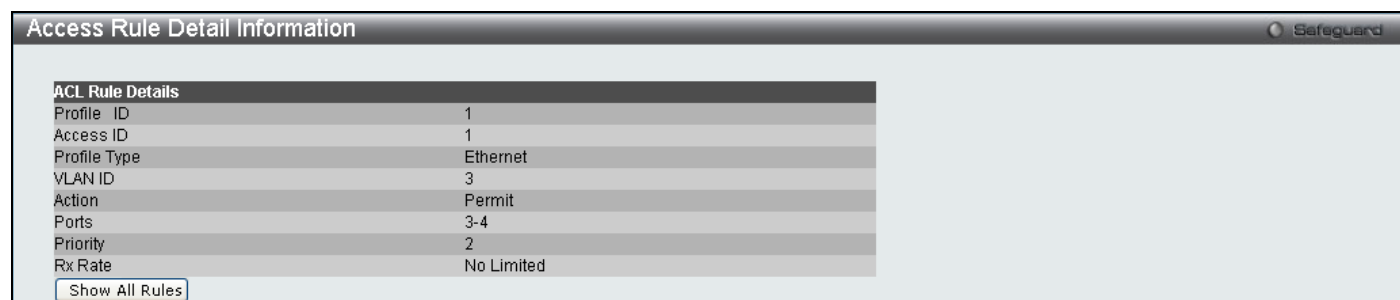
<b>Precedence</b>	header.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Rx Rate (1-15624)</b>	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640Kbit/sec.) The user may select a value between 1 and 15624 or tick the No Limit check box. The default setting is No Limit.
<b>Counter</b>	Specifies whether counter feature will be enabled/disabled This is optional, the default is disabled. If the rule is not binded with flow_meter, then all packet matched will be countered. If the rule is binded with flow_meter, then "counter" here will be overridden.
<b>Ports</b>	Specifies the access rule will take effect on one port or a range of ports.
<b>VLAN Name</b>	Specifies the access rule will take effect on the VLAN Name specified.
<b>VLAN ID</b>	Specifies the access rule will take effect on the VLAN ID specified.

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



**Figure 6 - 8 Access Rule List (Ethernet)**

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



**Figure 6 - 9 Access Rule Detail Information (Ethernet)**

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

Figure 6 - 10 Add IPv4 ACL Profile

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

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

Parameter	Description
<b>VLAN</b>	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.
<b>DSCP</b>	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.
<b>Source IP Mask</b>	Enter an IP address mask for the source IP address.
<b>Destination IP Mask</b>	Enter an IP address mask for the destination IP address.
<b>ICMP Type</b>	<ul style="list-style-type: none"> <li><i>icmp</i> – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.</li> <li><i>type &lt;value 0-255&gt;</i> – Specifies that the Switch will examine the type field within each packet.</li> <li><i>code &lt;value 0-255&gt;</i> – Specifies that the Switch will examine the code field within each packet.</li> </ul>
<b>Protocol</b>	<p>Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines:</p> <p>Select <b>ICMP</b> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p>Select <b>Type</b> to further specify that the access profile will apply an ICMP type value, or specify <b>Code</b> to further specify that the access profile will apply an ICMP</p>

code value.

Select **IGMP** to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.

Select **Type** to further specify that the access profile will apply an IGMP type value

Select **TCP** to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize), **fin** (finish).

**src port mask** – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter.

**dst port mask** – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter.

Select **UDP** to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.

**src port mask** – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff) to be filtered.

**dst port mask** – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) to be filtered.

**Protocol\_id <0x0-0xff>** – Enter a value defining the protocol ID in the packet header to mask.

**user\_define\_mask <hex 0x0-0xffffffff>** – Enter a value defining the mask options behind the IP header.

Click **Apply** to implement changes made.

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

Access Profile List Safeguard

Add ACL Profile  Total Used Rule Entries / Total Unused Rule Entries: 1 / 1535

Profile ID	Profile Name	Profile Type	Owner Type			
1	RG	Ethernet	ACL	Show Details	Add/View Rules	Delete
3	DG	IP	ACL	Show Details	Add/View Rules	Delete

**Figure 6 - 11 Access Profile List (IPv4)**

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

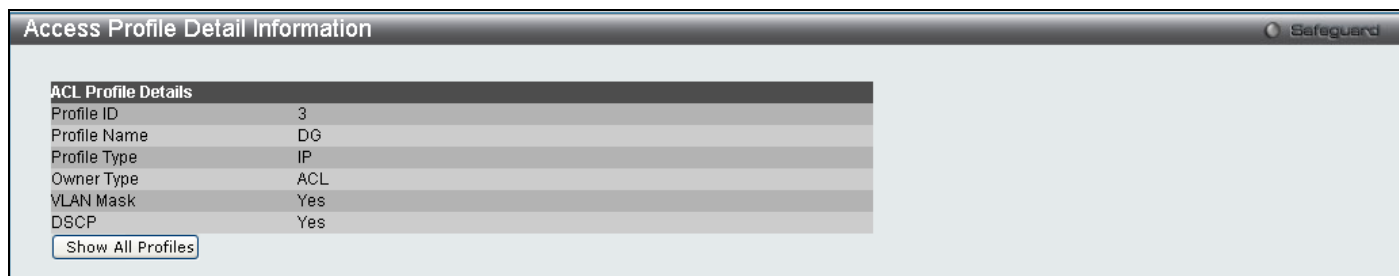


Figure 6 - 12 Access Profile Details (IPv4)

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

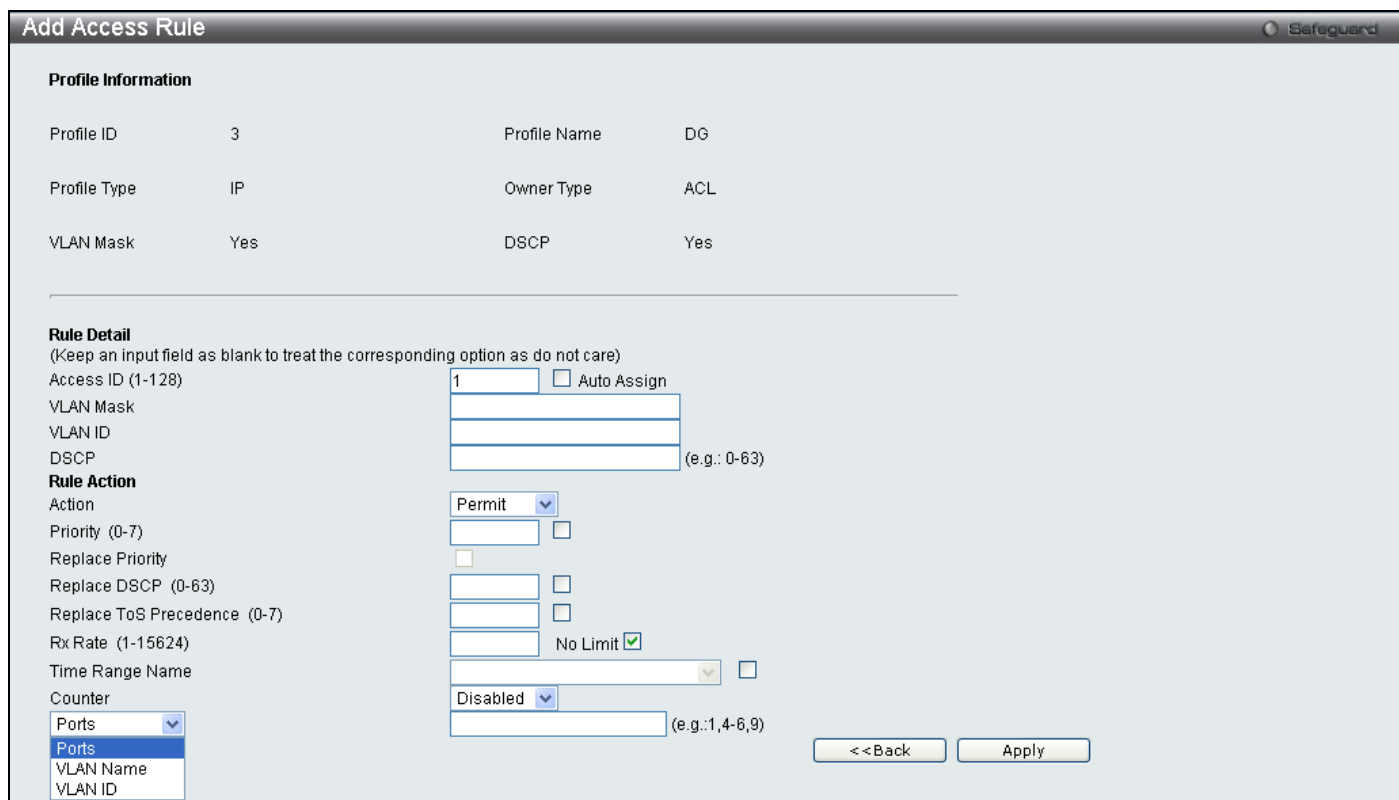


Figure 6 - 13 Access Profile (IPv4)

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

Parameter	Description
<b>Access ID (1-128)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 128.
<b>Action</b>	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 to 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.
<b>Priority (0-7)</b>	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
<b>Replace Priority</b>	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the

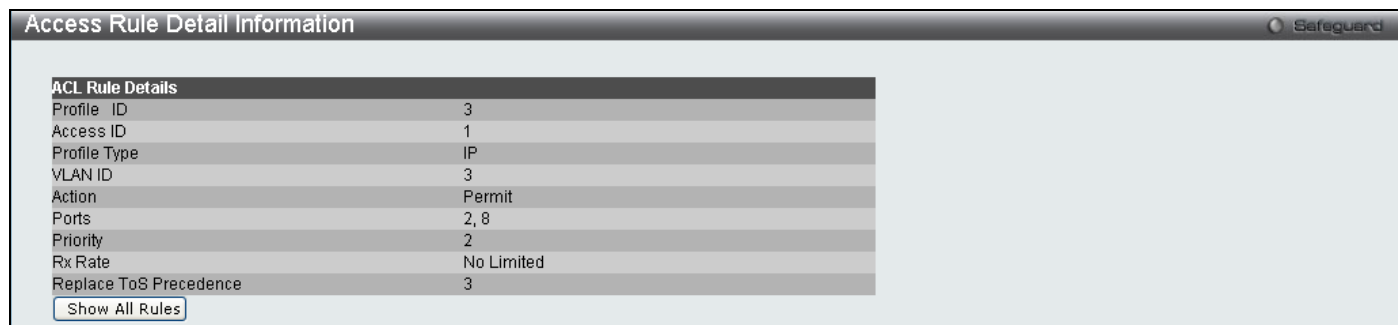
	Switch
<b>Replace DSCP</b>	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
<b>Replace ToS Precedence</b>	Select this option to instruct the Switch to replace the Type of Service as part of the packet header.
<b>VLAN Mask</b>	Allows the entry of a name for a previously configured VLAN.
<b>VLAN ID</b>	Allows the entry of a VLAN ID for a previously configured VLAN.
<b>DSCP</b>	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.
<b>ICMP</b>	Select <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
<b>Rx Rate (1-15624)</b>	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640Kbit/sec.) The user may select a value between 1 and 15624 or tick the No Limit check box. The default setting is No Limit.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Counter</b>	Enable or disable the counter settings.
<b>Ports</b>	Specifies that the access rule will take effect on one port or a range of ports.
<b>VLAN Name</b>	Specifies the access rule will take effect on the VLAN Name specified.
<b>VLAN ID</b>	Specifies the access rule will take effect on the VLAN ID specified.

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



**Figure 6 - 14 Access Rule List (IPv4)**

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



**Figure 6 - 15 Access Rule Detail Information**

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



**Add ACL Profile**
Safeguard

**Select Profile ID**

**Select ACL Type**

Ethernet ACL

IPv6 ACL

**Profile Name**

IPv4 ACL

Packet Content ACL

**You can select the field in the packet to create filtering mask**

IPv6 Class	IPv6 Flow Label	IPv6 TCP	IPv6 UDP	IPv6 Address
------------	-----------------	----------	----------	--------------

**IPv6 Class**

IPv6 Class

**IPv6 Flow Label**

IPv6 Flow Label

**TCP**

TCP


Source Port Mask (0-FFFF)

Destination Port Mask (0-FFFF)

Figure 6 - 16 Add IPv6 ACL Profile

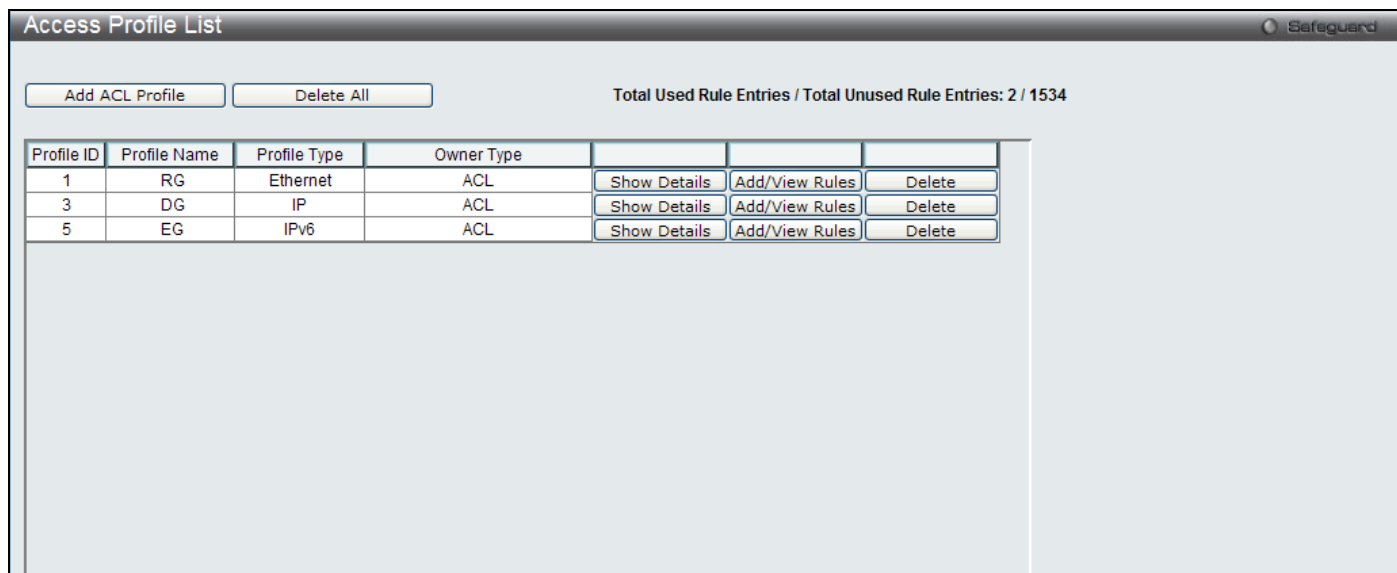
Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the Access Profile List page click **Back**.

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

Parameter	Description
<b>IPv6 Class</b>	Ticking this check box 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.
<b>IPv6 Flow Label</b>	Ticking this check box will instruct the Switch to examine the <i>flow label</i> field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
<b>IPv6 TCP</b>	Ticking this check box will specify that the rule applies to TCP traffic. The user can enter a specific TCP Source Port Mask or TCP Destination Port Mask.
<b>IPv6 UDP</b>	Ticking this check box will specify that the rule applies to UDP traffic. The user can enter a specific UDP Source Port Mask or UDP Destination Port Mask.
<b>IPv6 Address</b>	<p><i>IPv6 Source Address</i> – Enter an IPv6 address to be used as the source address mask.</p> <p><i>IPv6 Destination Address</i> – Enter an IPv6 address that will be used as the destination address mask.</p> <div style="text-align: center; margin-top: 10px;">  <p><b>NOTE:</b> At any one time the user can only choose IPv6 class and IPv6 Flow Label together or IPv6 Address by itself.</p> </div>

Click **Apply** to implement changes made.

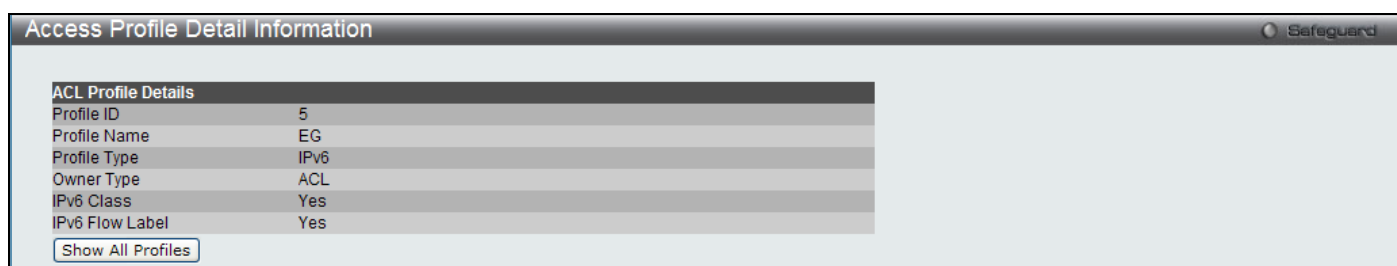
Click **Create** to view the new Access Profile List entry in the **Access Profile List** table shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details**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



Profile ID	Profile Name	Profile Type	Owner Type			
1	RG	Ethernet	ACL	Show Details	Add/View Rules	Delete
3	DG	IP	ACL	Show Details	Add/View Rules	Delete
5	EG	IPv6	ACL	Show Details	Add/View Rules	Delete

**Figure 6 - 17 Access Profile List (IPv6)**

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



ACL Profile Details	
Profile ID	5
Profile Name	EG
Profile Type	IPv6
Owner Type	ACL
IPv6 Class	Yes
IPv6 Flow Label	Yes

Show All Profiles

**Figure 6 - 18 Access Profile Details (IPv6)**

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

Add Access Rule
Safeguard

---

**Profile Information**

Profile ID	5	Profile Name	EG
Profile Type	IPv6	Owner Type	ACL
IPv6 Class	Yes	IPv6 Flow Label	Yes
TCP Source Port	-	TCP Destination Port	-

---

**Rule Detail**  
(Keep an input field as blank to treat the corresponding option as do not care)

Access ID (1-128)   Auto Assign

Class  (e.g.: 0-255)

Flow Label  (e.g.: 0-FFFFF)

TCP Source Port (0-65535)   TCP

TCP Destination Port (0-65535)

**Rule Action**

Action

Priority (0-7)

Replace Priority

Replace DSCP (0-63)

Replace ToS Precedence (0-7)

Rx Rate (1-15624)  No Limit

Time Range Name

Counter

(e.g.:1,4-6,9)

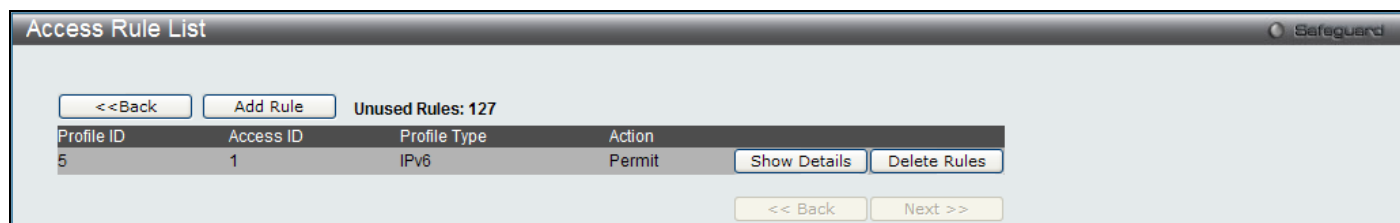
Figure 6 - 19 Access Profile (IPv6)

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

Parameter	Description
<b>Access ID (1-128)</b>	Enter a unique identifier number for this access. This value can be set from 1 to 128.
<b>Class</b>	Specifies the IPv6 Class. Enter a value between 0 – 255.
<b>Flow Label</b>	Specifies the IPv6 Flow Label. Enter a value between 0 – FFFFF.
<b>Action</b>	<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 to be filtered.</p> <p>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.</p>
<b>Priority (0-7)</b>	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
<b>Replace Priority</b>	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
<b>Replace DSCP</b>	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.
<b>Replace ToS Precedence</b>	Select this option to instruct the Switch to replace the Type of Service as part of the packet header.
<b>Class</b>	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

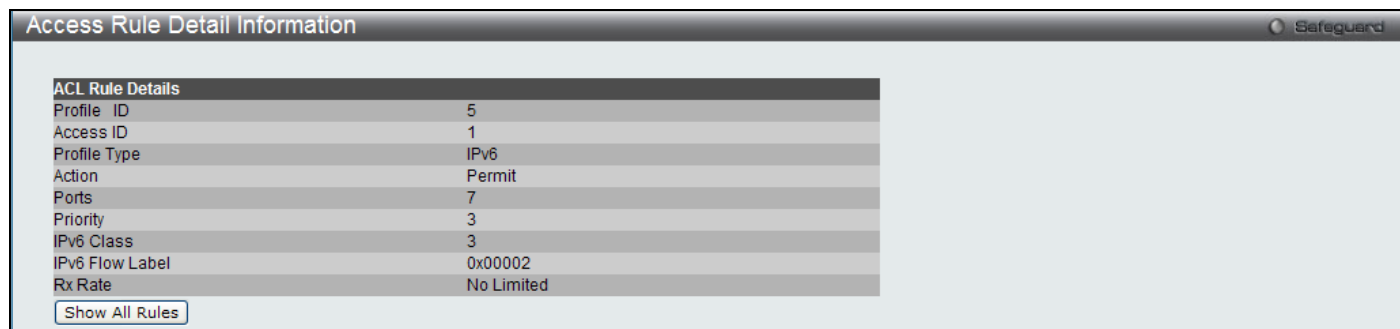
	Precedence bits field in IPv4.
<b>Rx Rate (1-15624)</b>	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640Kbit/sec.) The user may select a value between 1 and 15624 or tick the No Limit check box. The default setting is No Limit.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Counter</b>	Enable or disable the counter settings.
<b>Ports</b>	Specifies that the access rule will take effect on one port or a range of ports.
<b>VLAN Name</b>	Specifies the access rule will take effect on the VLAN Name specified.
<b>VLAN ID</b>	Specifies the access rule will take effect on the VLAN ID specified.

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



**Figure 6 - 20 Access Rule List (IPv6)**

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



**Figure 6 - 21 Access Rule Detail Information (IPv6)**

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

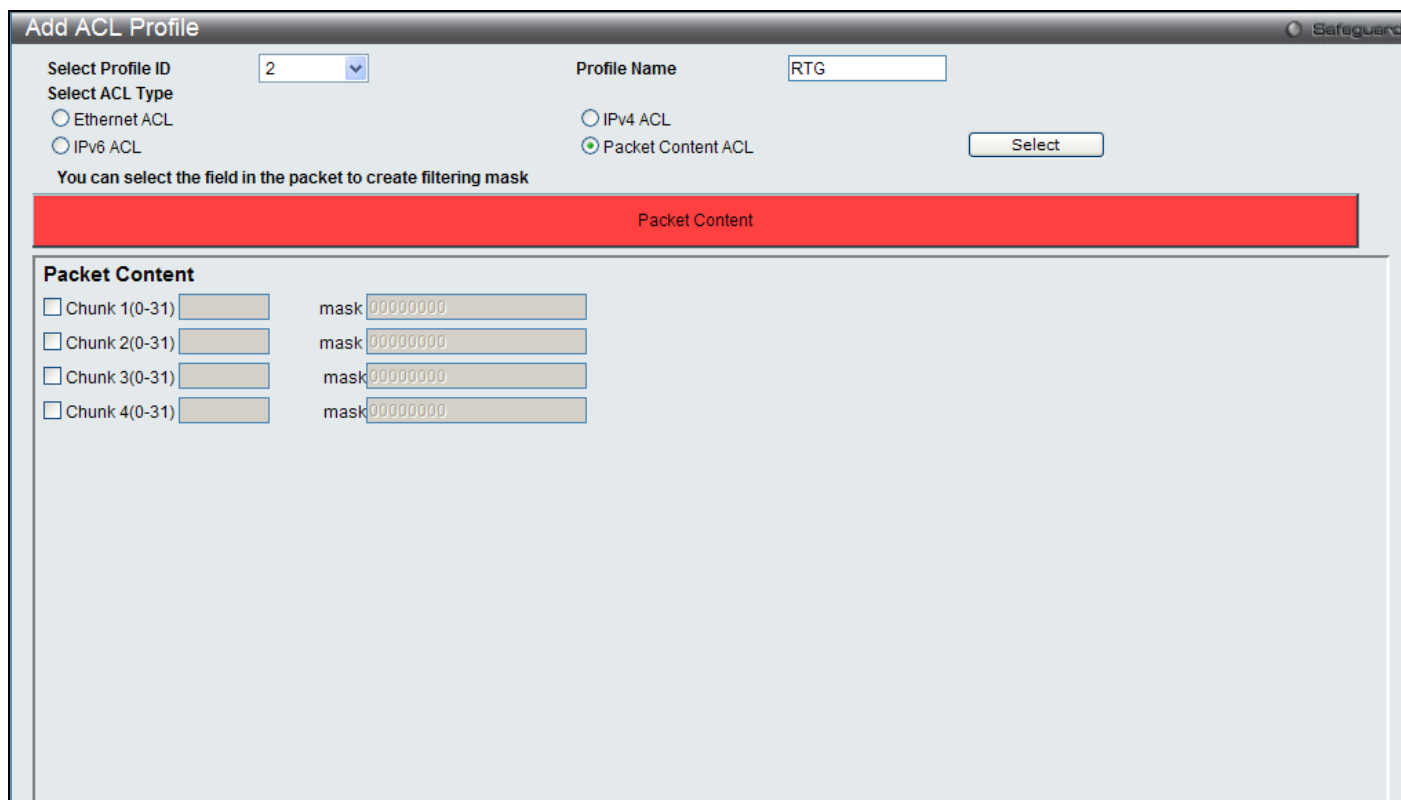


Figure 6 - 22 Add Packet Content ACL Profile

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

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

Parameter	Description														
<b>Chunk</b>	<p>Allows users to examine up to 4 specified offset_chunks within a packet at one time and specifies the frame content offset and mask. There are 4 chunk offsets and masks that can be configured. A chunk mask presents 4 bytes. 4 offset_chunks can be selected from a possible 32 predefined offset_chunks as described below:</p> <p>offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4.</p> <table border="1"> <thead> <tr> <th>chunk0</th> <th>chunk1</th> <th>chunk2</th> <th>.....</th> <th>chunk29</th> <th>chunk30</th> <th>chunk31</th> </tr> </thead> <tbody> <tr> <td>B126, B127, B0, B1</td> <td>B2, B3, B4, B5</td> <td>B6, B7, B8, B9</td> <td>.....</td> <td>B114, B115, B116, B117</td> <td>B118, B119, B120, B121</td> <td>B122, B123, B124, B125</td> </tr> </tbody> </table> <p>Example: offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1 offset_chunk_1 0 0xffff will match packet byte offset,0,1</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 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</p>	chunk0	chunk1	chunk2	.....	chunk29	chunk30	chunk31	B126, B127, B0, B1	B2, B3, B4, B5	B6, B7, B8, B9	.....	B114, B115, B116, B117	B118, B119, B120, B121	B122, B123, B124, B125
chunk0	chunk1	chunk2	.....	chunk29	chunk30	chunk31									
B126, B127, B0, B1	B2, B3, B4, B5	B6, B7, B8, B9	.....	B114, B115, B116, B117	B118, B119, B120, B121	B122, B123, B124, B125									

able to inspect any specified content of a packet in different protocol layers.

Click **Apply** to implement changes made.

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

Profile ID	Profile Name	Profile Type	Owner Type			
1	RG	Ethernet	ACL	Show Details	Add/View Rules	Delete
2	RTG	Packet Content	ACL	Show Details	Add/View Rules	Delete
3	DG	IP	ACL	Show Details	Add/View Rules	Delete
5	EG	IPv6	ACL	Show Details	Add/View Rules	Delete

**Figure 6 - 23 Access Profile List (Packet Content)**

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

ACL Profile Details	
Profile ID	2
Profile Name	RTG
Profile Type	Packet Content
Owner Type	ACL
Chunk 1	3, Value: 0x00000700

**Figure 6 - 24 Access Profile Details (Packet Content)**

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

Add Access Rule
Safeguard

---

**Profile Information**

Profile ID	2	Profile Name	rtg
Profile Type	Packet Content	Owner Type	ACL
Chunk 1	2, Value: 0x00000001		

---

**Rule Detail**  
(Keep an input field as blank to treat the corresponding option as do not care)

Access ID (1-128)	<input type="text" value="1"/>	<input type="checkbox"/>	Auto Assign
Chunk 1	<input type="text"/>	<input type="checkbox"/>	
Chunk 2	<input type="text"/>	<input type="checkbox"/>	
Chunk 3	<input type="text"/>	<input type="checkbox"/>	
Chunk 4	<input type="text"/>	<input type="checkbox"/>	

**Rule Action**

Action	Permit	<input type="checkbox"/>	
Priority (0-7)	<input type="text"/>	<input type="checkbox"/>	
Replace Priority	<input type="checkbox"/>		
Replace DSCP (0-63)	<input type="text"/>	<input type="checkbox"/>	
Replace ToS Precedence (0-7)	<input type="text"/>	<input type="checkbox"/>	
Rx Rate (1-15624)	<input type="text"/>	<input checked="" type="checkbox"/>	No Limit
Time Range Name	<input type="text"/>	<input type="checkbox"/>	
Counter	Disabled	<input type="checkbox"/>	

Ports  
 Ports  
 VLAN Name  
 VLAN ID

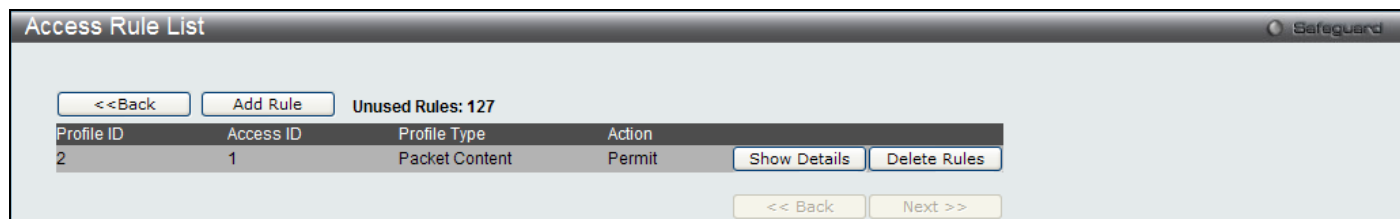
Figure 6 - 25 Access Profile (Packet Content)

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

Parameter	Description
<b>Access ID (1-128)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 128.
<b>Action</b>	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 to 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.
<b>Priority (0-7)</b>	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
<b>Replace DSCP</b>	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.
<b>Replace ToS Precedence</b>	Select this option to instruct the Switch to replace the Type of Service as part of the packet header.
<b>Chunk</b>	This field will instruct the Switch to mask the packet header beginning with the offset value specified.
<b>Rx Rate (1-15624)</b>	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64Kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640Kbit/sec.) The user may select a value between 1 and 15624 or tick the No Limit check box. The default setting is No Limit.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.

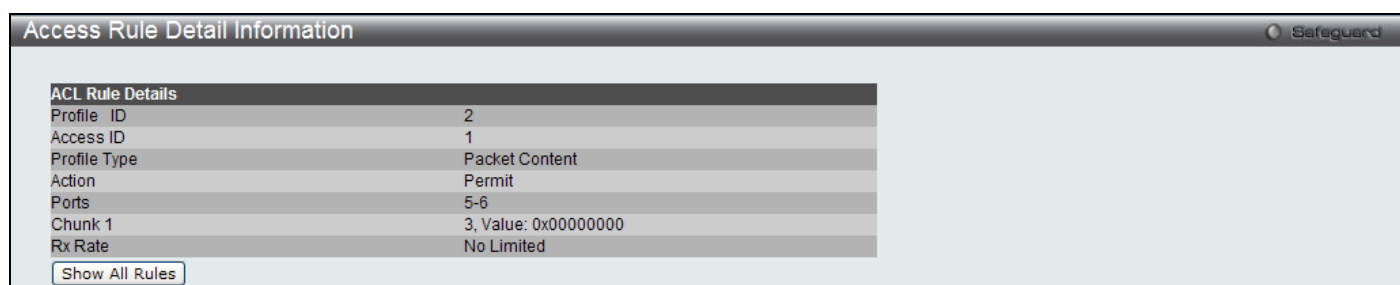
<b>Counter</b>	Enable or disable the counter settings.
<b>Ports</b>	Specifies that the access rule will take effect on one port or a range of ports.
<b>VLAN Name</b>	Specifies the access rule will take effect on the VLAN Name specified.
<b>VLAN ID</b>	Specifies the access rule will take effect on the VLAN ID specified.

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



**Figure 6 - 26 Access Rule List (Packet Content)**

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



**Figure 6 - 27 Access Rule Detail Information (Packet Content)**



**NOTE:** Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC Address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN. For a more detailed explanation on how ARP works and how to employ D-Link's advanced unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix B, at the end of this manual.

## 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.

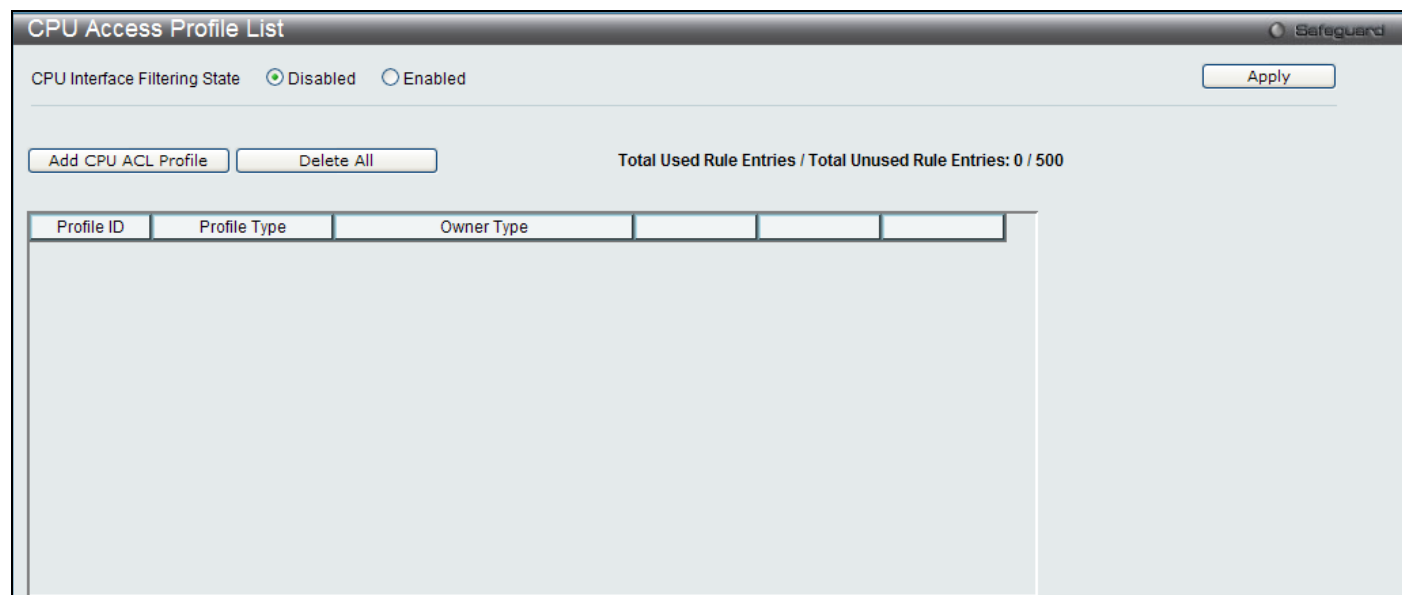


## CPU Access Profile List

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

Choose Enabled to enable CPU packets to be scrutinized by the Switch and Disabled to disallow this scrutiny.



**Figure 6 - 28 CPU Access Profile List window**

This window displays the CPU Access Profile List entries created on the Switch (one CPU access profile of each type has been created for explanatory purposes). To view the configurations for an entry, click the corresponding **Show Details** button.

To add an entry to the CPU Access Profile List, click the **Add CPU ACL Profile** button. This will open the **Add CPU ACL Profile** 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 - 29 Add CPU ACL Profile window for Ethernet

Parameter	Description
<b>Select Profile ID</b>	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from 1 to 5.
<b>Select ACL Type</b>	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content Mask to specify a mask to check the content of the packet header.
<b>Source MAC Mask</b>	Enter a MAC address mask for the source MAC address.
<b>Destination MAC Mask</b>	Enter a MAC address mask for the destination MAC address.
<b>802.1Q VLAN</b>	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.
<b>802.1P</b>	Selecting this option instructs the Switch to specify that the access profile will apply only to packets with this 802.1p priority value.
<b>Ethernet Type</b>	Selecting 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.

To view the settings of a previously correctly created profile, click the corresponding **Show Details** button on the **CPU Access Profile List** window to view the following window:

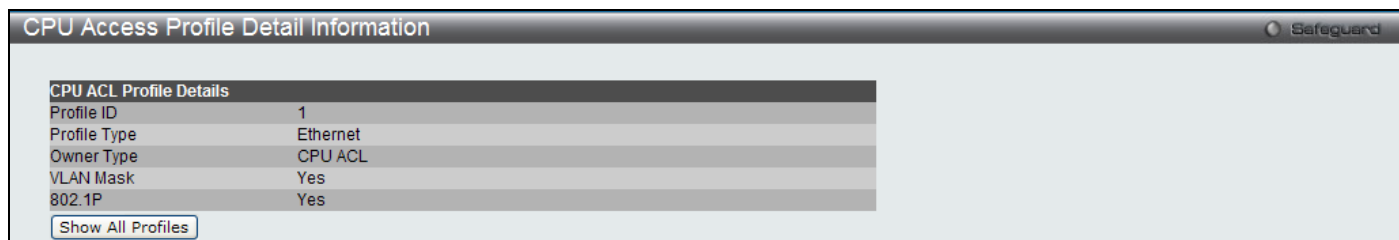


Figure 6 - 30 CPU Access Profile Detail Information window for Ethernet

The window shown below is the **Add CPU ACL Profile** window for IP (IPv4).

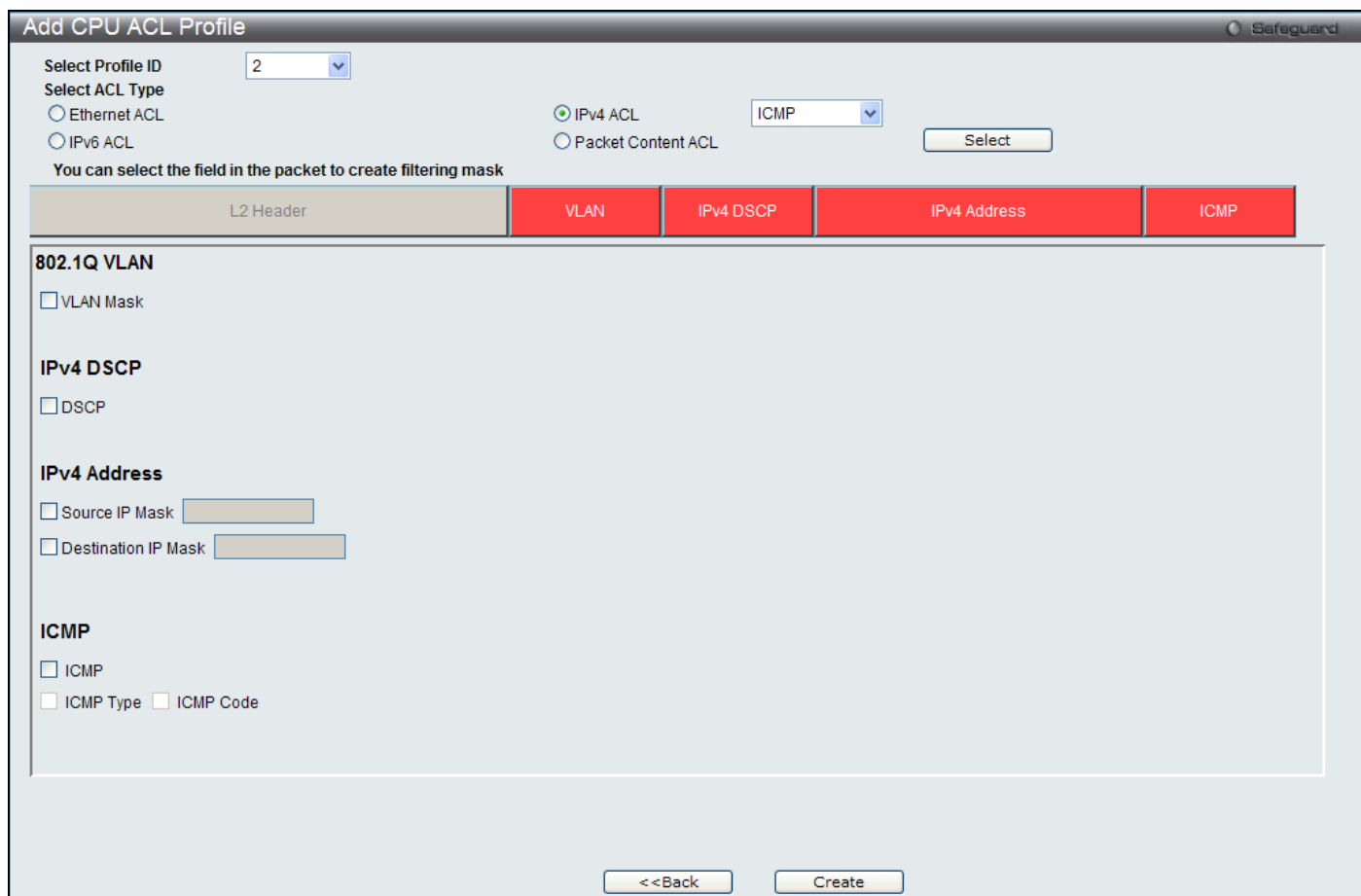


Figure 6 - 31 Add CPU ACL Profile window for IP (IPv4)

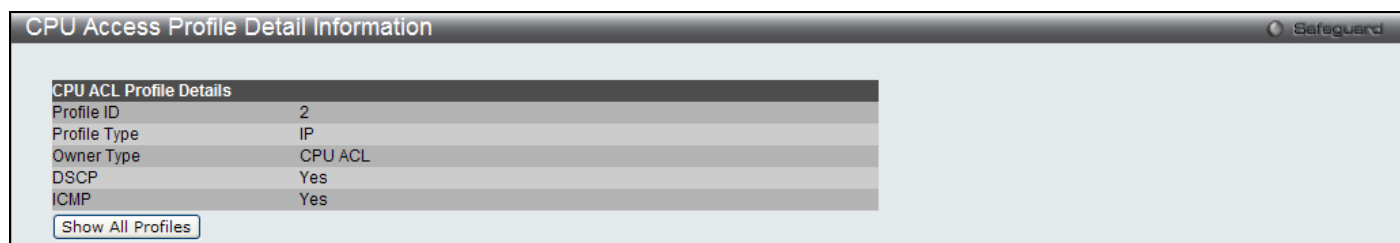
The following parameters may be configured for the IP (IPv4) filter.

Parameter	Description
<b>Select Profile ID</b>	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from 1 to 5.
<b>Select ACL Type</b>	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content Mask to specify a mask to check the content of the packet header.
<b>802.1Q VLAN</b>	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.
<b>IPv4 DSCP</b>	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.
<b>Source IP Mask</b>	Enter an IP address mask for the source IP address.

<b>Destination IP Mask</b>	Enter an IP address mask for the destination IP address.
<b>Protocol</b>	<p>Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines:</p> <p>Select <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p style="padding-left: 40px;">Select <i>Type</i> to further specify that the access profile will apply an ICMP type value, or specify <i>Code</i> to further specify that the access profile will apply an ICMP code value.</p> <p>Select <i>IGMP</i> to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.</p> <p style="padding-left: 40px;">Select <i>Type</i> to further specify that the access profile will apply an IGMP type value.</p> <p>Select <i>TCP</i> to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires a source port mask and/or a destination port mask is to be specified. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish).</p> <p style="padding-left: 40px;"><i>src port mask</i> – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter.</p> <p style="padding-left: 40px;"><i>dst port mask</i> – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter.</p> <p>Select <i>UDP</i> to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.</p> <p style="padding-left: 40px;"><i>src port mask</i> – Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff).</p> <p style="padding-left: 40px;"><i>dst port mask</i> – Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff).</p> <p><i>Protocol_id &lt;0x0-0xff&gt;</i> – Enter a value defining the protocol ID in the packet header to mask.</p> <p><i>user_define_mask &lt;hex 0x0-0xffffffff&gt;</i> – Enter a value defining the mask options behind the IP header.</p>

Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click the corresponding **Show Details** button on the **CPU Access Profile List** window to view the following window:




**Figure 6 - 32 CPU Access Profile Detail Information window for IP (IPv4)**

The window shown below is the **Add CPU ACL Profile** window for IPv6.

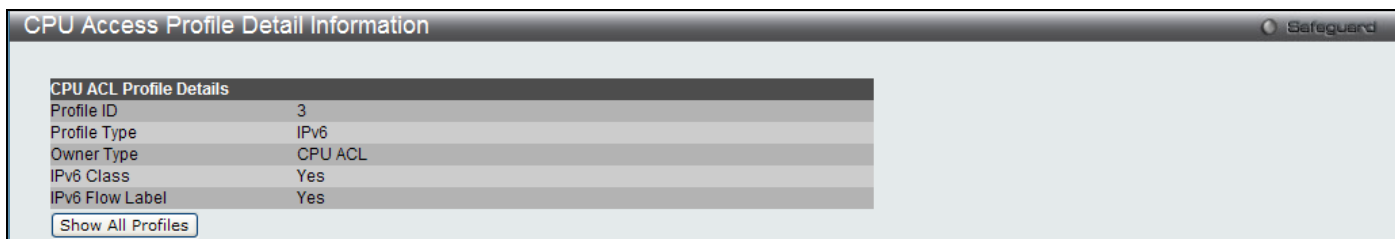
Figure 6 - 33 Add CPU ACL Profile window for IPv6

The following parameters may be configured for the IPv6 filter.

Parameter	Description
<b>Select Profile ID</b>	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from 1 to 5.
<b>Select ACL Type</b>	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content Mask to specify a mask to check the content of the packet header.
<b>IPv6 Class</b>	Checking this field 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.
<b>IPv6 Flow Label</b>	Checking this field will instruct the Switch to examine the <i>flow label</i> field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
<b>IPv6 Address</b>	<i>IPv6 Source Address</i> – Enter an IPv6 address to be used as the source address mask. <i>IPv6 Destination Address</i> – Enter an IPv6 address that will be used as the destination address mask.  <p><b>NOTE:</b> At any one time the user can only choose IPv6 class and IPv6 Flow Label together or IPv6 Address by itself.</p>

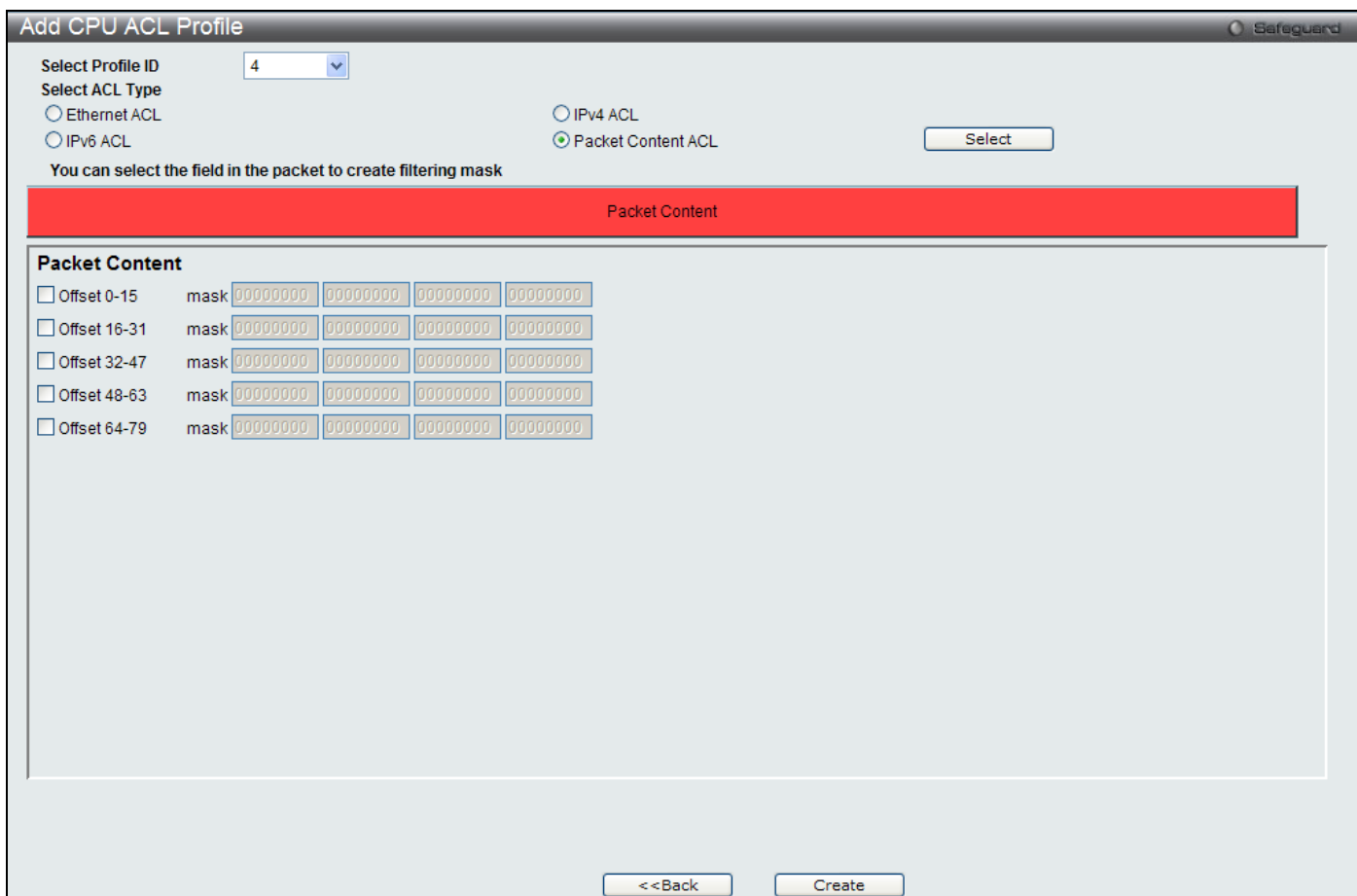
Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click the corresponding **Show Details** button on the **CPU Access Profile List** window to view the following window:



**Figure 6 - 34 CPU Access Profile Detail Information window for IPv6**

The window shown below is the **Add CPU ACL Profile** window for Packet Content.



**Figure 6 - 35 Add CPU ACL Profile window for Packet Content**

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

Parameter	Description
<b>Select Profile ID</b>	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from 1 to 5.
<b>Select ACL Type</b>	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content Mask to specify a mask to check the content of the packet header.
<b>Offset</b>	This field will instruct the Switch to mask the packet header beginning with the offset value specified: <ul style="list-style-type: none"> <li>0-15 – Enter a value in hex form to mask the packet from the beginning of the packet to</li> </ul>

the 15th byte.

- 16-31 – Enter a value in hex form to mask the packet from byte 16 to byte 31.
- 32-47 – Enter a value in hex form to mask the packet from byte 32 to byte 47.
- 48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63.
- 64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click **Apply** to set this entry in the Switch’s memory.

To view the settings of a previously correctly created profile, click the corresponding **Show Details** button on the **CPU Access Profile List** window to view the following window:

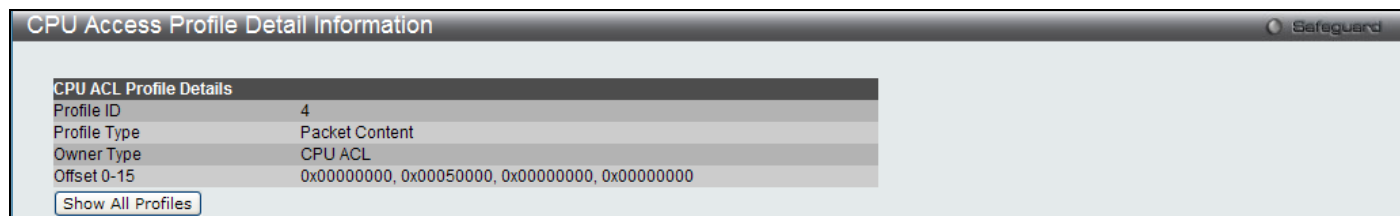


Figure 6 - 36 CPU Access Profile Detail Information window for Packet Content

**To establish the rule for a previously created CPU Access Profile:**

To configure the Access Rules for Ethernet, open the **CPU Access Profile List** window and click **Add/View Rules** for an Ethernet entry. This will open the following window.

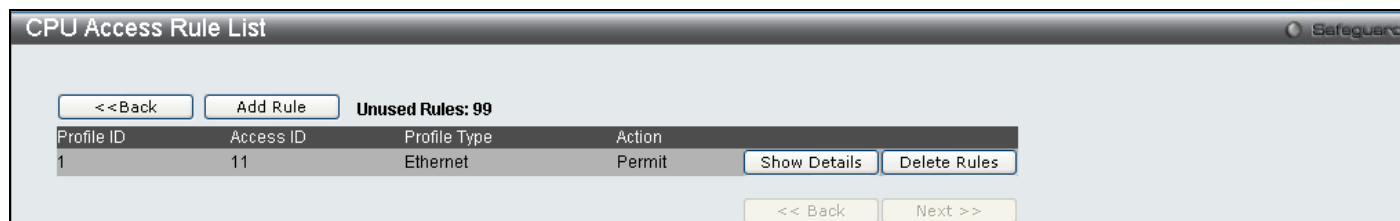


Figure 6 - 37 CPU Access Rule List window for Ethernet

To remove a previously created rule, click the corresponding **Delete Rules** button. To add a new Access Rule, click the **Add Rule** button:

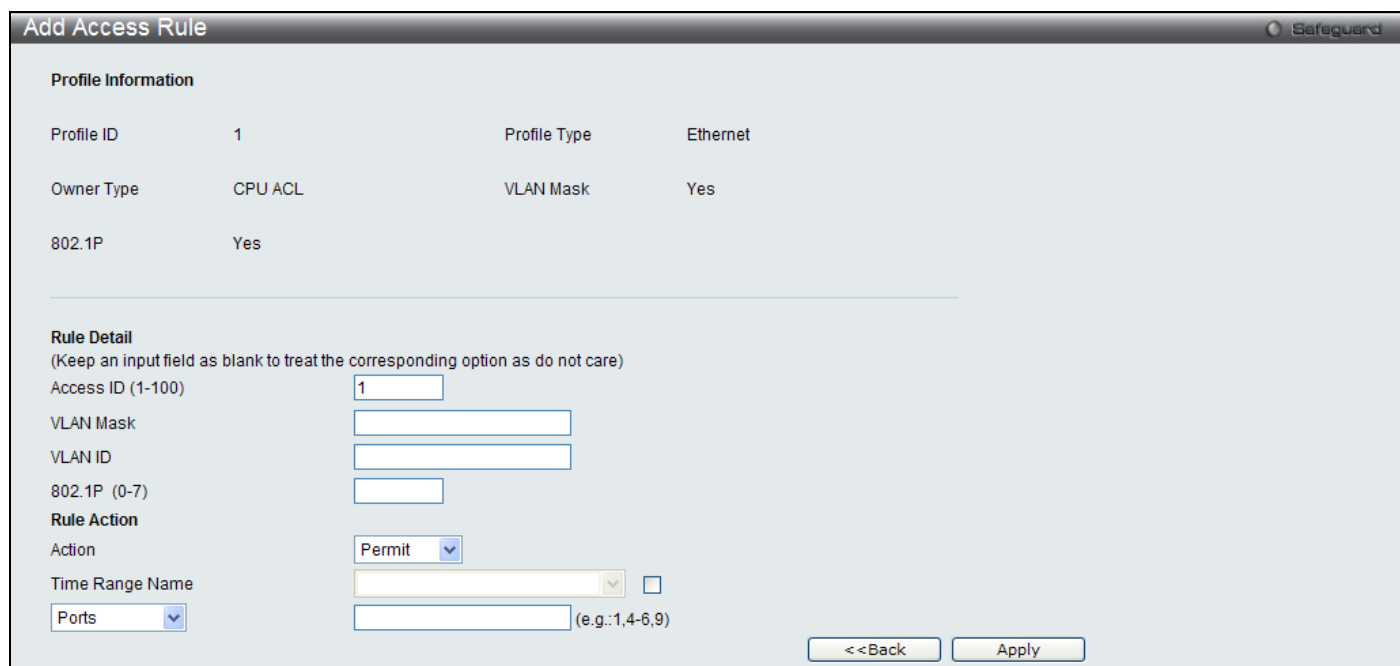


Figure 6 - 38 Add Access Rule window for Ethernet

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

Parameter	Description
<b>Access ID (1-100)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 100.

<b>Action</b>	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 to be filtered.
<b>Ethernet Type (0-FFFF)</b>	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Ports</b>	Specifies the access rule will take effect on one port or a range of ports.

To view the settings of a previously correctly configured rule, click the corresponding **Show Details** button on the **CPU Access Rule List** window to view the following window:

CPU ACL Rule Details	
Profile ID	1
Access ID	1
Profile Type	Ethernet
VLAN ID	3
Action	Permit
Ports	3
802.1P	2

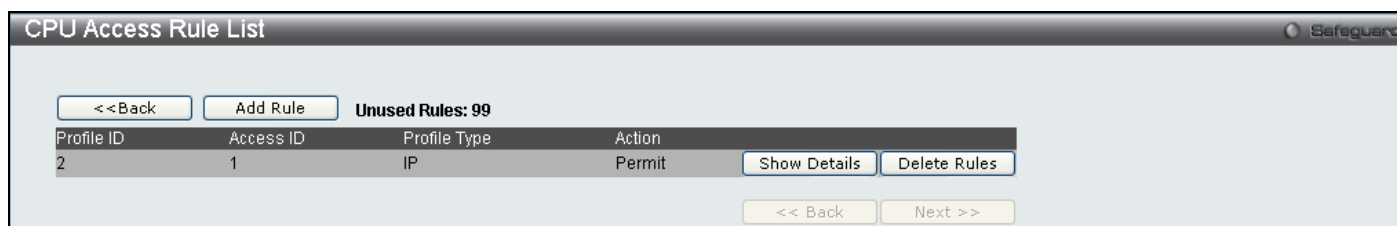
Show All Rules

**Figure 6 - 39 CPU Access Rule Detail Information window for Ethernet**



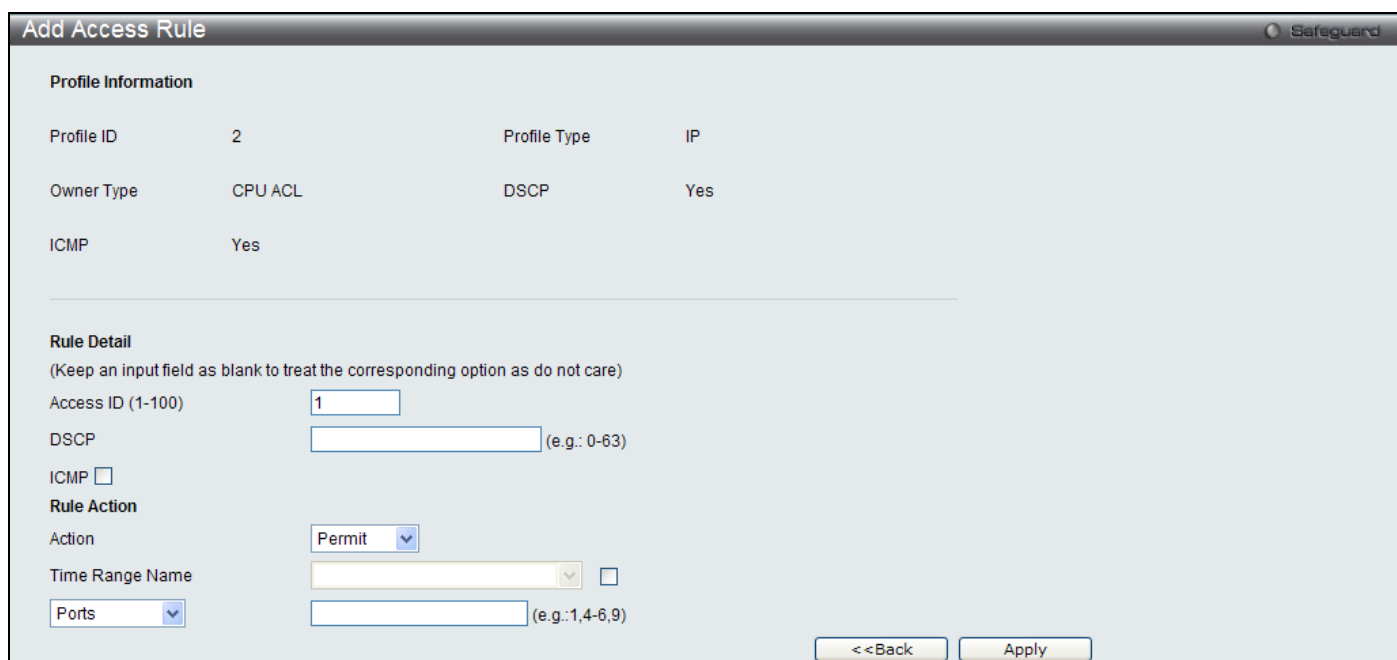
**To establish the rule for a previously created CPU Access Profile:**

To configure the Access Rules for IP, open the **CPU Access Profile List** window and click **Add/View Rules** for an IP entry. This will open the following window.



**Figure 6 - 40 CPU Access Rule List window for IP**

To remove a previously created rule, click the corresponding **Delete Rules** button. To add a new Access Rule, click the **Add Rule** button:



**Figure 6 - 41 Add Access Rule window for IP**

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

Parameter	Description
<b>Access ID (1-100)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 100.
<b>Action</b>	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 to be filtered.
<b>DSCP</b>	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header. Enter a value between 0 and 63.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Ports</b>	Specifies the access rule can take effect on one port or a range of ports.

To view the settings of a previously correctly configured rule, click the corresponding **Show Details** button on the **CPU Access Rule List** window to view the following window:

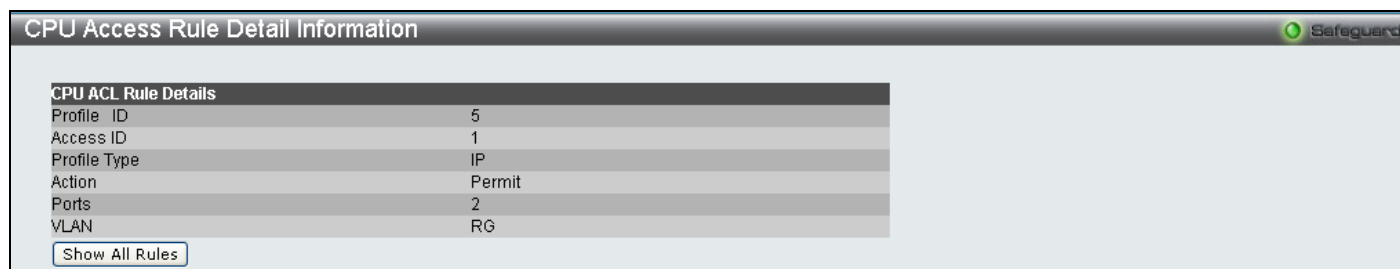


Figure 6 - 42 CPU Access Rule Detail Information window for IP

**To establish the rule for a previously created CPU Access Profile:**

To configure the Access Rules for IP, open the **CPU Access Profile List** window and click **Add/View Rules** for an IPv6 entry. This will open the following window.

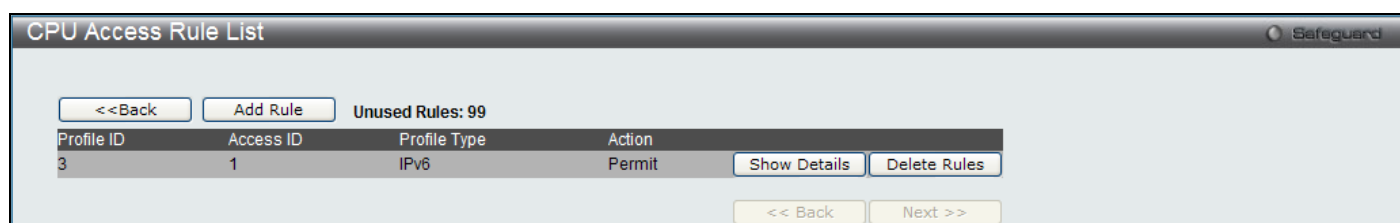


Figure 6 - 43 CPU Access Rule List window for IPv6

To remove a previously created rule, click the corresponding **Delete Rules** button. To add a new Access Rule, click the **Add Rule** button:

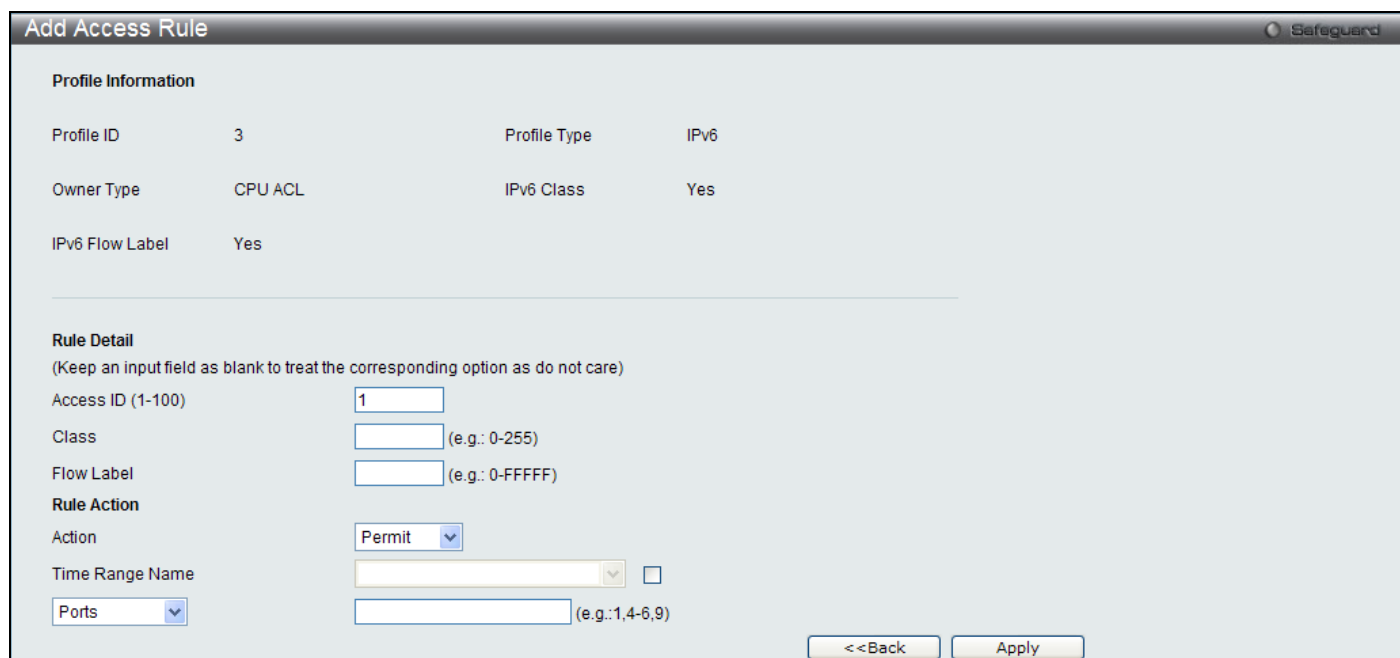


Figure 6 - 44 Add Access Rule window for IPv6

To set the Access Rule for IPv6, adjust the following parameters and click **Apply**.

Parameter	Description
<b>Access ID (1-100)</b>	Enter a unique identifier number for this access. This value can be set from 1 to 100.
<b>Action</b>	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 to be filtered.
<b>Class</b>	Enter an IPv6 Class. The class can be between 0 – 255.
<b>Flow Label</b>	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-

	default quality of service or real time service packets.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Ports</b>	Specifies the access rule can take effect on one port or a range of ports.

To view the settings of a previously correctly configured rule, click the corresponding **Show Details** button on the **CPU Access Rule List** window to view the following window:

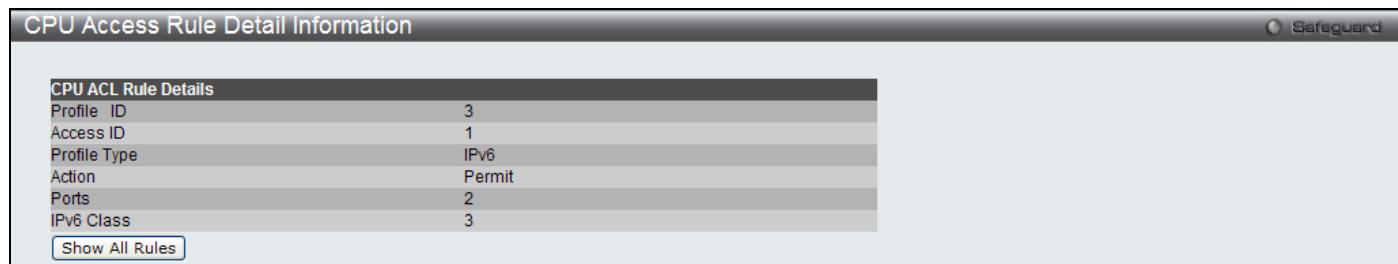


Figure 6 - 45 CPU Access Rule Detail Information window for IPv6

**To establish the rule for a previously created CPU Access Profile:**

To configure the Access Rules for IP, open the **CPU Access Profile List** window and click **Add/View Rules** for a Packet Content entry. This will open the following window.

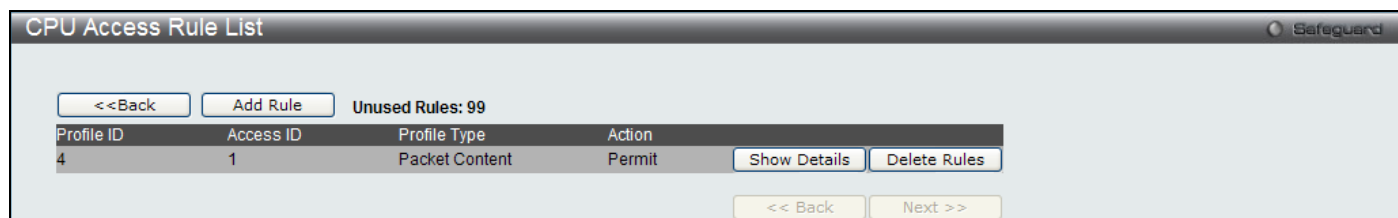


Figure 6 - 46 CPU Access Rule List window for Packet Content

To remove a previously created rule, click the corresponding **Delete Rules** button. To add a new Access Rule, click the **Add Rule** button:

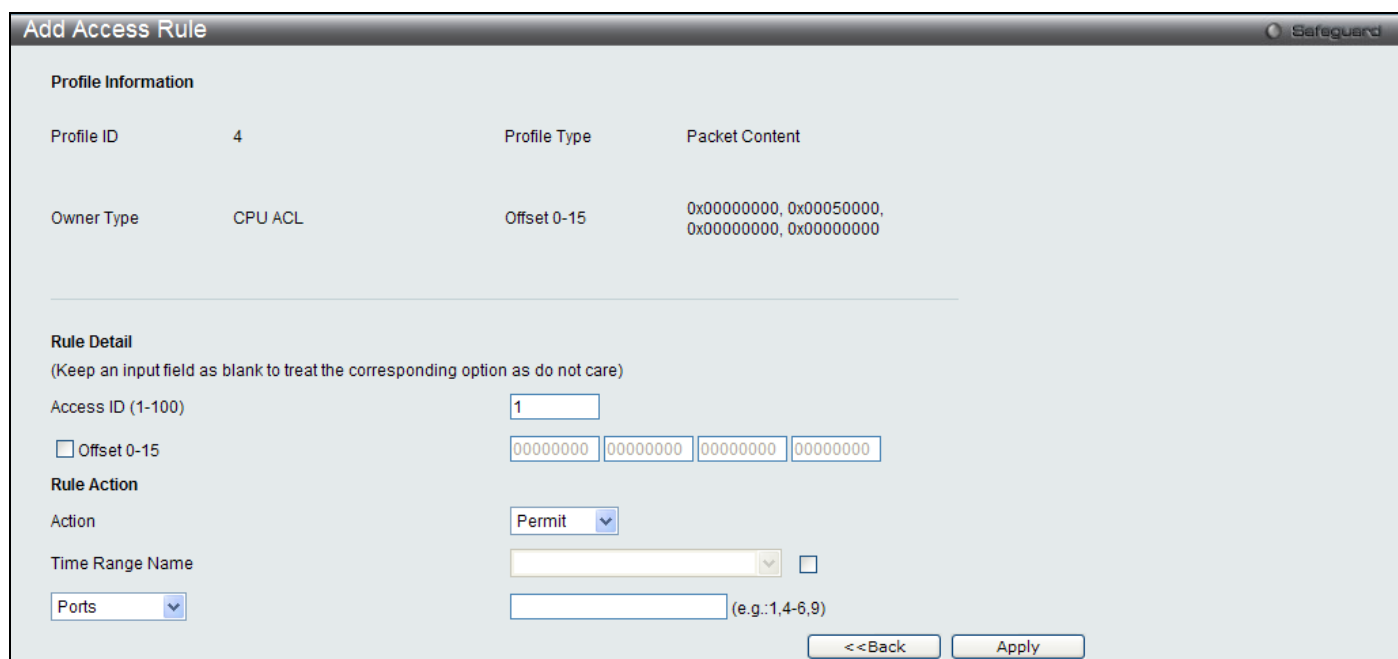


Figure 6 - 47 Add Access Rule window for Packet Content

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

Parameter	Description
<b>Access ID (1-100)</b>	Type in a unique identifier number for this access. This value can be set from 1 to 100.
<b>Action</b>	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 to be filtered.
<b>Offset</b>	This field will instruct the Switch to mask the packet header beginning with the offset value specified: Offset 0-15 – Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. Offset 16-31 – Enter a value in hex form to mask the packet from byte 16 to byte 31. Offset 32-47 – Enter a value in hex form to mask the packet from byte 32 to byte 47. Offset 48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63. Offset 64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79.
<b>Time Range Name</b>	Tick the check box and enter the name of the Time Range settings that has been previously configured in the <b>Time Range Settings</b> window. This will set specific times when this access rule will be implemented on the Switch.
<b>Ports</b>	Specifies the access rule can take effect on one port or a range of ports.

To view the settings of a previously correctly configured rule, click the corresponding **Show Details** button on the **CPU Access Rule List** window to view the following window:

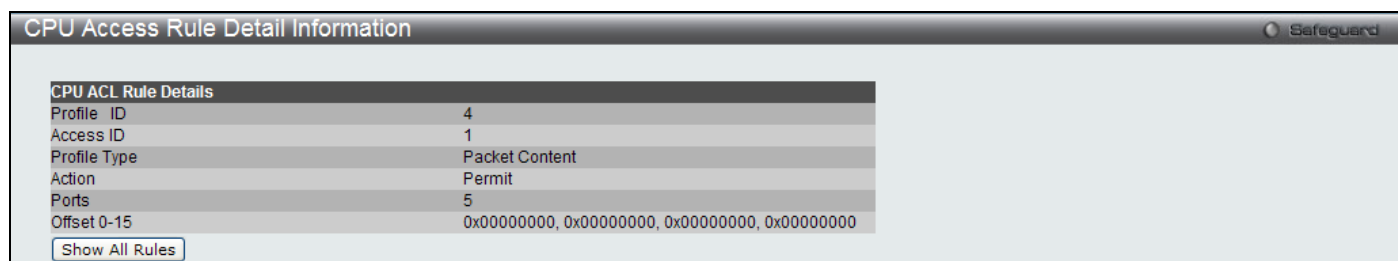


Figure 6 - 48 CPU Access Rule Detail Information window for Packet Content

## ACL Finder

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

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

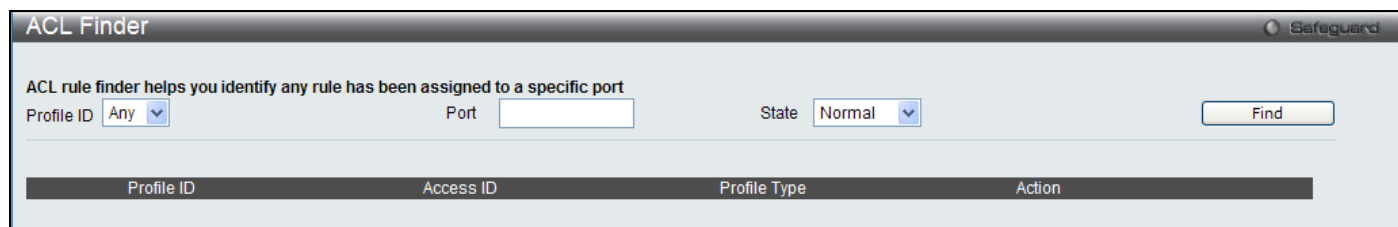
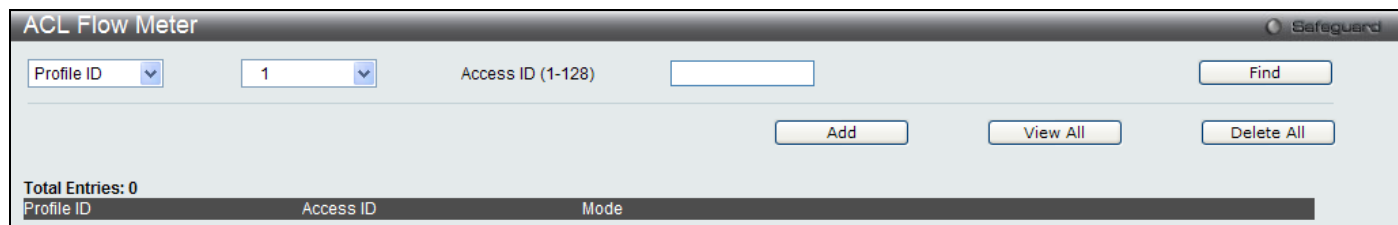


Figure 6 - 49 ACL Finder window

## ACL Flow Meter

ACL Flow Metering Table is a per flow bandwidth control used to limit the bandwidth of the ingress traffic. When the 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 view this window, click **ACL > ACL Flow Meter** as shown below:

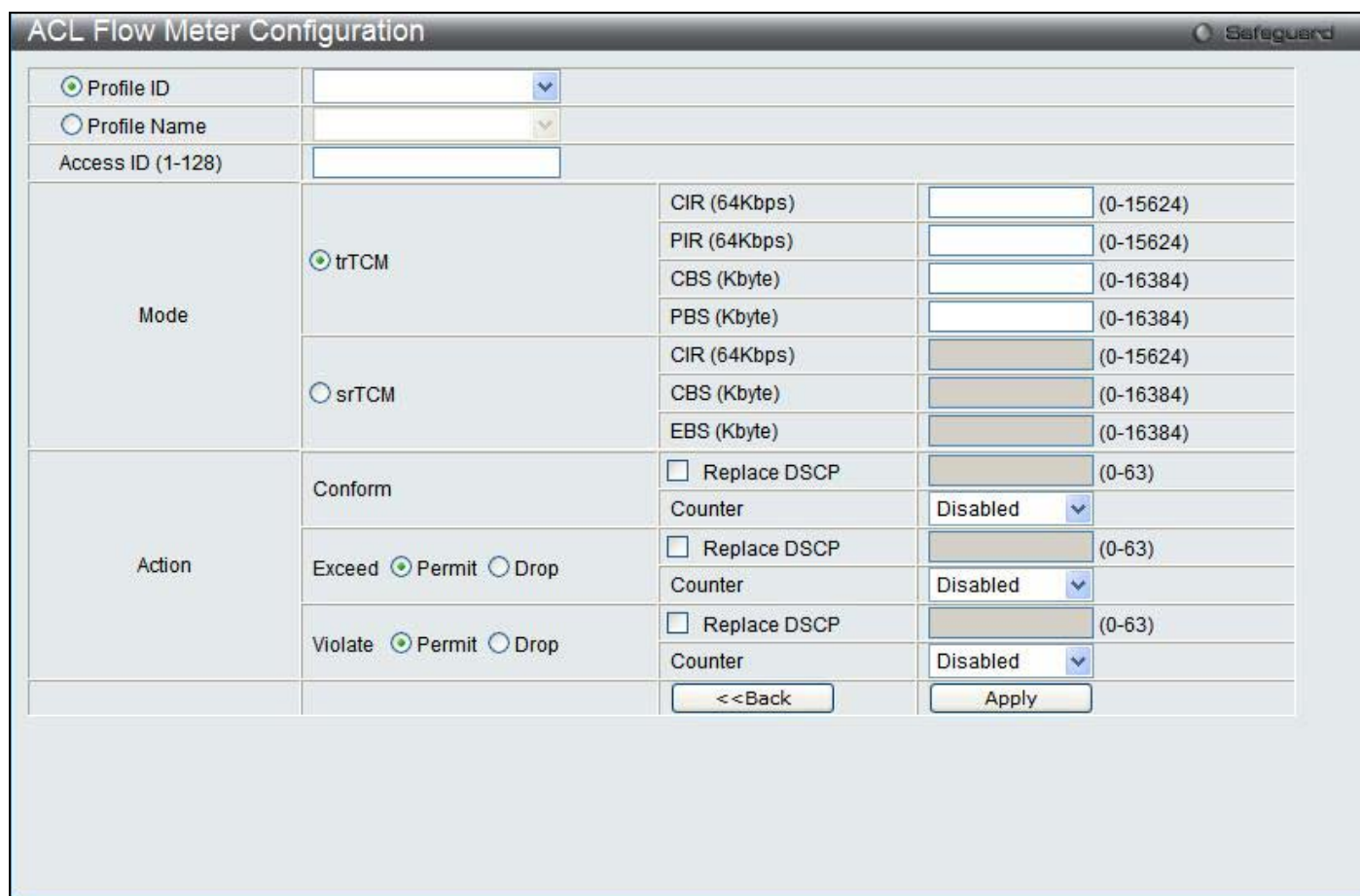


**Figure 6 - 50 ACL Flow Meter window**

The following fields may be configured:

Parameter	Description
<b>Profile ID</b>	The pre-configured Profile ID for which to configure the Flow Metering parameters.
<b>Access ID</b>	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 - 51 ACL Flow Meter - Add window**

The following fields may be configured:

Parameter	Description
<b>Profile ID</b>	Use the drop down menu to select the pre-configured Profile ID that will be used to configure the Flow Metering parameters.
<b>Profile Name</b>	Use the drop down menu to select the pre-configured Profile Name.

<b>Access ID (1-128)</b>	Enter the Access ID that will be used to configure the Flow Metering parameters, enter a value between 1 and 128.
<b>Mode</b>	<p>Select the mode to be used either <i>trTCM</i> or <i>srTCM</i> and enter the corresponding information.</p> <p><b>trTCM</b> – Two Rate Three Color Marker, marks packets green, yellow or red based on two rates and two burst sizes. It is useful when peak rates need to be enforced.</p> <ul style="list-style-type: none"> <li>• <b>CIR(64Kbps) value 0-15624</b> – Specifies the Committed Information Rate of the packet. The unit is 64Kbps. That is to say, 1 means 64Kbps.</li> <li>• <b>PIR(64Kbps) value 0-15624</b> – Specifies the Peak Information Rate of the packet. The unit is 64Kbps. That is to say, 1 means 64Kbps.</li> <li>• <b>CBS(Kbyte) value 0-16384</b> – Specifies the Committed Burst Size of the packet. The unit is Kbyte. That is to say, 1 means 1Kbyte. This parameter is optional and the default value is 4*1024. The max value is 16*1024.</li> <li>• <b>PBS(Kbyte) value 0-16384</b> – Specifies the Peak Burst Size of the packet. The unit is Kbyte. That is to say, 1 means 1Kbyte. This parameter is optional and the default value is 4*1024. The max value is 16*1024.</li> </ul> <p><b>srTCM</b> – Single Rate Three Color Marker, marks packets green, yellow or red based on a rate and two burst sizes. This is useful when only burst size matters.</p> <ul style="list-style-type: none"> <li>• <b>CIR(64Kbps) value 0-15624</b> – Specifies the Committed Information Rate of the packet. The unit is 64Kbps. That is to say, 1 means 64Kbps.</li> <li>• <b>CBS(Kbyte) value 0-16384</b> – Specifies the Committed Burst Size of the packet. The unit is Kbyte. That is to say, 1 means 1Kbyte. The maximum value is 16*1024.</li> <li>• <b>EBS(Kbyte) value 0-16384</b> – Specifies the Excess Burst Size of the packet. The unit is Kbyte. That is to say, 1 means 1Kbyte. The maximum value is 16*1024.</li> </ul>
<b>Action</b>	<p><b>Conform</b> – Specifies the action when the packet is in “green color” mode.</p> <ul style="list-style-type: none"> <li>• <b>Replace DSCP</b> – Allows you to change the dscp of the packet</li> <li>• <b>Counter</b> – Allows you to set the counter of the packet.</li> </ul> <p><b>Exceed</b> – Specifies the action when the packet is in “yellow color” mode.</p> <ul style="list-style-type: none"> <li>• <b>Permit</b> – Permits the packet.</li> <li>• <b>Replace DSCP</b> – Allows you to change the DSCP of the packet.</li> <li>• <b>Counter</b> – Allows you to set the counter of the packet.</li> <li>• <b>Drop</b> – Drops the packet.</li> </ul> <p><b>Violate</b> – Specifies the action when the packet is in “red color” mode.</p> <ul style="list-style-type: none"> <li>• <b>Permit</b> – Permits the packet.</li> <li>• <b>Replace DSCP</b> – Allows you to change the DSCP of the packet.</li> <li>• <b>Counter</b> – Allows you to set the counter of the packet.</li> <li>• <b>Drop</b> – Drops the packet.</li> </ul>

Click **Apply** to implement changes made, click **Back** to return to the ACL Flow Meter.

## Section 7

# Monitoring

*Device Status*

*Cable Diagnostic*

*CPU Utilization*

*Port Utilization*

*Packet Size*

*Memory Utilization*

*Packets*

*Errors*

*Port Access Control*

*Browse ARP Table*

*VLAN*

*IGMP Snooping*

*MLD Snooping*

*Browse Session Table*

*CFM*

*MAC Address Table*

*Browse VLAN Counter Statistics*

*Ethernet OAM*

*Historical Counter & Utilization*

*System Log*

## Device Status

The Device Status window displays status information for Power Status, Temperature and Side Fan Status.

To view this window, click **Monitoring > Device Status** as shown below:



**Figure 7 - 1 Device Status window**

Click the **Refresh** button to update the status table.

## Cable Diagnostic

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 Diagnostic** as shown below:

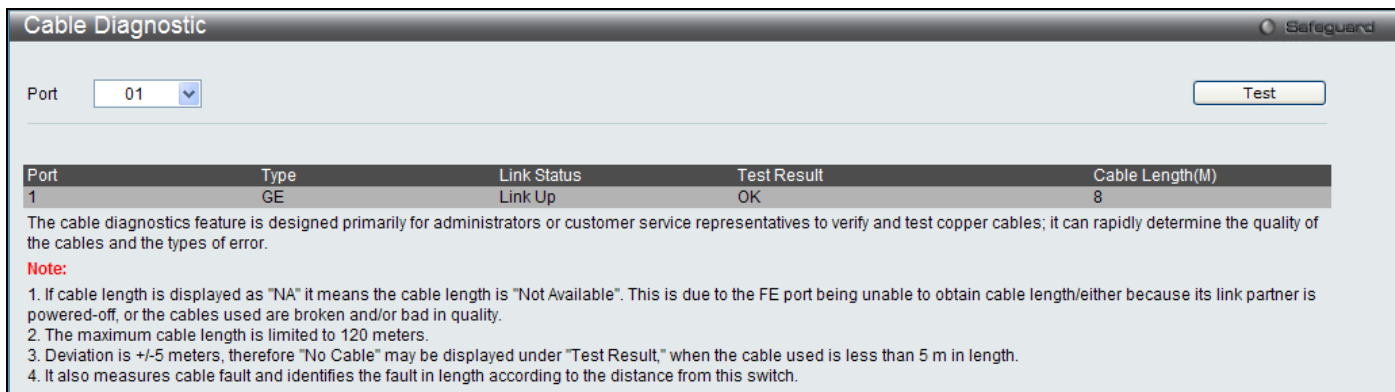


Figure 7 - 2 Cable Diagnostic window

Enter the port number you wish to test and click **Test**, the results will be display on the lower half of the table.

## CPU Utilization

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

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

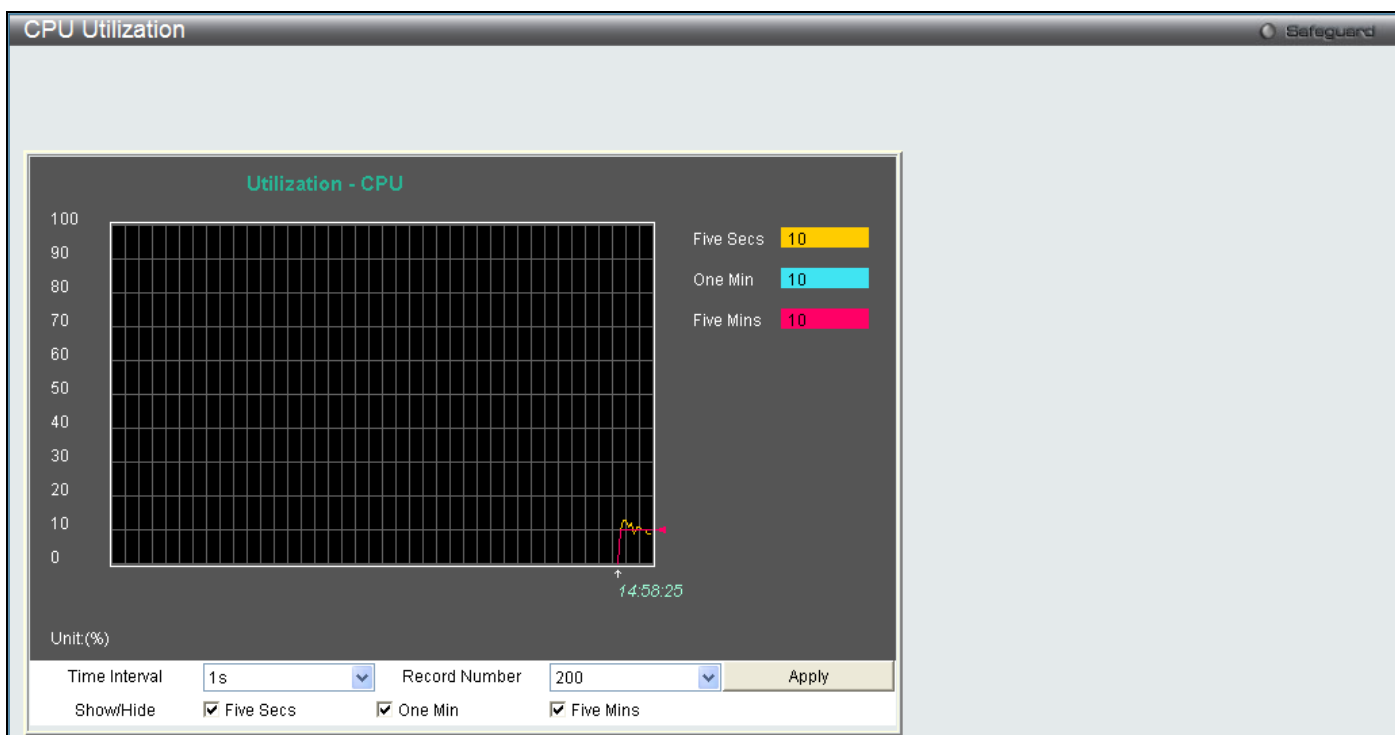


Figure 7 - 3 CPU Utilization window

To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

Change the view parameters as follows:

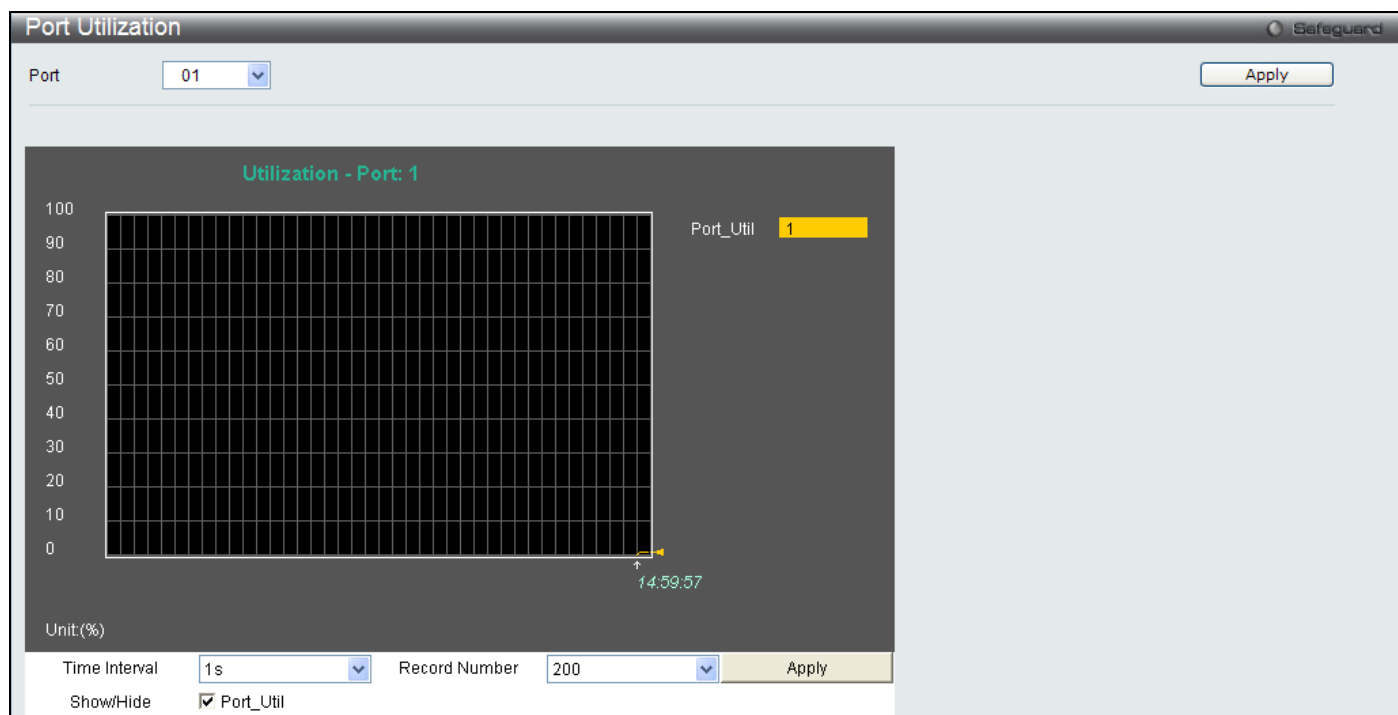
Parameter	Description
<b>Time Interval</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check whether or not to display Five Secs, One Min, and Five Mins.



## Port Utilization

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

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



**Figure 7 - 4 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.

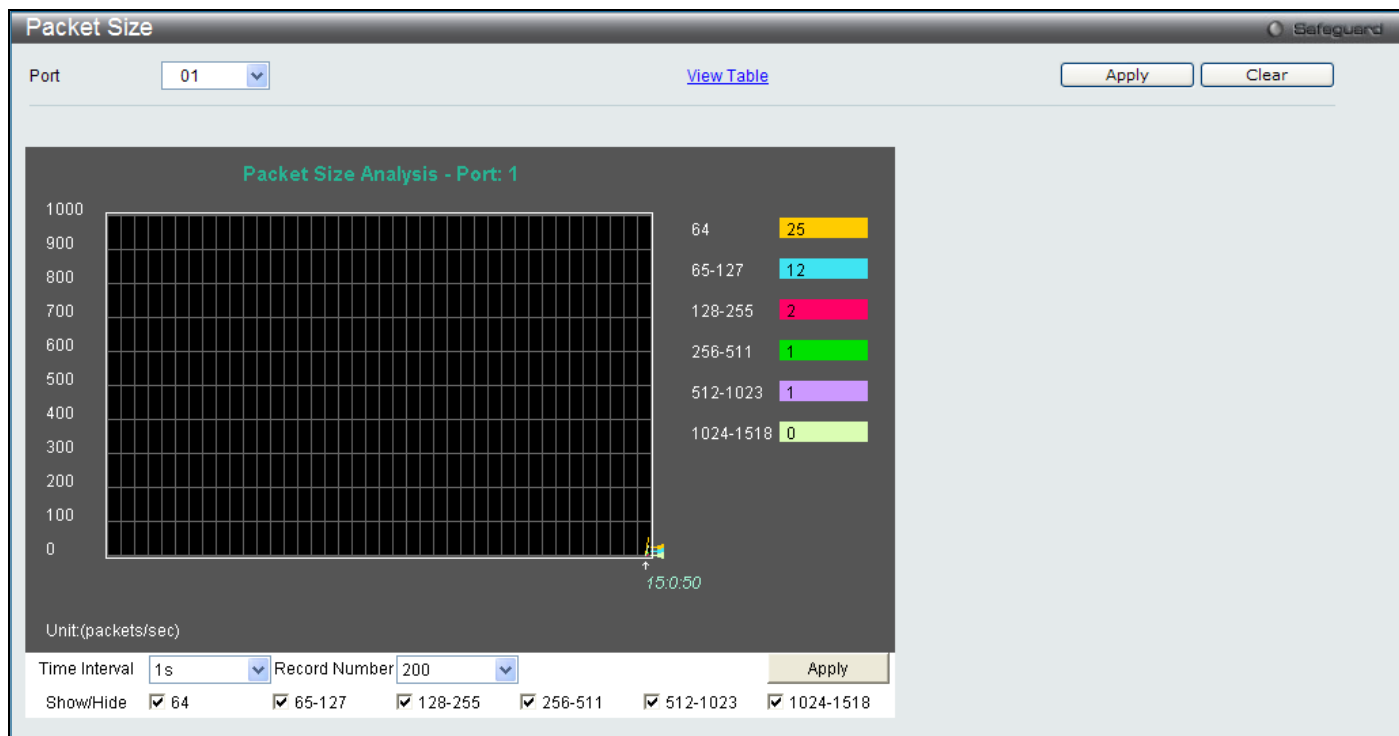
Change the view parameters as follows:

Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is <i>200</i> .
<b>Show/Hide</b>	Check whether or not to display Port Util.

## Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Packet Size** as shown below:



**Figure 7 - 5 Packet Size window**

To view the **Packet Size Table** window, click the link [View Table](#), which will show the following table:



**Figure 7 - 6 Packet Size Table window**

The following fields can be set or viewed:

Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>64</b>	The total number of packets (including bad packets) received that were 64 octets in length

	(excluding framing bits but including FCS octets).
<b>65-127</b>	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).
<b>128-255</b>	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).
<b>256-511</b>	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).
<b>512-1023</b>	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).
<b>1024-1518</b>	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).
<b>Show/Hide</b>	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<a href="#">View Table</a>	Clicking this button instructs the Switch to display a table rather than a line graph.
<a href="#">View Graphic</a>	Clicking this button instructs the Switch to display a line graph rather than a table.

## Memory Utilization

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

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

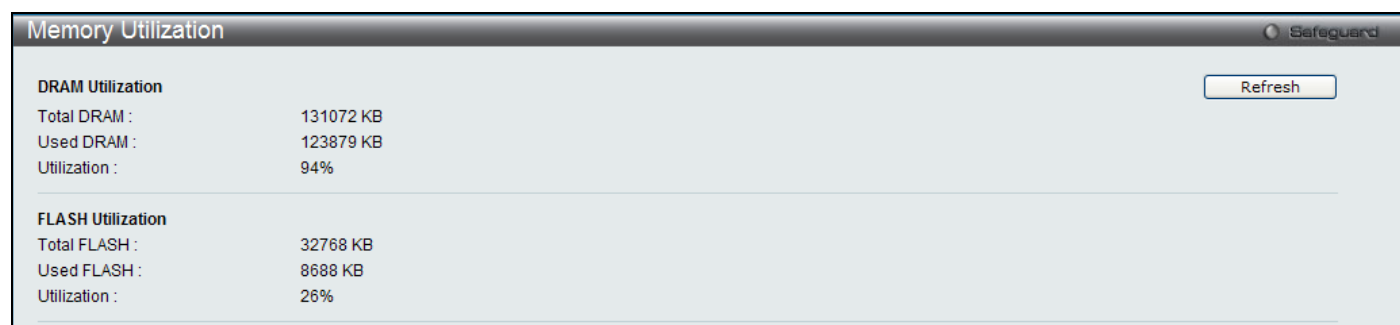


Figure 7 - 7 Packet Size Table window

Click **Refresh** to reload the display.

## Packets

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

### Received (RX)

This table displays the RX packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Packets > Received (RX)** as shown below:

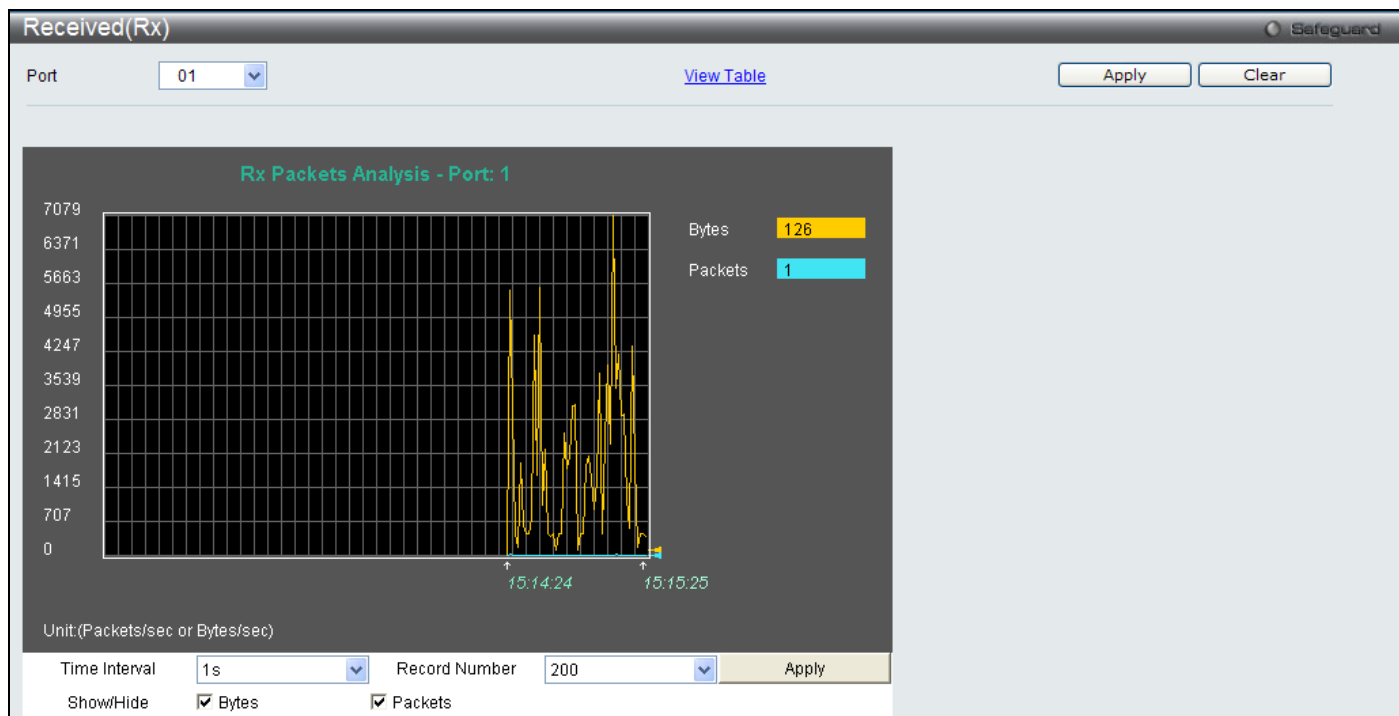


Figure 7 - 8 Received (RX) window (for Bytes and Packets)

To view the Received (RX) Table window, click [View Table](#).



Figure 7 - 9 Received (RX) Table window (for Bytes and Packets)

The following fields may be set or viewed:

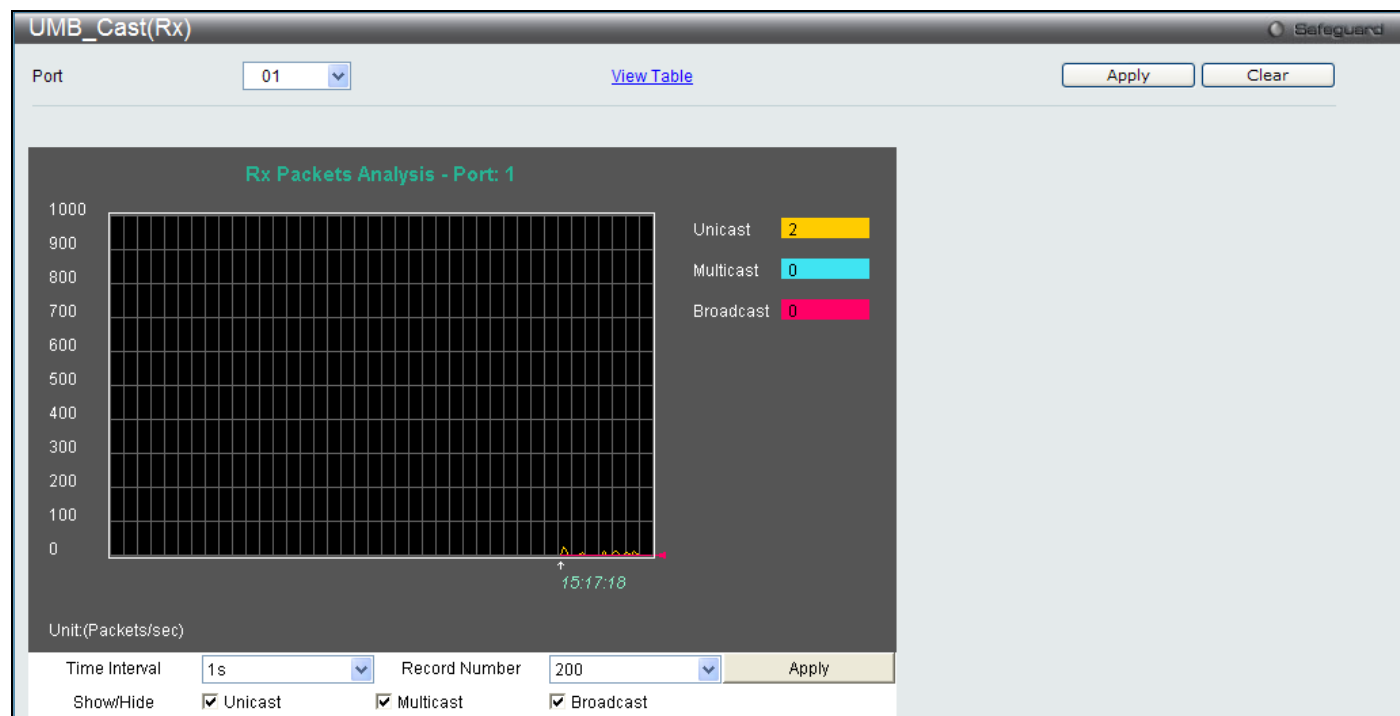
Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

<b>Bytes</b>	Counts the number of bytes received on the port.
<b>Packets</b>	Counts the number of packets received on the port.
<b>Unicast</b>	Counts the total number of good packets that were received by a unicast address.
<b>Multicast</b>	Counts the total number of good packets that were received by a multicast address.
<b>Broadcast</b>	Counts the total number of good packets that were received by a broadcast address.
<b>Show/Hide</b>	Check whether to display Bytes and Packets.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<a href="#">View Table</a>	Clicking this button instructs the Switch to display a table rather than a line graph.
<a href="#">View Graphic</a>	Clicking this button instructs the Switch to display a line graph rather than a table.

## UMB\_cast (RX)

This table displays the UMB\_cast RX Packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Packets > UMB\_cast (RX)** as shown below:



**Figure 7 - 10 UMB\_cast (RX) window (for Unicast, Multicast, and Broadcast Packets)**

To view the **UMB\_cast (RX) Table** window, click the [View Table](#) link.



**Figure 7 - 11 UMB\_cast (RX) Table window (for Unicast, Multicast, and Broadcast Packets)**

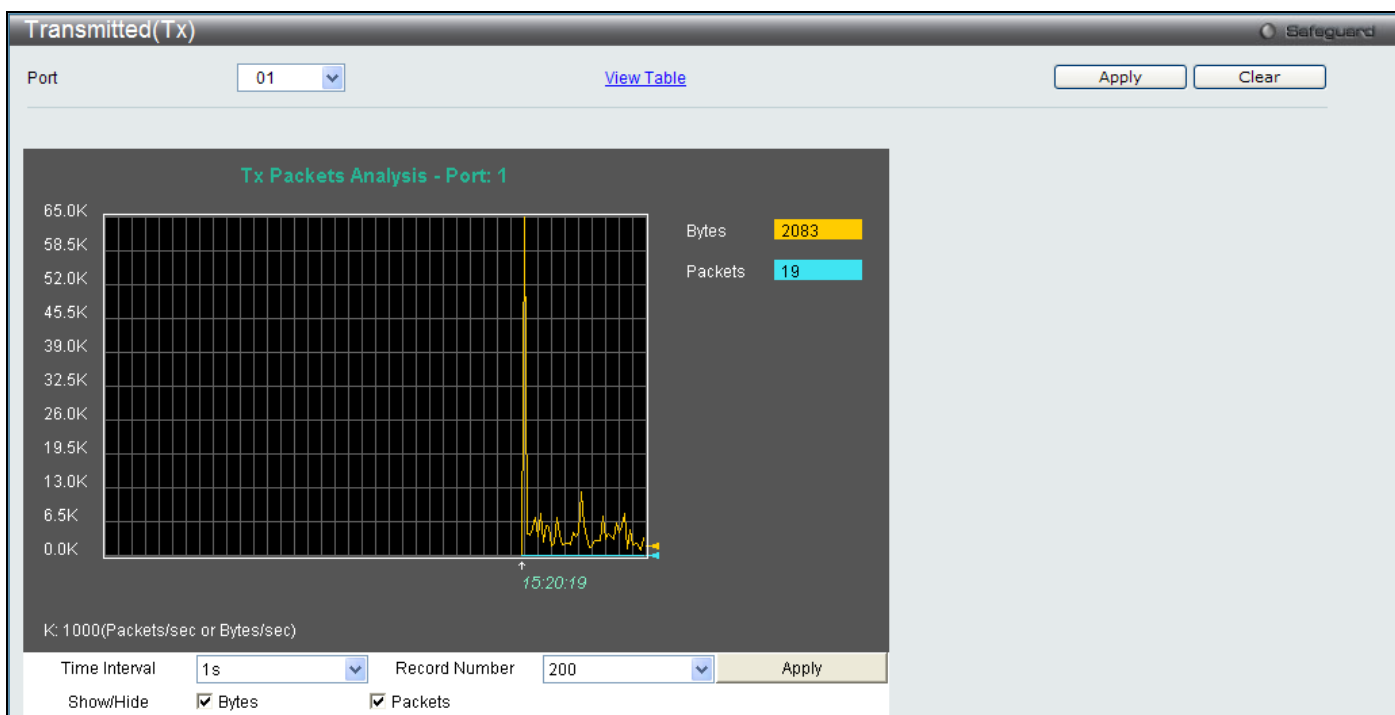
The following fields may be set or viewed:

Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Bytes</b>	Counts the number of bytes successfully sent on the port.
<b>Packets</b>	Counts the number of packets successfully sent on the port.
<b>Unicast</b>	Counts the total number of good packets that were received by a unicast address.
<b>Multicast</b>	Counts the total number of good packets that were received by a multicast address.
<b>Broadcast</b>	Counts the total number of good packets that were received by a broadcast address.
<b>Show/Hide</b>	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<a href="#">View Table</a>	Clicking this button instructs the Switch to display a table rather than a line graph.
<a href="#">View Graphic</a>	Clicking this button instructs the Switch to display a line graph rather than a table.

## Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Packets > Transmitted (TX)** as shown below:



**Figure 7 - 12 Transmitted (TX) window (for Bytes and Packets)**

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



**Figure 7 - 13 Transmitted (TX) Table window (for Bytes and Packets)**

The following fields may be set or viewed:

Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is

	200.
<b>Bytes</b>	Counts the number of bytes successfully sent on the port.
<b>Packets</b>	Counts the number of packets successfully sent on the port.
<b>Unicast</b>	Counts the total number of good packets that were transmitted by a unicast address.
<b>Multicast</b>	Counts the total number of good packets that were transmitted by a multicast address.
<b>Broadcast</b>	Counts the total number of good packets that were transmitted by a broadcast address.
<b>Show/Hide</b>	Check whether or not to display Bytes and Packets.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<a href="#">View Table</a>	Clicking this button instructs the Switch to display a table rather than a line graph.
<a href="#">View Graphic</a>	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 this window, click **Monitoring > Errors > Received (RX)** as shown below:

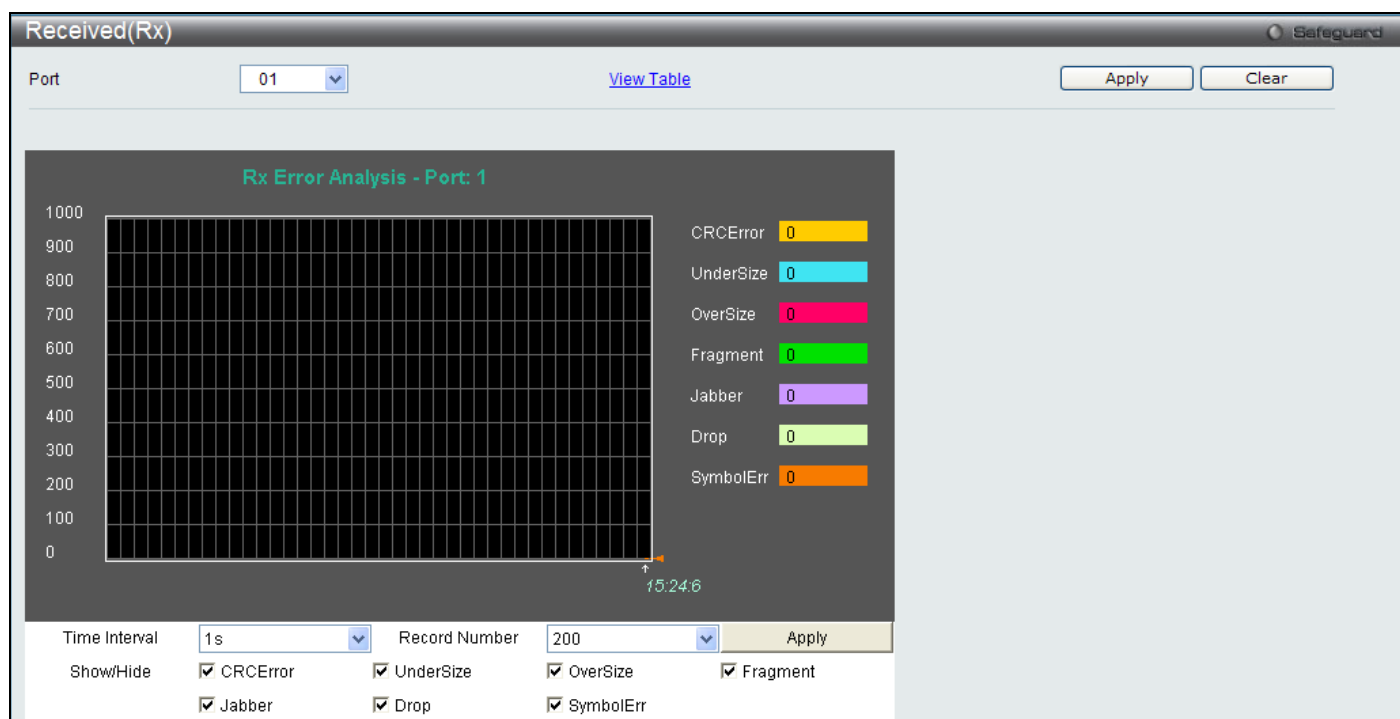


Figure 7 - 14 Received (RX) window (for errors)

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'. A 'View Graphic' link is visible. The main area contains a table with two columns: 'Rx Error' and 'RX Frame'. The table lists seven error types, all with a value of 0. Above the table, there are controls for 'Port: 1', '1s', and an 'OK' button.

Rx Error	RX Frame
CRCError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Drop	0
Symbol	0

Figure 7 - 15 Received (RX) Table window (for errors)

The following fields can be set:

Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is <i>200</i> .
<b>CRCErr</b>	Counts otherwise valid packets that did not end on a byte (octet) boundary.
<b>UnderSize</b>	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.
<b>OverSize</b>	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.
<b>Fragment</b>	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
<b>Jabber</b>	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.
<b>Drop</b>	The number of packets that are dropped by this port since the last Switch reboot.
<b>Symbol</b>	Counts the number of packets received that have errors received in the symbol on the physical labor.
<b>Show/Hide</b>	Check whether or not to display CRCErr, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<a href="#">View Table</a>	Clicking this button instructs the Switch to display a table rather than a line graph.
<a href="#">View Graphic</a>	Clicking this button instructs the Switch to display a line graph rather than a table.

## Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Errors > Transmitted (TX)** as shown below:

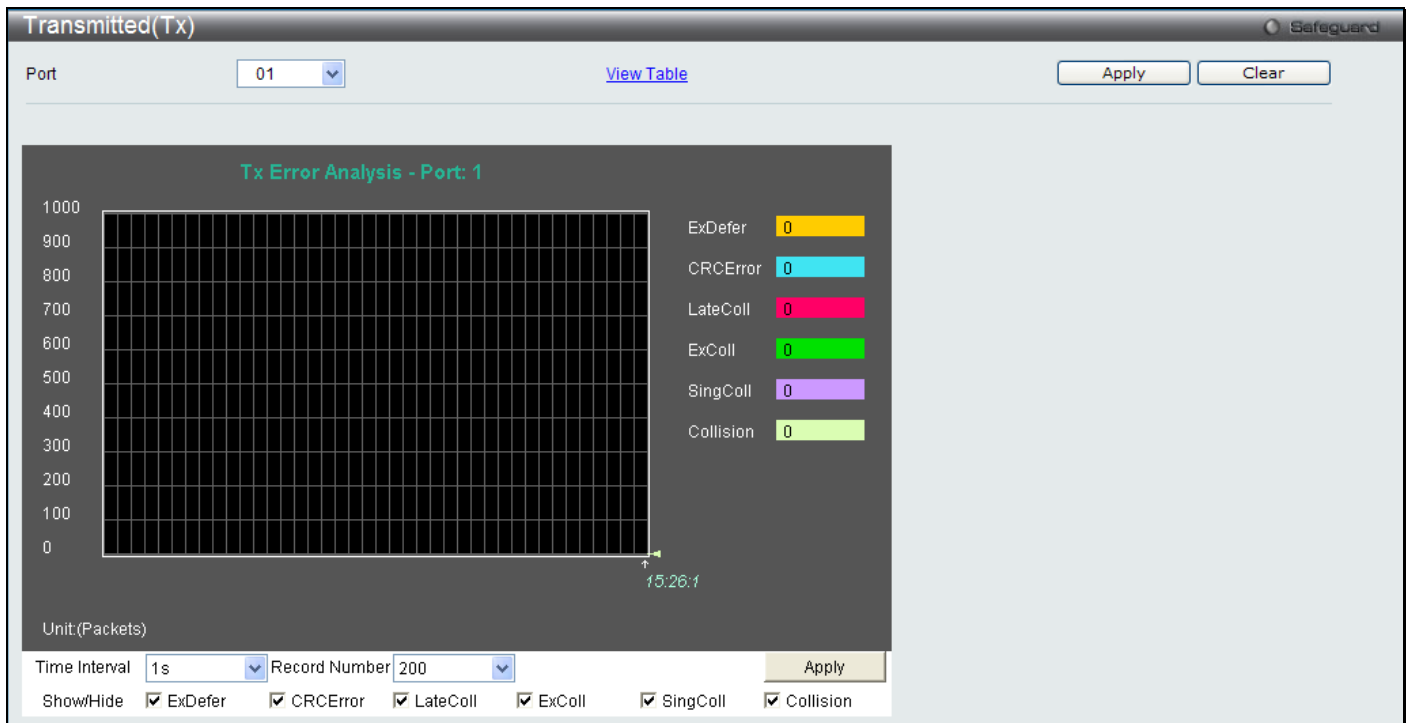


Figure 7 - 16 Transmitted (TX) window (for errors)

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



Figure 7 - 17 Transmitted (TX) Table window (for errors)

The following fields may be set or viewed:

Parameter	Description
<b>Port</b>	Use the drop-down menu to choose the port that will display statistics.
<b>Time Interval</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>ExDefer</b>	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.

<b>CRC Error</b>	Counts otherwise valid packets that did not end on a byte (octet) boundary.
<b>LateColl</b>	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
<b>ExColl</b>	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
<b>SingColl</b>	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
<b>Collision</b>	An estimate of the total number of collisions on this network segment.
<b>Show/Hide</b>	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<a href="#">View Table</a>	Clicking this button instructs the Switch to display a table rather than a line graph.
<a href="#">View Graphic</a>	Clicking this button instructs the Switch to display a line graph rather than a table.

## Port Access Control

The following 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 this window, click **Monitoring > Port Access Control > RADIUS Authentication** as shown below:

ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNum
1	0			0
2	0			0
3	0			0

**Figure 7 - 18 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
<b>InvalidServerAddresses</b>	The number of RADIUS Access-Response packets received from unknown addresses.
<b>Identifier</b>	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same

	as sysName in MIB II.)
<b>ServerIndex</b>	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
<b>AuthServerAddress</b>	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
<b>ServerPortNumber</b>	The UDP port the client is using to send requests to this server.
<b>RoundTripTime</b>	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.
<b>AccessRequests</b>	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
<b>AccessRetransmissions</b>	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
<b>AccessAccepts</b>	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
<b>AccessRejects</b>	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
<b>AccessChallenges</b>	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
<b>AccessResponses</b>	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.
<b>BadAuthenticators</b>	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
<b>PendingRequests</b>	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.
<b>Timeouts</b>	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.
<b>UnknownTypes</b>	The number of RADIUS packets of unknown type which were received from this server on the authentication port
<b>PacketsDropped</b>	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 this window, click **Monitoring > Port Access Control > RADIUS Account Client** as shown below:

ServerIndex	InvalidServerAddr	Identifier	ServerAddr
1	0		
2	0		
3	0		

**Figure 7 - 19 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:

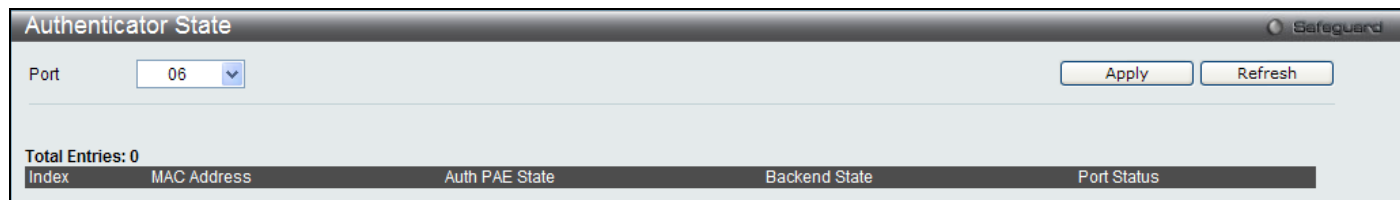
Parameter	Description
<b>InvalidServerAddresses</b>	The number of RADIUS Accounting-Response packets received from unknown addresses.
<b>Identifier</b>	The NAS-Identifier of the RADIUS account. (This is not necessarily the same as sysName in MIB II.)
<b>ServerIndex</b>	The identification number assigned to each RADIUS Accounting server that it shares a secret with.
<b>ServerAddress</b>	The (conceptual) table listing the RADIUS accounting servers with which it shares a secret.
<b>ServerPortNumber</b>	The UDP port it is using to send requests to this server.
<b>RoundTripTime</b>	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
<b>Requests</b>	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
<b>Retransmissions</b>	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.
<b>Responses</b>	The number of RADIUS packets received on the accounting port from this server.
<b>MalformedResponses</b>	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.
<b>BadAuthenticators</b>	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
<b>PendingRequests</b>	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.
<b>Timeouts</b>	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.
<b>UnknownTypes</b>	The number of RADIUS packets of unknown type which were received from this server on the accounting port.

<b>PacketsDropped</b>	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.
-----------------------	--

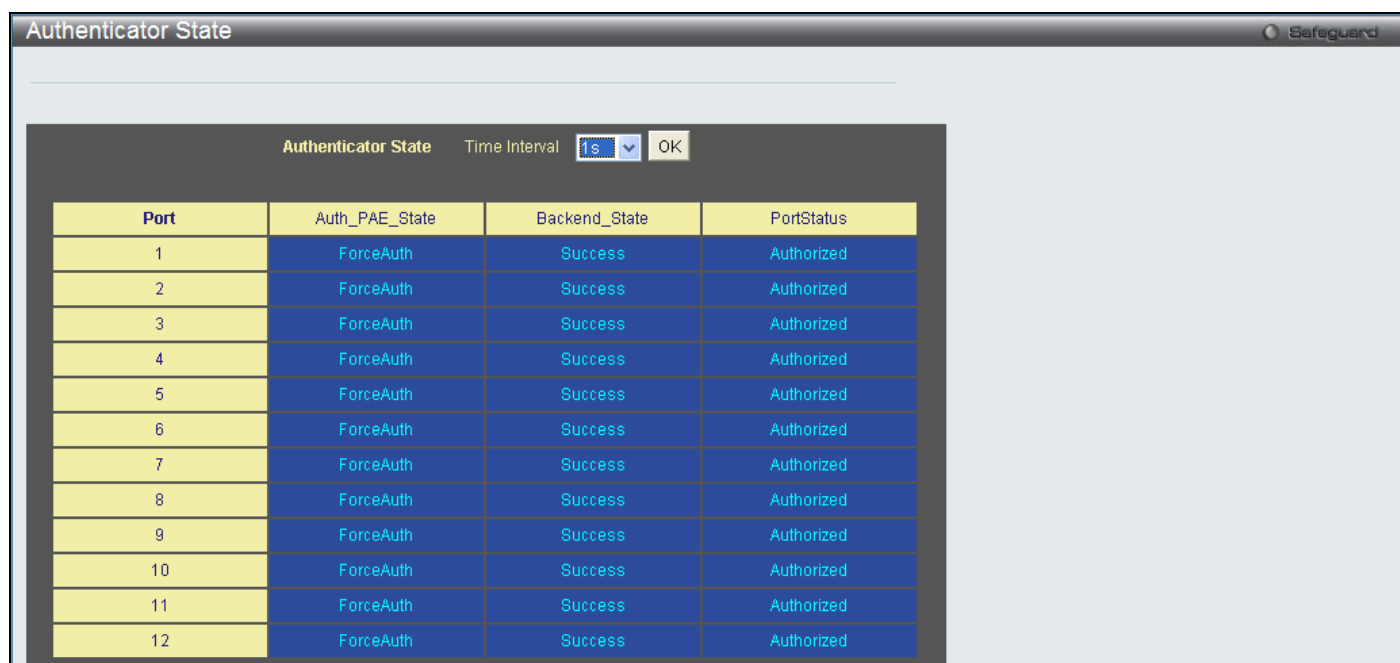
## Authenticator State

The following section describes the 802.1X Status on the Switch.

To view this window, click **Monitoring > Port Access Control > Authenticator State** as shown below:



**Figure 7 - 20 Authenticator State window (for MAC-based 802.1X)**



**Figure 7 - 21 Authenticator State window (for Port-based 802.1X)**

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
<b>MAC Address</b>	The MAC Address of the device of the corresponding index number.
<b>Auth PAE State</b>	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.
<b>Backend State</b>	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.
<b>Port Status</b>	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 this window, click **Monitoring > Port Access Control > Authenticator Statistics** as shown below:

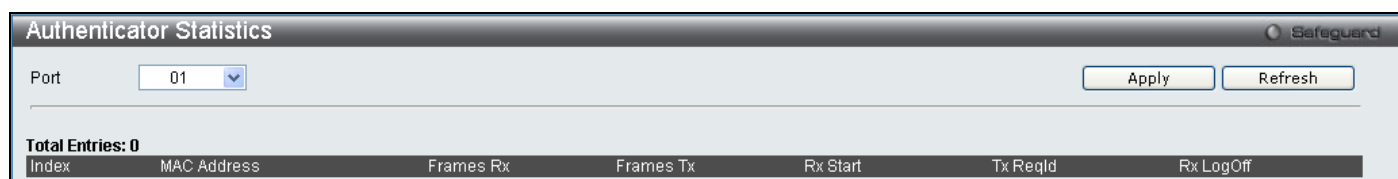


Figure 7 - 22 Authenticator Statistics window (for MAC-based 802.1X)

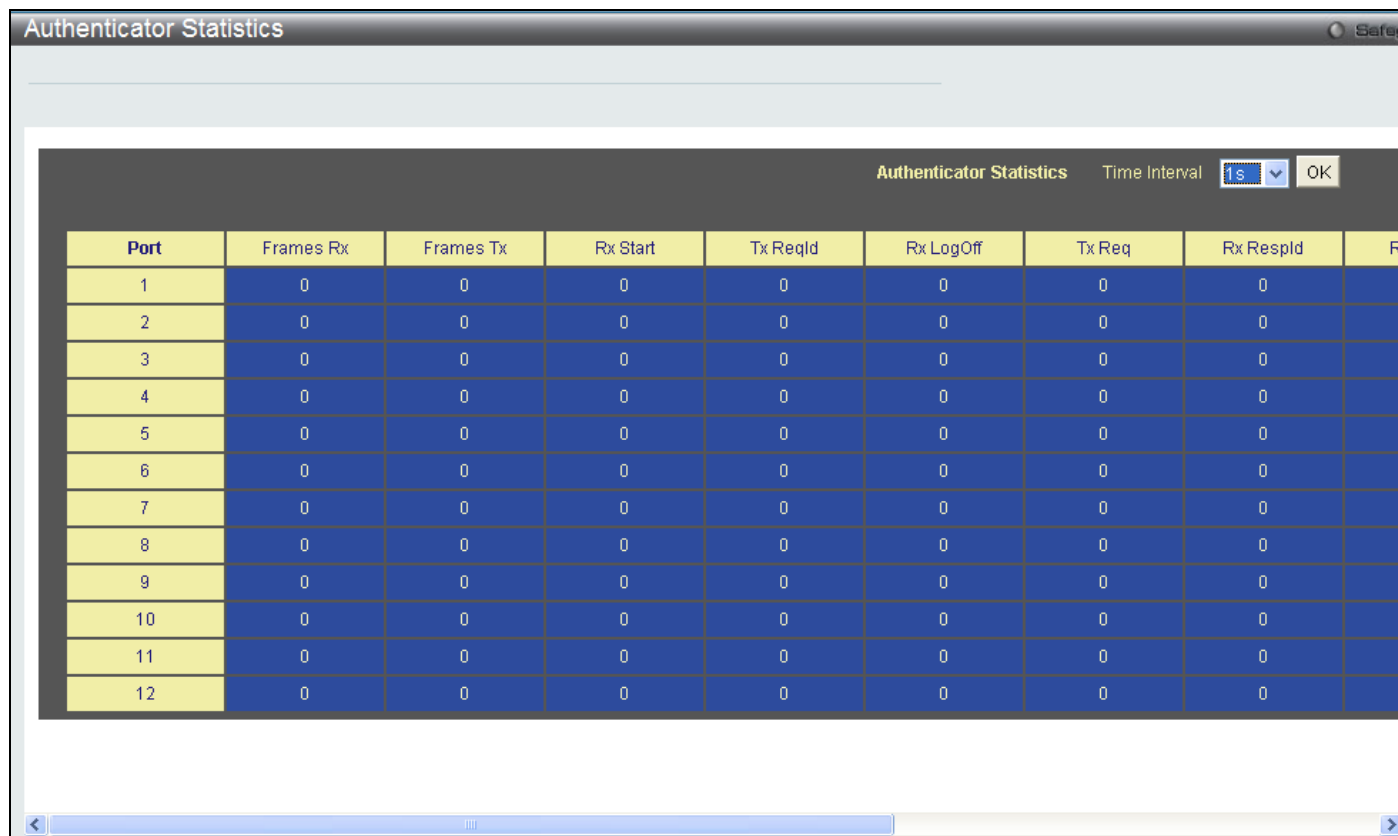


Figure 7 - 23 Authenticator Statistics window (for Port-based 802.1X)

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
<b>Port</b>	The identification number assigned to the Port by the System in which the Port resides.
<b>Frames Rx</b>	The number of valid EAPOL frames that have been received by this Authenticator.
<b>Frames Tx</b>	The number of EAPOL frames that have been transmitted by this Authenticator.
<b>Rx Start</b>	The number of EAPOL Start frames that have been received by this Authenticator.
<b>TxReqId</b>	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
<b>RxLogOff</b>	The number of EAPOL Logoff frames that have been received by this Authenticator.
<b>Tx Req</b>	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
<b>Rx Respld</b>	The number of EAP Resp/Id frames that have been received by this Authenticator.



<b>Rx Resp</b>	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
<b>Rx Invalid</b>	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
<b>Rx Error</b>	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
<b>Last Version</b>	The protocol version number carried in the most recently received EAPOL frame.
<b>Last Source</b>	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 this window, click **Monitoring > Port Access Control > Authenticator Session Statistics** as shown below:

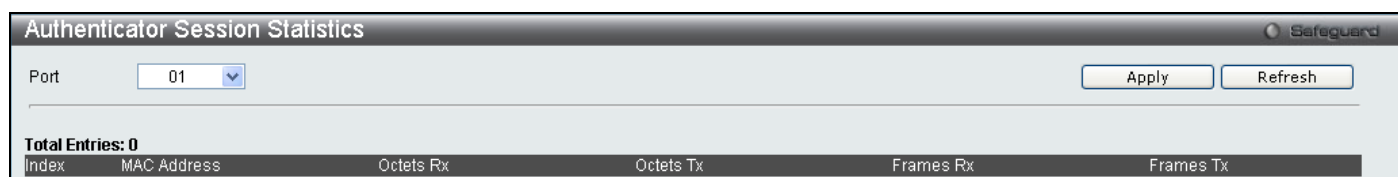


Figure 7 - 24 Authenticator Session Statistics window (for MAC-based 802.1X)

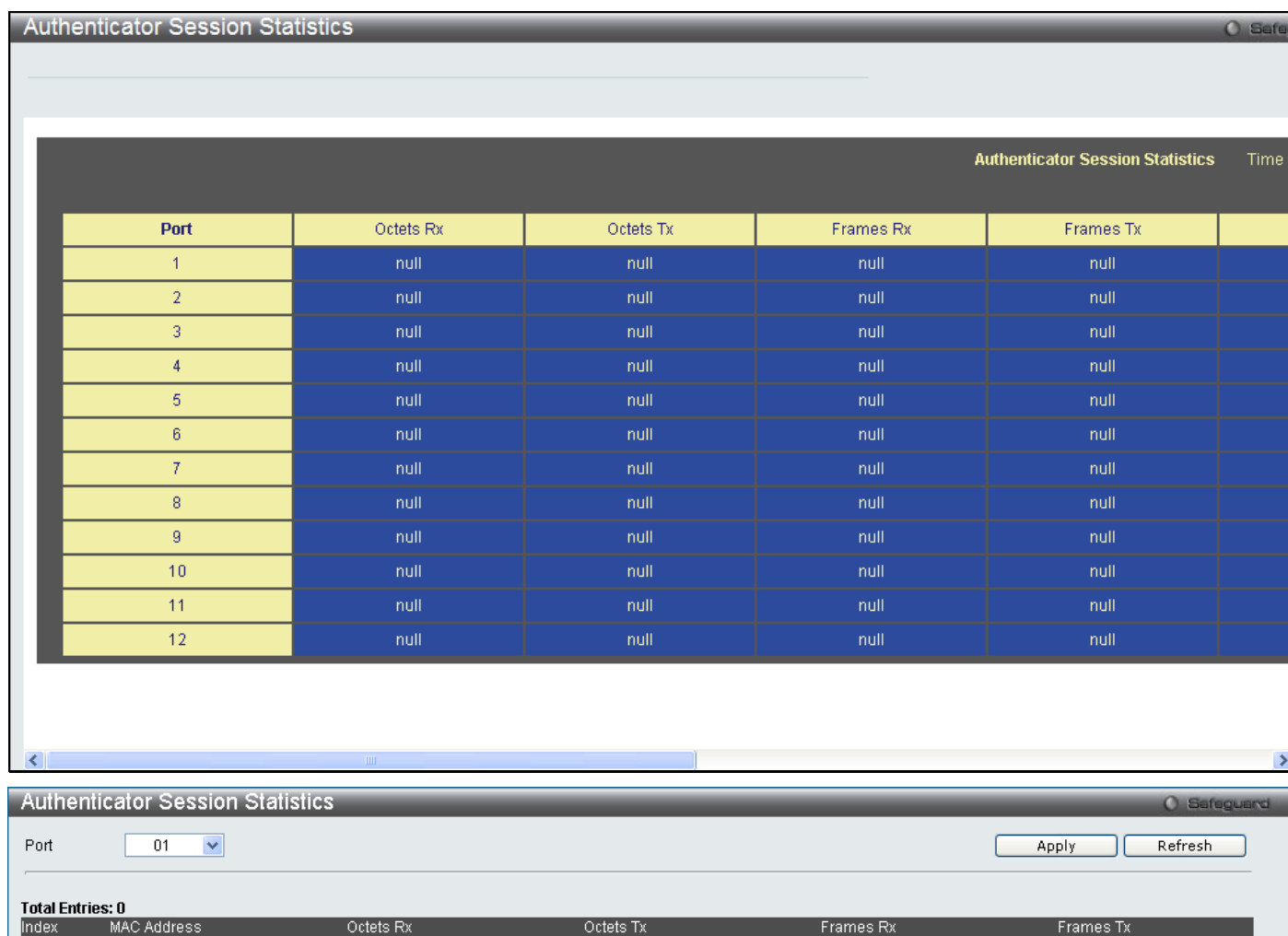


Figure 7 - 25 Authenticator Session Statistics window (for Port-based 802.1X)

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
<b>Port</b>	The identification number assigned to the Port by the System in which the Port resides.
<b>Octets Rx</b>	The number of octets received in user data frames on this port during the session.
<b>Octets Tx</b>	The number of octets transmitted in user data frames on this port during the session.
<b>Frames Rx</b>	The number of user data frames received on this port during the session.
<b>Frames Tx</b>	The number of user data frames transmitted on this port during the session.
<b>ID</b>	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
<b>Authentic Method</b>	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentication Server – The Authentication Server is external to the Authenticator’s System. (2) Local Authentication Server – The Authentication Server is located within the Authenticator’s System.
<b>Time</b>	The duration of the session in seconds.
<b>Terminate Cause</b>	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
<b>UserName</b>	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 this window, click **Monitoring > Port Access Control > Authenticator Diagnostics** as shown below:

The screenshot shows a window titled "Authenticator Diagnostics" with a table containing 7 columns: Port, Connect Enter, Connect LogOff, Auth Enter, Auth Success, Auth Timeout, and Auth Fail. The rows represent ports 1 through 12, with all values in the data columns being 0.

Port	Connect Enter	Connect LogOff	Auth Enter	Auth Success	Auth Timeout	Auth Fail
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

Figure 7 - 26 Authenticator Diagnostics window

The following fields can be viewed:

Parameter	Description
<b>Port</b>	The identification number assigned to the Port by the System in which the Port resides.
<b>Connect Enter</b>	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
<b>Connect LogOff</b>	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
<b>Auth Enter</b>	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.
<b>Auth Success</b>	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).
<b>Auth Timeout</b>	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).
<b>Auth Fail</b>	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).
<b>Auth Reauth</b>	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
<b>Auth Start</b>	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.
<b>Auth LogOff</b>	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.
<b>Authed Reauth</b>	Counts the number of times that the state machine transitions from AUTHENTICATED to

	CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
<b>Authed Start</b>	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.
<b>Authed LogOff</b>	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.
<b>Responses</b>	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.
<b>AccessChallenges</b>	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.
<b>OtherReqToSupp</b>	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.
<b>NonNakRespFromSup</b>	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.
<b>Bac Auth Success</b>	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.
<b>Bac Auth Fail</b>	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** as shown below:

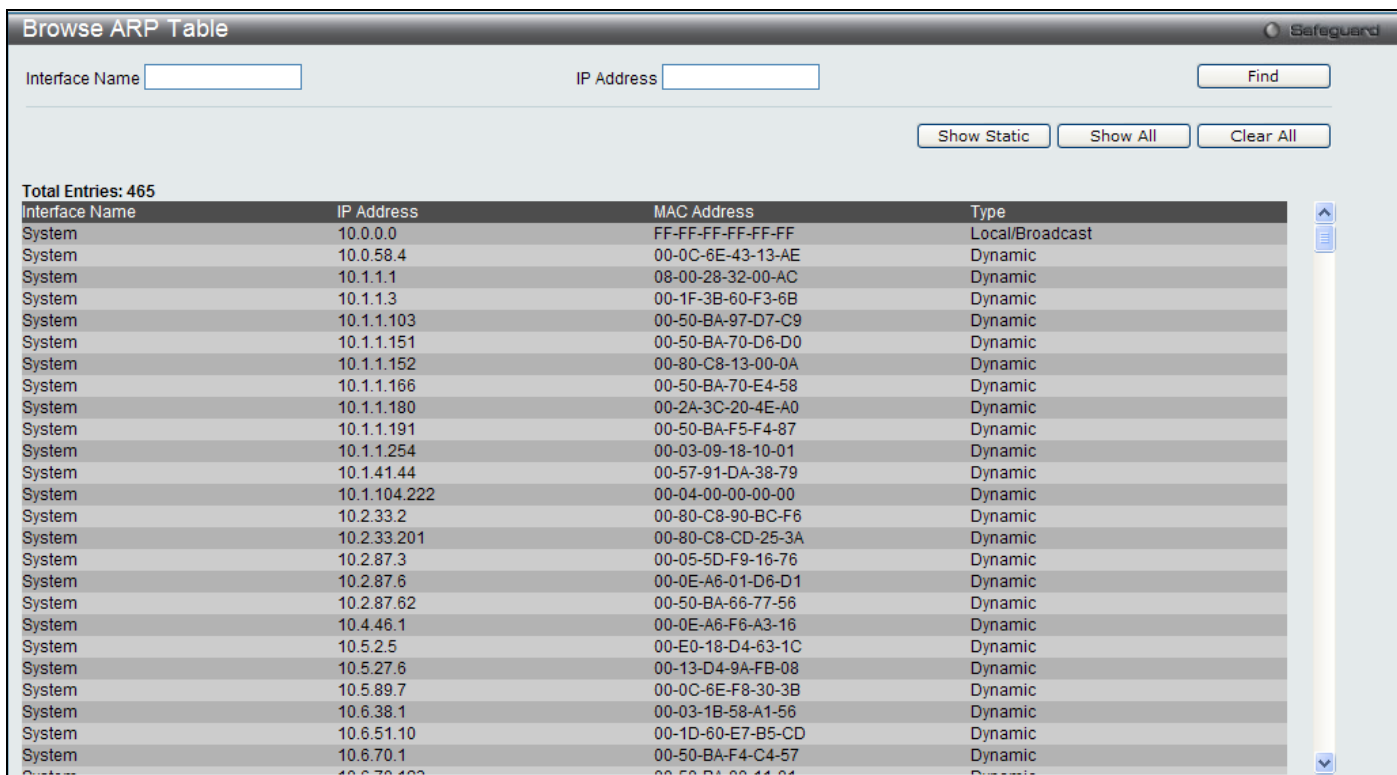


Figure 7 - 27 Browse ARP Table window

## VLAN

The following windows are used to configure the VLAN settings of the Switch.

### 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 > VLAN > Browse VLAN** as shown below:

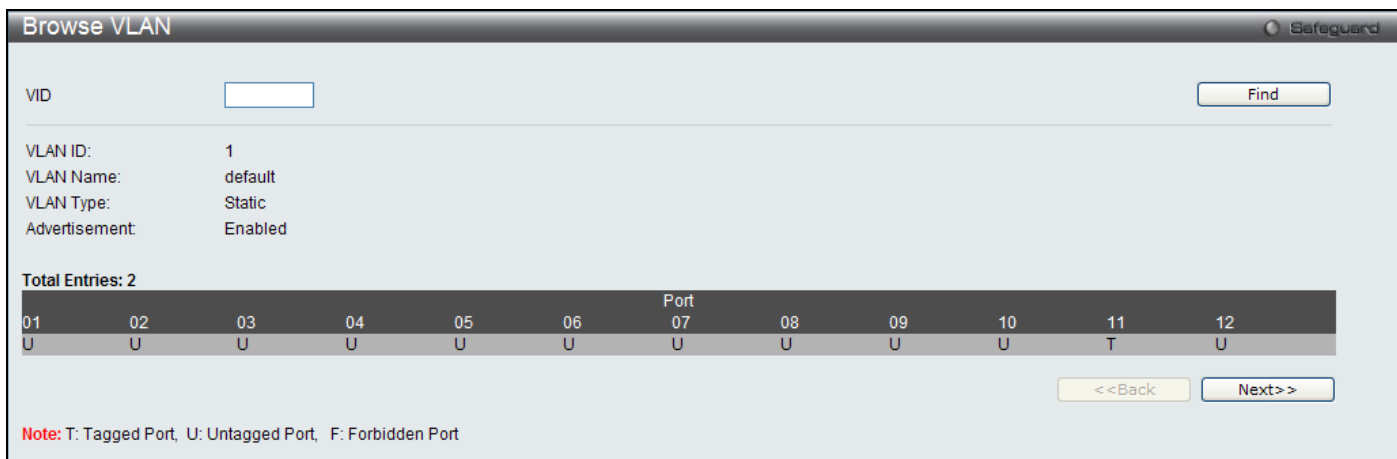


Figure 7 - 28 Browse VLAN window

## Show VLAN Ports

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 > VLAN > Show VLAN Ports** as shown below:

Port	VID	Untagged	Tagged	Dynamic	Forbidden
1	1	X	-	-	-

Figure 7 - 29 Show VLAN Ports 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 view this window, click **Monitoring > IGMP Snooping > Browse IGMP Router Port** as shown below:

01	02	03	04	05	06	Port 07	08	09	10	11	12

Figure 7 - 30 Browse IGMP Router Port window

## IGMP Snooping Group

This window allows the Switch's IGMP Snooping Group Table to be viewed. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The number of IGMP reports that were snooped is displayed in the Reports field.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Group** as shown below:

**Figure 7 - 31 IGMP Snooping Group window**

Enter the appropriate information and click **Find**, the information will be shown in the IGMP Snooping Group Table.

The following field can be viewed:

Parameter	Description
<b>VLAN Name</b>	The VLAN ID of the multicast group.
<b>VLAN List (e.g.:1,4-6)</b>	The VLAN ports of the multicast group.
<b>Group IP Address</b>	The IP address of the multicast group.



**NOTE:** To configure IGMP snooping for the Switch, go to the **L2 Features** folder and select **IGMP Snooping > IGMP Snooping Settings**.

## IGMP Snooping Forwarding Table

This window will display the current IGMP forwarding information on the Switch.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Forwarding Table** as shown below:

**Figure 7 - 32 IGMP Snooping Forwarding Table window**

Enter the *VLAN Name* or *VLAN ID* you wish to view and click **Find**, the information will be displayed in the lower half of the window.

## Browse IGMP Snooping Counter

This window is used to view the current IGMP snooping statistics on the Switch.

To view this window, click **Monitoring > IGMP Snooping > Browse IGMP Snooping Counter** as shown below:

Figure 7 - 33 Browse IGMP Snooping Counter window

Enter the **VLAN Name**, **VLAN List** or **Port List** of the VLAN you wish to view and click **Find**.

## 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 view this window, click **Monitoring > MLD Snooping > Browse MLD Router Port** as shown below:

Figure 7 - 34 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 Name present in the Switch by entering that VLAN Name in the empty field shown below, and clicking the **Find** button. The number of MLD reports that were snooped is displayed in the Reports field.

To view this window, click **Monitoring > MLD Snooping > MLD Snooping Group** as shown below:



MLD Snooping Group Safeguard

VLAN Name   
 VLAN List (e.g.: 1,4-6)   
 Group IP Address

MLD Snooping Group Table Total Entries: 0

VID	VLAN Name	Source	Group	Member Port	Router Port	Group Type	UP Time	Expiry Time	Filter Mode
-----	-----------	--------	-------	-------------	-------------	------------	---------	-------------	-------------

**Figure 7 - 35 MLD Snooping Group window**

Enter a VLAN Name or VLAN List and Group IP Address in the appropriate field and click the **Find** button.

## MLD Snooping Forwarding Table

This window is used to display the current MLD snooping forwarding information on the Switch.

To view this window, click **Monitoring > MLD Snooping > MLD Snooping Forwarding Table** as shown below:

MLD Snooping Forwarding Table Safeguard

VLAN Name 
 VLAN ID (e.g.: 1,4-6)

Total Entries: 0

VLAN Name	Source IP	Multicast Group	Port Member
-----------	-----------	-----------------	-------------

**Figure 7 - 36 MLD Snooping Forwarding Table window**

Enter the appropriate information and click **Find**.

## Browse MLD Snooping Counter

This window is used to display the current MLD snooping counter information on the Switch.

To view this window, click **Monitoring > MLD Snooping > Browse MLD Snooping Counter** as shown below:

Figure 7 - 37 Browse MLD Snooping Counter window

## Browse Session Table

This window displays the management sessions since the Switch was last rebooted.

To view this window, click **Monitoring > Browse Session Table** as shown below:

ID	Live Time	From	Level	Name
8	07:08:28.690	Serial Port	5	Anonymous

Figure 7 - 38 Browse Session Table window

## CFM

The following windows are used to configure the Connectivity Fault Management settings of the Switch.

## CFM Packet Counter List

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 List** as shown below:

Port	AllPkt	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

Note:CCM:Continuity Check Message , (LBM,LBR):Loopback Message and Response , (LTM,LTR):Linktrace Message and Response

Figure 7 - 39 CFM Packet Counter List window

## CFM Packet Counter CCM List

This window displays the CCM database entries on the Switch.

To view this window, click **Monitoring > CFM > CFM Packet Counter CCM List** as shown below:

MEP Name	VID	Port	Level	Direction	XCON	Error	Normal
Total:					0	0	0

Figure 7 - 40 CFM Packet Count CCM List window

## Browse CFM Fault MEP

This window will display the fault conditions detected by the MEPs on the Switch.

To view this window, click **Monitoring > CFM > Browse CFM Fault MEP** as shown below:

MD Name	MA Name	MEPID	Status
<i>Note:MD (Max:22 characters):Maintenance Domain , MA (Max:22 characters):Maintenance Association , MEP:Maintenance Endpoint</i>			

Figure 7 - 41 Browse CFM Fault MEP window

## Browse CFM Port MP List

This window is used to browse the CFM port MP list on the Switch.

To view this window, click **Monitoring > CFM > Browse CFM Port MP List** as shown below:

MD Name	MA Name	MEPID	Level	Direction	VID
<i>Note:MD:Maintenance Domain , MA:Maintenance Association , MEP:Maintenance Endpoint</i>					

Figure 7 - 42 Browse CFM Port MP List window

The following parameters can be configured:

Parameter	Description
<b>Port</b>	The port to which the MAC address below corresponds.
<b>Level (0-7)</b>	The MD level of the entry you wish to view.
<b>Direction</b>	The direction of the MEP. <i>Inward</i> indicates an inward facing MEP. <i>Outward</i> indicates an outward facing MEP.
<b>VLAN ID</b>	The VLAN identifier of the entry you wish to view.

Click **Find** to see the entry displayed in the table.

## 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 this window, click **Monitoring > MAC Address Table** as shown below:

VID	VLAN Name	MAC Address	Port	Type
1	default	00-00-30-28-00-01	5	Dynamic
1	default	00-00-32-00-28-01	5	Dynamic
1	default	00-00-81-00-00-01	5	Dynamic
1	default	00-00-81-9A-F2-F4	5	Dynamic
1	default	00-00-E2-2F-44-EC	5	Dynamic
1	default	00-00-EB-A4-50-5A	5	Dynamic
1	default	00-00-F0-78-EB-00	5	Dynamic
1	default	00-01-11-22-33-02	5	Dynamic
1	default	00-01-6C-CE-62-E0	5	Dynamic
1	default	00-02-A5-FD-66-97	5	Dynamic

Figure 7 - 43 MAC Address Table window

The functions used in the MAC address table are described below:

Parameter	Description
<b>Port</b>	The port to which the MAC address below corresponds.
<b>VLAN Name</b>	Enter a VLAN Name for the forwarding table to be browsed by.
<b>MAC Address</b>	Enter a MAC address for the forwarding table to be browsed by.
<b>Find</b>	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
<b>Clear Dynamic Entries</b>	Clicking this button will allow the user to delete all dynamic entries of the address table.
<b>View All Entry</b>	Clicking this button will allow the user to view all entries of the address table.
<b>Clear All Entry</b>	Clicking this button will allow the user to delete all entries of the address table.

## Browse VLAN Counter Statistics

This window is used to view the VLAN properties including received packets and received byte statistics.

To view this window, click **Monitoring > Browse VLAN Counter Statistics Table** as shown below:

VID	Port	Frame Type	RX Frames / RX Bytes	Frames Per Sec / Bytes Per Sec
-----	------	------------	----------------------	--------------------------------

Figure 7 - 44 Browse VLAN Counter Statistics window

The functions used in the VLAN Counter Statistic table are described below:

Parameter	Description
<b>VID List (e.g.:1,4-6)</b>	Specifies the VLAN ID list that you wish to view.
<b>VLAN Name</b>	Specifies the VLAN Name.
<b>VID (1-4094)</b>	Specifies the VLAN ID.
<b>Port List</b>	Specifies the ports that are attached to the VLAN.

Enter the appropriate information and click **Find**, the information will be displayed in the VLAN Counter Statistics Table. To remove an entry enter the appropriate information and click **Clear**, to remove all entries click **Clear All**.

## 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 - 45 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:

**Browse Ethernet OAM Statistics** Safeguard

Port List (e.g.:1,4-6)   All Ports Clear

---

**Ethernet OAM Statistics**

**Port 1**

Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDU Tx	0	Organization Specific OAMPDU Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		

**Port 2**

Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDU Tx	0	Organization Specific OAMPDU Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		

**Port 3**

Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDU Tx	0	Organization Specific OAMPDU Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		

**Port 4**

Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDU Tx	0	Organization Specific OAMPDU Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		

Figure 7 - 46 Browse Ethernet OAM Statistics window

## Historical Counter & Utilization

This folder contains two windows to view statistics about packets sent and received by the Switch and Historical Utilization of the CPU and memory.

### Browse Historical Counter

This window is used to display statistics about the packets sent and received by the Switch. The counters are set up in 15 minute and one day intervals. There is a maximum of five 15 minute historical statistic entries supported for each port, with one being the most recent 15 minutes of data. The Switch also displays statistics based on a per day basis, with a maximum of two historical statistic entries supported.

To view this window, click **Monitoring > Historical Counter & Utilization > Browse Historical Counter** as shown below:

**Figure 7 - 47 Browse Historical Counter window**

The following parameters may be configured:

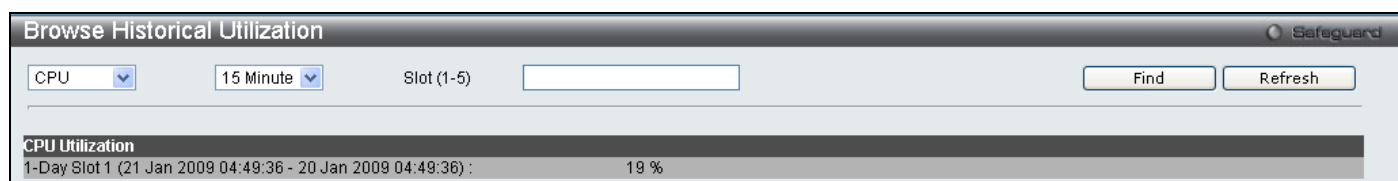
Parameter	Description
<b>Port</b>	Specifies the port you wish to view.
<b>Packet/Error</b>	Specifies information regarding valid packets or error packets.
<b>15 Minutes/1 Day</b>	Choose whether to view information relating to 15 minute intervals or 1 day intervals. <i>15 Minutes</i> – Specifies statistics based on 15 minute intervals. <i>1 Day</i> – Specifies statistics based on one day intervals.
<b>Slot 1-5</b>	Specifies the slot number to display. <i>1-5</i> – Specifies that the 15 minute intervals will be displayed in chronological order with 1 being the most recent. <i>1-2</i> – Specifies that the daily intervals will be displayed in chronological order with 1 being the most recent.

Enter the appropriate information and click **Find**.

## Browse Historical Utilization

This window displays information regarding the historical utilization of the CPU and memory. The counters are set up in 15 minute and one day intervals. There is a maximum of five 15 minute historical utilization entries supported for each port, with one being the most recent 15 minutes of data. The Switch also displays utilization information based on a per day basis, with a maximum of two historical statistic entries supported.

To view this window, click **Monitoring > Historical Counter & Utilization > Browse Historical Utilization** as shown below:



**Figure 7 - 48 Browse Historical Utilization window**

The following parameters may be configured:

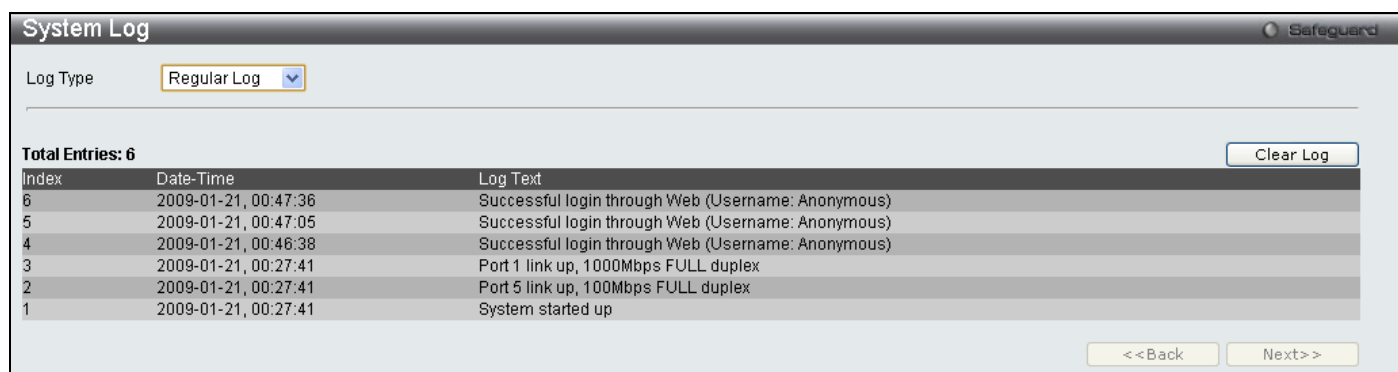
Parameter	Description
<b>CPU/Memory</b>	Specify CPU or Memory to display the historical utilization information.
<b>15 Minutes/1 Day</b>	Choose whether to view information relating to 15 minute intervals or 1 day intervals. <i>15 Minutes</i> – Specifies historical utilization information based on 15 minute intervals. <i>1 Day</i> – Specifies historical utilization information based on one day intervals.
<b>Slot 1-5</b>	Specifies the slot number to display. <i>1-5</i> – Specifies that the 15 minute intervals will be displayed in chronological order with 1 being the most recent. <i>1-2</i> – Specifies that the daily intervals will be displayed in chronological order with 1 being the most recent.

Enter the appropriate information and click **Find** the information will be displayed in the CPU Utilization table.

## System Log

This window is used to view the Switch's history log, as compiled by the Switch's management agent.

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



**Figure 7 - 49 System Log window**

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Click **Next** to go to the next page of the **System Log** window. Clicking **Clear Log** will allow the user to clear the Switch History Log.

The information in the table is categorized as:



Parameter	Description
<b>Log Type</b>	Choose the type of log to view. There are two choices: <i>Regular Log</i> – Choose this option to view regular switch log entries, such as logins or firmware transfers. <i>Attack Log</i> – Choose this option to view attack log files, such as spoofing attacks.
<b>Index</b>	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
<b>Date-Time</b>	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
<b>Log Text</b>	Displays text describing the event that triggered the history log entry.

## Section 8

# Save Services and Tools

**Save Configuration ID 1**

**Save Configuration ID 2**

**Save Log**

**Save All**

**Configuration File Backup & Restore**

**Upload Log File**

**Reset**

**Download Firmware**

**Reboot System**

The four **Save** windows include: **Save Configuration 1**, **Save Configuration 2**, **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\_ID\_1** to save the configuration file indexed as Image file 1. To use this file for configuration it must be designated as the *Boot* configuration.
- **Save Configuration\_ID\_2** to save the configuration file indexed as Image file 2. To use this file for configuration it must be designated as the *Boot* configuration.
- **Save Log** to save only the current log.
- **Save All** to save the current configuration file indexed as Image file 1 and save the current log.

## Save Configuration ID 1

Open the **Save** drop-down menu at the top of the Web manager and click **Save Configuration ID 1** to open the following window:

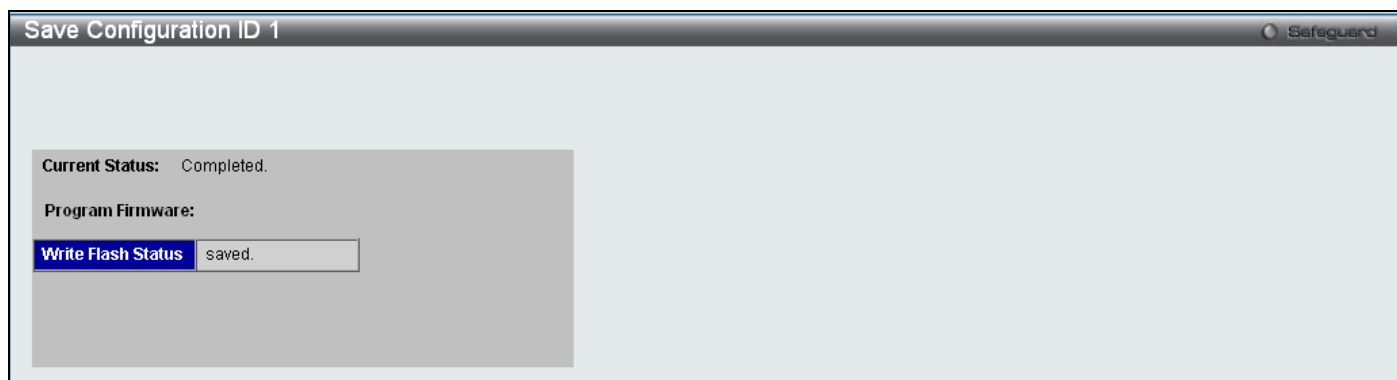


Figure 8 - 1 Save Configuration ID 1 window

## Save Configuration ID 2

Open the **Save** drop-down menu at the top of the Web manager and click **Save Configuration ID 2** to open the following window:

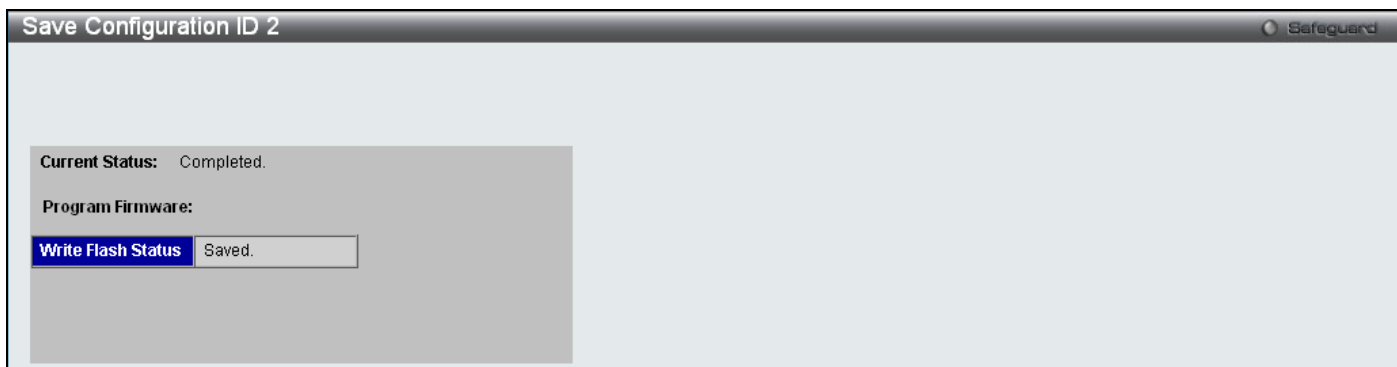


Figure 8 - 2 Save Configuration ID 2 window

## Save Log

Open the **Save** drop-down menu at the top of the Web manager and click **Save Log** to open the following window:

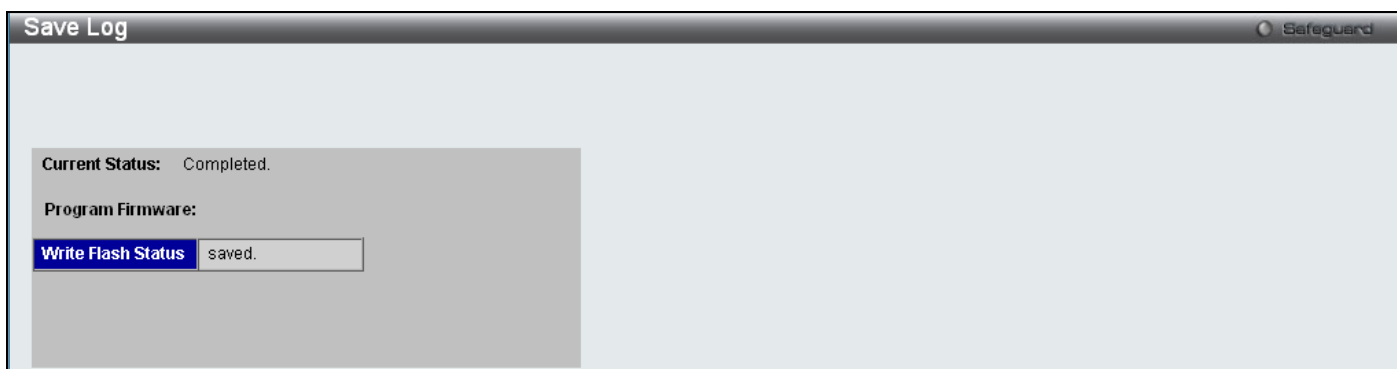


Figure 8 - 3 Save Log window

## Save All

Open the **Save** drop-down menu at the top of the Web manager and click **Save All** to open the following window:

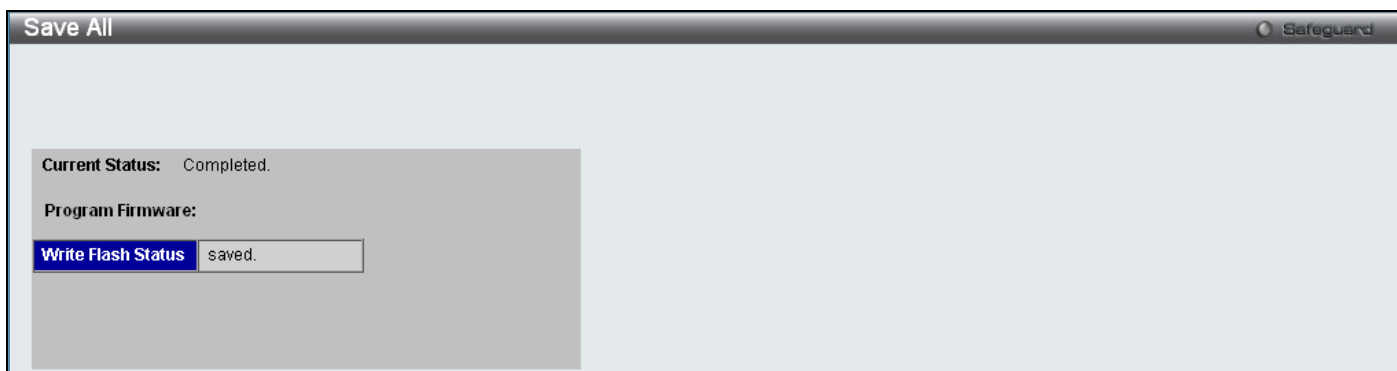


Figure 8 - 4 Save All window

## Configuration File Backup & Restore

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

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

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

Figure 8 - 5 Configuration File Backup & Restore window

## Upload Log File

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

Figure 8 - 6 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.

Option	Description
<input checked="" type="radio"/> Reset	Proceed with system reset except IP address, log, user account and banner.
<input type="radio"/> Reset Config	Switch will be reset to factory defaults.
<input type="radio"/> Reset System	Switch will be reset to factory defaults and reboot.

Figure 8 - 7 Reset System window

## Download Firmware

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

Figure 8 - 8 Download Firmware window

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

## Reboot System

The following window is used to restart the Switch.

Figure 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

## Mitigating ARP Spoofing Attacks Using Packet Content ACL

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. This protocol is vulnerable because it can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce ARP protocol, ARP spoofing attacks, and the counter measure brought by D-Link's switches to counter the ARP spoofing attack.

- How Address Resolution Protocol works**

In the process of ARP, PC A will, firstly, issue an ARP request to query PC B's MAC address. The network structure is shown in Figure-1.

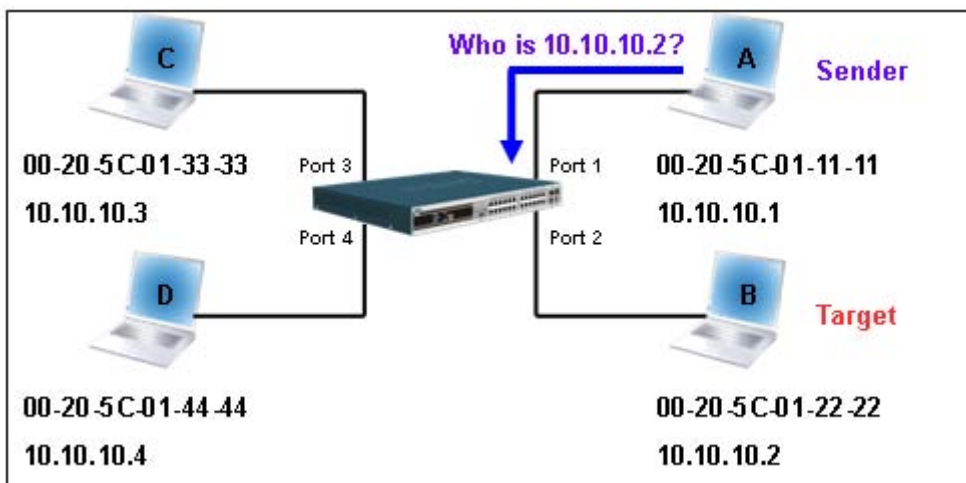


Figure-1

In the mean time, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00" while PC B's IP address will be written into the "Target Protocol Address", shown in Table-1.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP request	00-20-5C-01-11-11	<u>10.10.10.1</u>	<u>00-00-00-00-00-00</u>	<u>10.10.10.2</u>

Table -1 (ARP Payload)

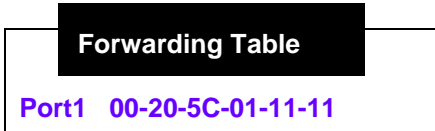
The ARP request will be encapsulated into Ethernet frame and sent out. As can be seen in Table-2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via a broadcast, the "Destination address" is in the format of an Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Destination	Source address	Ether-type	ARP	FCS
-------------	----------------	------------	-----	-----

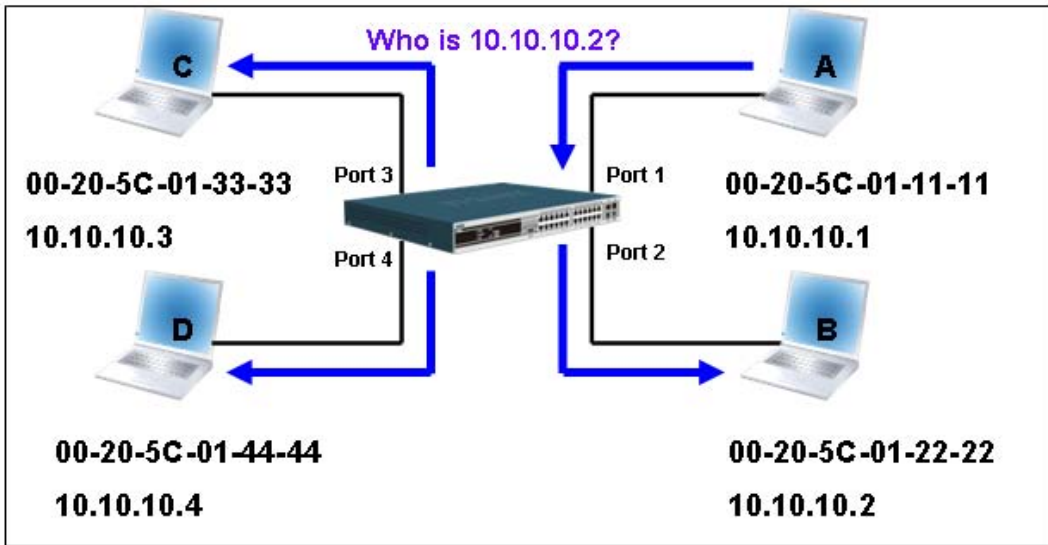
<b>address</b>				
<u>FF-FF-FF-FF-FF-FF</u>	<u>00-20-5C-01-11-11</u>			

**Table-2 (Ethernet frame format)**

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.

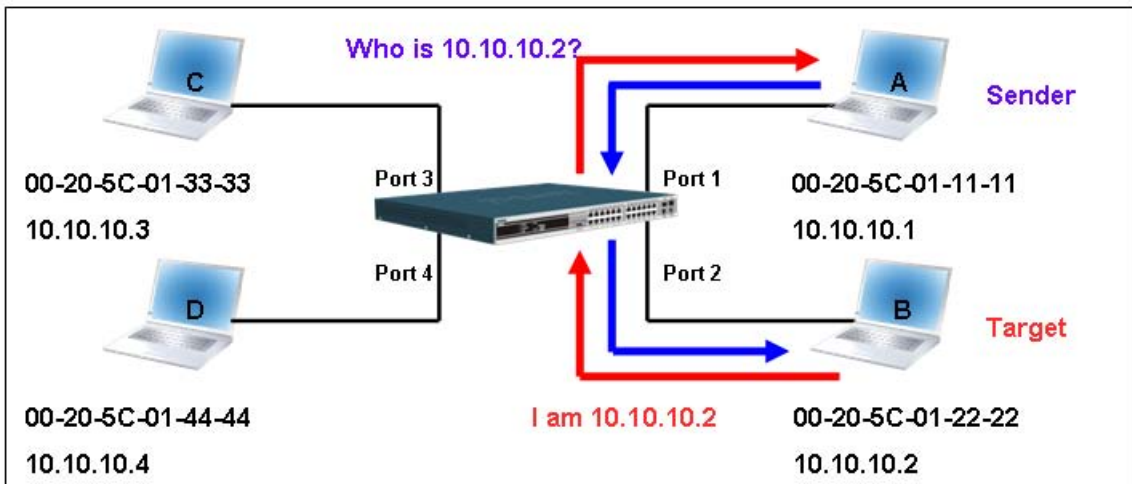


In addition, when the switch receives the broadcast ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure -2).



**Figure - 2**

When the switch floods the frame of ARP requests to the network, all PCs will receive and examine the frame but only PC B will reply to the query as the destination IP address of PC B matches (see Figure-3).



**Figure-3**

When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload shown in Table-3. The ARP reply will be then encapsulated into the Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP reply	<u>00-20-5C-01-11-11</u>	<u>10.10.10.1</u>	<u>00-20-5C-01-22-22</u>	<u>10.10.10.2</u>

**Table – 3 (ARP Payload)**

When PC B replies the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table-4).

Destination address	Source address	Ether-type	ARP	FCS
<u>00-20-5C-01-11-11</u>	<u>00-20-5C-01-22-22</u>			

**Table – 4 (Ethernet frame format)**

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

#### Forwarding Table

Port1 00-20-5C-01-11-11

Port2 00-20-5C-01-22-22



## How ARP spoofing attacks a network

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

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

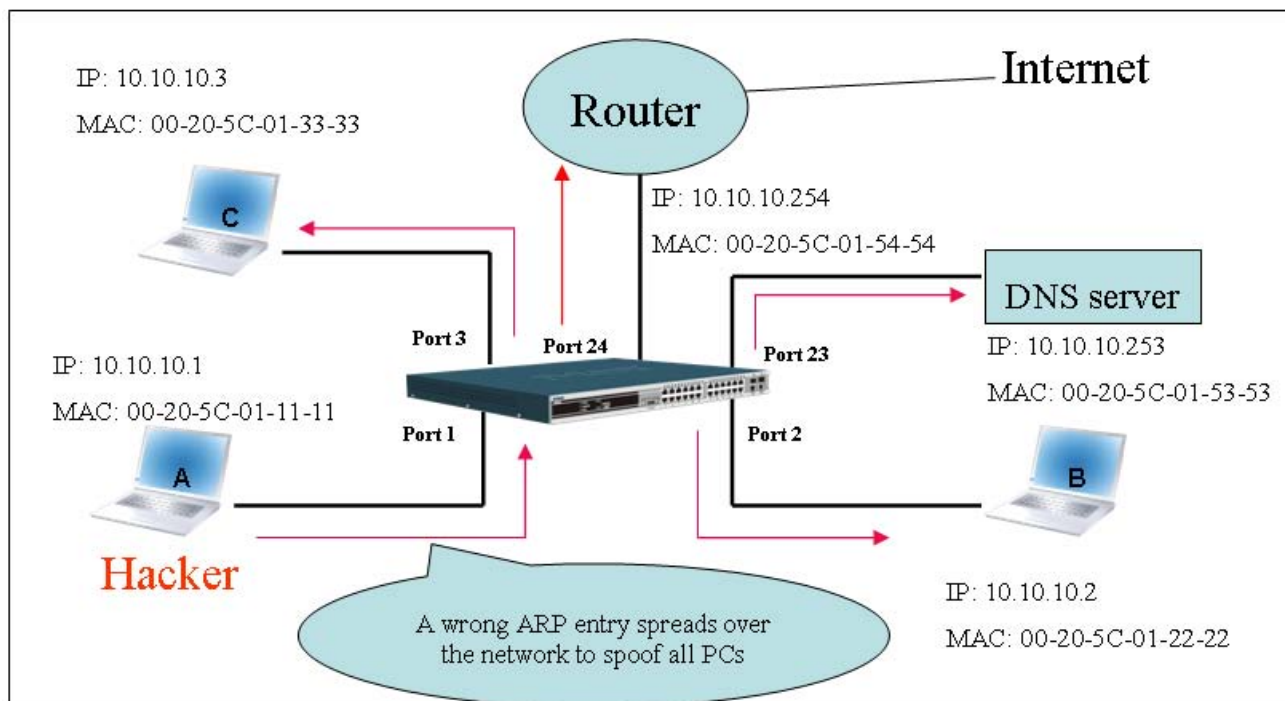


Figure-4

In the Gratuitous ARP packet, the "Sender protocol address" and "Target protocol address" are filled with the same source IP address. The "Sender H/W Address" and "Target H/W address" are filled with the same source MAC address. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender's MAC and IP address. The format of Gratuitous ARP is shown in Table-5.

Ethernet			Gratuitous ARP									
Destination address	Source address	Ethernet type	H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address	
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)	
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					ARP reply	<u>00-20-5C-01-11-11</u>	<u>10.10.10.254</u>	<u>00-20-5C-01-11-11</u>	<u>10.10.10.254</u>	

Table-5

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast ONE Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim's PC to think that it is a router and cheats the router to think it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker but the users will not notice anything happening.

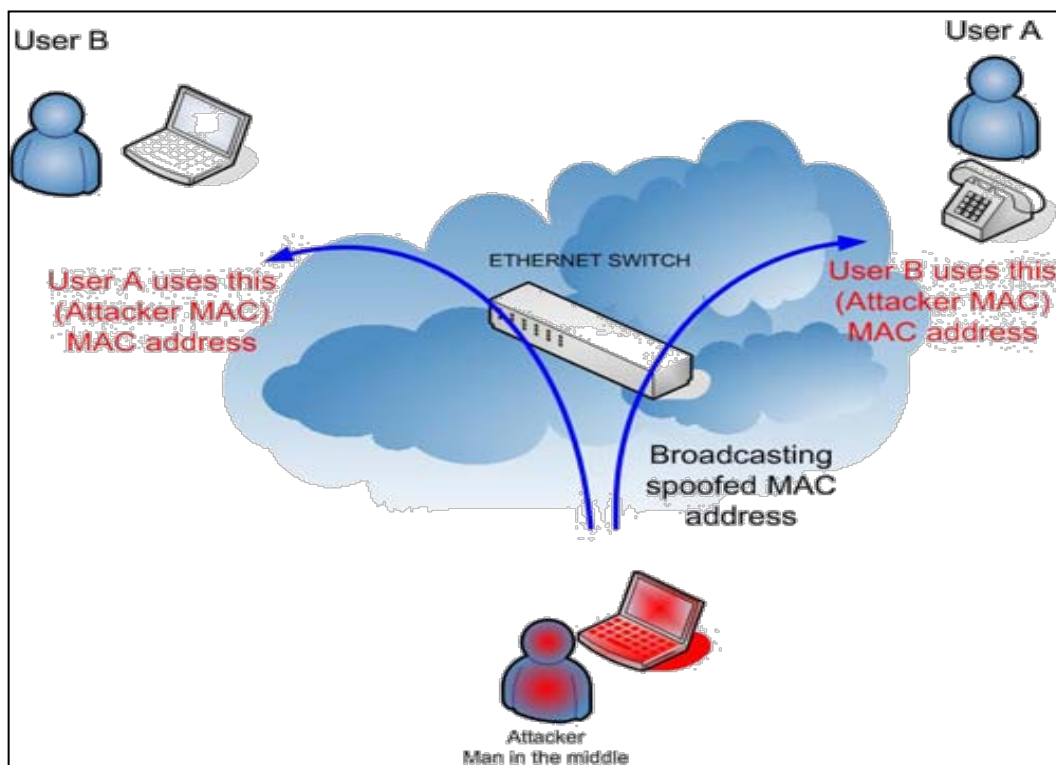
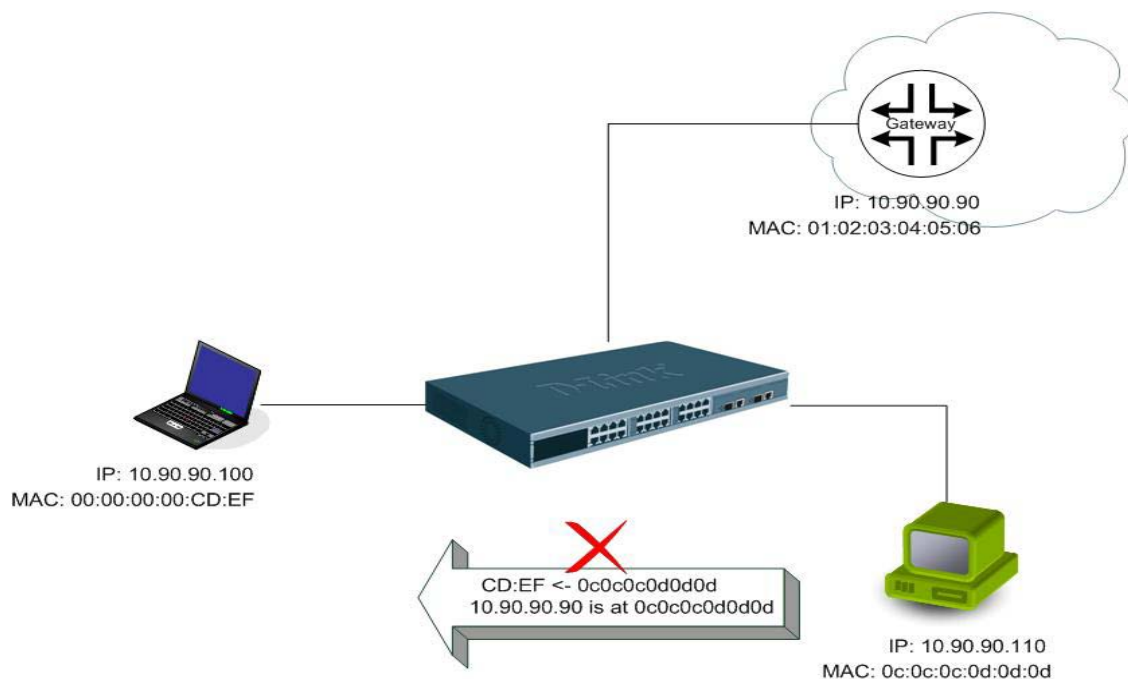


Figure-5

- **Prevent ARP spoofing via packet content ACL**

Concerning the common DoS attack today caused by the ARP spoofing, D-Link managed switch can effectively mitigate it via its unique Packet Content ACL.

For that reason the basic ACL can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here using Packet Content ACL on Switch to block the invalid ARP packets which contain fake gateway's MAC and IP binding.



## Example topology

### Configuration:

The configuration logic is listed below:

1. Only when the ARP matches the Source MAC address in Ethernet, the Sender MAC address and Sender IP address in the ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

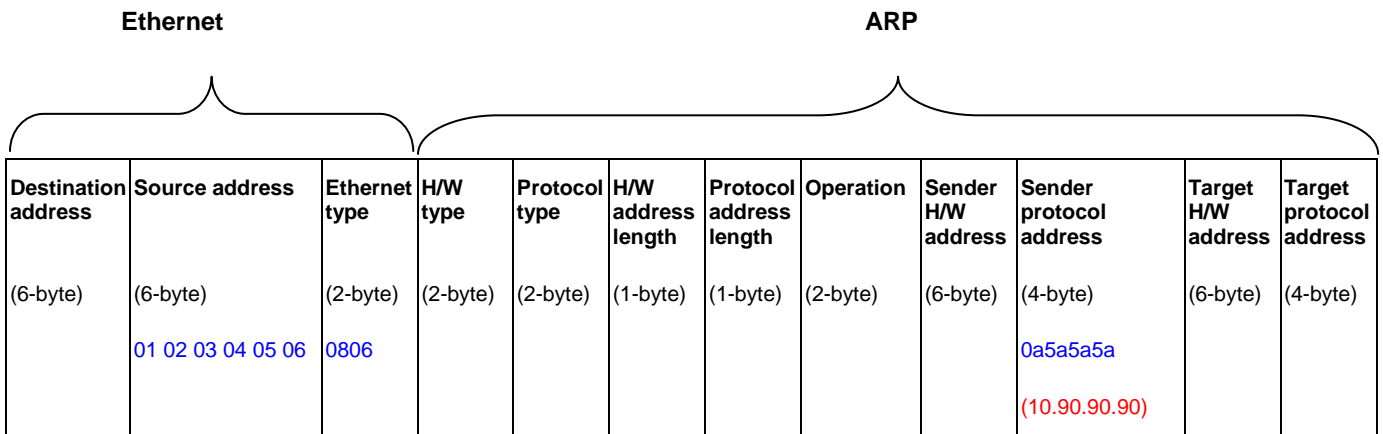
The design of Packet Content ACL on the DGS-3700 Series enables users to inspect any offset\_chunk. An offset\_chunk is a 4-byte block in a HEX format which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of 4 offset\_chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset\_chunks can be applied to each profile and a switch. Therefore, careful consideration is needed for planning the configuration of the valuable offset\_chunks.

In Table-6, you will notice that the Offset\_Chunk0 starts from 127 and ends at the 2<sup>nd</sup> byte. It can also be found that the offset\_chunk is scratched from 1 but not zero.

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk15	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

**Table-6:** Chunk and Packet offset Indicates a completed ARP packet contained in the Ethernet frame, which is the pattern for the calculation of packet offset.



**Table-7:** A completed ARP packet contained in Ethernet frame

	Command	Description
<b>Step1</b>	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match <b>Ethernet Type</b> and <b>Source MAC</b> address.
<b>Step2</b>	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-27 permit	- Configure access profile 1 - Only if the gateway's ARP packet that contains the correct <b>Source MAC</b> in Ethernet frame can pass through the switch.
<b>Step3</b>	create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000FFFF Ethernet Type(2-byte) offset_chunk_2 7 0x0000FFFF Sdr IP(First 2-byte) offset_chunk_3 8 0xFFFF0000 Sdr IP(Last 2-byte)	- Create access profile 2 - The first Chunk starts from Chunk 3: mask for <b>Ethernet Type</b> (Blue in Table-6: 13 <sup>th</sup> & 14 <sup>th</sup> bytes) - The second Chunk starts from Chunk 7: mask for <b>Sender IP (First 2-byte)</b> in ARP packet (Green in Table-6: 29 <sup>th</sup> & 30 <sup>th</sup> bytes) - The third Chunk starts from Chunk 8: mask for <b>Sender IP (Last 2-byte)</b> in ARP packet (Brown in Table-6: 31 <sup>st</sup> & 32 <sup>nd</sup> bytes)
<b>Step4</b>	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 Ethernet Type(2-byte): ARP offset_chunk_2 0x00000A5A Sdr IP(First 2-byte): 10.90 offset_chunk_3 0x5A5A0000 Sdr IP(Last 2-byte): 90.90 port 1-27 deny	- Configure access profile 2 - The rest ARP packets whose <b>Sender IP</b> claim they are the gateway's IP will be dropped.
<b>Step5</b>	Save	- Save config

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

	Log message upload was unsuccessful	Log message upload by <console   telnet   WEB   SSH   SNMP   SIM> was unsuccessful! (Username: <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>)	Informational
	Login failed through Web	Login failed through Web (Username: <username>)	Warning
	Logout through Web	Logout through Web (Username: <username>)	Informational
SSL	Successful login through Web(SSL)	Successful login through Web(SSL) (Username: <username>)	Informational
	Login failed through Web(SSL)	Login failed through Web(SSL) (Username: <username>)	Warning
	Logout through Web(SSL)	Logout through Web(SSL) (Username: <username>)	Informational
	Web(SSL) session timed out	Web(SSL) session timed out (Username: <username>)	Informational
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr> )	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational
STP	Topology changed	Topology changed (Instance:%d, Port:%d)	Informational
	New Root selected	CIST New Root bridge selected (MAC:%s, Priority:%d)	Informational
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational

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



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

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

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

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

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

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

		<portNum>, VID: <vlanID>)	
	Login Fail	MAC-AC login rejected (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Warning
	Aged out	MAC-AC host aged out (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Informational

## DGS-3700 Series Trap List

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

## Proprietary Trap List

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

swPowerStatusChg 1.3.6.1.4.1.171.12.11.2.2.2.0.1	swPowerStatusChgSeverity	V2	EQUIPMENT-MIB	Warning
swFanFailure 1.3.6.1.4.1.171.12.11.2.2.3.0.1	swFanFailureSeverity	V2	EQUIPMENT-MIB	Warning
swFanRecover 1.3.6.1.4.1.171.12.11.2.2.3.0.2	swFanRecoverSeverity	V2	EQUIPMENT-MIB	Warning
swMacBasedAuthLoggedSuccess 1.3.6.1.4.1.171.12.35.11.1.0.1	swMacBasedAuthLoggedSuccess	V2	MBA-MIB	Warning
SwMacBasedAuthLoggedFail 1.3.6.1.4.1.171.12.35.11.1.0.2	SwMacBasedAuthLoggedFail	V2	MBA-MIB	Warning
SwMacBasedAuthAgesOut 1.3.6.1.4.1.171.12.35.11.1.0.3	SwMacBasedAuthAgesOut	V2	MBA-MIB	Warning
SwExternalAlarm 1.3.6.1.4.1.171.12.11.2.2.5.0.1	swExternalAlarm	V2	EQUIPMENT-MIB	Warning
SwDdmAlarmTrap 1.3.6.1.4.1.171.12.72.4.0.1	swDdmAlarmTrap	V2	DDM-MIB	Warning
SwDdmWarningTrap 1.3.6.1.4.1.171.12.72.4.0.2	swDdmWarningTrap	V2	DDM-MIB	Warning
swL2PortLoopOccurred 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.3	swL2PortLoopOccurred	V2	L2Mgmt-MIB	Warning
swL2PortLoopRestart 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.4	swL2PortLoopRestart	V2	L2Mgmt-MIB	Warning
swL2VlanLoopOccurred 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.5	swL2VlanLoopOccurred	V2	L2Mgmt-MIB	Warning
swL2VlanLoopRestart 1.3.6.1.4.1.171.11.102.1.1.2.100.1.2.0.6	swL2VlanLoopRestart	V2	L2Mgmt-MIB	Warning



## Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**line speed:** See baud rate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Password Recovery Procedure

This section describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

**Complete these steps to reset the password:**

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] ( Shift + 6 ) to enter the "Password Recovery Mode". Once the Switch enters the "Password Recovery Mode", all ports on the Switch will be disabled.

```

Boot Procedure V1.00.B06
-----

Power On Self Test ..... 100%

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

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

The switch is now entering Password Recovery Mode:_
  
```

```

The switch is currently in Password Recovery Mode.
>
  
```

3. In the "Password Recovery Mode" only the following commands can be used.

Command	Parameters
reset config	The reset config command resets the whole configuration will be back to the default value
reboot	The reboot command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The reset account command deletes all the previously created accounts.
reset password	The reset password command resets the password of the specified user. If a username is not specified, the password of all users will be

Command	Parameters
{<username>}	reset.
show account	The show account command displays all previously created accounts.