D-Link
Building Networks for People

xStack

User Manual

Product Model: xStack™ DES-3528

Layer 2 Managed Stackable Fast Ethernet Switch

Release 1.2

June 2008 P/N：651ES3500025G

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Table of Contents

Preface x
Intended Readers xi
Typographical Conventions xi
Notes, Notices, and Cautions xi
Safety Instructions xii
Safety Cautions xii
General Precautions for Rack-Mountable Products xiii
Protecting Against Electrostatic Discharge xiv
Introduction 1
Gigabit Ethernet Technology 1
Switch Description 1
Features 2
Ports 2
Front-Panel Components 2
LED Indicators 2
Rear Panel Description 4
Side Panel Description 4
Gigabit Combo Ports 4
Installation 6
Package Contents 6
Before You Connect to the Network 6
Installing the Switch without the Rack 7
Installing the Switch in a Rack 7
Mounting the Switch in a Standard 19" Rack 8
Power On (AC Power) 8
Power Failure 8
Connecting the Switch 9
Switch to End Node 9
Switch to Hub or Switch 9
Connecting To Network Backbone or Server 11
Introduction to Switch Management 12
Management Options 12
Web-based Management Interface 12
SNMP-Based Management 12
Connecting the Console Port (RS-232 DCE) 12
First Time Connecting to the Switch 14
Password Protection 14
SNMP Settings 15
IP Address Assignment 16
Web-based Switch Configuration 18

Introduction 18
Login to Web Manager 18
Web-based User Interface 19
Web Pages 20
Configuration 21
Device Information 22
System Information 22
Serial Port Settings 23
IP Address 23
Port Configuration 26
Port Settings 26
Port Description 28
Port Error Disabled 29
Static ARP Settings 30
User Accounts 31
System Log Configuration 33
System Log Settings 33
System Log Server 33
System Severity Settings 35
DHCP/BOOTP Relay 36
DHCP/BOOTP Relay Global Settings 36
DHCP/BOOTP Relay Interface Settings 38
DHCP Auto Configuration Settings 39
MAC Address Aging Time 39
Web Settings 40
Telnet Settings 40
Password Encryption 40
Clipaging Settings 40
Firmware Information 41
Dual Configuration Settings 41
Ping Test 43
SNTP Settings 44
Time Settings 44
TimeZone Settings 45
MAC Notification Settings 46
MAC Notification Global Settings 46
MAC Notification Port Settings 47
SNMP Settings 48
SNMP Global State 49
SNMP View Table 49
SNMP Group Table 50
SNMP User Table 51
SNMP Community Table 52

SNMP Host Table 53
SNMP Engine ID 53
SNMP Trap Configuration 54
Time Range Settings 54
Single IP Settings 55
SIM Settings 56
Topology 57
Tool Tips 60
Right-Click 61
Menu Bar 63
Firmware Upgrade 64
Configuration File Backup/Restore 64
Upload Log 65
L2 Features 66
Jumbo Frame 66
VLANs 66
Understanding IEEE 802.1p Priority 66
VLAN Description 67
IEEE 802.1Q VLANs 67
Double VLANs 73
802.1Q VLAN 74
Click Apply to implement changes made.QinQ 77
QinQ 78
VLAN Translation Settings 79
802.1v Protocol VLAN 80
802.1v Protocol Group Settings 80
802.1v Protocol VLAN Settings 80
GVRP Settings 82
GVRP Timer Settings 83
Asymmetric VLAN Settings 83
MAC-based VLAN Settings 84
PVID Auto Assign Settings 84
Port Trunking 85
LACP Port Settings 87
Traffic Segmentation 88
IGMP Snooping 89
IGMP Snooping Settings 89
IGMP Snooping Multicast VLAN Settings 90
IP Multicast Profile Settings 91
Limited Multicast Range Settings 92
Multicast Filtering Mode 92
Max Multicast Group Settings 93
MLD Snooping Settings 94

MLD Snooping Settings 94
Port Mirror 96
Loopback Detection Settings 97
Spanning Tree 98
STP Bridge Global Settings 100
STP Port Settings 102
MST Configuration Identification 103
STP Instance Settings 104
MSTP Port Information 105
Forwarding & Filtering 106
Unicast Forwarding 106
Multicast Forwarding 106
LLDP 107
LLDP Global Settings 107
LLDP Port Settings 108
LLDP Management Address List 109
LLDP Basic TLVs Settings 109
LLDP Dot1 TLVs Settings 110
LLDP Dot3 TLVs Settings 111
LLDP Statistics System 111
LLDP Local Port Information 112
LLDP Remote Port Information 113
QoS 114
Advantages of QoS 114
Understanding QoS 115
HOL Blocking Pevention 116
Bandwidth Control 116
Traffic Control 117
802.1p Default Priority 119
802.1p User Priority 120
QoS Scheduling Mechanism 120
SRED 121
SRED Settings 121
SRED Drop Counter 123
DSCP Trust Settings 123
DSCP Map Settings 124
802.1p Map Settings 125
Security 126
Safeguard Engine 126
Trusted Host 128
IP-MAC-Port Binding 128
IMP Global Settings 129
IMP Port Settings 129

IMP Entry Settings 131
DHCP Snooping Entries 132
MAC Block List 132
Port Security 132
Port Security Settings 132
Port Security FDB Entries 133
DHCP Server Screening Settings 134
DHCP Screening Port Settings 134
DHCP Offer Filtering 135
802.1X 136
802.1x Port-Based and MAC-Based Access Control 136
Understanding 802.1x Port-based and MAC-based Network Access Control 139
Port-Based Network Access Control 139
MAC-Based Network Access Control 140
802.1X Force Disconnect 141
802.1X Settings 141
802.1X User 143
Authentication RADIUS Server 143
Initialize Port(s) 144
Reauthenticate Port(s) 144
Guest VLAN 145
Guest VLAN Configuration 146
SSL Settings 146
Download Certificate 147
Ciphersuite 147
SSH 149
SSH Settings 149
SSH Authmode and Algorithm Settings 150
SSH User Authentication Lists 151
Access Authentication Control 153
Authentication Policy Settings 154
Application Authentication Settings 154
Authentication Server Group 155
Authentication Server 156
Login Method Lists 157
Enable Method Lists 158
Local Enable Password Settings 159
RADIUS Accounting Services 160
MAC-Based Access Control 161
Notes About MAC-Based Access Control 161
MAC Based Access Control Settings 161
MAC Based Access Control Local Settings 163
Web Authentication 164
Conditions and Limitations 164

Web-based Access Control Settings 165
Web-based Access Control User Settings 166
JWAC (Japanese Web-based Access Control) 167
JWAC Global Settings 167
JWAC Port Settings 169
JWAC User Account 170
NetBIOS Filtering 170
NetBIOS Filtering Settings 170
ACL 172
ACL Configuration Wizard 172
Access Profile List 173
CPU Interface Filtering 190
CPU Access Profile List 191
ACL Finder 203
ACL Flow Meter 203
Monitoring 206
Device Status 206
CPU Utilization 206
Port Utilization 207
Packet Size 208
Packets 210
Received (RX) 210
UMB_cast (RX) 213
Transmitted (TX) 214
Errors 216
Received (RX) 216
Transmitted (TX) 218
Port Access Control 219
RADIUS Authentication 219
RADIUS Account Client 221
Authenticator State 223
Authenticator Statistics 224
Authenticator Session Statistics 226
Authenticator Diagnostics 227
Browse ARP Table 229
Browse VLAN 229
Show VLAN Ports 230
Browse Router Port 230
Browse MLD Router Port 230
Browse Session Table 231
IGMP Snooping Group 231
MLD Snooping Group 232

JWAC Host Table 232
MAC Address Table 233
System Log 233
Save Services and Tools 235
Save Configuration ID 1 235
Save Configuration ID 2 236
Save Log 236
Save All 236
Configuration File Backup & Restore 237
Upload Log File 237
Reset 237
Download Firmware 238
Reboot System 238
Technical Specifications 239
Mitigating ARP Spoofing Attacks Using Packet Content ACL 244
System Log Entries 252
Cable Lengths 261
Glossary 262
Tech Support 273

Preface

The ***DES-3528 Manual*** is divided into sections that describe the system installation and operating instructions with examples.

Section 1, Introduction – Describes the Switch and its features.

Section 2, Installation – Helps you get started with the basic installation of the Switch and also describes the front panel, rear panel, side panels, and LED indicators of the Switch. Included in this section is a description of how to hook up the DC power supply for the DES-3528 switch.

Section 3, Connecting the Switch – Tells how you can connect the Switch to your Ethernet/Fast Ethernet network.

Section 4, Introduction to Switch Management – Introduces basic Switch management features, including password protection, SNMP settings, IP address assignment and connecting devices to the Switch.

Section 5, Introduction to Web-based Switch Management – Talks about connecting to and using the Web-based switch management feature on the Switch.

Section 6, Configuration – A detailed discussion about configuring some of the basic functions of the Switch, including accessing the System information, Serial Port Settings, IP Address, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, System Severity Settings, DHCP/BOOTP Relay, DHCP Auto Configuration Settings, MAC Address Aging Time, Web Settings, Telnet Settings, Password Encryption, Clipaging Settings, Firmware Information, Dual Configuration Settings, Ping Test, SNTP Settings, MAC Notification Settings, SNMP Settings, Time Range Settings, and Single IP Management.

Section 7, L2 Features – A discussion of the Layer 2 features on the Switch, including Jumbo Frame, 802.1Q VLAN, QinQ, 802.1v Protocol VLAN, GVRP Settings, GVRP Timer Settings, Asymmetric VLAN Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, IGMP Snooping, MLD Snooping Settings, Port Mirror, Loopback Detection Settings, Spanning Tree, Forwarding & Filtering, and LLDP.

Section 8, 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 and SRED.

Section 9, 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, JWAC, and NetBIOS Filtering Services.

Section 10, 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 11, Monitoring – Features information about the monitoring functions on the Switch including, Device Status, CPU Utilization, Port Utilization, Packet Size, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, Show VLAN Ports, Browse Router Ports, Browse MLD Router Ports, Browse Session Table, IGMP Snooping, MLD Snooping Group, JWAC Host Table, MAC Address Table, and System Log.

Section 12, 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, Technical Specifications – The technical specifications of the DES-3528 switch.

Appendix B, 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 C, 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 D, Cable Lengths – Information on cable types and maximum distances.

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

Intended Readers

The ***DES-3528 Manual*** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

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

Notes, Notices, and Cautions

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

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

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

Safety Instructions

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

Safety Cautions

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

- Observe and follow service markings.

  Do not service any product except as explained in your system documentation.

  Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.

  Only a trained service technician should service components inside these compartments.

- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:

  The power cable, extension cable, or plug is damaged.

  An object has fallen into the product.

  The product has been exposed to water.

  The product has been dropped or damaged.

  The product does not operate correctly when you follow the operating instructions.

- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage on the power supply is set to match the power available at your location:

  115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan

  100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan

  230 V/50 Hz in most of Europe, the Middle East, and the Far East

- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical

ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.

- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  Install the power supply before connecting the power cable to the power supply.

  Unplug the power cable before removing the power supply.

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

General Precautions for Rack-Mountable Products

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

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

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

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

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

Protecting Against Electrostatic Discharge

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

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

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

Section 1

Introduction

Gigabit Ethernet Technology

Switch Description

Features

Ports

Front-Panel Components

LED indicators

Rear Panel Description

Side Panel Description

Gigabit Combo Ports

The DES-3528 layer 2 Fast Ethernet switch is a member of the D-Link xStack family. Ranging from 10/100Mbps edge switches to core gigabit switches, the xStack switch family has been future-proof designed to provide a stacking architecture with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

The following manual describes the installation, maintenance and configurations concerning the xStack DES-3528 switch. Please take note that if this device was purchased outside of Europe, certain cosmetic differences between the actual switch and images in this document will be apparent to the reader, such as the faceplate and the manual cover. The DES-3528 has already joined the xStack family for the European market and is soon to be xStack converted, universally. Changes are made to the appearance of the device only and no configuration or internal hardware alterations occur.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet are essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users using applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your sub networks.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies.

Switch Description

The DES-3528 switch is equipped with unshielded twisted-pair (UTP) cable ports providing dedicated 10 or 100 Mbps bandwidth. The Switch has 24 UTP ports and Auto MDI-X/MDI-II convertible ports that can be used for uplinking to another switch. These ports can be used for connecting PCs, printers, servers, hubs, routers, switches and other networking devices. The dual speed ports use standard twisted-pair cabling and are ideal for segmenting networks into small, connected sub networks for superior performance. Each 10/100 port can support up to 200 Mbps of throughput in full-duplex mode.

In addition, the Switch has 2 SFP combo ports. These two-gigabit combo ports are ideal for connecting to a server or network backbone. This stackable Switch enables the network to use some of the most demanding multimedia and imaging applications concurrently with other user applications without creating bottlenecks. The built-in console interface can be used to configure the Switch's settings for priority queuing, VLANs, and port trunk groups, port monitoring, and port speed.

NOTE: For the remainder of this manual, all hardware versions of the DES-3528 switch will be referred to as simply the Switch or the DES-3528.

Features

IEEE 802.3 10BASE-T compliant

IEEE 802.3u 100BASE-TX compliant

IEEE 802.1p Priority Queues

IEEE 802.3x flow control in full duplex mode

IEEE 802.3ad Link Aggregation Control Protocol support.

IEEE 802.1x Port-based and MAC-based Access Control

IEEE 802.1Q VLAN

IEEE 802.1D Spanning Tree, IEEE 802.1W Rapid Spanning Tree and IEEE 802.1s Multiple Spanning Tree support

Access Control List (ACL) support

Single IP Management support

Access Authentication Control utilizing TACACS, XTACACS and TACACS+

Dual Image Firmware

Simple Network Time Protocol support

MAC Notification support

Asymmetric VLAN support

System and Port Utilization support

System Log Support

Support port-based enable and disable

Address table: Supports up to 16K MAC addresses per device

Supports a packet buffer of up to 1 Mbyte

Supports Port-based VLAN Groups

Port Trunking with flexible load distribution and fail-over function

IGMP Snooping support

SNMP support

Secure Sockets Layer (SSL) and Secure Shell (SSH) support

Port Mirroring support

MIB support for:

RFC1213 MIB II

RFC1493 Bridge

RFC1757 RMON

RFC1643 Ether-like MIB

RFC2233 Interface MIB

Private MIB

RFC2674 for 802.1p

IEEE 802.1x MIB

RS-232 DCE console port for Switch management

Provides parallel LED display for port status such as link/act, speed, etc.

High performance switching engine performs forwarding and filtering at full wire speed, maximum 14, 881 packets/sec on each 10Mbps Ethernet port, and maximum 148,810 packet/sec on 100Mbps Fast Ethernet port.

Full- and half-duplex for both 10Mbps and 100Mbps connections. Full duplex allows the switch port to simultaneously transmit and receive data. It only works with connections to full-duplex-capable end stations and switches. Connections to a hub must take place at half-duplex

Support broadcast storm filtering

Non-blocking store and forward switching scheme capability to support rate adaptation and protocol conversion

Supports by-port Egress/Ingress rate control.

Supports IP-MAC Port Binding.

Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed

Supports STP Loopback Detection

Safeguard Engine Support

Ports

Twenty-four high-performance (MDI-X/MDI-II) ports for connecting to end stations, servers, hubs and other networking devices.

All UTP ports can auto-negotiate between 10Mbps and 100Mbps, half-duplex and full duplex, and feature flow control.

Two SFP combo ports for connecting to another switch, server, or network backbone.

RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

NOTE: For customers interested in D-View, D-Link Corporation's proprietary SNMP management software, go to the D-Link Website (www.dlink.com) and download the software and manual.

Front-Panel Components

The front panel of the Switch consists of LED indicators for power and for each 10/100 Mbps twisted-pair ports, and two combo 1000Base-T/SFP ports.

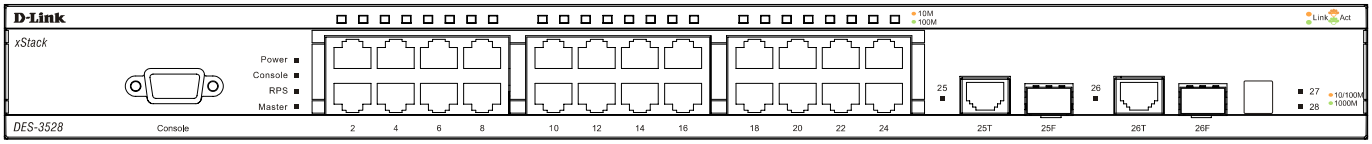


Figure 1- 1. Front Panel View of the DES-3528 switch

Comprehensive LED indicators display the status of the Switch and the network.

LED Indicators

The Switch supports LED indicators for Power, Console, RPS and Port LEDs. The following shows the LED indicators for the DES-3528 switch along with an explanation of each indicator. LEDs and there corresponding meanings are displayed below.

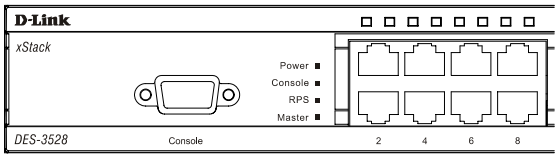


Figure 1- 2. LED Indicators on DES-3528 switch

LED indicators

Location	LED Indicative	Color	Status	Description
Per Device	**Power**	Green	Solid Light	Power On
			Light off	Power Off
	Console	Green	Solid Light	Console on
			Blinking	POST is in progress.
			Light off	Console off

	RPS	Green	Solid Light	RPS is in Use
			Light Off	RPS Off
	Master(MS)	Green	Solid Light	When the device is the stacking master.
			Light Off	Not the Stacking Master.
	Stacking ID	Green	Capable 1-8	The Box ID is assigned either by the user (static mode) or by the system (automatic mode). When the box becomes a primary master the 7 segment works as bu-function. That is box ID and “H” indicate as primary Master and the display will be shown by turn. That is boxID- > H -> boxID -> H…
LED Per 10/100 Mbps Port	**Link/Act/Speed**	Green/Amber	Solid Green	When there is a secure 100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a Fast Ethernet connected port.
			Solid Amber	When there is a secure 10Mbps Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at an Ethernet connected port.
			Light off	No link
LED Per GE Port	**Link/Act/Speed mode for 1000BASE-T ports**	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 10/100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 10/100Mbps Fast Ethernet connected port.
			Light off	No link
	Link/Act/Speed mode for SFP ports	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 100Mbps connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at the ports.
			Light off	No link

Rear Panel Description

The rear panel of the Switch contains an AC power connector.

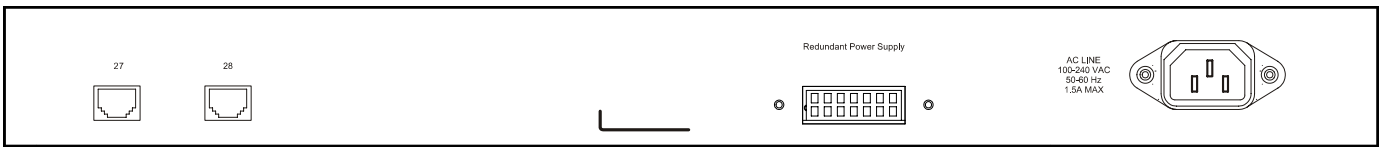


Figure 1- 3. Rear panel view of the DES-3528

The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

The rear panel also includes two 1000Mbps Copper ports and an outlet for an optional external power supply. When power fails, the optional external RPS will take over all the power immediately and automatically.

Side Panel Description

The left and right-hand panel of the Switch contains a heat vent.

The heat vents are used to dissipate heat. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

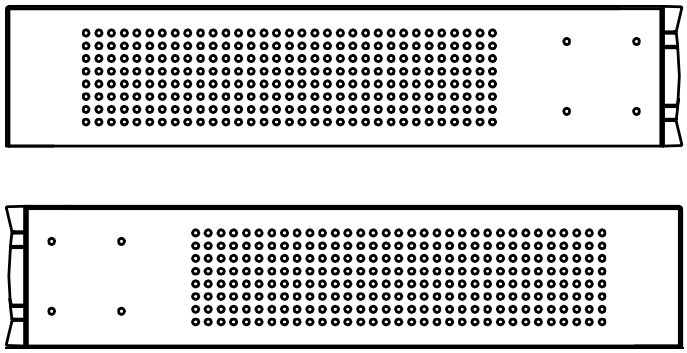


Figure 1- 4. Side panels of the DES-3528

Gigabit Combo Ports

In addition to the 24 10/100 Mbps ports, the Switch features two Gigabit Ethernet Combo ports. These two ports are 1000BASE-T copper ports (provided) and SFP ports (optional). See the diagram below to view the two SFP port modules being plugged into the Switch. Please note that although these two front panel modules can be used simultaneously. At the same time, only one copper port or one SFP port can link up for each combo port. The SFP port will always have the highest priority.

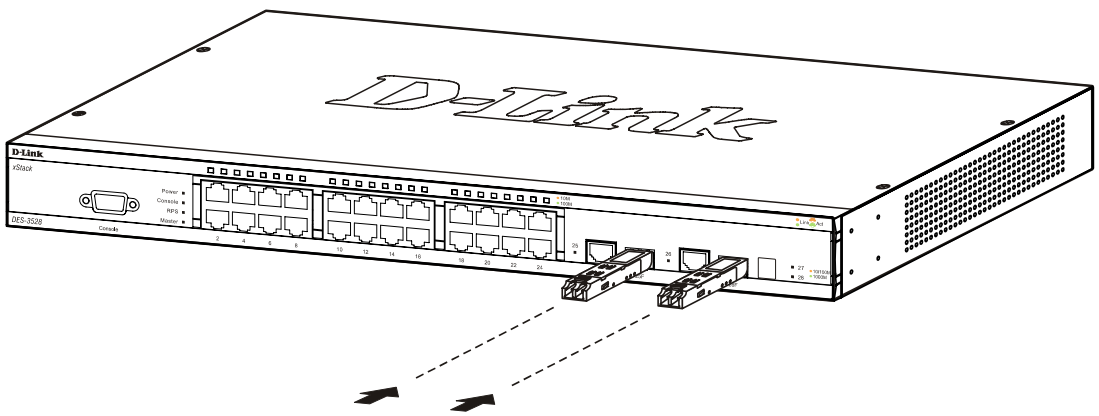


Figure 1- 5. Inserting the SFP modules into the DES-3528

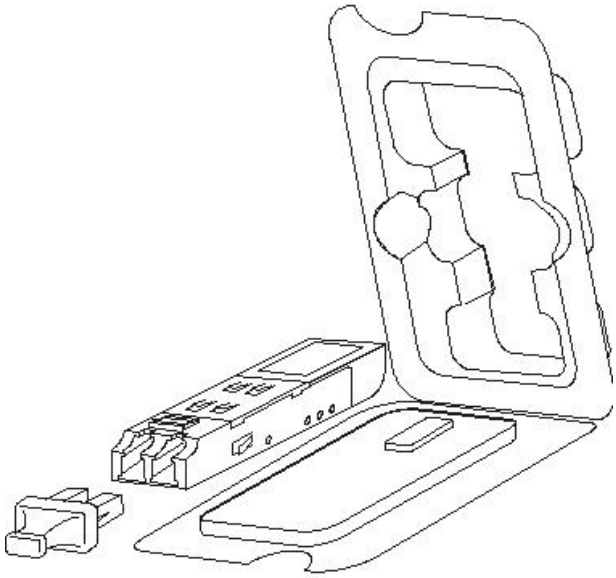


Figure 1- 6. Installing the SFP Module

SECTION 2

Installation

Package Contents

Before You Connect to the Network

Installing the Switch without the Rack

Rack Installation

Power On

Package Contents

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

One xStack DES-3528 stand-alone switch

One AC power cord

This manual

Registration card

Mounting kit (two brackets and screws)

Four rubber feet with adhesive backing

RS-232 console cable

If any item is found missing or damaged, please contact your local D-Link Reseller for replacement.

Before You Connect to the Network

The site where you install the Switch may greatly affect its performance. Please follow these guidelines for setting up the Switch.

Install the Switch on a sturdy, level surface that can support at least 6.6 lb. (3 kg) of weight. Do not place heavy objects on the Switch.

The power outlet should be within 1.82 meters (6 feet) of the Switch.

Visually inspect the power cord and see that it is fully secured to the AC power port.

Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation.

Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.

Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.

When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches and prevent it from scratching other surfaces.

Installing the Switch without the Rack

When installing the Switch on a desktop or shelf, the rubber feet included with the Switch should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow enough ventilation space between the Switch and any other objects in the vicinity.

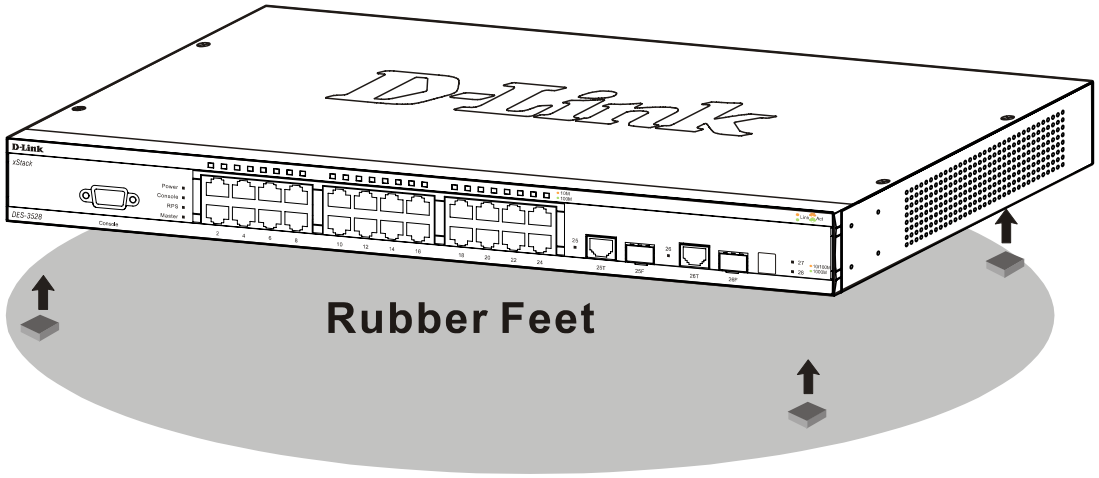


Figure 2- 1. Preparing the DES-3528 for installation on a desktop or shelf

Installing the Switch in a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.

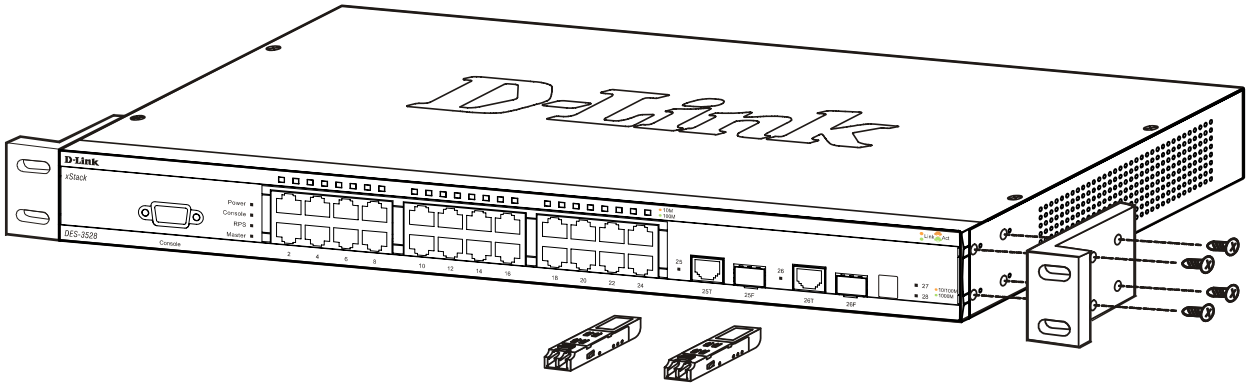


Figure 2- 2. Fasten mounting brackets to the DES-3528

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figure 2-3 below.

Mounting the Switch in a Standard 19" Rack

CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing components in a rack, do not pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in injury.

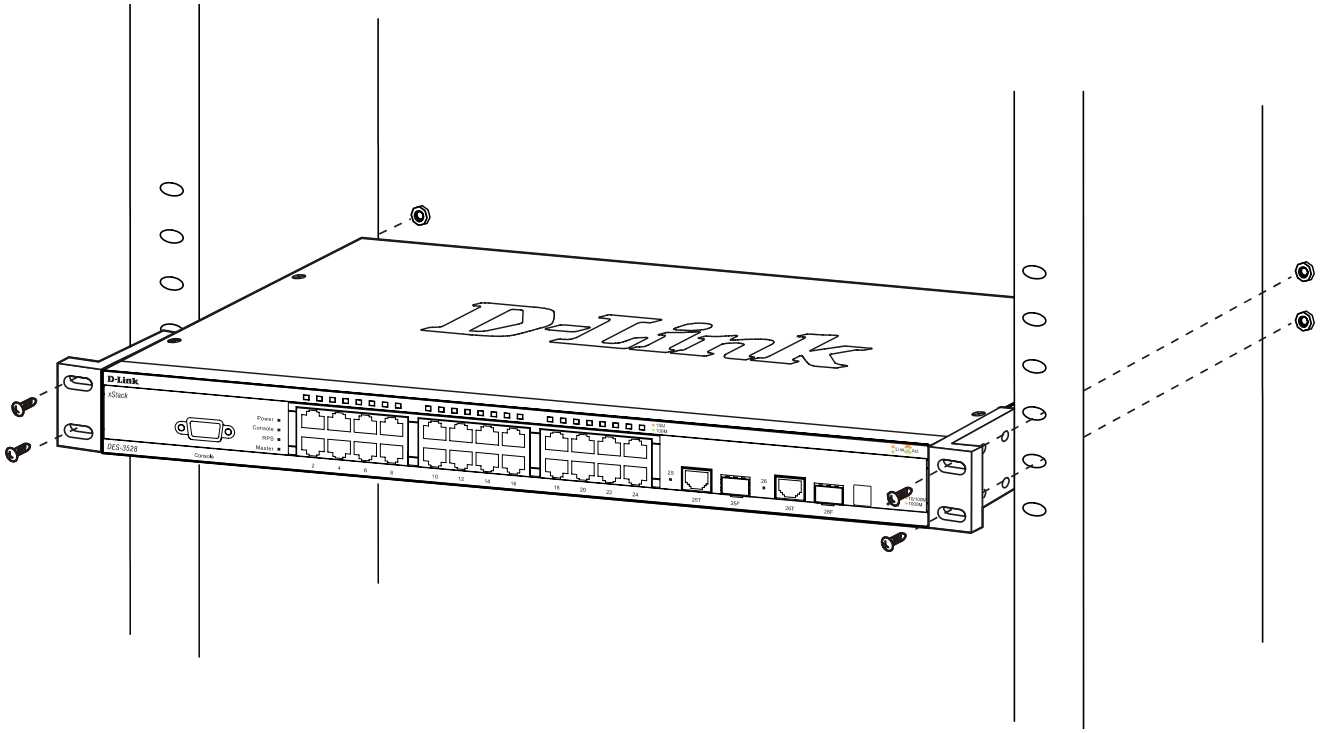


Figure 2- 3. Installing the DES-3528 in a rack

Power On (AC Power)

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet.

After the Switch is powered on, the LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.

Power Failure

As a precaution for AC power supply units, in the event of a power failure, unplug the Switch. When power has resumed, plug the Switch back in.

Section 3

Connecting the Switch

Switch to End Node

Switch to Hub or Switch

Connecting To Network Backbone or Server

NOTE: All 24 high-performance NWay Ethernet ports can support both MDI-II and MDI-X connections.

Switch to End Node

End nodes include PCs outfitted with a 10, 100 or 1000 Mbps RJ-45 Ethernet/Fast Ethernet Network Interface Card (NIC) and most routers.

An end node can be connected to the Switch via a twisted-pair Category 3, 4, or 5 UTP/STP cable. The end node should be connected to any of the ports of the Switch.

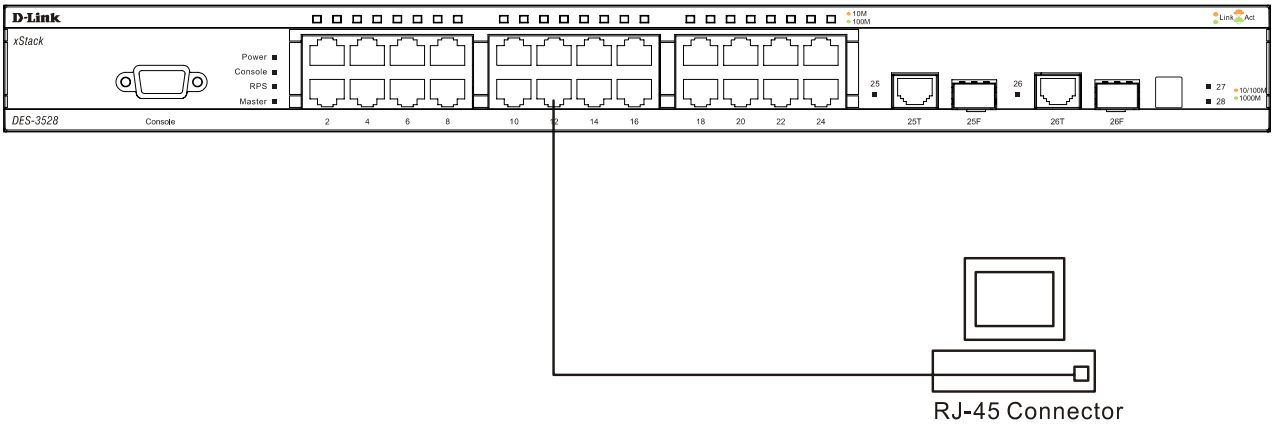


Figure 3- 1. DES-3528 connected to an end node

The Link/Act LEDs for each UTP port will light green or amber when the link is valid. A blinking LED indicates packet activity on that port.

Switch to Hub or Switch

These connections can be accomplished in a number of ways using a normal cable.

A 10BASE-T hub or switch can be connected to the Switch via a twisted-pair Category 3, 4 or 5 UTP/STP cable.

A 100BASE-TX hub or switch can be connected to the Switch via a twisted -pair Category 5 UTP/STP cable.

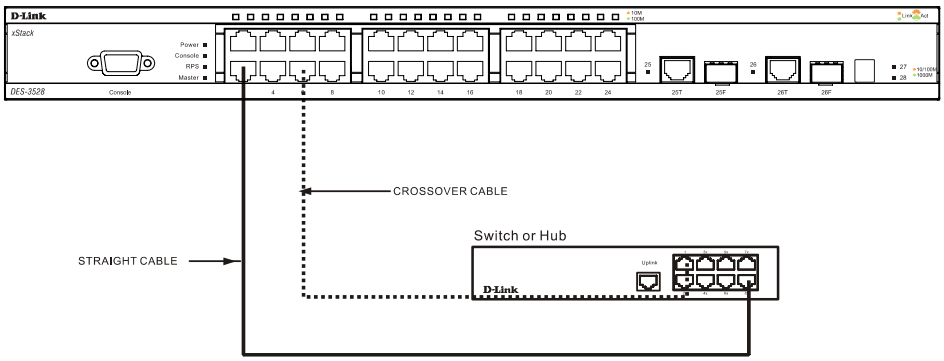


Figure 3- 2. DES-3528 connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

Connecting To Network Backbone or Server

The two SFP combo ports are ideal for linking to a network backbone or server. The copper ports operate at a speed of 1000, 100 or 10Mbps in full or half duplex mode. The fiber optic ports can operate at 100Mbps or 1000Mbps in full duplex mode.

Connections to the Gigabit Ethernet ports are made using fiber optic cable or Category 5E copper cable, depending on the type of port. A valid connection is indicated when the Link LED is lit.

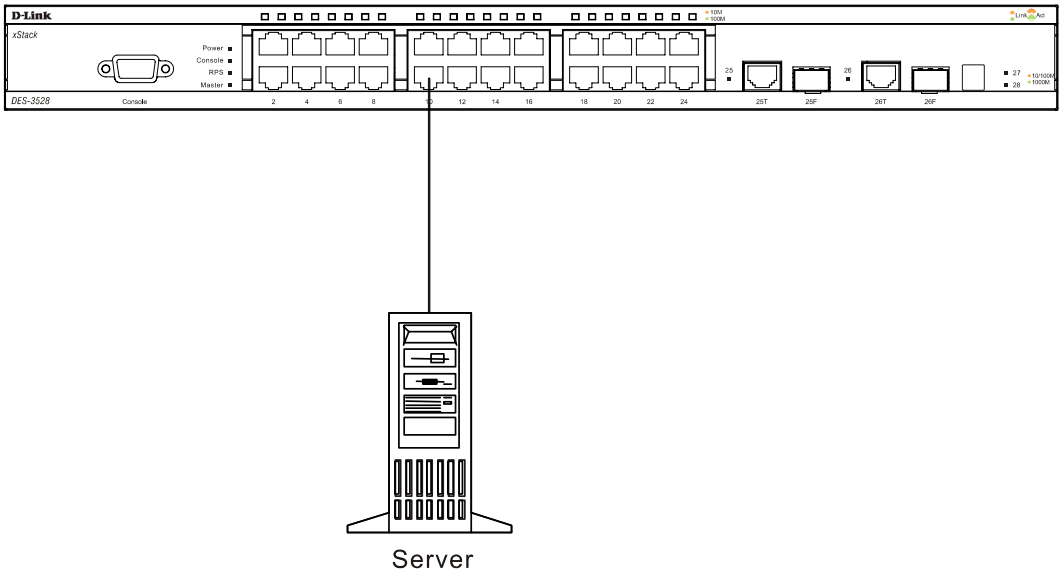


Figure 3- 3. Connecting the DES-3500 Series switch to a Server

Section 4

Introduction to Switch Management

Management Options

Web-based Management Interface

SNMP-Based Management

Managing User Accounts

Command Line Console Interface through the Serial Port

Connecting the Console Port (RS-232 DCE)

First Time Connecting to the Switch

Password Protection

SNMP Settings

IP Address Assignment

Management Options

This system may be managed out-of-band through the console port on the front panel or in-band using Telnet. The user may also choose the web-based management, accessible through a web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser, such as Netscape Navigator (version 6.2.3 and higher) or Microsoft® Internet Explorer (version 6.0).

SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0 and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Connecting the Console Port (RS-232 DCE)

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a female DB-9 connector, implemented as a data communications equipment (DCE) connection.

To use the console port, you need the following equipment:

A terminal or a computer with both a serial port and the ability to emulate a terminal.

A null modem or Parallel RS-232 cable with a male DB-9 connector for the console port on the Switch.

To connect a terminal to the console port:

1. Connect the male connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
3. Select the appropriate serial port (COM port 1 or COM port 2).
4. Set the data rate to **115200 baud**.
5. Set the data format to **8 data bits**, **1 stop bit**, and **no parity**.
6. Set flow control to **none**.

7. Under **Properties**, select **VT100** for Emulation mode.
8. Select **Terminal** keys for **Function**, **Arrow**, and **Ctrl** keys. Ensure that you select Terminal keys (not Windows keys).

NOTE: When you use HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 allows you to use arrow keys in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

9. After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
10. After the boot sequence completes, the console login screen displays.
11. If you have not logged into the command line interface (CLI) program, press the **Enter** key at the User name and password prompts. There is no default user name and password for the Switch. The administrator must first create user names and passwords. If you have previously set up user accounts, log in and continue to configure the Switch.
12. Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the ***DES-3528 CLI Manual*** on the documentation CD for a list of all commands and additional information on using the CLI.
13. When you have completed your tasks, exit the session with the logout command or close the emulator program.
14. Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100. You will be able to set the emulation by clicking on the **File** menu in you HyperTerminal window, clicking on **Properties** in the drop-down menu, and then clicking the **Settings** tab. This is where you will find the **Emulation** options. If you still do not see anything, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear on your console screen. This is where the user will enter commands to perform all the available management functions. The Switch will prompt the user to enter a user name and a password. Upon the initial connection, there is no user name or password and therefore just press enter twice to access the command line interface.

```
                    DES-3528 Fast Ethernet Switch
                        Command Line Interface

                      Firmware: Build 1.00.B030
    Copyright(C) 2008 D-Link Corporation. All rights reserved.


Username:
```

Figure 4- 1. Initial screen after first connection

First Time Connecting to the Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

NOTE: The passwords used to access the Switch are case-sensitive; therefore, "S" is not the same as "s."

When you first connect to the Switch, you will be presented with the first login screen.

NOTE: Press Ctrl+R to refresh the screen. This command can be used at any time to force the console program in the Switch to refresh the console screen.

Press **Enter** in both the Username and Password fields. You will be given access to the command prompt **DES-3528:5#** shown below:

There is no initial username or password. Leave the Username and Password fields blank.

```
                DES-3528 Fast Ethernet Switch
                   Command Line Interface

                  Firmware: Build 1.00.B030
    Copyright(C) 2008 D-Link Corporation. All rights reserved.

Username:

PassWord:

DES-3528:5#
```

Figure 4- 2. Command Prompt

NOTE: The first user automatically gets Administrator level privileges. It is recommended to create at least one Admin-level user account for the Switch.

Password Protection

The Switch does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. Once logged in using a predefined administrator-level user name, users will have privileged access to the Switch's management software.

After your initial login, define new passwords for both default user names to prevent unauthorized access to the Switch, and record the passwords for future reference.

To create an administrator-level account for the Switch, follow these steps:

At the CLI login prompt, enter **create account admin** followed by the *<user name>* and press the **Enter** key.

The switch will then prompt the user for a password. Type the *<password>* used for the administrator account being created and press the **Enter** key.

Again, the user will be prompted to enter the same password again to verify it. Type the same password and press the **Enter** key.

Successful creation of the new administrator account will be verified by a Success message.

NOTE: Passwords are case sensitive. User names and passwords can be up to 15 characters in length.

The sample below illustrates a successful creation of a new administrator-level account with the user name "newmanager".

```
DES-3528:5# create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password: ********
Enter the new password again for confirmation: ********

Success.


DES-3528:5#
```

Figure 4- 3. New administrator level account

NOTICE: CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all your configuration changes in nonvolatile storage, you must use the save command to copy the running configuration file to the startup configuration.

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 DES-3528 supports SNMP versions 1, 2c, and 3. You can specify which version of SNMP 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.

SNMP v.3 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 SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.

Using SNMP v.3 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 SNMP v.3 in that SNMP messages may be encrypted. To read more about how to configure SNMP v.3 settings for the Switch read the section entitled Management.

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.

IP Address Assignment

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 Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "**show switch**" into the command line interface, as shown below.

```
DES-3528:5#show switch
Command: show switch

Device Type         : DES-3528 Fast Ethernet Switch
MAC Address         : 00-01-02-03-04-00
IP Address          : 10.24.73.21 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : Build 1.00.B005
Firmware Version    : Build 1.00.B030
Hardware Version    : A1
System Name         :
System Location     :
System Contact      :
Spanning Tree       : Disabled
GVRP                : Disabled
IGMP Snooping       : Disabled
MLD Snooping        : Disabled
TELNET              : Enabled (TCP 23)
WEB                 : Enabled (TCP 80)
SNMP                : Enabled
SSL Status          : Disabled
SSH Status          : Disabled
802.1x              : Disabled

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 4- 4. Show switch command

The Switch's MAC address can also be found from the Web management program on the **Switch Information (Basic Settings)** window on the **Configuration** menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands

config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy

Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

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

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

```
DES-3528:5#config ipif System ipaddress 10.90.90.90/255.0.0.0
Command: config ipif System ipaddress 10.90.90.90/8


Success.


DES-3528:5#
```

Figure 4- 5. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.90.90.90 with a subnet mask of 255.0.0.0. (the CIDR form was used to set the address (10.90.90.90/8). The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

Section 5

Web-based Switch Configuration

Introduction

Login to Web manager

Web-Based User Interface

Basic Setup

Reboot

Basic Switch Setup

Network Management

Switch Utilities

Network Monitoring

IGMP Snooping Status

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.

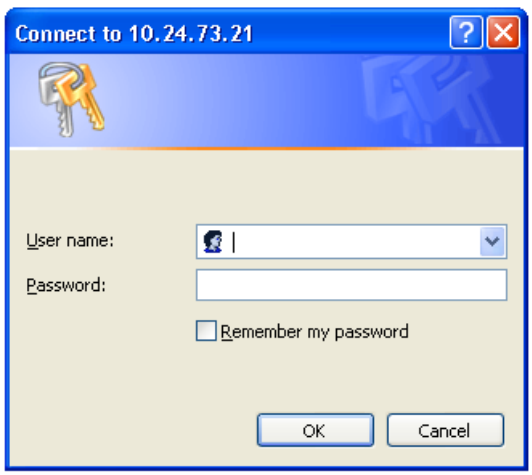


Figure 5- 1. Enter Network Password dialog

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.

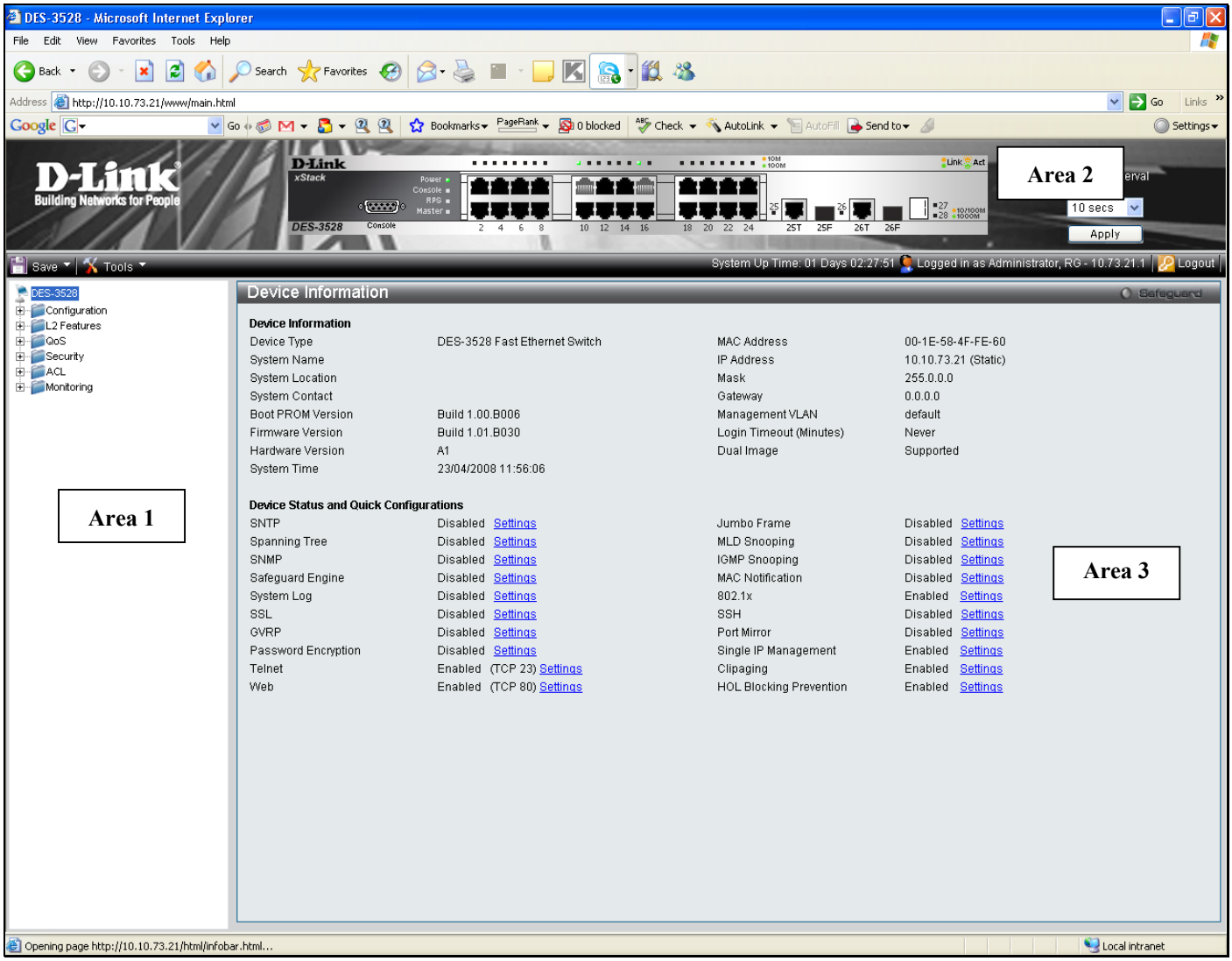


Figure 5- 2. Main Web-Manager page

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 – Contains windows concerning configuring the basic functions of the Switch, including accessing the System information, Serial Port Settings, IP Address, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, System Severity Settings, DHCP/BOOTP Relay, DHCP Auto Configuration Settings, MAC Address Aging Time, Web Settings, Telnet Settings, Password Encryption, Clipaging Settings, Firmware Information, Dual Configuration Settings, Ping Test, SNTP Settings, MAC Notification Settings, SNMP Settings, Time Range Settings and Single IP Management.

Layer 2 Features – Contains windows concerning Layer 2 features of the Switch, including Jumbo Frame, 802.1Q VLAN, QinQ, 802.1v Protocol VLAN, GVRP Settings, GVRP Timer Settings, Asymmetric VLAN Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, IGMP Snooping, MLD Snooping Settings, Port Mirror, Loopback Detection Settings, Spanning Tree, Forwarding & Filtering and LLDP.

QoS – Contains windows concerning HOL Prevention Settings, Bandwidth Control, Traffic Control, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Mechanism and SRED.

Security – Contains windows for 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, JWAC and NetBIOS Filtering Services.

ACL – Contains the window for ACL Configuration Wizard, Access Profile List, CPU Access Profile List, ACL Finder, and ACL Flow Meter.

Monitoring – Contains windows for Device Status, CPU Utilization, Port Utilization, Packet Size, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, Show VLAN Ports, Browse Router Ports, Browse MLD Router Ports, Browse Session Table, IGMP Snooping, MLD Snooping Group, JWAC Host Table, MAC Address Table 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 6

Configuration

System Information
Serial Port Settings
IP Address
Port Configuration
Static ARP Settings
User Accounts
System Log Configuration
System Severity Settings
DHCP/BOOTP Relay
MAC Address Aging Time
Web Settings
Telnet Settings
Password Encryption
Clipaging Settings
Firmware Information
Dual Configuration Settings
Ping Test
SNTP Settings
MAC Notification Settings
SNMP Settings
Time Range Settings
Single IP Management

Device Information

This window contains the main settings for all major functions on the Switch and appears automatically when you log on. To return to the **Device Information** window, click the **DES-3528 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**, and **Hardware Version**. This information is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status. Some functions are hyper-linked to their configuration window for easy access from the **Device Information** window.

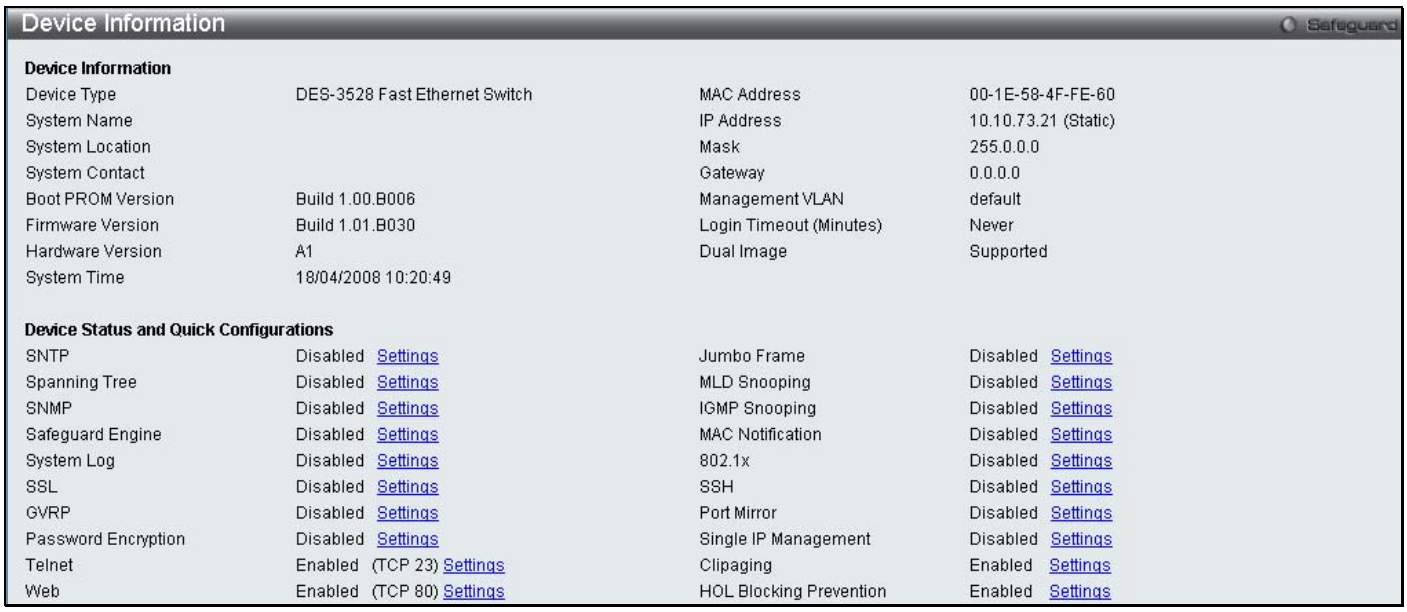


Figure 6- 1. Device Information window

System Information

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

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

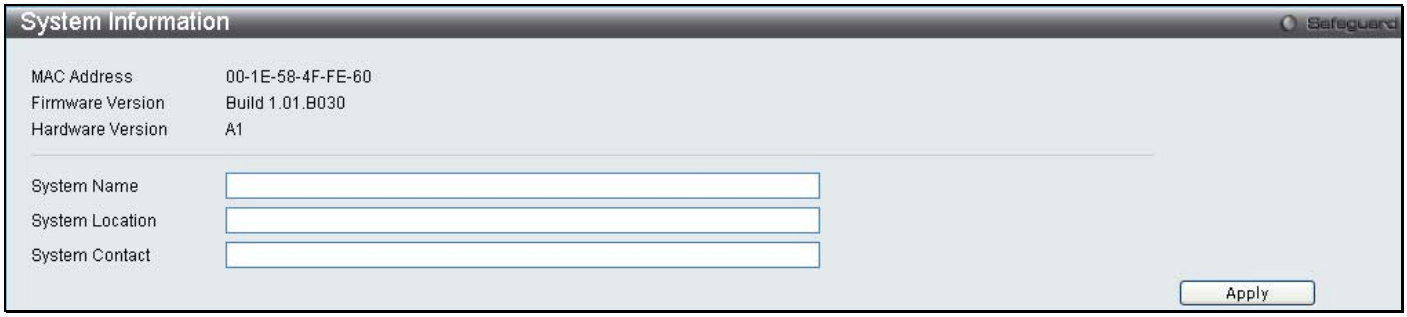


Figure 6- 2. System Information window

The fields that can be configured are described below:

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

Click **Apply** to implement changes made.

Serial Port Settings

The following window contains information about the Serial Port Settings to view this window click **Configuration** > **Serial Port Settings:**

Figure 6- 3. Serial Port Settings window

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

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 *DES-3528 CLI Manual* or return to Section 4 of this manual for more information. To change IP settings using the web manager you must access the **IP Address** window located in the **Configuration** folder.

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

Figure 6- 4. IP Address Settings window

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 IP Address Settings options are:

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

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

Setting the Switch's IP Address using the Console Interface

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

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

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy.** Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

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

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

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

Port Configuration

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

Port Settings

Click **Configuration** > **Port Configuration > Port Settings** to display the following window:

To configure switch ports:

1. Choose the port or sequential range of ports using the From…To… port pull-down menus.

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

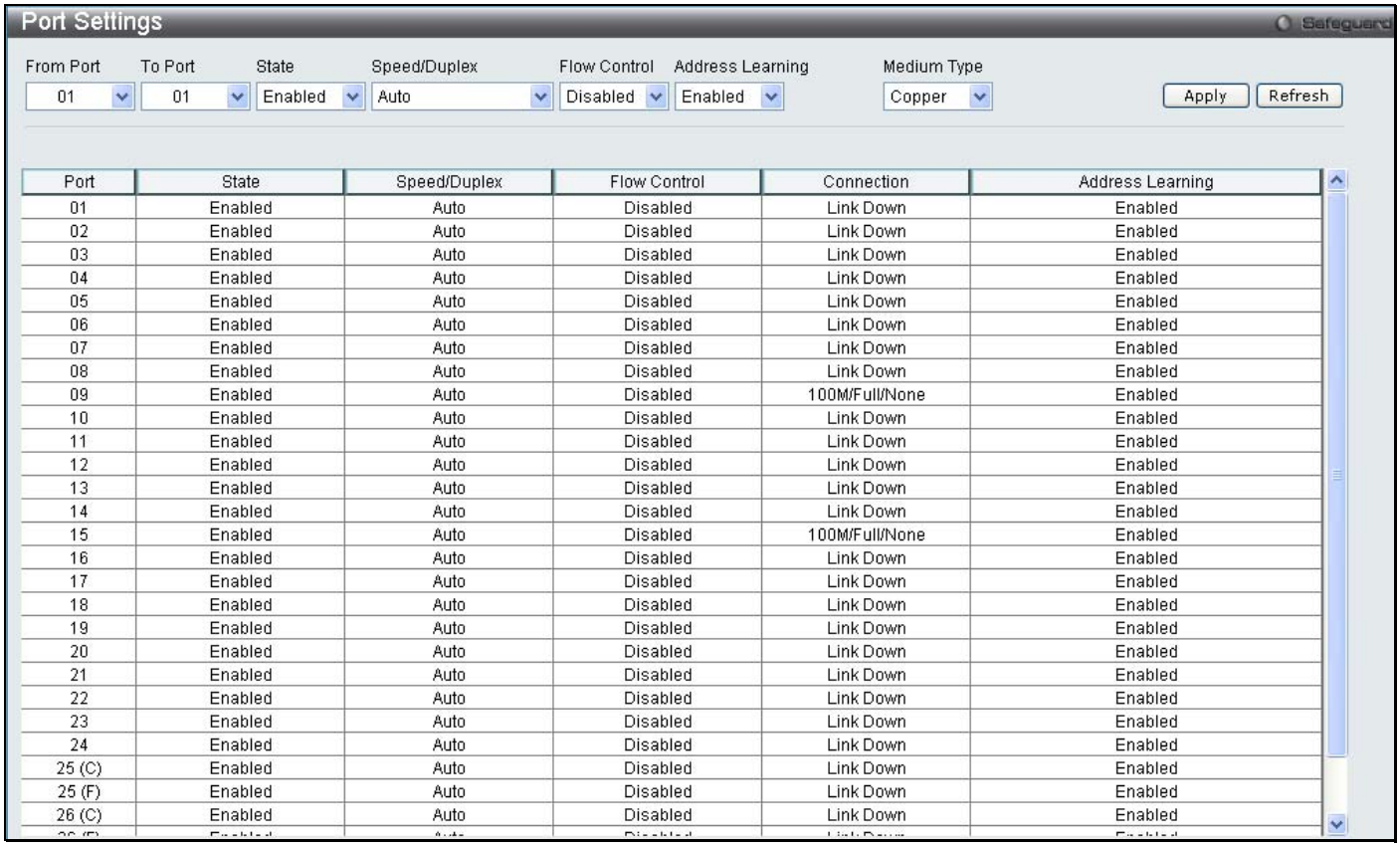


Figure 6- 5. Port Settings window

The following parameters can be configured:

Parameter	Description
From Port…. To Port	Use the pull-down menus to select the port or range of ports to be configured.
State	Toggle this field to either enable or disable a given port or group of ports.
Speed/Duplex	Toggle the **Speed/Duplex** field to either select the speed and duplex/half-duplex state of the port. *Auto* denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The *Auto* setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *Auto*, *10M/Half*, *10M/Full, 100M/Half* and *100M/Full*, *1000M/Full_M, 1000M/Full_S* and *1000M/Full*. There is no automatic adjustment of port settings with any option other than Auto. The Switch allows the user to configure two types of gigabit connections; *1000M/Full_M* and *1000M/Full_S*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M/Full_M* (master) and *1000M/Full_S* (slave) parameters refer to connections running

	a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (*1000M/Full_M)* will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (*1000M/Full_S)* uses loop timing, where the timing comes form a data stream received from the master. If one connection is set for *1000M/Full_M*, the other side of the connection must be set for *1000M/Full_S*. Any other configuration will result in a link down status for both ports.
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and *Auto* ports use an automatic selection of the two. The default is *Disabled*.
Address Learning	When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. The default setting is *Enabled*.
Medium Type	This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be set at *Fiber* and the Combo 1000BASE-T ports should be set at *Copper*.

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

Port Description

The Switch supports a port description feature where the user may name various ports on the Switch. To assign names to various ports, click **Configuration** > **Port Configuration** > **Port Description** to view the following window:

Use the **From** and **To** 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 tranport 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).

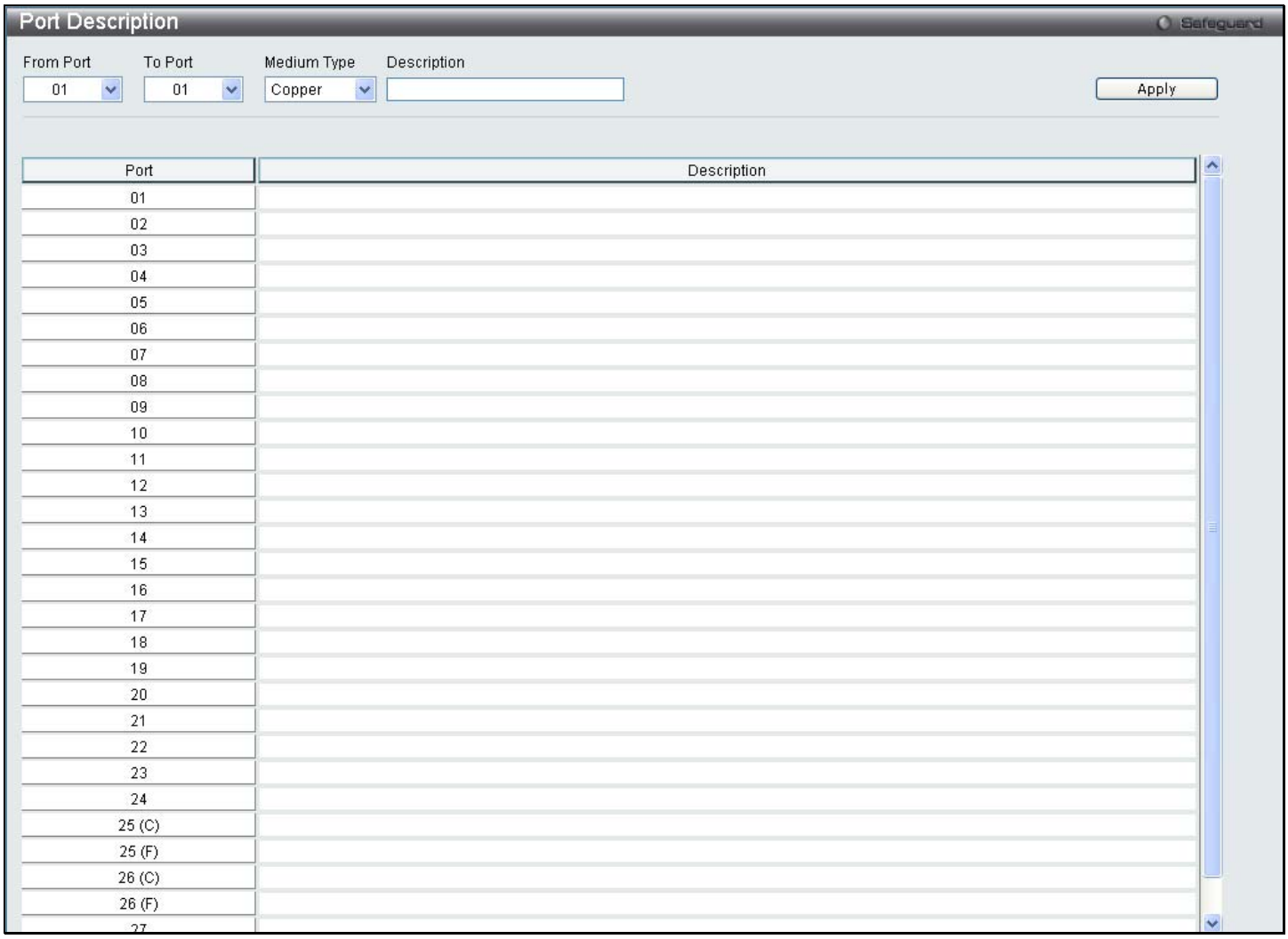


Figure 6- 6. Port Description window

Port Error Disabled

The following window will display the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status. To view this window, click **Configuration** > **Port Configuration > Port Error Disabled**.

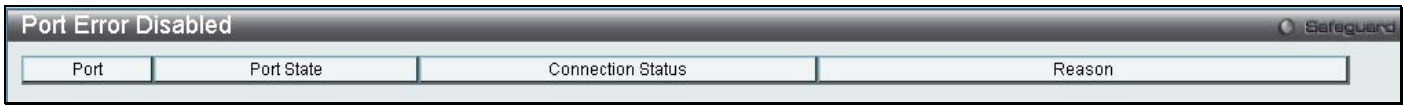


Figure 6- 7. Port Error Disabled window

The following parameters are displayed:

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

Static ARP Settings

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

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

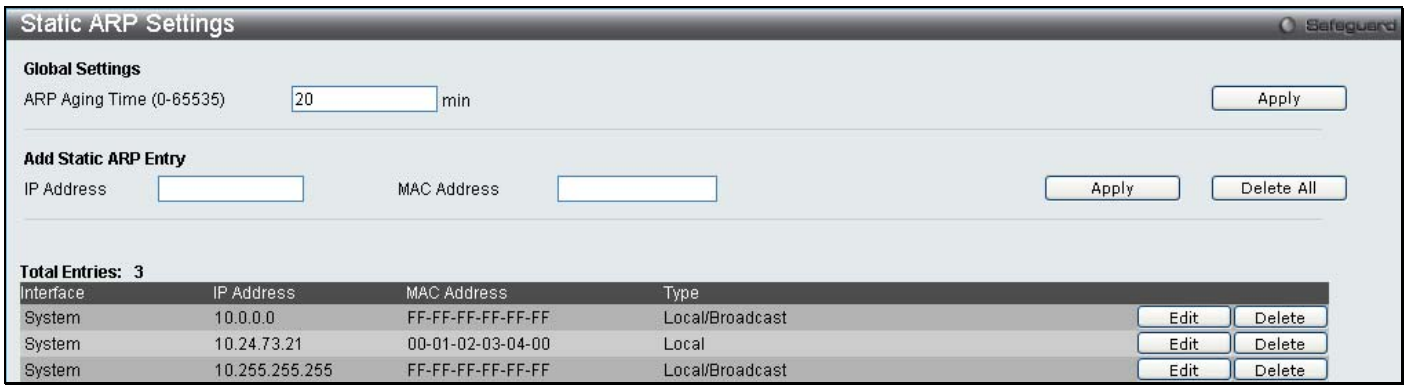


Figure 6- 8. Static ARP Settings window

The following fields can be set:

Parameter	Description
ARP Aging Time (0-65535)	The user may globally set the maximum amount of time, in 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.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To completely clear the Static ARP Settings, click the **Delete All** button.

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.**

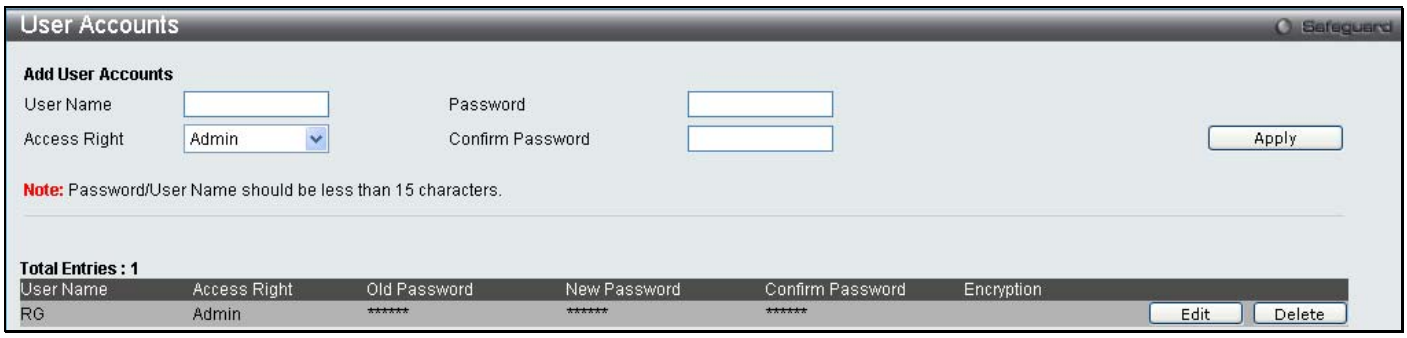


Figure 6- 9. User Accounts window

The following fields can be set:

Parameter	Description
User Name	The name of the user, an alphanumeric string of up to 15 characters.
Access Right	There are three levels of user privileges, **Admin, Operator** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** or **Operator** level privileges. There are 3 levels of security offered on the Switch, the **Operator** level privilege will allow users to configure and view configurations on the Switch, except for those involving security features, which are still left to the **Admin** level privilege. **Operator** level users can be authenticated through either the local authentication method of the Switch, or through the Access Authentication Control feature, discussed later in this document. Once the user has logged in to the Switch in the **Operator** level, certain security screens and windows will not be made available to view, or to configure. Only **Admin** level users have access to these features. (**Table 6-1** below summarizes **Admin, Operator** and **User** level privileges)
New Password	Enter a password for the new user.
Confirm New Password	Retype the new password.

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

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

Admin, Operator and User Privileges

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

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

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

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

Table 6- 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 configure the system log settings click **Configuration** > **System Log Configuration** > **System Log Settings:**

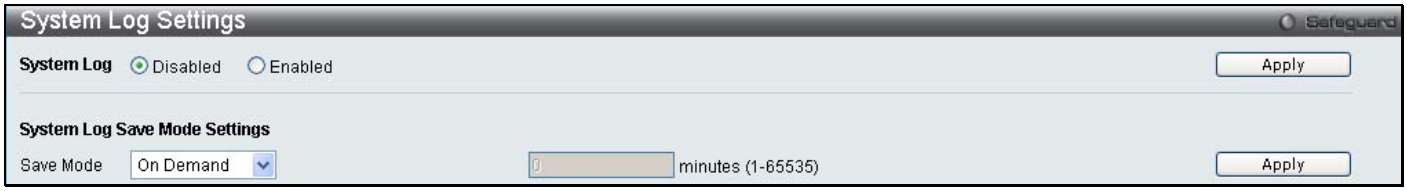


Figure 6- 10. System Log Settings window

The following parameters can be set:

Parameter	Description
Save Mode	Use this drop-down menu to choose the method that will trigger a log entry. You can choose between *On Demand*, *Log Trigger*, and *Time Interval*.
Minutes (1-65535)	Enter a time interval, in seconds, for which you would like a log entry to be made.

To add a new entry, enter the appropriate information and click **Apply**. To save the current Log Settings, click **Save Log Now**.

System Log Server

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

To configure the system log settings click **Configuration** > **System Log Configuration** > **System Log Server:**

Figure 6- 11. System Log Server window

The following parameters can be set:

Parameter	Description
Server ID	Syslog server settings index (1-4).
Server IP Address	The IP address of the Syslog server.
UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is *514*.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *All*.

Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values that the Switch is currently employing. **Numerical Facility Code**
	0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon **16 local use 0 (local0)** **17 local use 1 (local1)** **18 local use 2 (local2)** **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)**
Status	Choose *Enabled* or *Disabled* 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. In the **Configuration** folder, click **System Severity Settings**, to view the window shown below.

Figure 6- 12. System Severity Settings

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

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

The relay hops count limit allows the maximum number of hops (routers) that the DHCP/BOOTP 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 BOOTREQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between *0* and *65,536* seconds, with a default value of *0* seconds.

DHCP/BOOTP Relay Global Settings

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

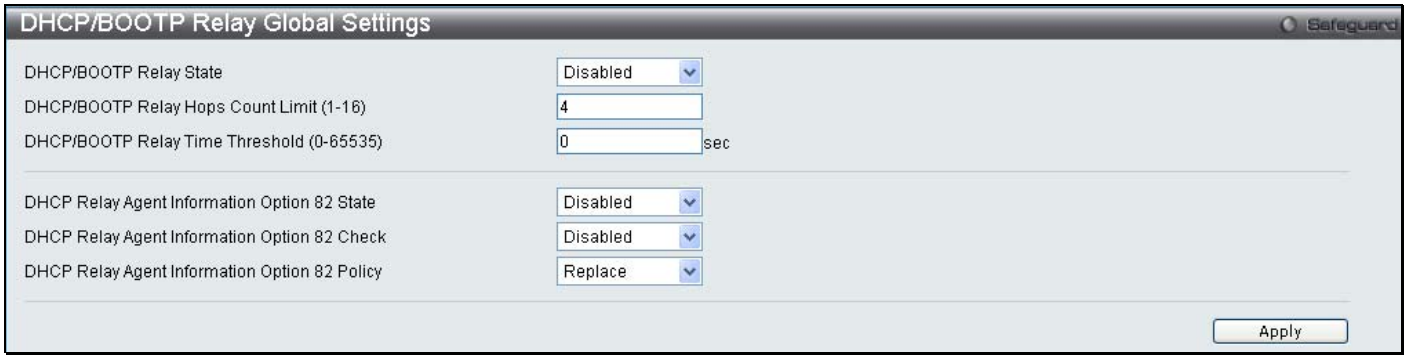


Figure 6- 13. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
BOOTP Relay State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is *Disabled*
BOOTP Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is *4*.
BOOTP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP/BOOTP packet. If a value of 0 is entered, the Switch will not process the value in the **seconds** field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.
DHCP Relay Agent Information Option 82 State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is *Disabled.* *Enabled* – When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *Disabled* - If the field is toggled to *Disabled* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the

	check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field. *Enabled* – When the field is toggled to *Enable*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *Disabled* - When the field is toggled to *Disabled*, the relay agent will not check the validity of the packet's option 82 field.
DHCP Relay Agent Information Option 82 Policy	This field can be toggled between *Replace, Drop,* and *Keep* by using the pull-down menu. It is used to set the Switches policy for handling packets when the **DHCP Agent Information Option 82 Check** is set to *Disabled*. The default is *Replace.* *Replace* - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.

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 in the DES-3528 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

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

Remote ID sub-option format:

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

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

Figure 6- 14. Circuit ID and Remote ID Sub-option Format

DHCP/BOOTP Relay Interface Settings

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

Figure 6- 15. DHCP/BOOTP Relay Interface Settings and DHCP/BOOTP Relay Interface Table window

The following parameters may be configured or viewed.

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

DHCP Auto Configuration Settings

The DHCP autoconfiguration function on the Switch will load a previously saved configuration file for current use. When DHCP autoconfiguration 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.

Figure 6- 16. 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, type in a value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1,000,000* seconds. The default setting is *300* seconds.

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

Figure 6- 17. 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 access this table, click **Configuration** > **Web Settings:**

Figure 6- 18. Web Settings window

Telnet Settings

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

To access this table, click **Configuration** > **Telnet Settings:**

Figure 6- 19. Telnet Settings window

Password Encryption

Password Encryption Status can be *Enabled* or *Disabled* in this window, it is *Disabled* by default.

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

Figure 6- 20. Password Encryption window

Clipaging Settings

Clipaging Status can be *Enabled* or *Disabled* in this window, it is *Enabled* by default.

To access this table, click **Configuration** > **Clipaging Settings:**

Figure 6- 21. Clipaging Settings window

Firmware Information

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

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

Figure 6- 22. Firmware Information window

This window holds the following information:

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

Dual Configuration Settings

The following window is used to configure firmware information set in the Switch. The xStack DES-3528 has the capability to store two firmware images in its memory.

To access this table, click **Configuration** > **Dual Configuration Settings:**

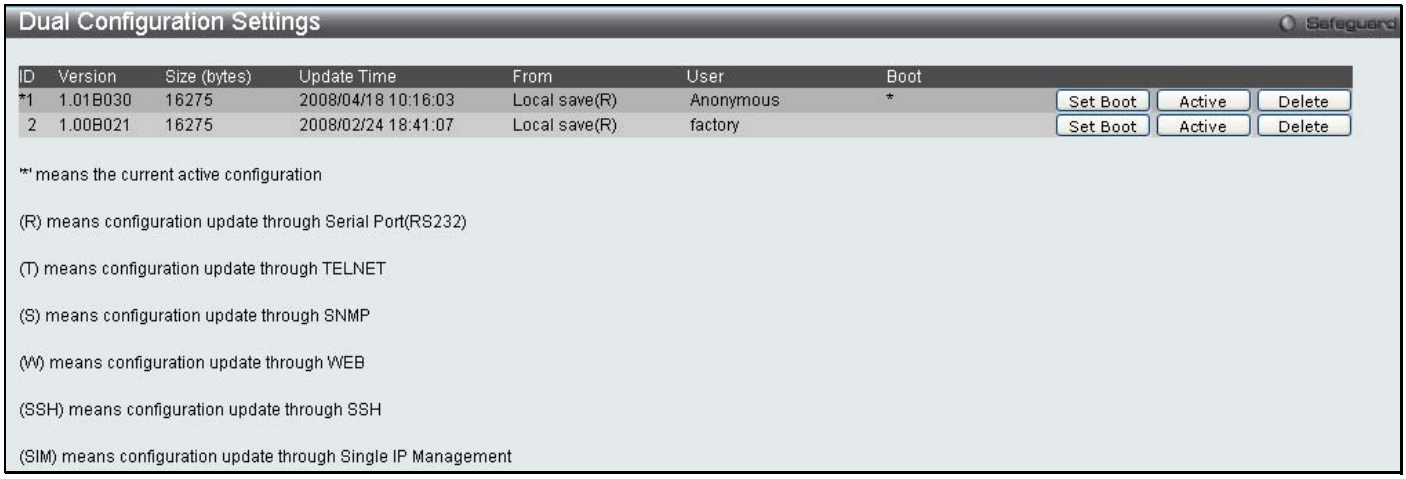


Figure 6- 23. Dual Configuration Settings

This window holds the following information:

Parameter	Description
ID	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.
Version	Displays the firmware version set in the Switch.
Size(bytes)	Displays the size of the configuration file, in bytes.
Update time	Displays the time that the configuration file was updated to the Switch.
From	Displays the location from which the configuration file was uploaded.
User	Displays the name of the user (device) that updated this configuration file. Unknown users will be displayed as Anonymous.
Boot	Click the **Boot** 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.
Active	Click the **Active** button to enable the configuration file settings.
Delete	Click the **Delete** 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 IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To access this table, click **Configuration** > **Ping Test:**

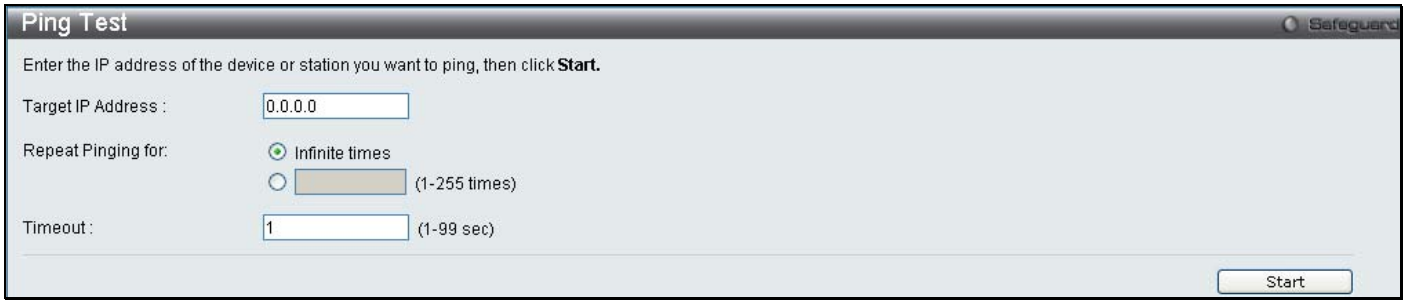


Figure 6- 24. Ping Test window

The user may use Infinite times radio button, in the **Repeat Pinging for** field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the **Target IP Address** by entering a number between *1* and *255*. Click **Start** to initiate the Ping program

SNTP Settings

Time Settings

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

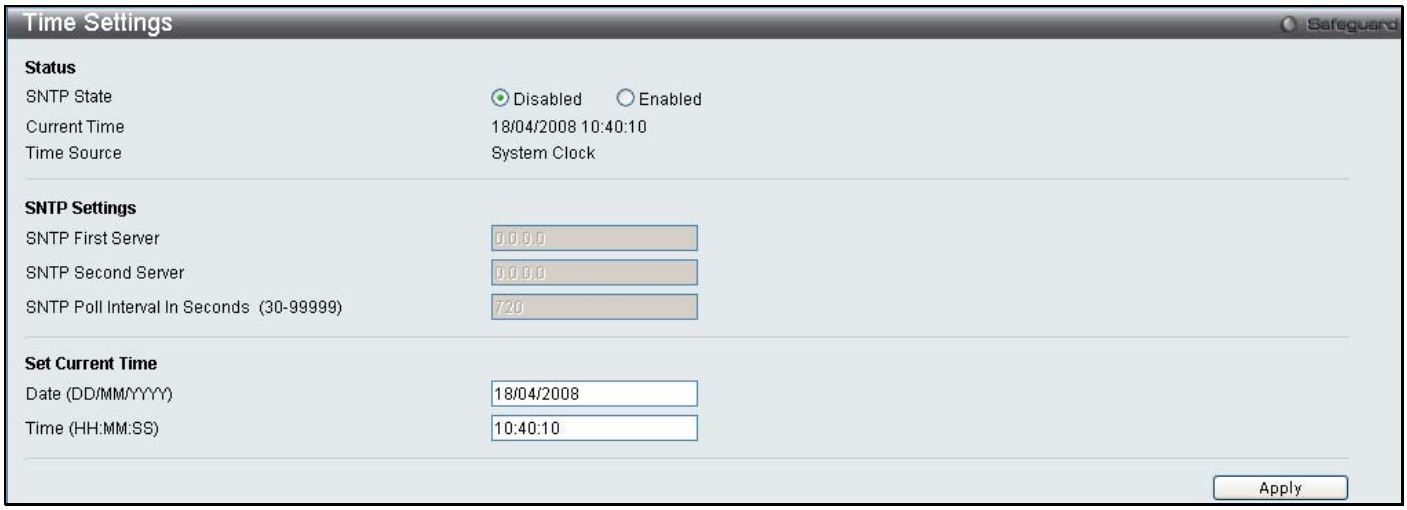


Figure 6- 25. Time Settings window

The following parameters can be set or are displayed:

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

Click **Apply** to implement changes made.

TimeZone Settings

The following window is used to configure time zones and Daylight Savings time settings for SNTP. To configure the time Zone Settings for the Switch, click **Configuration** > **SNTP Settings** > **TimeZone Settings:**

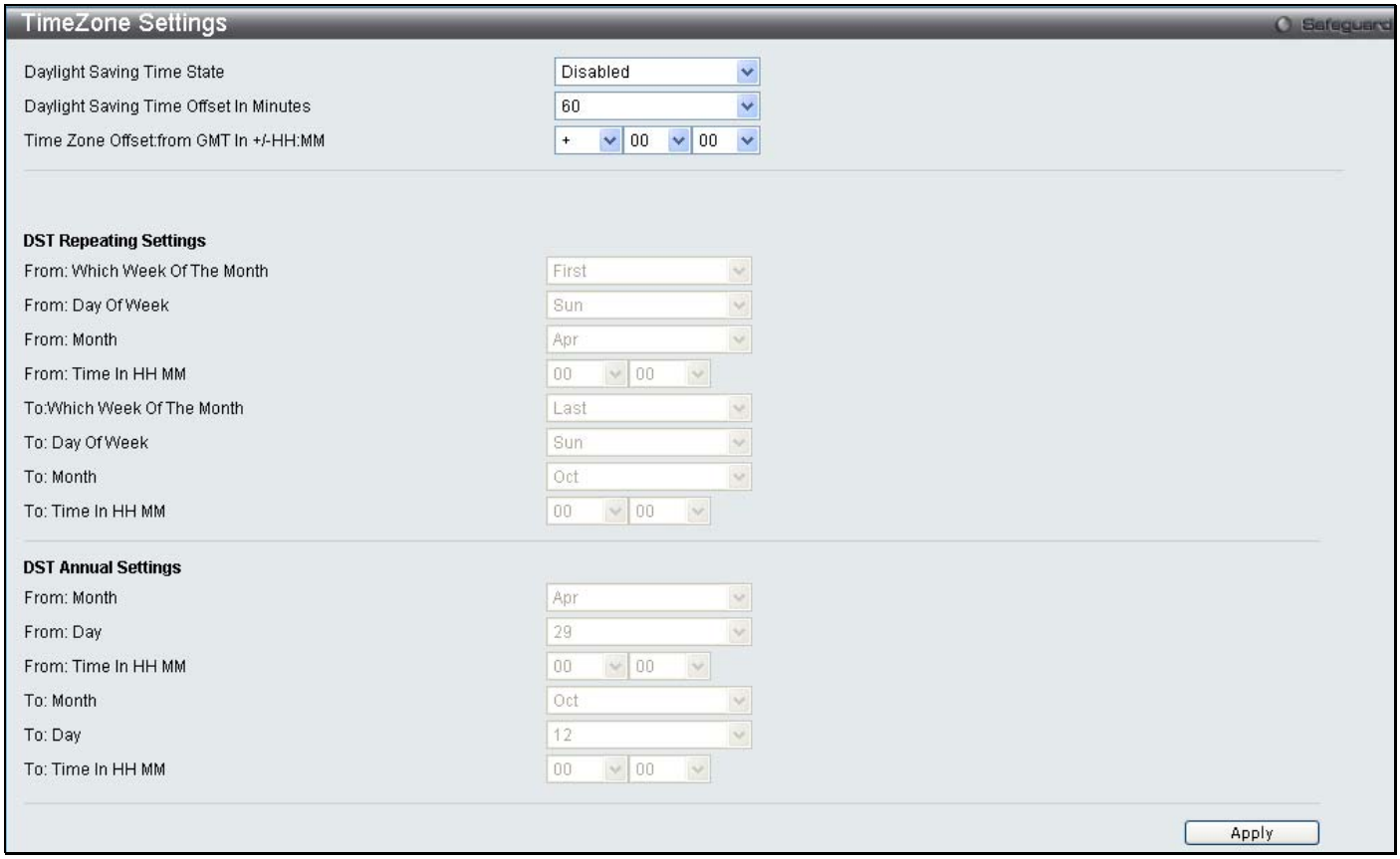


Figure 6- 26. Time Zone and DST Settings window

The following parameters can be set:

Parameter	Description
Time Zone and DST	
Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset - *30*, *60*, *90*, or *120* minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
DST Repeating Settings Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From :Which Week of the Month	Enter the week of the month that DST will start.
From: Day of the Week	Enter the day of the week that DST will start on.

Week	
From: Month	Enter the month DST will start on.
From: Time in HH:MM	Enter the time of day that DST will start on.
To: Which Week of the Month	Enter the week of the month the DST will end.
To: Day of the Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To:Time in HH:MM	Enter the time DST will end.
DST Annual Settings Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.	
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the week DST will start on, each year.
From: Time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the date DST will end on, each year.
To: Time in HH:MM	Enter the time of day that DST will end on, each year.

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

MAC Notification Settings

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

MAC Notification Global Settings

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

Figure 6- 27. MAC Notification Global Settings window

The following parameters may be viewed and modified:

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

Click **Apply** to implement changes.

MAC Notification Port Settings

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

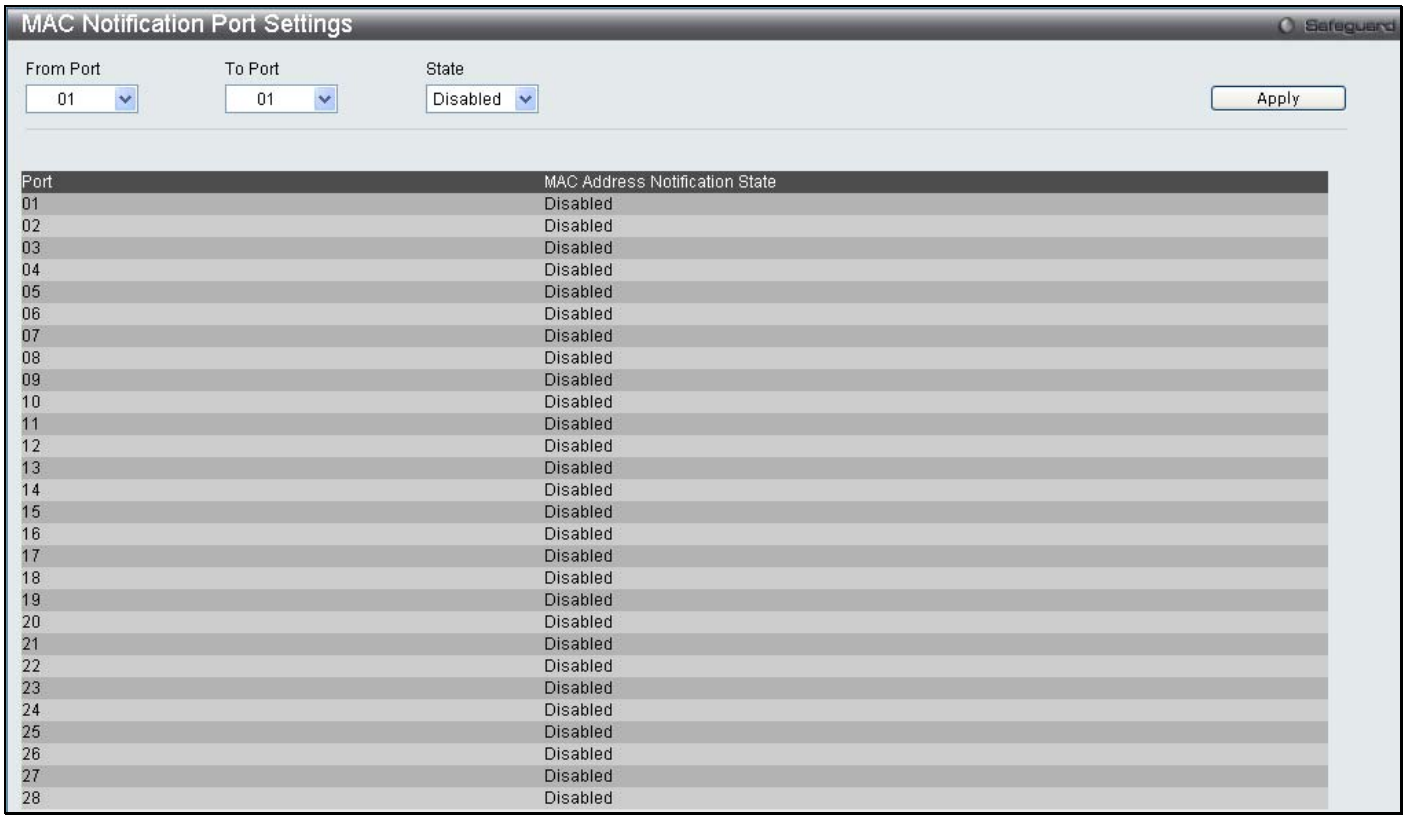


Figure 6- 28. MAC Notification Port Settings window

The following parameters may be modified:

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

Click **Apply** to implement changes.

SNMP Settings

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

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

The DES-3528 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 DES-3528 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 DES-3528 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

Use this table to globally enable or disable the SNMP Settings on the switch. To view this window, click **Configuration > SNMP Settings > SNMP Global State:**

Figure 6- 29. SNMP Global State 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 configure SNMP View Settings for the Switch, click **Configuration** > **SNMP Settings** > **SNMP View Table:**

Figure 6- 30. SNMP View Table window

The following parameters can be set:

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

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

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous menu. To view this window, click **Configuration** > **SNMP Settings** > **SNMP Group Table:**

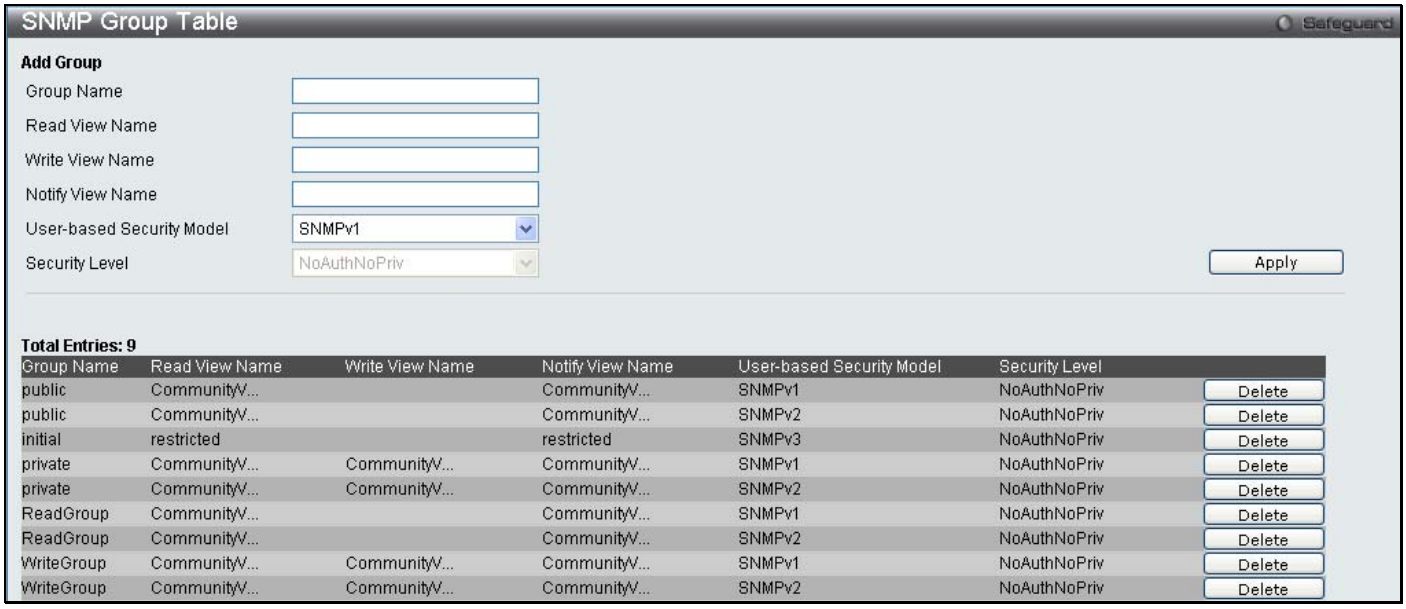


Figure 6- 31. SNMP Group Table window

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

The following parameters can be set:

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

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

SNMP User Table

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

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

Figure 6- 32. SNMP User Table window

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

The following parameters may be set:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V1* - Indicates that SNMP version 1 is in use. *V2* - Indicates that SNMP version 2 is in use. *V3* - Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	*None* – Indicates that there is no SNMP V3 Encryption *Password* – Indicates that there is SNMP V3 Encryption through a password *Key* – Indicates that there is SNMP V3 Encryption through a key.
Auth-Protocol by Password	*MD5* - Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by Password	*None* - Indicates that no authorization protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Auth-Protocol by Key	*MD5* - Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by password	*None* - Indicates that no authorization protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Password	Enter a Password when SNMP V3 Encryption is enabled for Password mode.
Key	Enter a Key when SNMP V3 Encryption is enabled for Key mode.

To implement changes made, click **Apply**.

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

Figure 6- 33. SNMP Community Table Configuration window

The following parameters can set:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	*Read Only* - Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* - Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

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

SNMP Host Table

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

Figure 6- 34. SNMP Host Table

The following parameters can set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* - Specifies that SNMP version 1 will be used. *SNMPV2c* - Specifies that SNMP version 2 will be used. *SNMPV3* - To specify that the SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify a NoAuthNoPriv security level. *AuthNoPriv* - To specify an AuthNoPriv security level. *AuthPriv* - To specify an AuthPriv security level.
Community String/ SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

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

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch. To display the Switch's SNMP Engine ID, click **Configuration** > **SNMP Settings** > **SNMP Engine ID**:

Figure 6- 35. SNMP Engine ID Configuration window

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

SNMP Trap Configuration

The following window is used to enable and disable trap settings for the SNMP function on the Switch. To view this window for configuration, click **Configuration > SNMP Settings > SNMP Trap Configuration**:

Figure 6-36. 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 open this window, click **Configuration > Time Range Settings**:

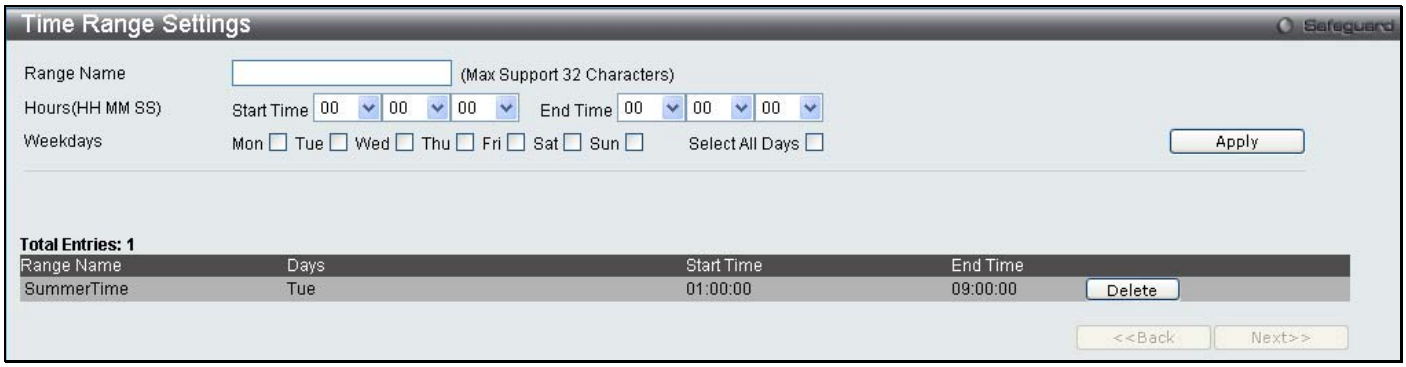


Figure 6-37. Time Range Settings window

Single IP Settings

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.

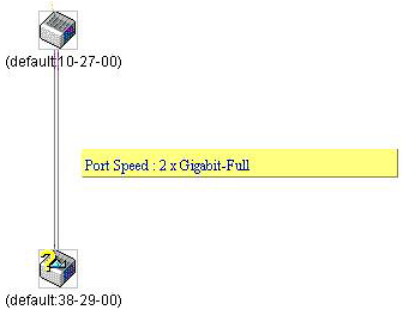
The Upgrade to v1.6

To better improve SIM management, the DES-3528 Switch has been upgraded to version 1.6 in this release. Many improvements have been made, including:

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

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

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

SIM Settings

All switches are set as Candidate (CaS) switches as their factory default configuration and Single IP Management will be disabled. To enable SIM for the Switch using the Web interface, click **Configuration** > **Single IP Managemnet > Single IP Settings** which will reveal the following window:

Figure 6- 38. 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**.

Figure 6- 39. Single IP Settings window (enabled)

The following parameters can be set:

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

Click **Apply** to implement the settings.

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

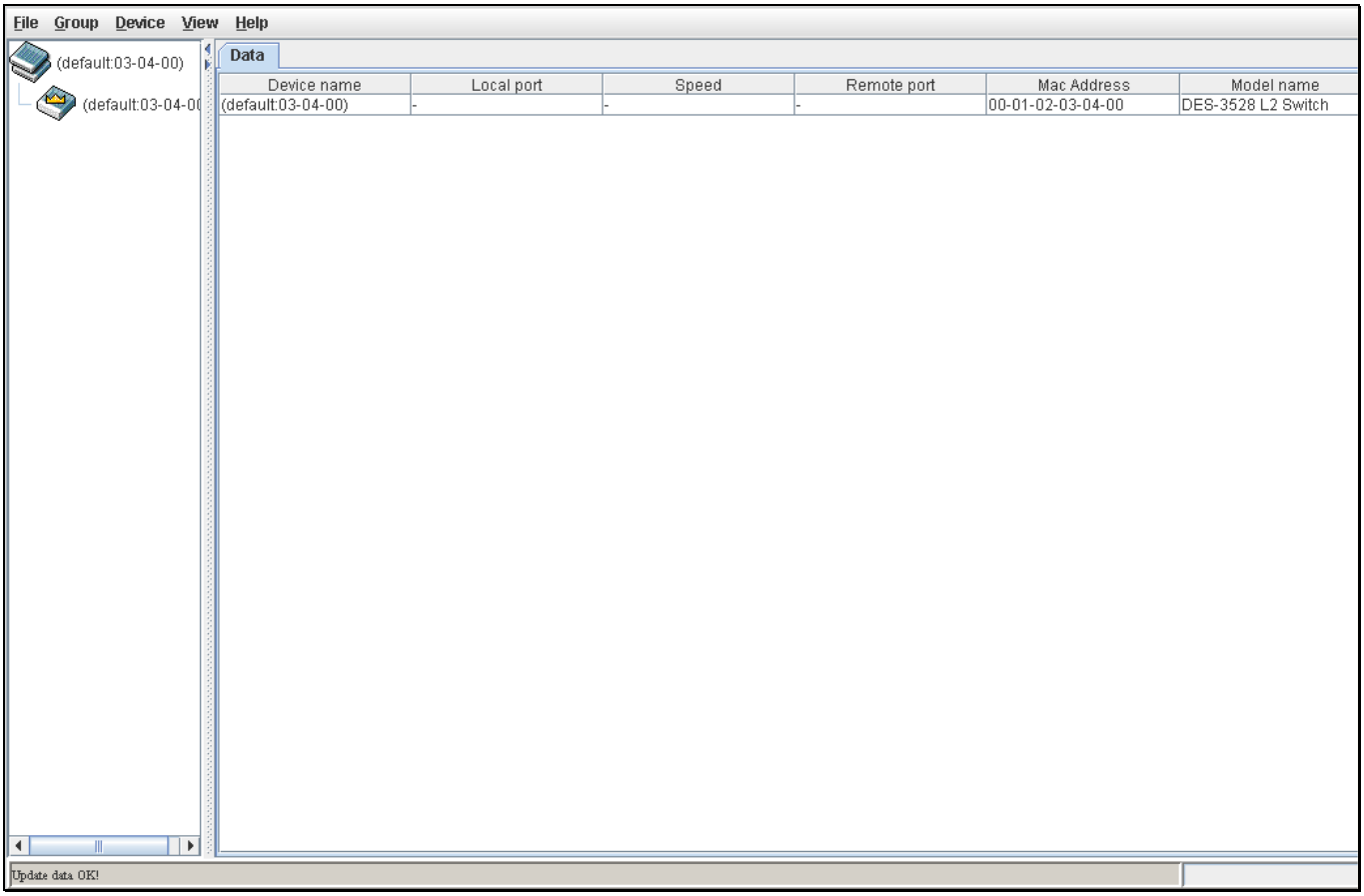


Figure 6- 40. Single IP Management window - Tree View

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

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

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

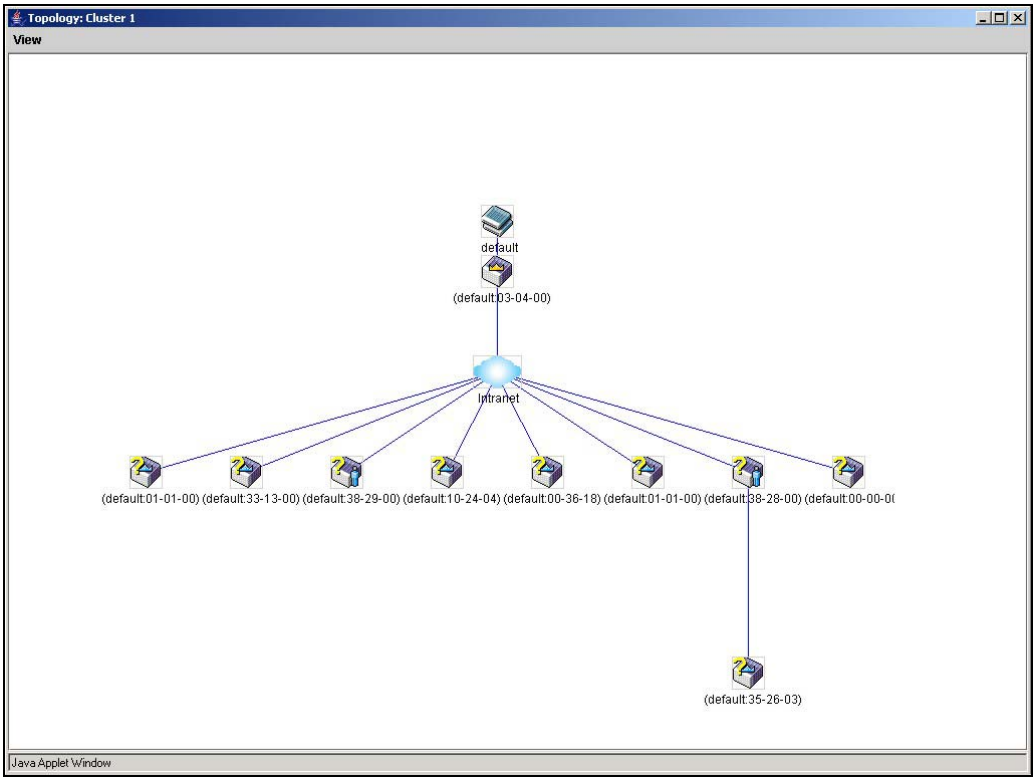


Figure 6- 41. Topology view

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.

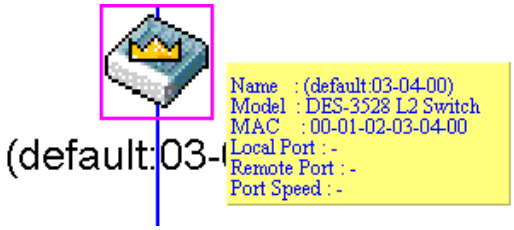


Figure 6- 42. Device Information Utilizing the Tool Tip

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

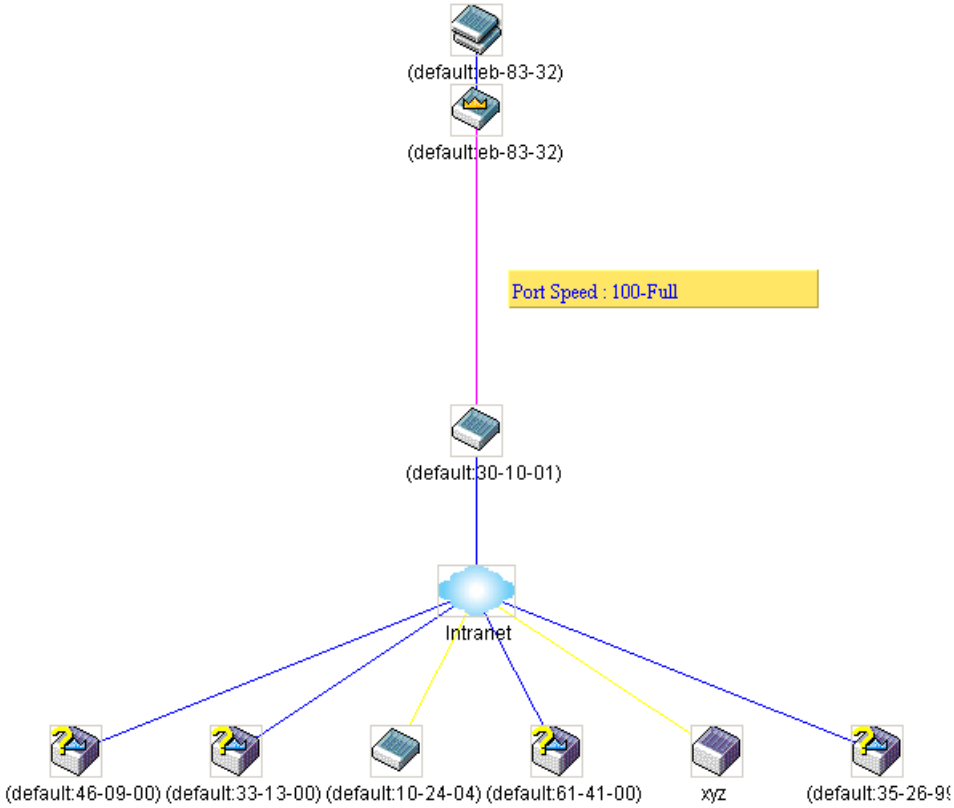


Figure 6- 43. Port Speed Utilizing the Tool Tip

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

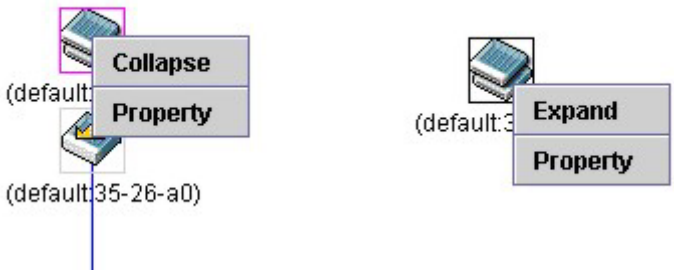


Figure 6- 44. Right-Clicking a Group Icon

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.

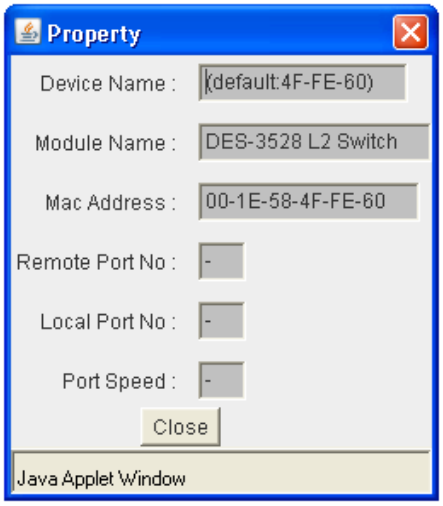


Figure 6- 45. Property window

This window holds the following information:

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

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

Commander Switch Icon

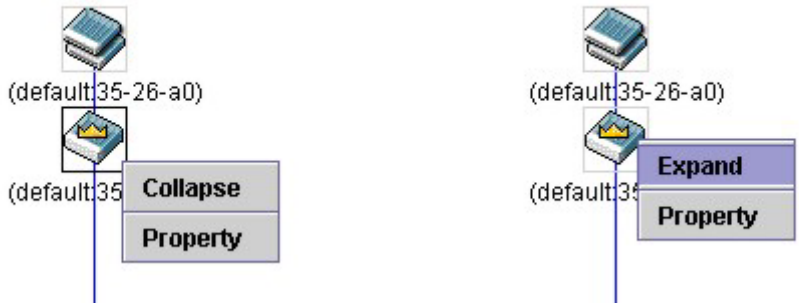


Figure 6- 46. Right-Clicking a Commander Icon

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

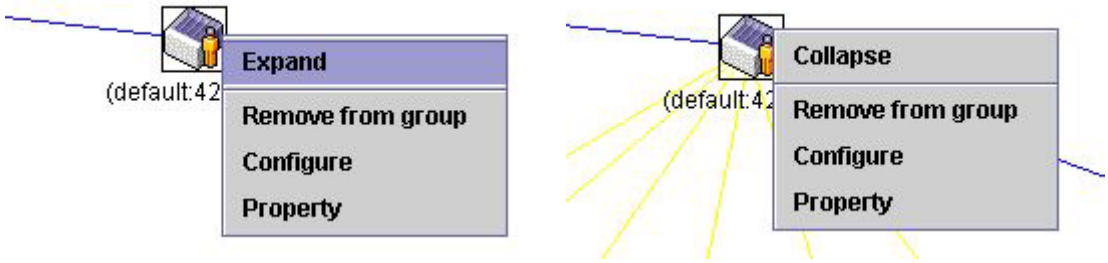


Figure 6- 47. Right-Clicking a Member icon

The following options may appear for the user to configure:

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

Expand - To expand the SIM group, in detail.

Remove from group - Remove a member from a group.

Configure - Launch the web management to configure the Switch.

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

Candidate Switch Icon

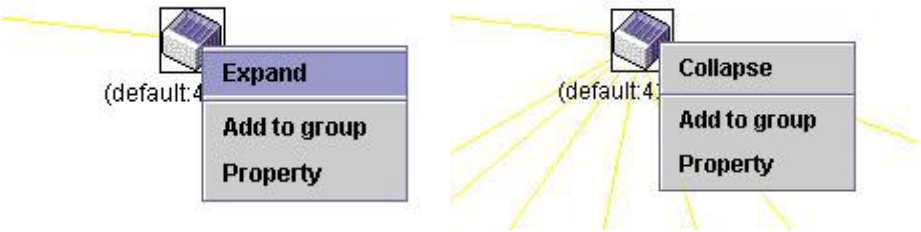


Figure 6- 48. Right-Clicking a Candidate icon

The following options may appear for the user to configure:

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

Expand - To expand the SIM group, in detail.

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

Figure 6- 49. 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 6- 50. 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 6- 51. 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 6- 52. 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 access the following window, click **Configuration > Single IP Management > Firmware Upgrade**.

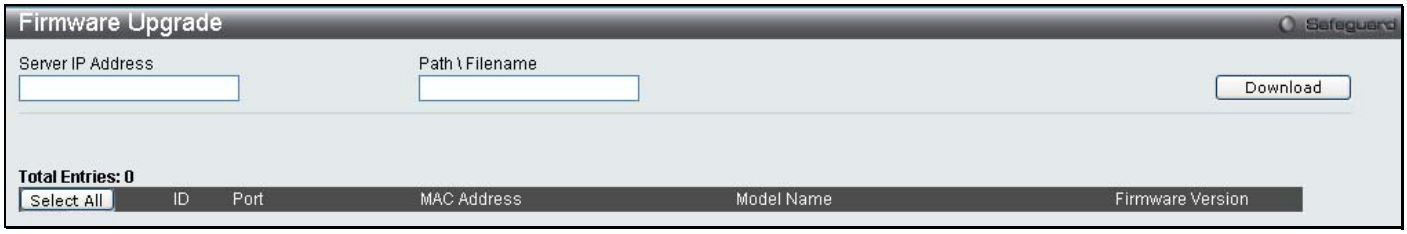


Figure 6- 53. Firmware Upgrade window

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 access the following window, click **Configuration > Single IP Management > Configuration File Backup/Restore**.

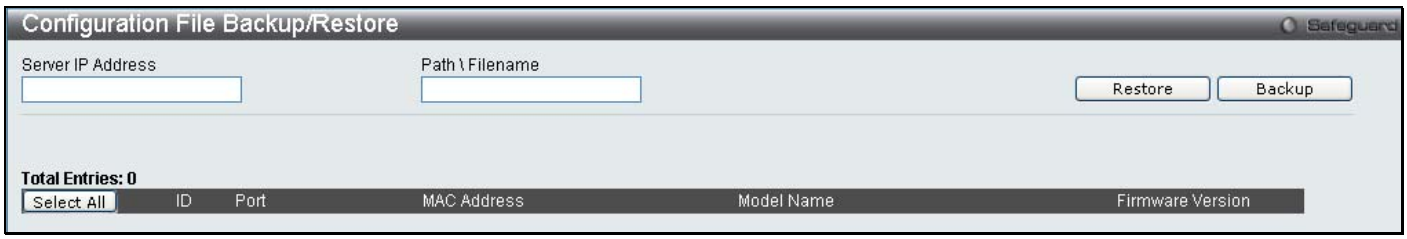


Figure 6- 54. Configuration File Backup/Restore window

Upload Log

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

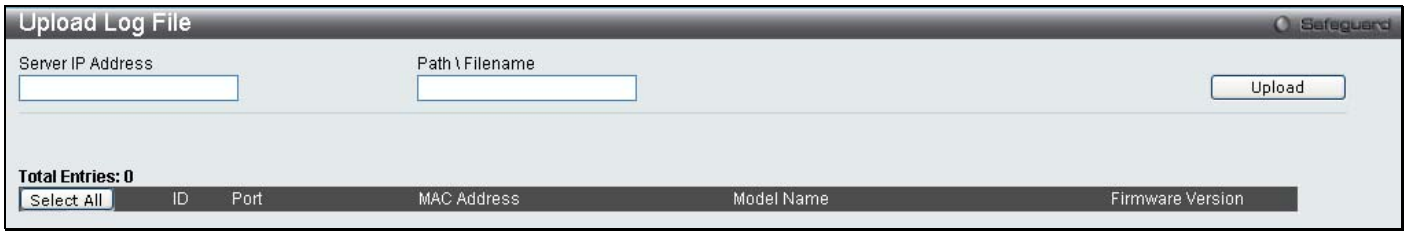


Figure 6- 55. Upload Log File window

Section 7

L2 Features

Jumbo Frame
802.1Q VLAN
QinQ
802.1v Protocol VLAN
GVRP Settings
GVRP Timer Settings
Asymmetric VLAN Settings
MAC-based VLAN Settings
PVID Auto Assign Settings
Port Trunking
LACP Port Settings
Traffic Segmentation
IGMP Snooping
MLD Snooping Settings
Port Mirror
Loopback Detection Settings
Spanning Tree
Forwarding and Filtering
LLDP

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 9K (and 9220 bytes tagged) can be transmitted by the Switch. To view this window click **L2 Features > Jumbo Frame.**

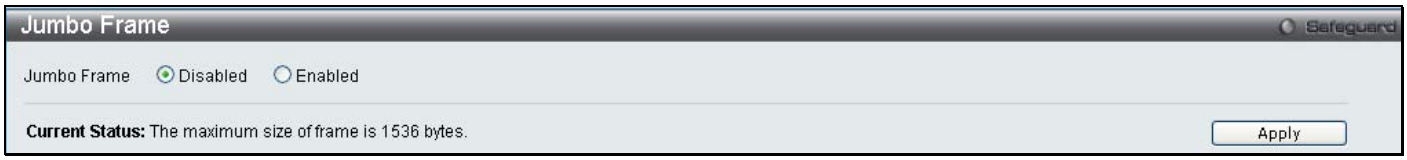


Figure 7- 1. Jumbo Frame window

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.

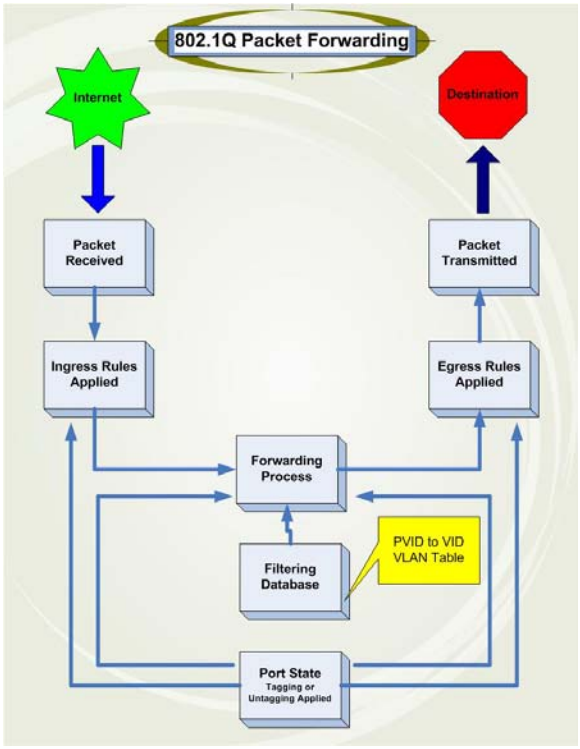


Figure 7- 2. IEEE 802.1Q Packet Forwarding

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.

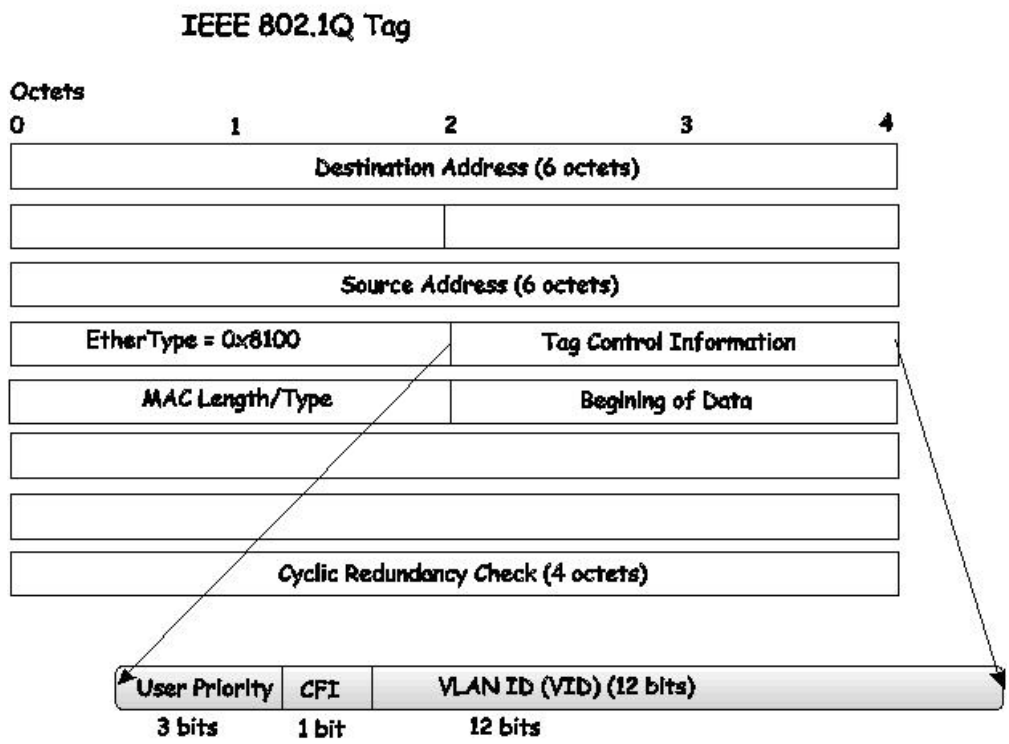


Figure 7- 3. IEEE 802.1Q Tag

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.

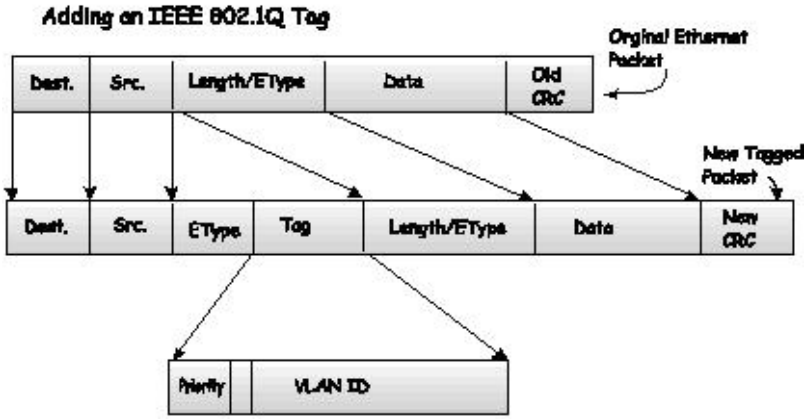


Figure 7- 4. Adding an IEEE 802.1Q Tag

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

Figure 7- 5. 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, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs 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:

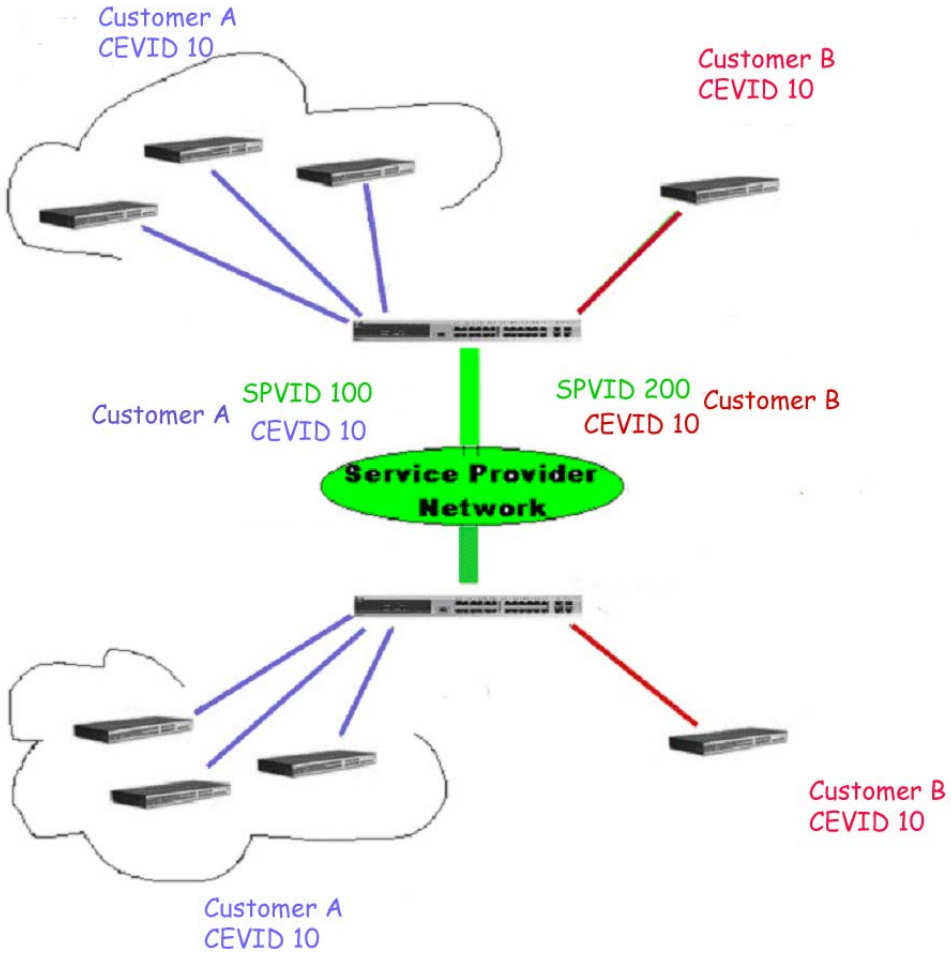


Figure 7- 6. Double VLAN Example

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), CEVLAN 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 seperate 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.**

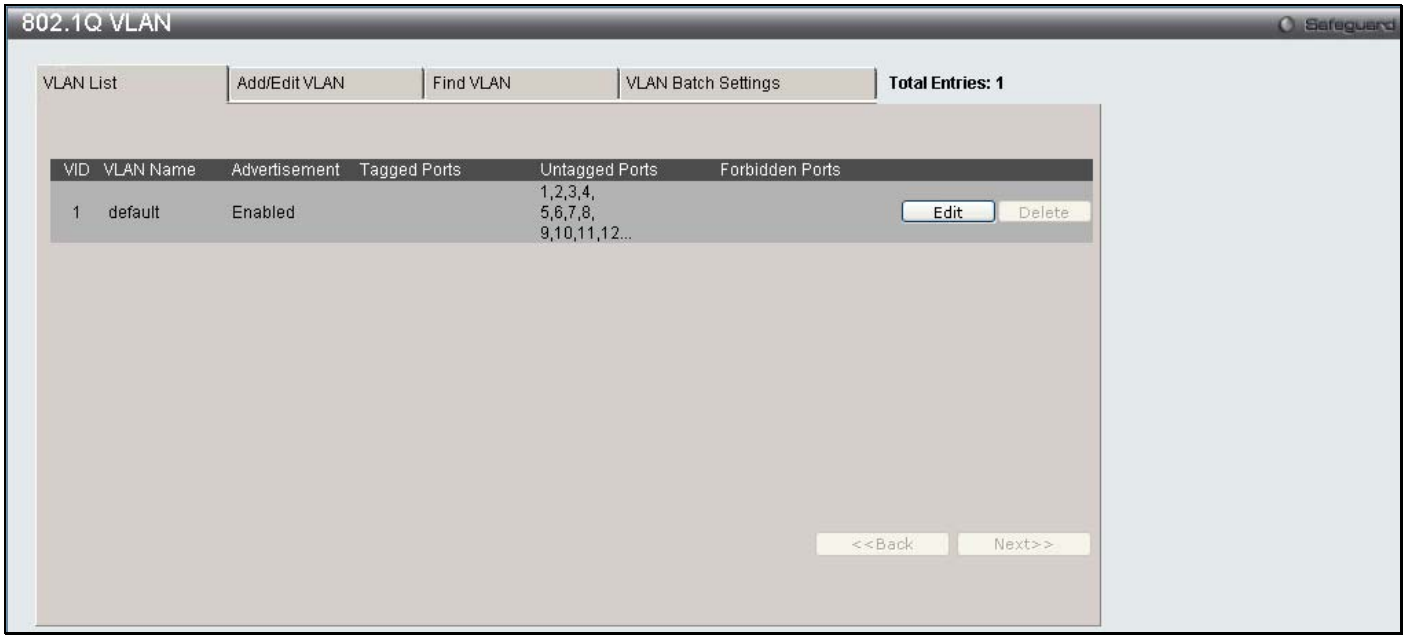


Figure 7- 7. Current 802.1Q Static VLANs Entries window

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.

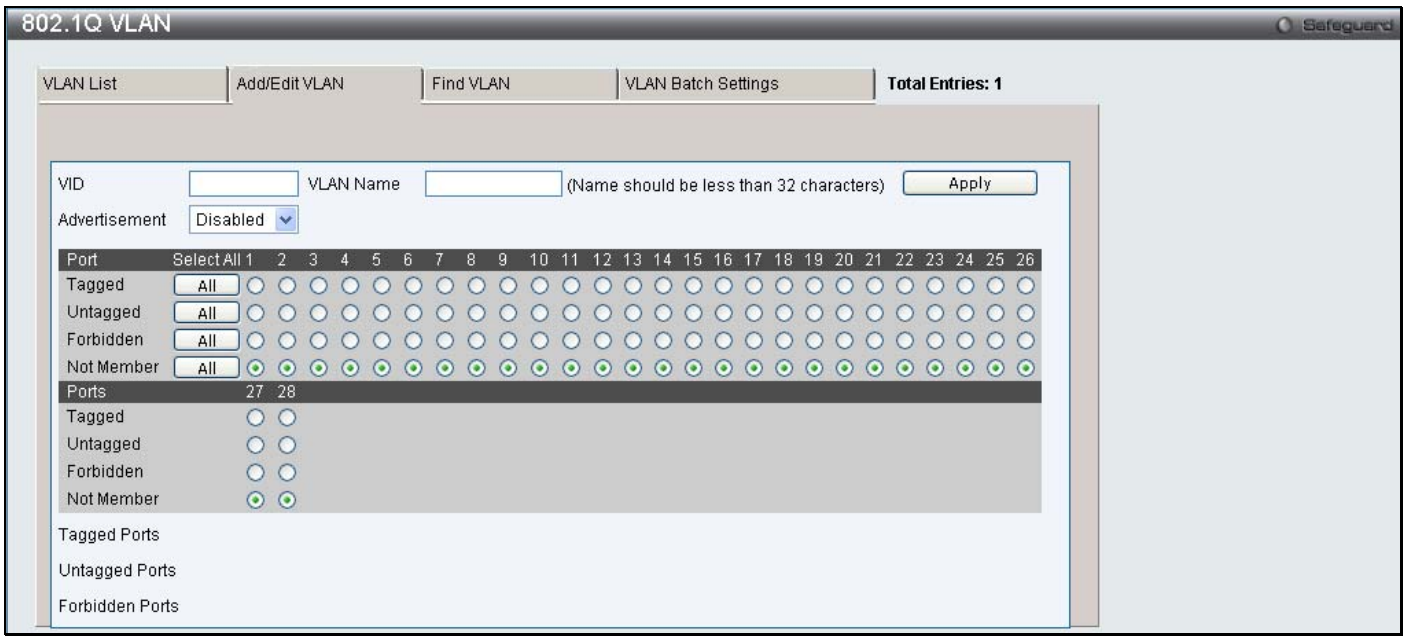


Figure 7- 8. 802.1Q VLAN window – Add/Edit VLAN Tab

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.

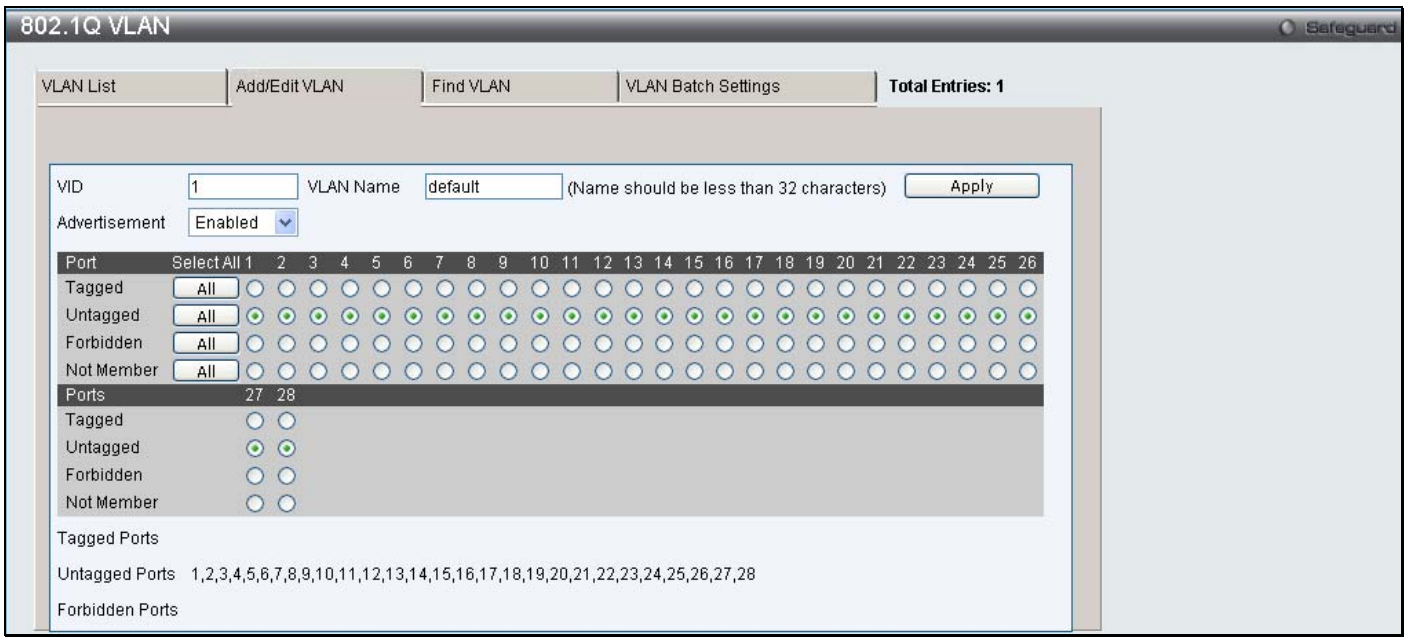


Figure 7- 9. 802.1Q VLAN window – Edit window

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

Parameter	Description
VID (VLAN ID)	Allows the entry of a VLAN ID, or displays the VLAN ID of an existing VLAN in the **Edit** window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for a new VLAN, or modifying the VLAN name in the **Edit** window. VLAN Name should be no more than 32 characters in length.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tagged	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.
Not Member	Allows an individual port to be specified as a non-VLAN member.

Click **Apply** to implement changes made.

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

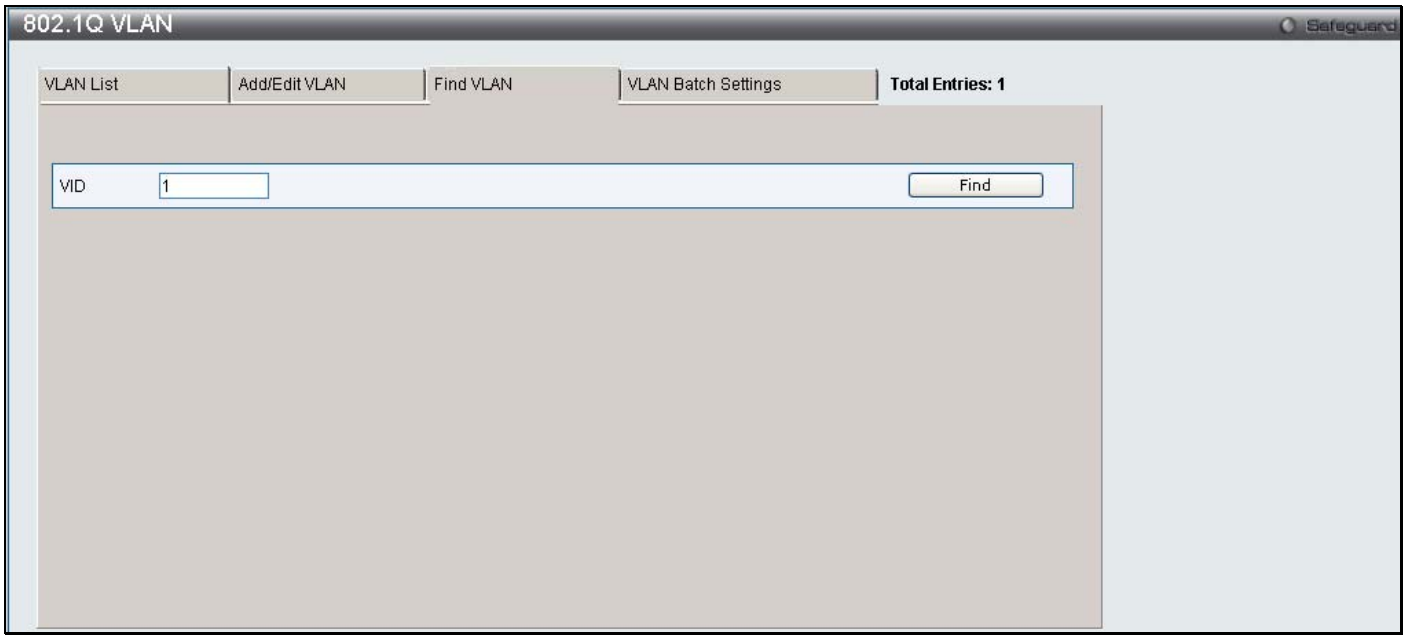


Figure 7- 10. 802.1Q VLAN window – Find VLAN window

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

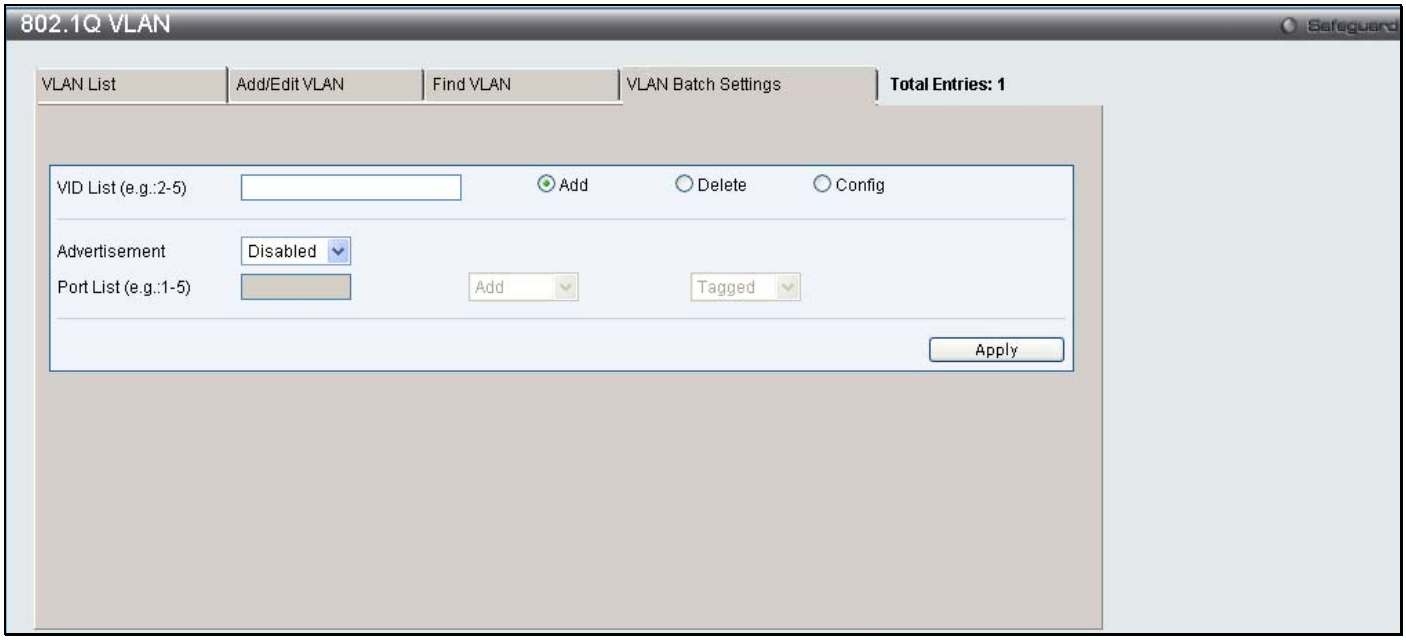


Figure 7- 11. 802.1Q VLAN window – VLAN Batch Settings window

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

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

Click Apply to implement changes made.

QinQ

This function allows the user to enable or disable the QinQ function. QinQ is designed for service providers to carry traffic from multiple users across a network. QinQ 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. QinQ 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. QinQ 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.**

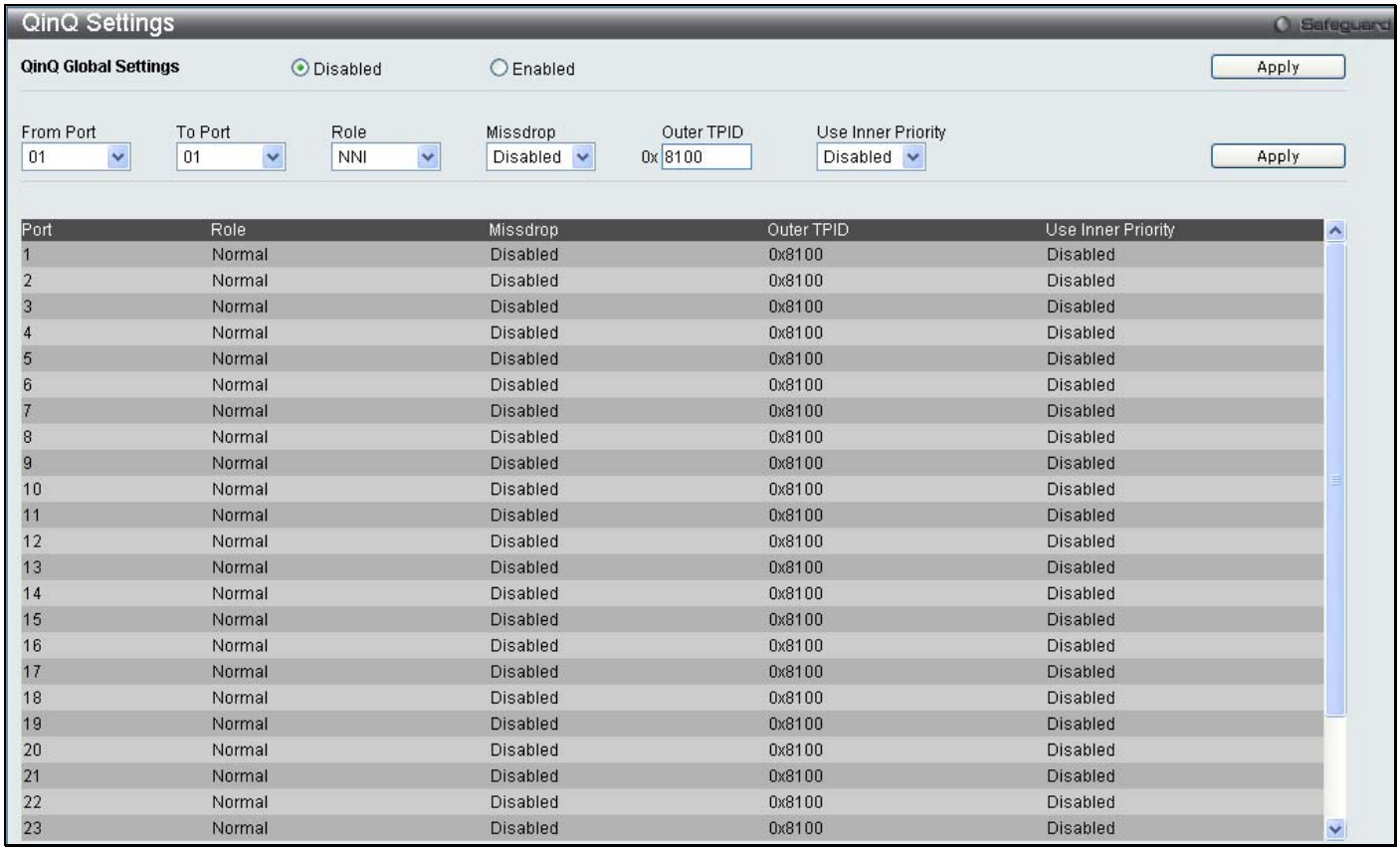


Figure 7- 12. QinQ Settings window

The following fields can be set:

Parameter	Description
From Port…To Port	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
Role	The user can choose between UNI or NNI role. *UNI* – To select a user-network interface which specifies that communication between the specified user and a specified network will occur. *NNI* – To select a network-to-network interface specifies that communication between two specified networks will occur.
Missdrop	Use the drop down menu to enable or disable missdrop. If missdrop is enabled, the packet that does not match any assignment rule in the QinQ profile will be dropped. If disabled, then

	the packet will be assigned to the PVID of the received port.
Outer TPID	The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.
Use Inner Priority	This is the priority given to the inner tag that is copied to the outer tag if this setting is enabled.

Click **Apply** to implement changes.

VLAN Translation Settings

VLAN translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network. To view this window click **L2 Features** > **QinQ** > **VLAN Translation Settings.**

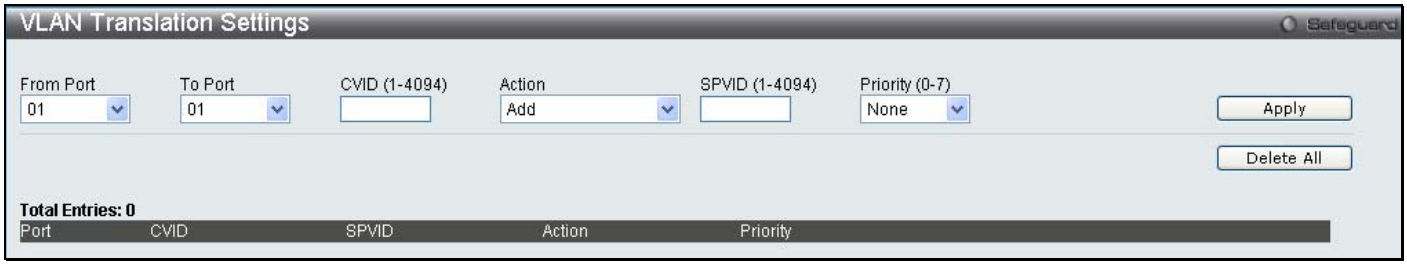


Figure 7- 13. VLAN Translation Settings window

The following fields can be set:

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

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:**

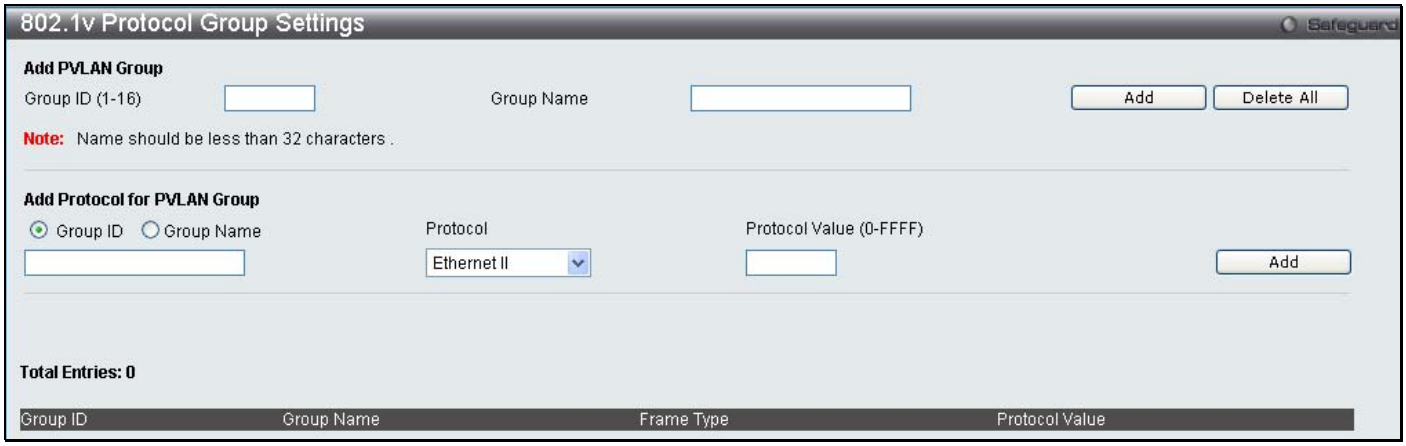


Figure 7- 14. 802.1v Protocol Group Settings window

The following fields can be set:

Parameter	Description
Group ID	Select an ID number for the group, between *1* and *16.*
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 characters.
Protocol	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Use the drop-down menu to toggle between *Ethernet_II, IEEE802.3_LLC* and *IEEE802.3_SNAP*.
Protocol Value (0-FFFF)	Enter a value for the Group.

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

802.1v Protocol VLAN Settings

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

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

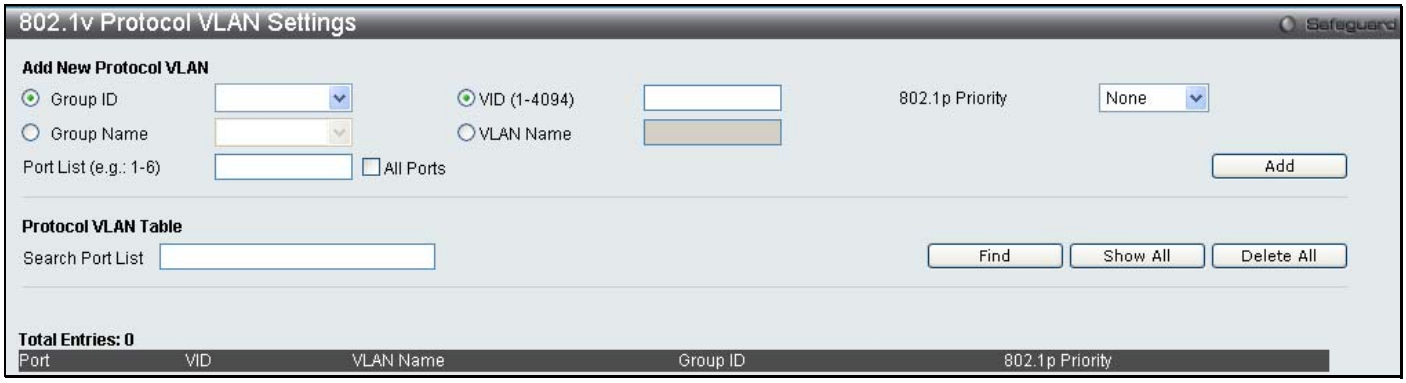


Figure 7- 15. Protocol VLAN Settings window

The following fields can be set:

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

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:**

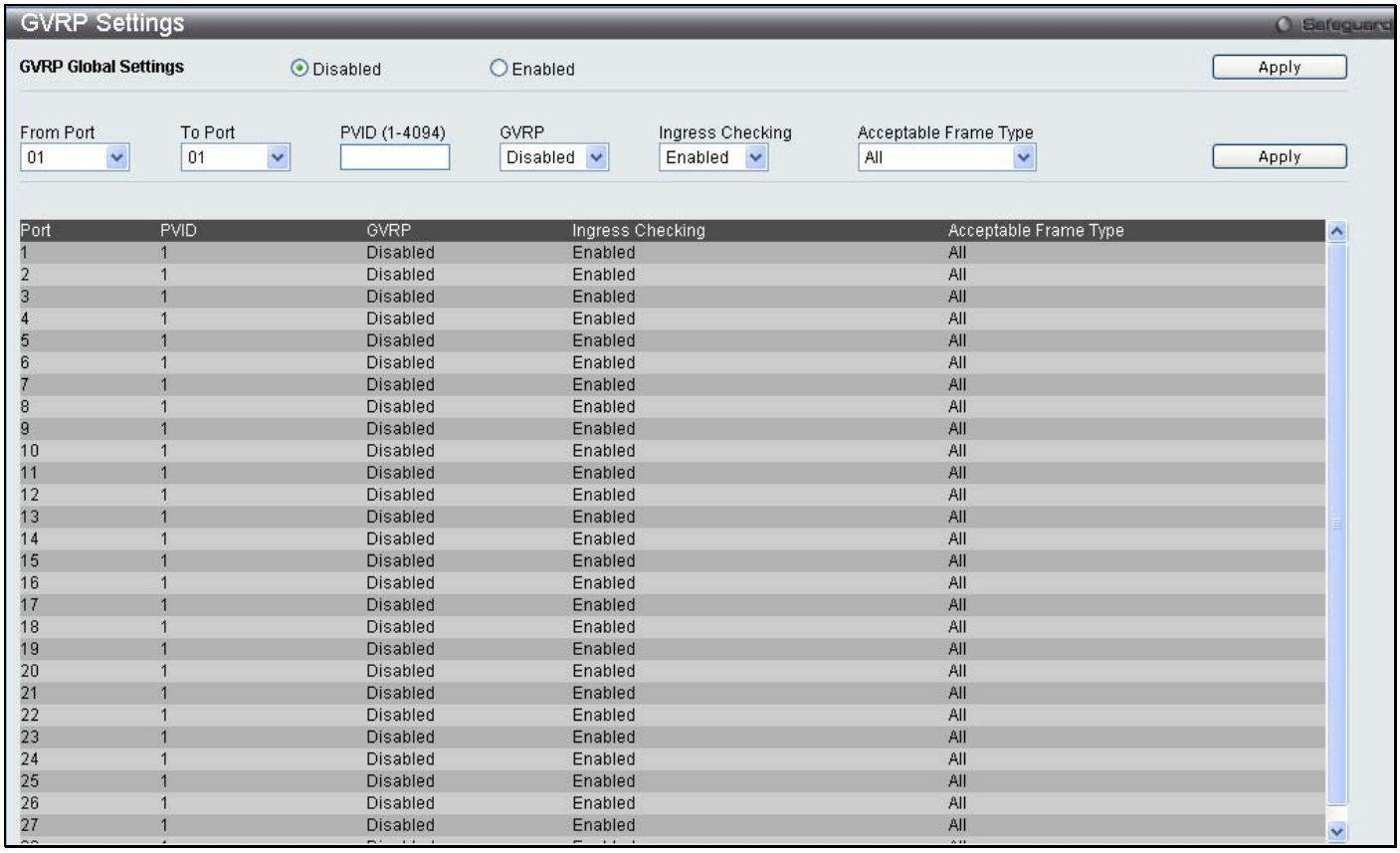


Figure 7- 16. GVRP Settings window

The following fields can be set:

Parameter	Description
From Port/To Port	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** window.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
PVID	The read-only field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
Ingress Check	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables ingress filtering. Ingress Checking is *Disabled* by default.
Acceptable Frame	This field denotes the type of frame that will be accepted by the port. The user may choose

Type	between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *Admit_All*, which mean both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.

Click **Apply** to implement changes made.

GVRP Timer 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 Timer Settings.

To view this window click **L2 Features** > **GVRP Timer Settings:**

Figure 7- 17. GVRP Timer Settings window

The following fields can be set:

Parameter	Description
Join Time (100-100000)	The time in milliseconds that specifies the amount of time between the Switch receiving the information about becoming a member of the group and actually joining the group. The default is *200*.
Leave Time (100-100000)	The time in milliseconds that specifies the maximum amount of time between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. The default is *600*. The **Leave Time** must be greater than 2 join times.
Leave All Time (100-100000)	The time in milliseconds that specifies the amount of time the Switch will take to Leave All groups. The default is *10000*. The **Leave All Time** must be greater than the **Leave Time**.

Click **Apply** to implement changes made.

Asymmetric VLAN Settings

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

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

Figure 7- 18. Asymmetric VLAN Settings window

Click **Apply** to implement changes.

MAC-based VLAN Settings

This table is used to create new MAC Based VLAN entries and search, edit and delete existing entries.

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

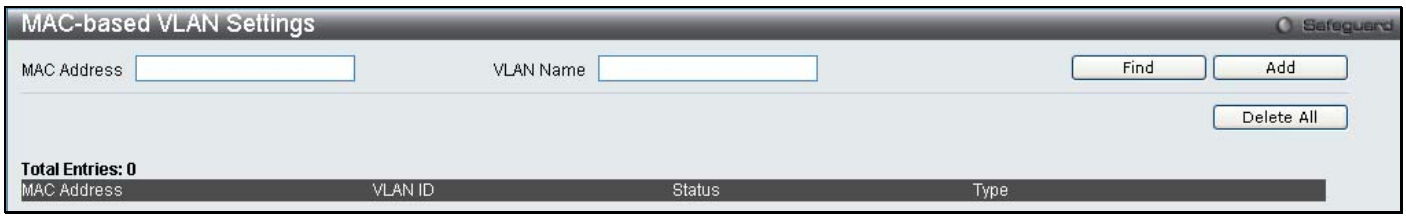


Figure 7- 19. MAC Based VLAN Settings window

The following fields can be set

Parameter	Description
MAC Address	Specify the MAC address to be reauthenticated by entering it into the **MAC Address** field.
VLAN Name	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 table is used to enable or disable the PVID Auto Assign Settings.

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

Figure 7- 20. 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. DES-3500 Series supports up to 8 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

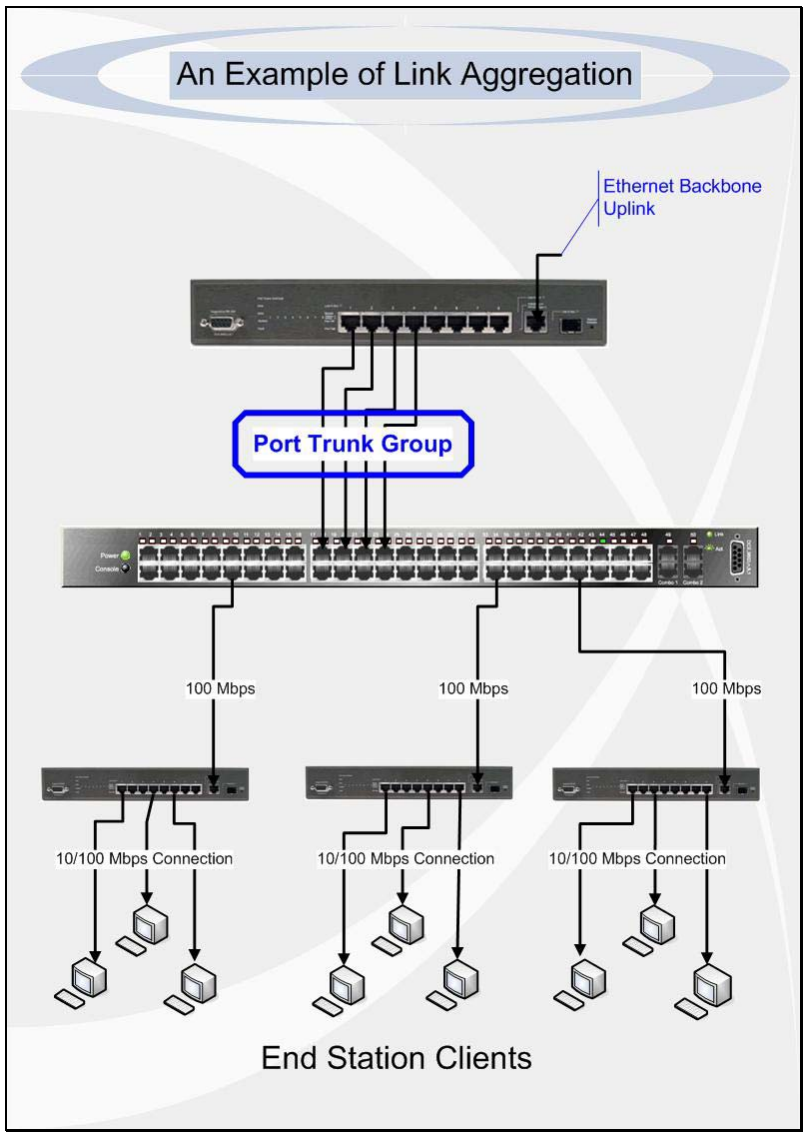


Figure 7- 21. Example of Port Trunk Group

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

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

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

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

The Switch allows the creation of up to 8 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 the Trunking Settings window click **L2 Features** > **Port Trunking:**

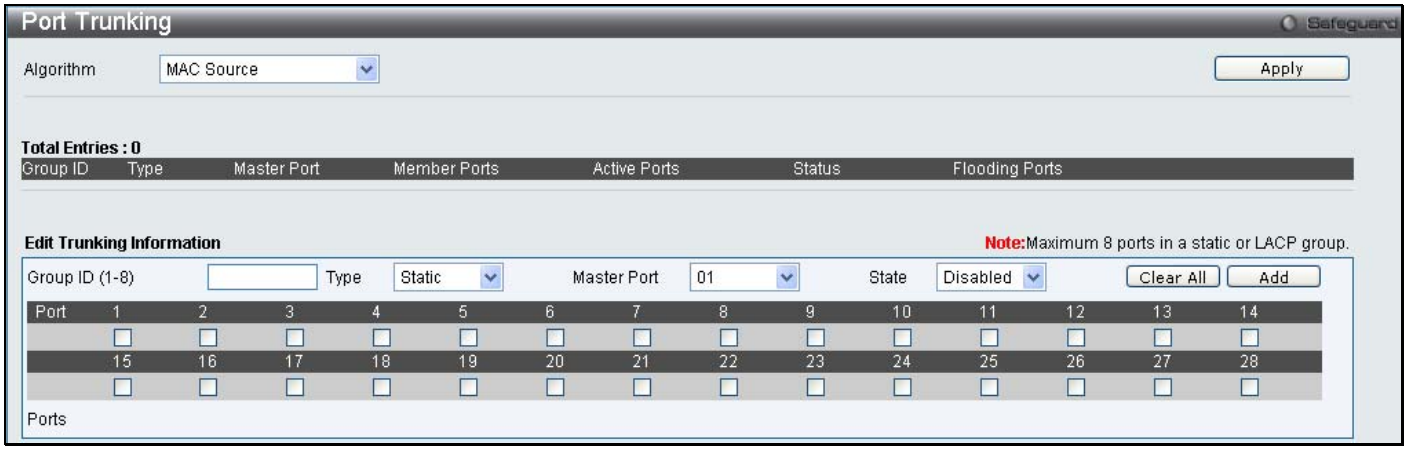


Figure 7- 22. Port Trunking window

The following fields can be set

Parameter	Description
Algorithm	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *MAC Source*, *MAC Destination*, *MAC Source Dest*, *IP Source, IP Destination* or *IP Source Dest* (See the Link Aggregation section of this manual).
Group ID	Select an ID number for the group, between *1* and *8*.
Type	This pull-down menu allows you to select between Static and LACP (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
State	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.
Active Port	Shows the port that is currently forwarding packets.
Member Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Flooding Port	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 the Trunking Settings window click **L2 Features** > **LACP Port Settings:**

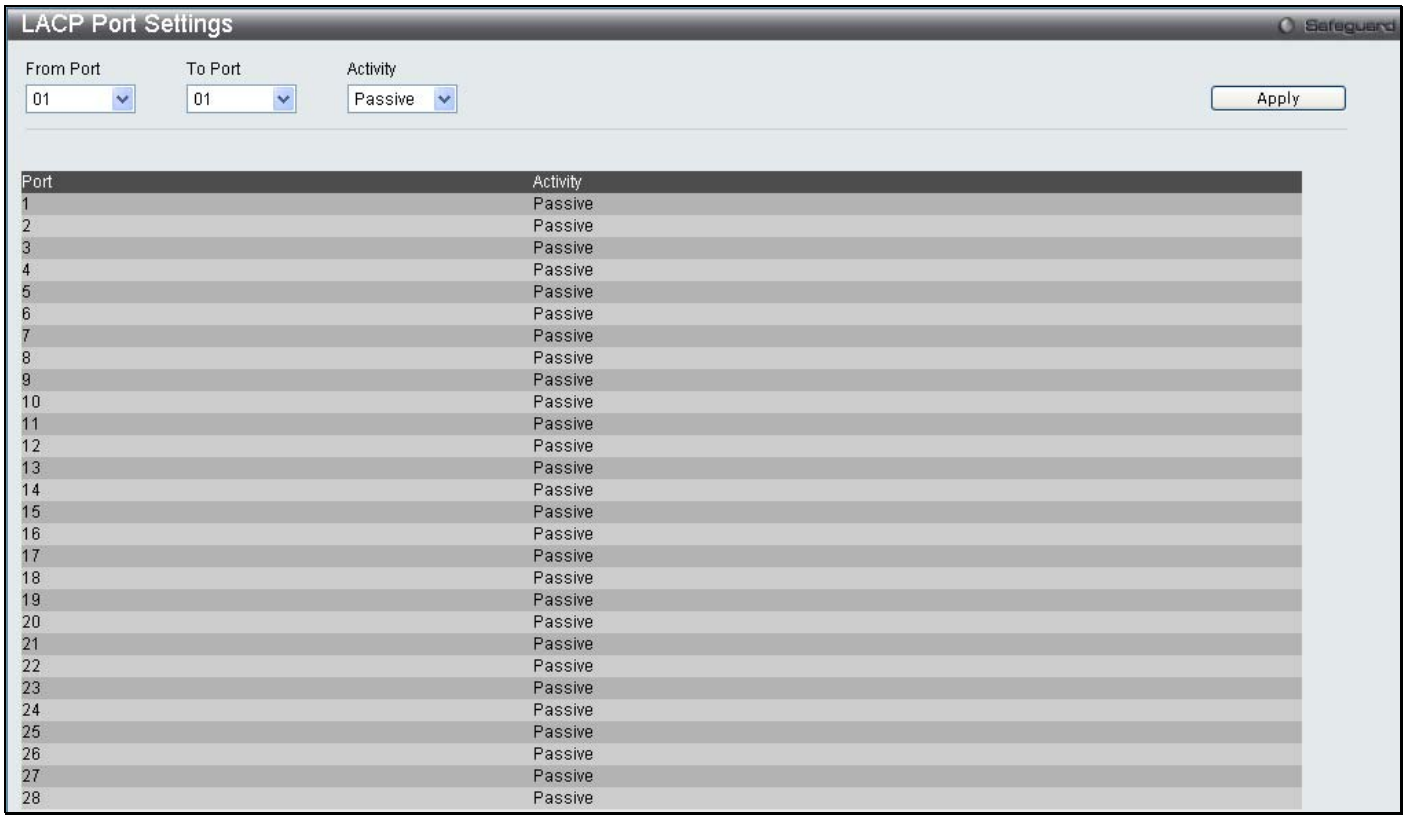


Figure 7- 23. LACP Port Settings window

The following fields can be set

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

Click **Apply** to implement changes made.

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 the Traffic Segmentation window click **L2 Features** > **Traffic Segmentation:**

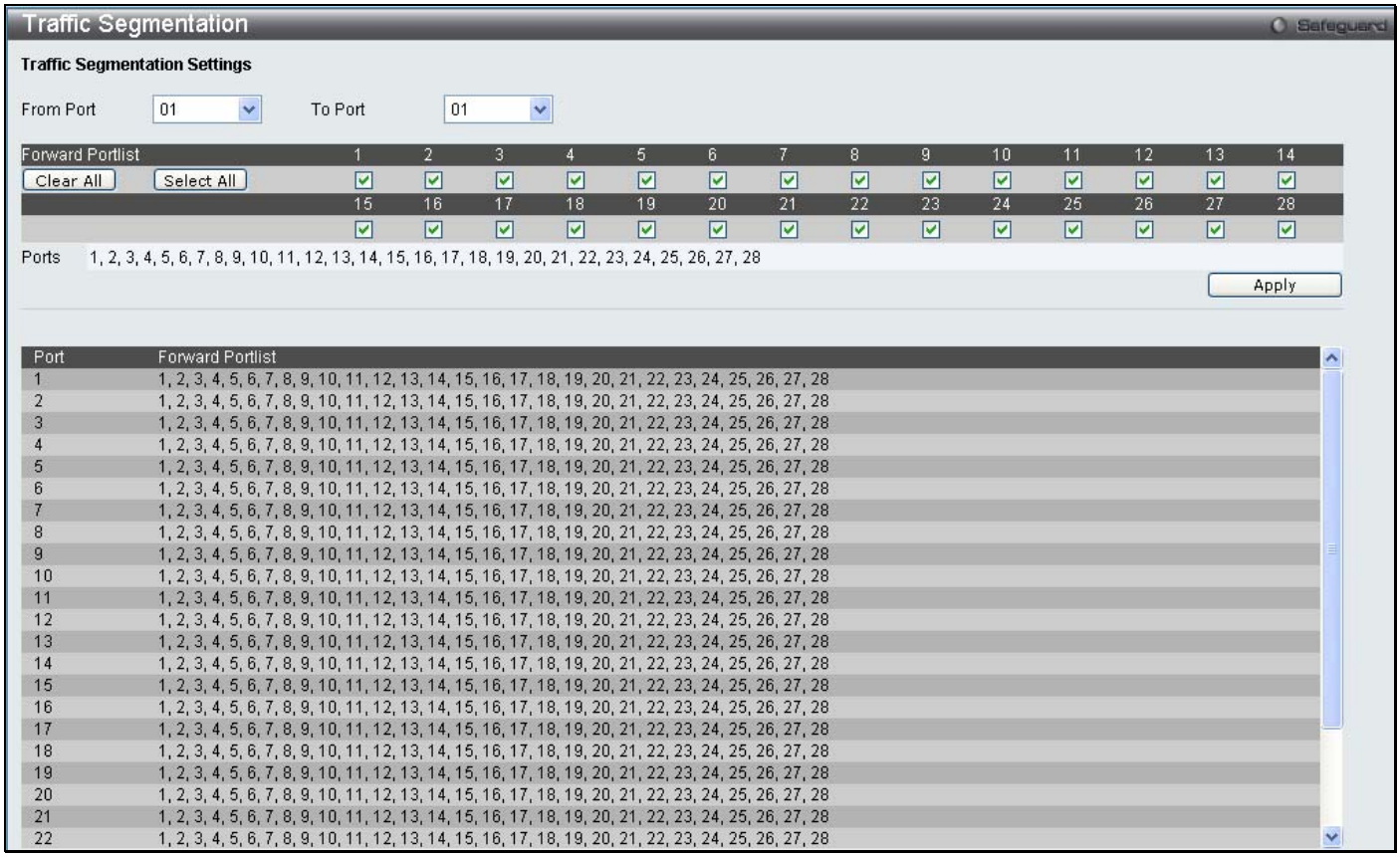


Figure 7- 24. Traffic Segmentation window

The following fields can be set

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

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

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 **DES-3528 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 the Traffic Segmentation window click **L2 Features** > **IGMP Snooping** > **IGMP Snooping Settings:**

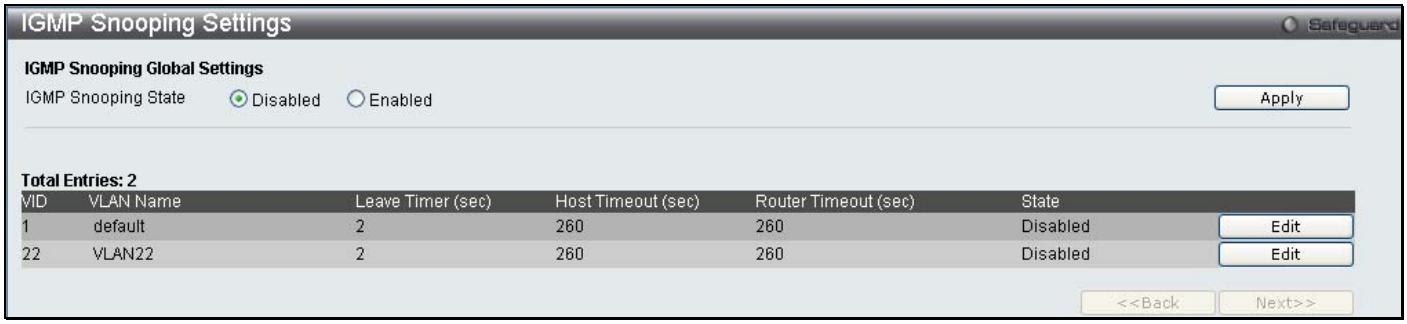


Figure 7- 25. IGMP Snooping Settings window

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

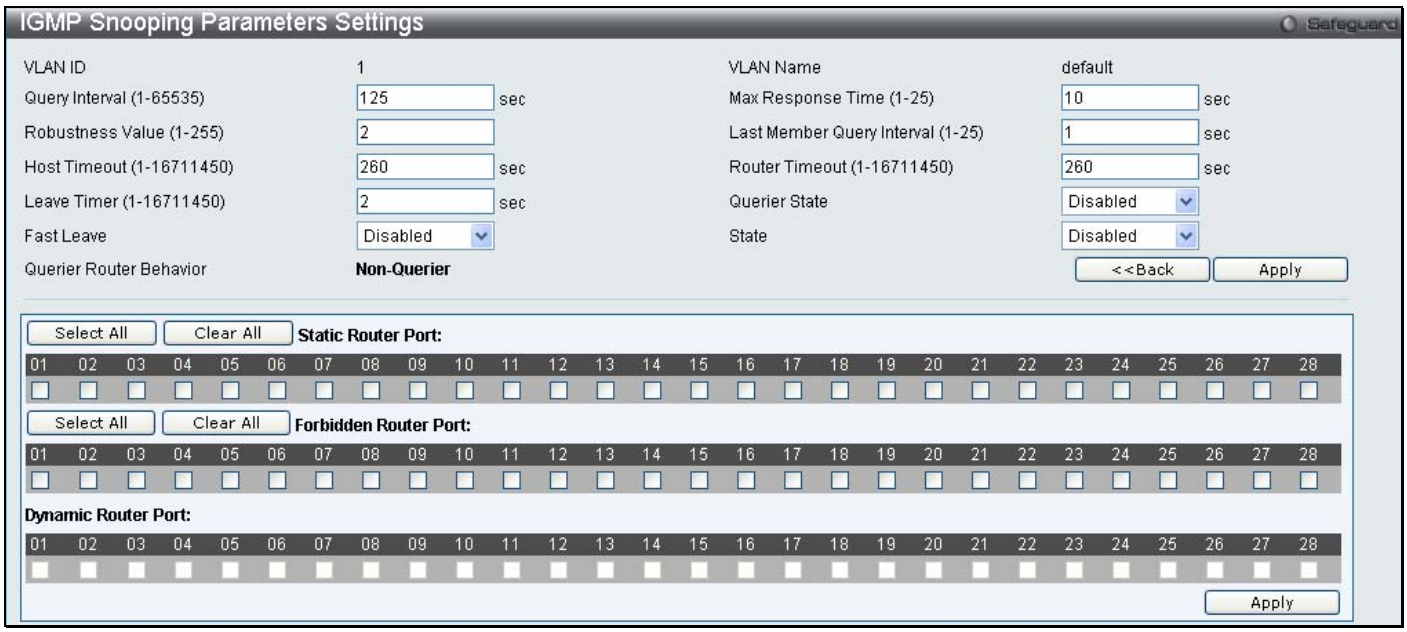


Figure 7- 26. IGMP Snooping Parameters Settings - Edit window

The following fields can be set

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.

Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between *1* and *65535* seconds are allowed. Default = *125*.
Max Response Time (1 - 25 Sec)	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = *10*.
Robustness Variable (1 – 255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. Default = *2*.
Last Member Query Interval (1 - 25 Sec)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = *1*.
Host Timeout (1 – 16711450)	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = *260*.
Router Timeout (1 – 16711450)	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = *260*.
Leave Timer (1 – 16711450)	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted.
Querier State	Choose Enabled to enable transmitting IGMP Query packets or Disabled to disable. The default is Disabled.
Fast Leave	This parameter allows the user to enable the Fast Leave function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch. The default is Disabled.
State	Select Enabled to implement IGMP Snooping. This field is Disabled by default.
Querier Router Behavior	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.

IGMP Snooping Multicast VLAN Settings

To configure the IGMP Snooping Multicast VLAN settings, click **L2 Features** > **IGMP Snooping** > **IGMP Snooping Multicast VLAN Settings:**

Figure 7- 27. IGMP Snooping Multicast VLAN Settings

The following fields can be set

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.

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

IP Multicast Profile Settings

The **IP Multicast Profile Settings** window allows the user to add a profile to which multicast address(es) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP Multicast address or range of IP Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports. To configure the IP Multicast Profile settings, click **L2 Features** > **IGMP Snooping** > **IP Multicast Profile Settings:**

Figure 7- 28. IP Multicast Profile Settings window

The following fields can be set

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

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

Figure 7- 29. IP Multicast Profile Settings – Edit window

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

Figure 7- 30. 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.

Limited Multicast Range Settings

The **Limited Multicast Range Settings** enables the user to configure the ports on the switch that will be involved in the Limited IP Multicast Range. The user can configure the range of multicast ports that will be accepted by the source ports to be forwarded to the receiver ports. To configure these settings, click **L2 Features** > **IGMP Snooping** > **Limited Multicast Range Settings:**

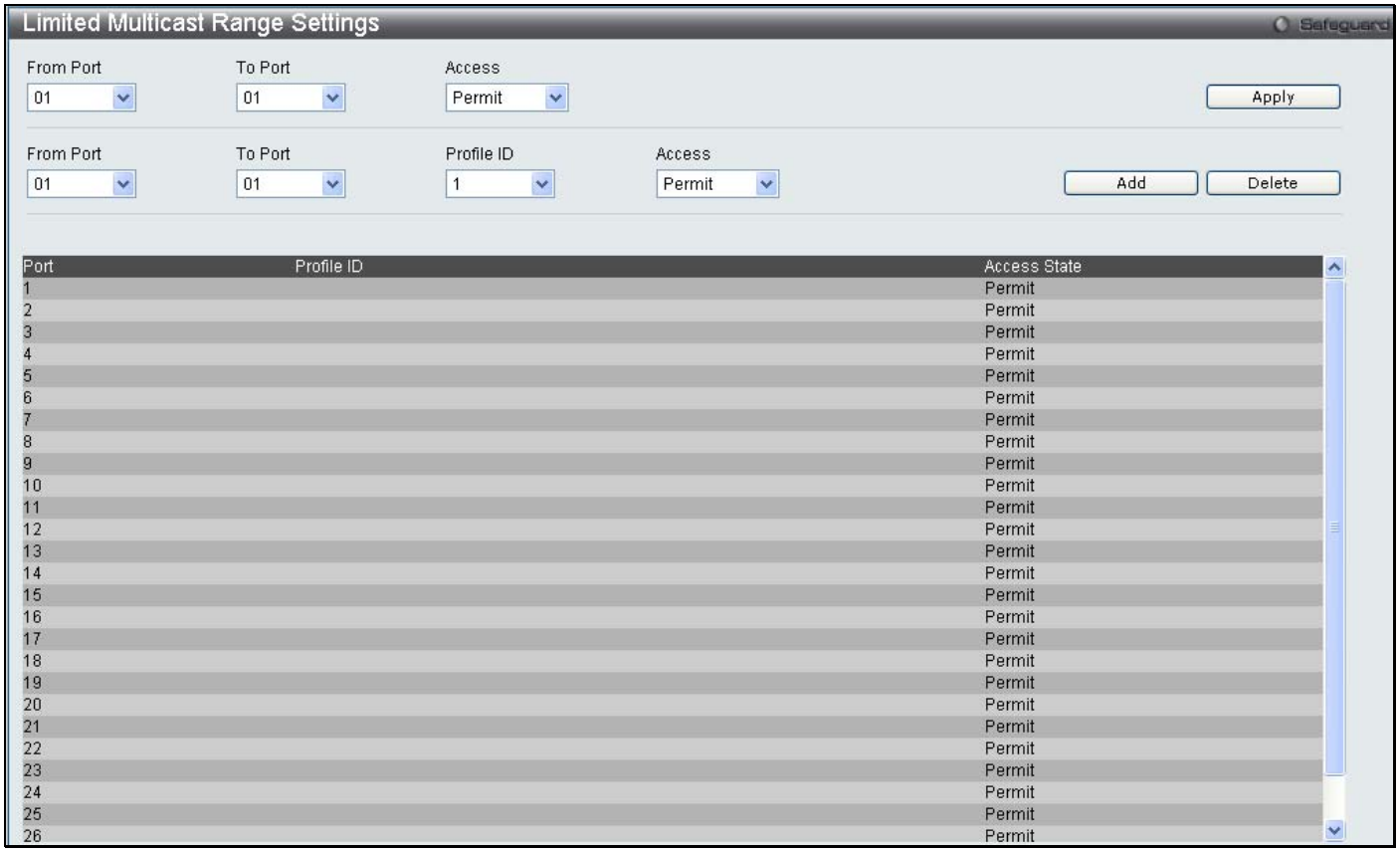


Figure 7- 31. Limited Multicast Range Settings window

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

Multicast Filtering Mode

The **Multicast Filtering Mode** enables the user to configure the ports on the switch that will be involved in the Multicast Filtering Mode. To configure these settings, click **L2 Features** > **IGMP Snooping** > **Multicast Filtering Mode:**

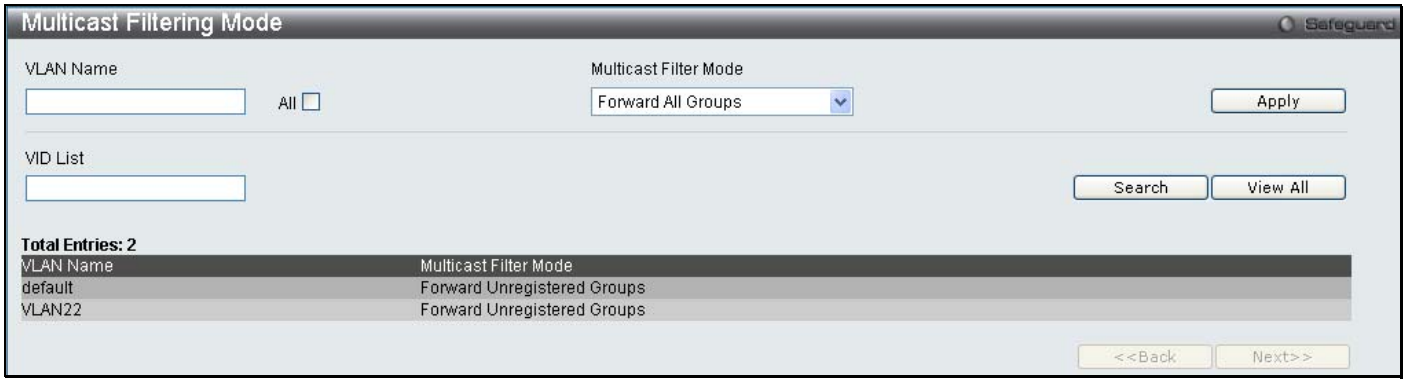


Figure 7- 32. Multicast Filtering Mode window

To add a new Multicast Filter enter the information and click **Apply**, to search for an entry click **Search**, and to view all the VLANs click the **View All** button.

Max Multicast Group Settings

The **Max Multicast Group Settings** enables the user to configure the ports on the switch that will be apart of the maximum filter group up to a maximum of 256. To configure these settings, click **L2 Features** > **IGMP Snooping** > **Max Multicast Group Settings**

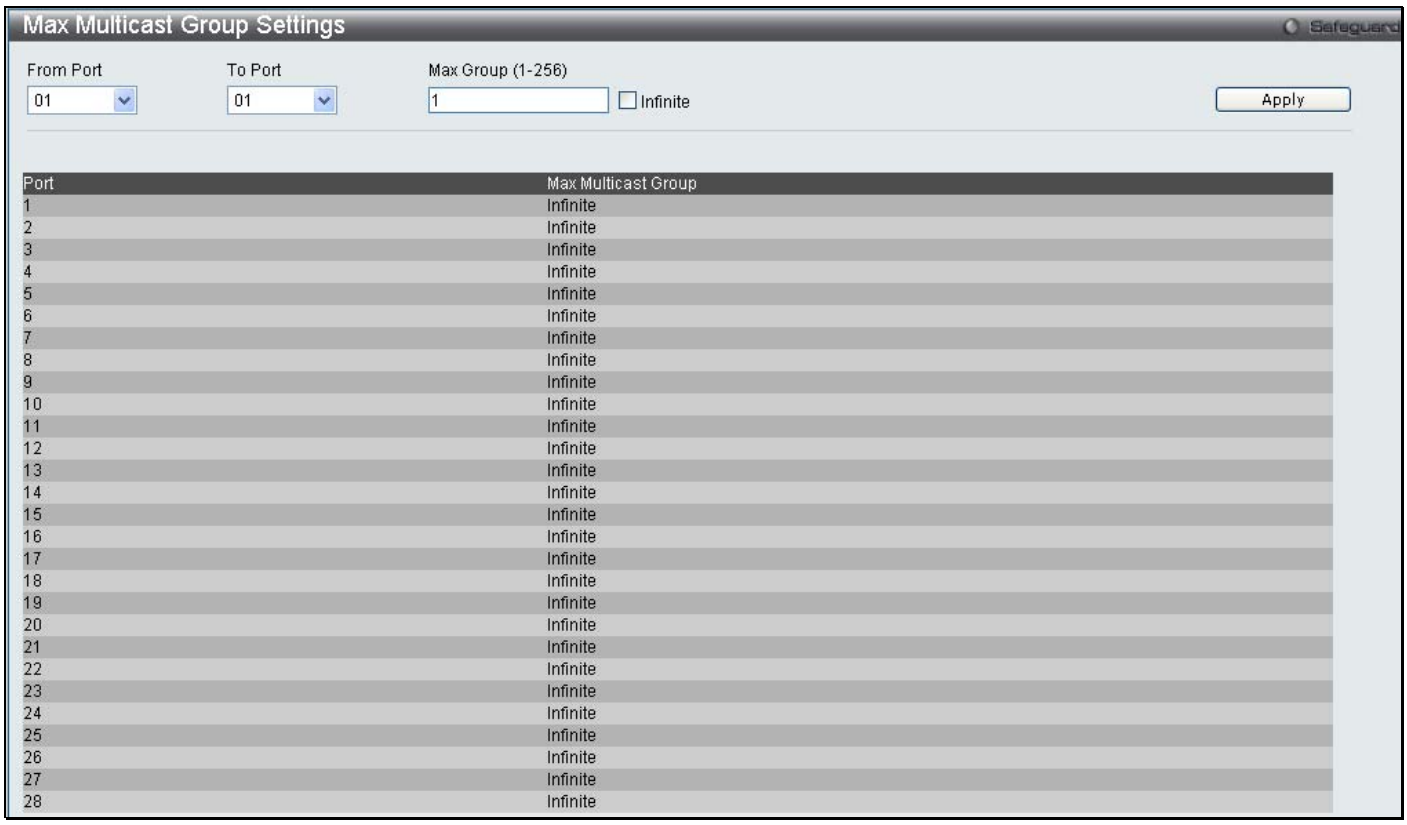


Figure 7- 33. Max Multicast Group Settings window

To add a Maximum Multicast Group range, enter the information and click **Apply.**

MLD Snooping Settings

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

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

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, click **L2 Features > MLD Snooping Settings**, which will open the following window.

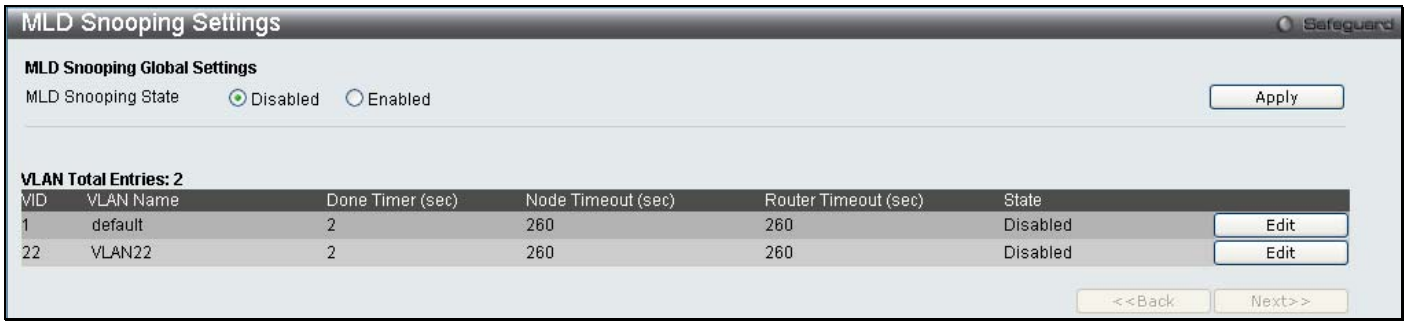


Figure 7- 34. MLD Snooping Settings - Window

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

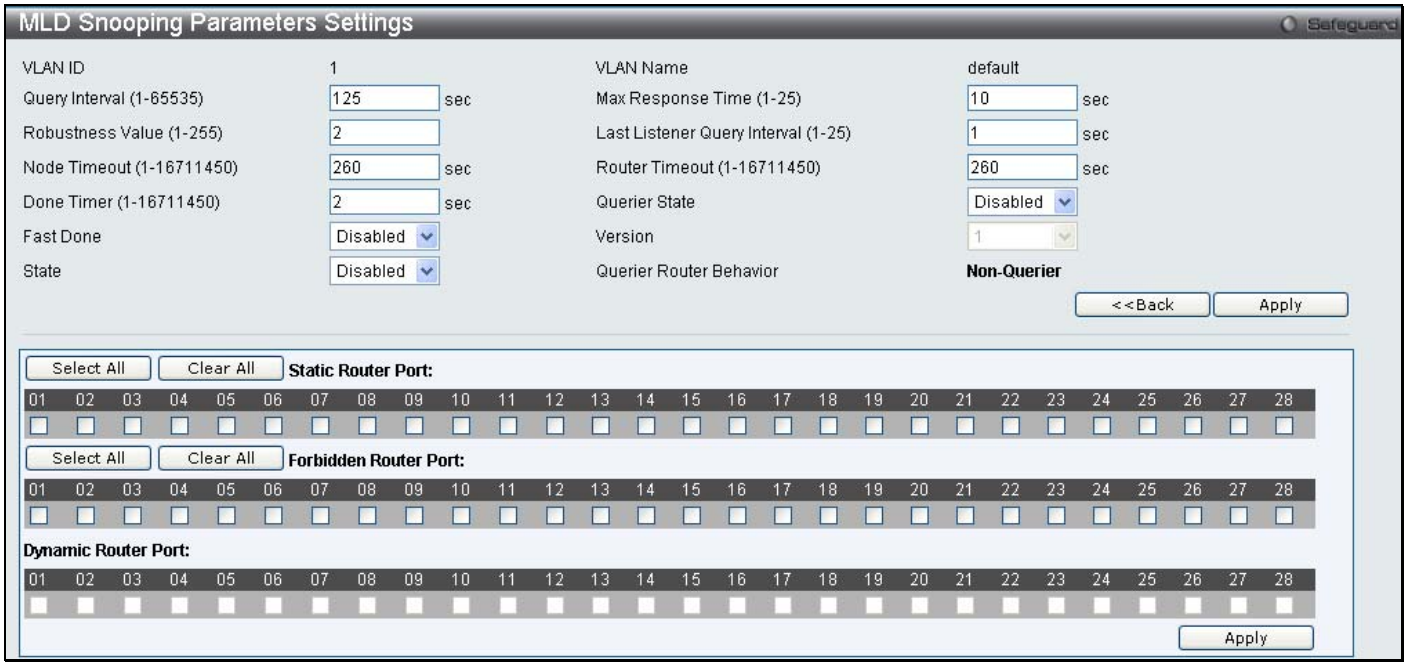


Figure 7- 35. MLD Snooping Settings – Edit Window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which to modify the MLD Snooping Settings.
Query Interval (1-65535 sec)	Allows the entry of a value between *1* and *65535* seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time (1-25 sec)	This determines the maximum amount of time in seconds allowed to wait for a response for MLD port listeners. The Max Response Time field allows an entry between *1* and *25* (seconds). Default = *10*.
Robustness Value (1-255)	Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval.
Last Listener Query Interval (1-25 sec)	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. A value between 1 and 25. The default is *1* second.
Node Timeout (1-16711450)	Specifies the link node timeout, in seconds. After this timer expires, this node will no longer be considered as listening node. The user may specify a time between *1* and *16711450* with a default setting of *260* seconds.
Router Timeout (1-16711450 sec)	Specifies the maximum amount of time a router can remain in the Switch's routing table as a listening node of a multicast group without the Switch receiving a node listener report. The user may specify a time between *1* and *16711450* with a default setting of 260 seconds.
Done Timer (1-16711450 sec)	Specifies the maximum amount of time a router can remain in the Switch after receiving a done message from the group without receiving a node listener report. The user may specify a time between *1* and *16711450* with a default setting of 2 seconds.
Querier State	The default is *Disabled*. If the field displays "Disabled", it will always be in MLD-Snooping non-querier state.
Fast Done	Used to enable or disable the *fast done* state of the switch. This field is disabled by default.

State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
Querier Router Behavior	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.
Fast Leave	This parameter allows the user to enable the *fast leave* function. Enabled, this function will allow members of a multicast group to leave the group immediately when a *leave* message is received by the Switch.

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

Port Mirror

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the **Port Mirror** window, click **Layer 2 Features** > **Port Mirror**.

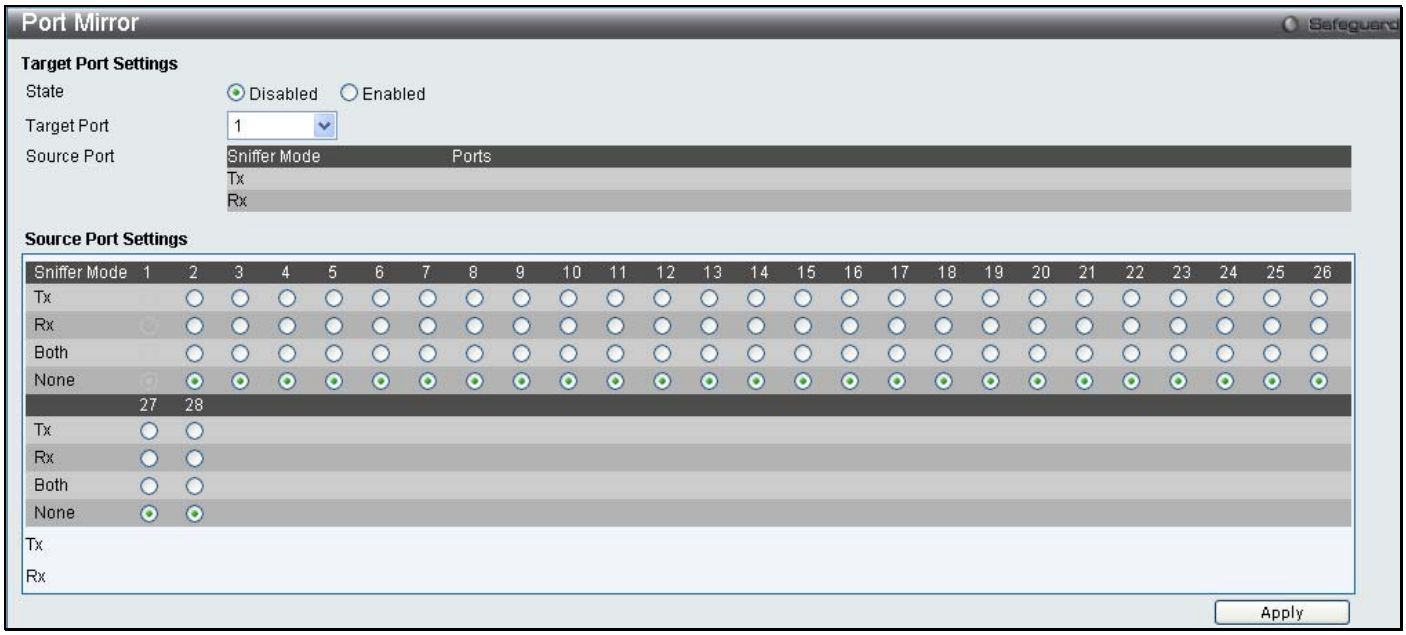


Figure 7- 36. Port Mirror window

To configure a mirror port:

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

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

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 CTP (Configuration Testing Protocol) packet has been looped back to the switch. When the Switch detects CTP 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**.

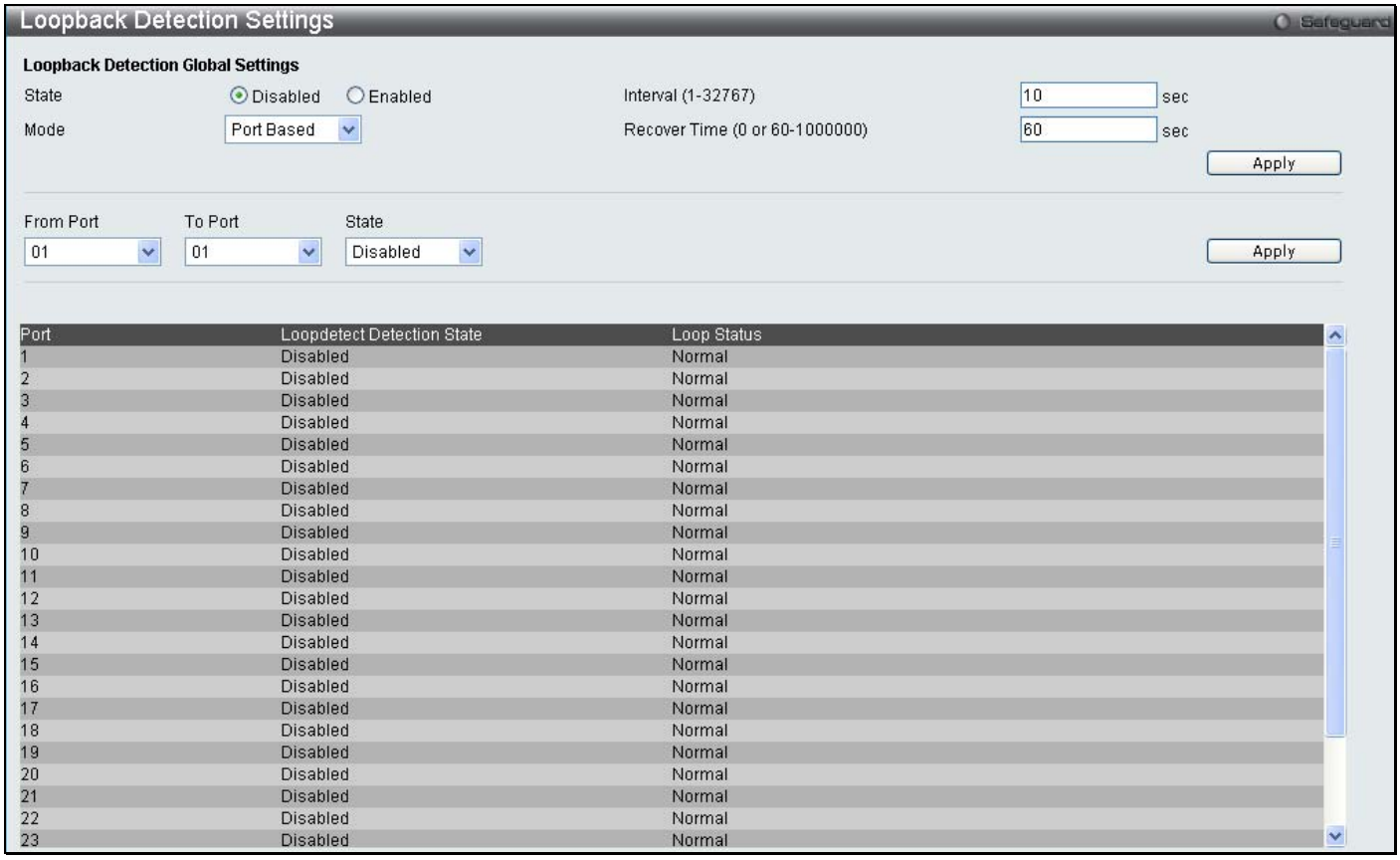


Figure 7- 37. Loopback Detection Settings window

Parameter	Description
Loopdetect State	Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*
Mode	Use the drop-down menu to toggle between *Port Based* and *VLAN Based*.
Interval (1-32767)	Set a Loopdetect Interval between *1* and *32767* seconds. The default is *10* seconds.
Recover Time (0 or 60-1000000)	Time allowed (in seconds) for recovery when a Loopback is detected. The Loopdetect Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loopdetect Recover Time. The default is *60* seconds.
From Port	Use the drop-down menu to select a beginning port number.
To Port	Use the drop-down menu to select an ending port number.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*

Click **Apply** to implement changes made.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 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 7- 1. Comparing Port States

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

Edge Port

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

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP, 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 LoopBack Prevention

When connected to other switches, STP is an important configuration in consistency for delivering packets to ports and can greatly improve the throughput of your switch. Yet, even this function can malfunction with the emergence of STP BPDU packets that occasionally loopback to the Switch, such as BPDU packets looped back from an unmanaged switch connected to the Switch. To maintain the consistency of the throughput, the Switch now implements the STP LoopBack prevention function.

When the STP LoopBack Detection function is enabled, the Switch will be protected against a loop occurring between switches. Once a BPDU packet returns to the Switch, this function will detect that there is an anomaly occurring and will place the receiving port in an error-disabled state. Consequentially, a message will be placed in the Switch's Syslog and will be defined there as "BPDU Loop Back on Port #".

Setting the LoopBack Timer

The LoopBack timer plays a key role in the next step the switch will take to resolve this problem. Choosing a non-zero value on the timer will enable the Auto-Recovery Mechanism. When the timer expires, the Switch will again look for its returning BPDU packet on the same port. If no returning packet is received, the Switch will recover the port as a Designated Port in the Discarding State. If another returning BPDU packet is received, the port will remain in a blocked state, the timer will reset to the specified value, restart, and the process will begin again.

For those who choose not to employ this function, the LoopBack Recovery time must be set to zero. In this case, when a BPDU packet is returned to the Switch, the port will be placed in a blocking state and a message will be sent to the Syslog of the switch. To recover the port, the administrator must disable the state of the problematic port and enable it again. This is the only method available to recover the port when the LoopBack Recover Time is set to 0.

Regulations and Restrictions for the LoopBack Detection Function

- All versions of STP (STP and RSTP) can enable this feature.
- May be configured globally (STP Global Bridge Settings).
- Neighbor switches of the Switch must have the capability to forward BPDU packets. Switches the fail to meet this requirement will disable this function for the port in question on the Switch.
- The default setting for this function is disabled.
- The default setting for the LoopBack timer is 60 seconds.
- This setting will only be operational if the interface is STP-enabled.

The LoopBack Detection feature can only prevent BPDU loops on designated ports. It can detect a loop condition occurring on the user's side connected to the edge port, but it cannot detect the LoopBack condition on the elected root port of STP on another switch

STP Bridge Global Settings

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

Figure 7- 38. STP Bridge Global Settings window

The following parameters can be set:

Parameter	Description
STP Status	Use the radio buttons to enable or disable the STP Status.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices: *STPCompatability* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* – Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is Enabled.
Bridge Max Age (6 - 40 Sec)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between *6* and *40* seconds. The default value is *20*.
Bridge Hello Time (1 - 10 Sec)	The Hello Time can be set from *1* to *10* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge.
Bridge Forward Delay (4 - 30 Sec)	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
TX Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6.*

Max Hops (1-20)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from *1* to *20*. The default is *20*.

Click **Apply** to implement changes made.

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

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

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

STP Port Settings

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

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

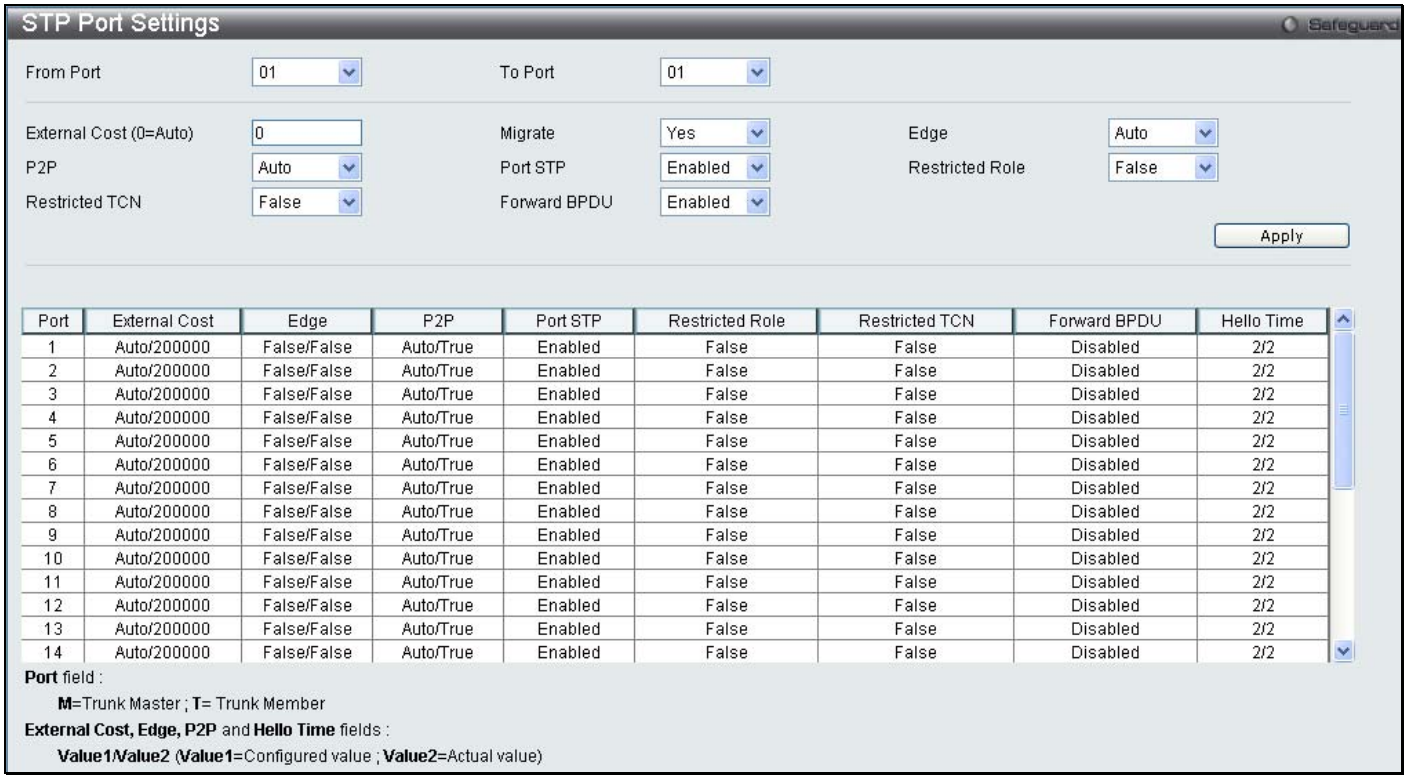


Figure 7- 39. STP Port Settings window

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

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

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

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

The following fields can be set:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
External Cost (*0 = Auto)*	**External Cost** - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto). *0 (auto)* - Setting *0* for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = *200000*. Gigabit port = *20000*. *value 1-200000000* - Define a value between *1* and *200000000* to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

Migrate	Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.
Edge	Choosing the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the *False* parameter indicates that the port does not have edge port status.
P2P	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *True*.
Port STP	Toggle from *Disabled* to *Enabled* to implement BPDU packet forwarding.
Restricted Role	Toggle between *True* and *False* to set the restricted role state of the packet.
Restricted TCN	Toggle between *True* and *False* to set the restricted TCN of the packet
Forward BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.

Click **Apply** to implement changes made.

MST Configuration Identification

The following windows in the **MST Configuration Identification** section allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one *CIST* or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

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

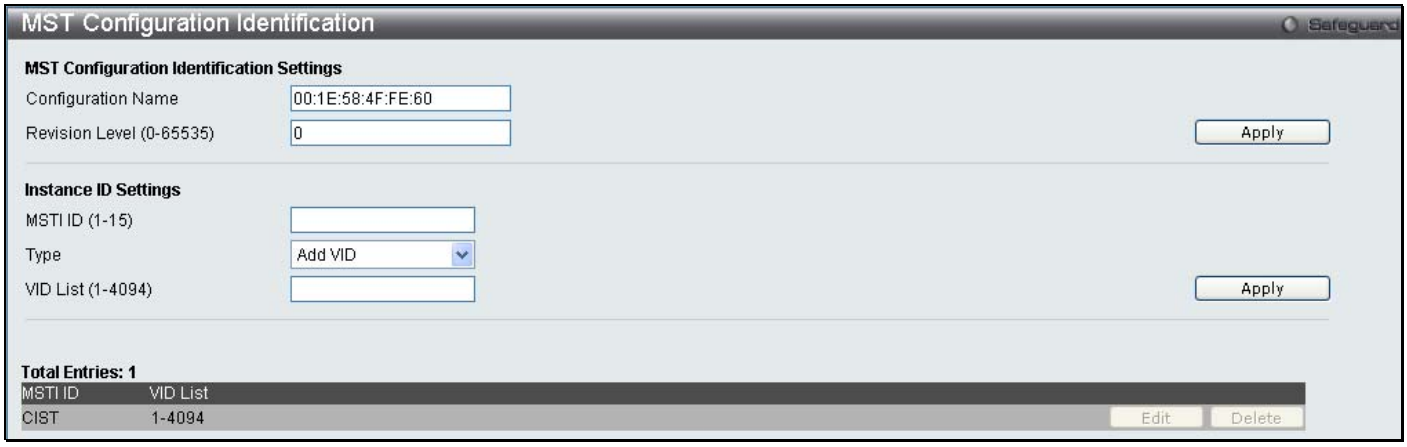


Figure 7- 40. MST Configuration Identification window

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the **STP Bridge Global Settings** window.
Revision Level (0-65535)	This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between *0* and *65535* with a default setting of *0*.
MSTI ID	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices. *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List	This field displays the VLAN IDs associated with the specific MSTI.

Click **Apply** for changes to take affect:

STP Instance Settings

The following window displays MSTIs currently set on the Switch.

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

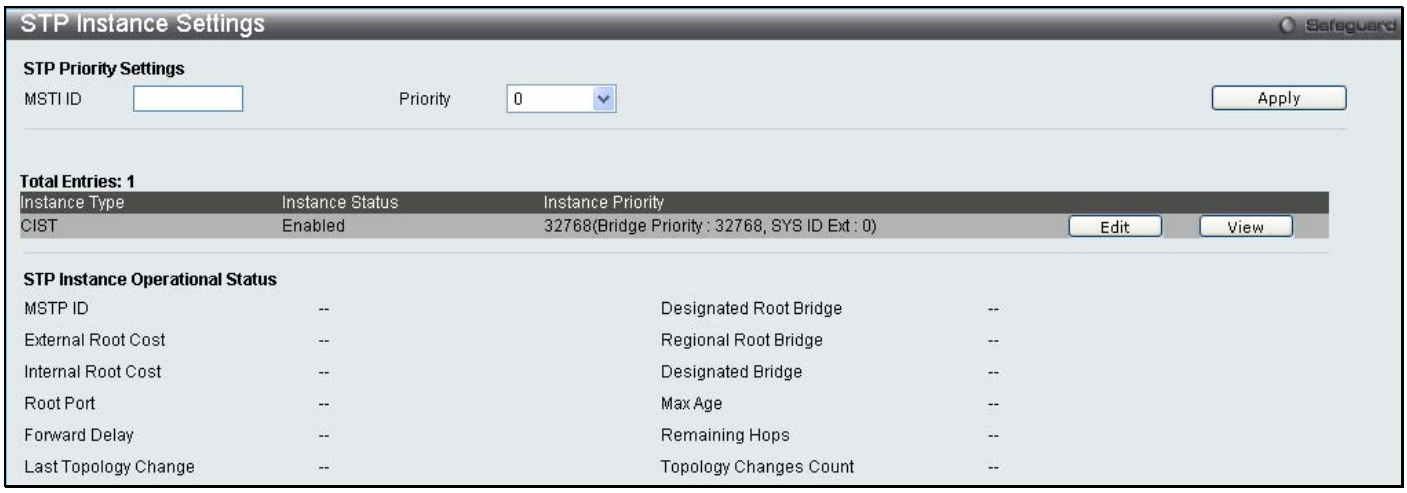


Figure 7- 41. STP Instance Settings window

The following information can be set:

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

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

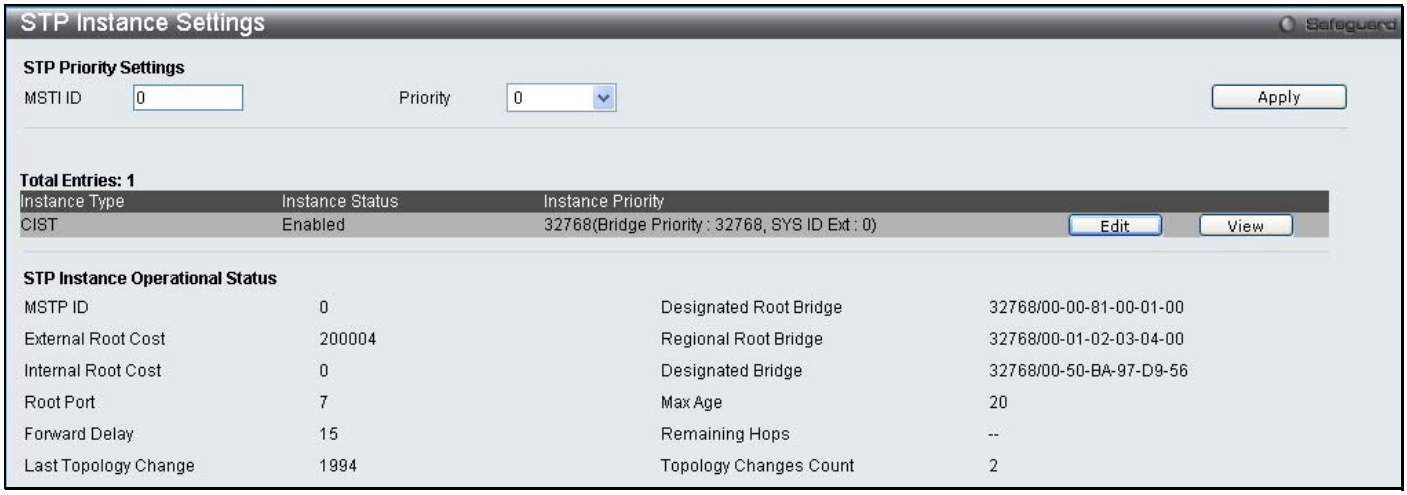


Figure 7- 42. STP Instance Settings - View window

MSTP Port Information

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

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

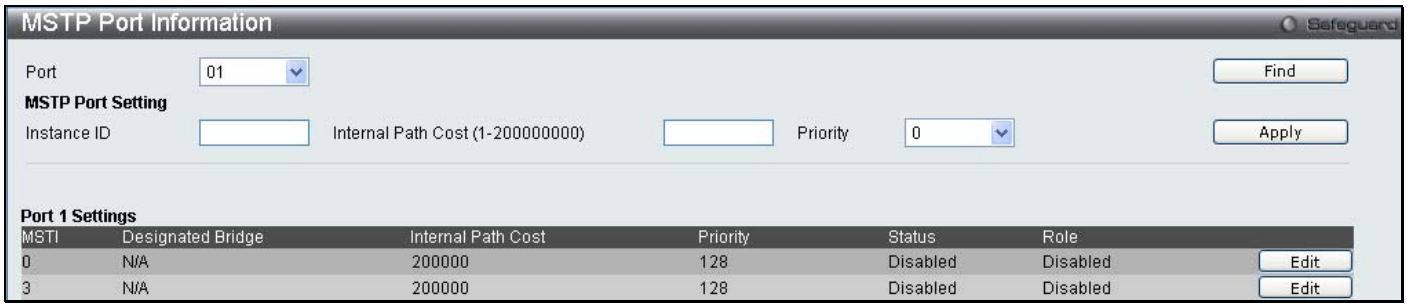


Figure 7- 43. MSTP Port Information window

The following parameters can be viewed or set:

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

Click **Apply** to implement changes made.

Forwarding & Filtering

This folder contains windows for Unicast Forwarding and Multicast Forwarding.

Unicast Forwarding

To view this window, Click **L2 Features** > **Forwarding & Filtering** > **Unicast Forwarding**.

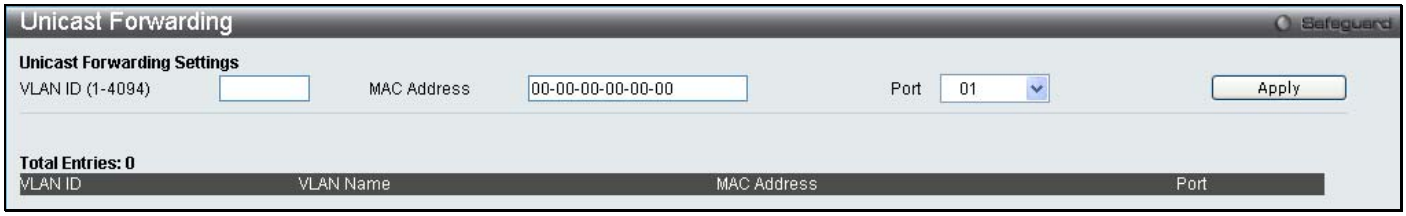


Figure 7- 44. Unicast Forwarding window

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

Parameter	Description
VLAN ID (1-4094)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port	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. Open the **Forwarding Filtering** folder and click on the **Multicast Forwarding** link to see the entry window below:

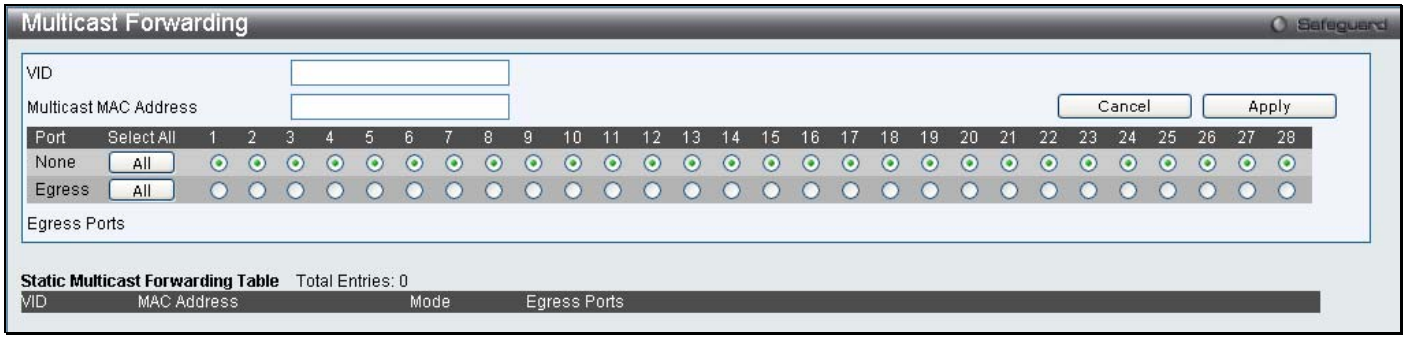


Figure 7- 45. Multicast Forwarding Settings window

The following parameters can be set:

Parameter	Description
VID	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	Allows the selection of ports that will be members of the static multicast group and ports either that are forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When None is

	chosen, the port will not be a member of the Static Multicast Group. *Egress* - The port is a static member of the multicast group.

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

LLDP

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

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

LLDP Global Settings

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

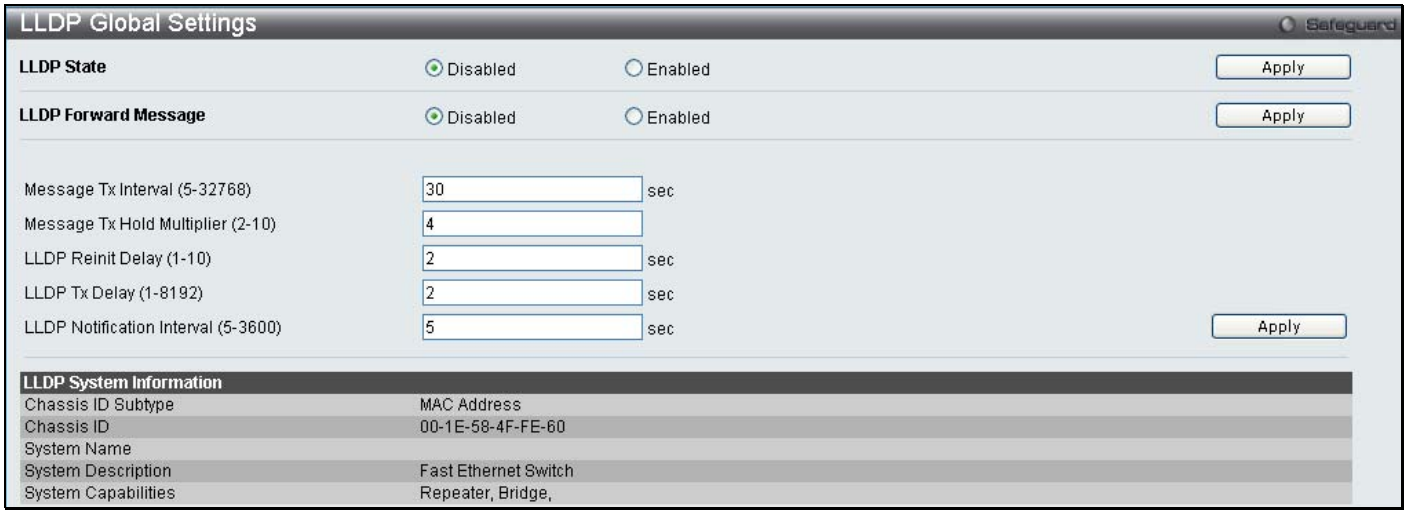


Figure 7- 46. LLDP Global Settings window

The following parameters can be set:

Parameter	Description
LLDP State	Used to Enable or Disable LLDP on the Switch.
LLDP Forward Message	Enable or Disable the message forwarding of the LLDP function, to advertise to other stations attached to the same IEEE 802 LAN.
Message TX Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (*5* to *32768*).
Message TX Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP Reinit Delay (1-10)	The LLDP reinitialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP Reinit Delay, enter a value in seconds (*1* to *10*).
LLDP TX Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (*1* to *8192*).

LLDP Notification Interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (*5* to *3600*).

Click **Apply** to implement changes made.

LLDP Port Settings

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

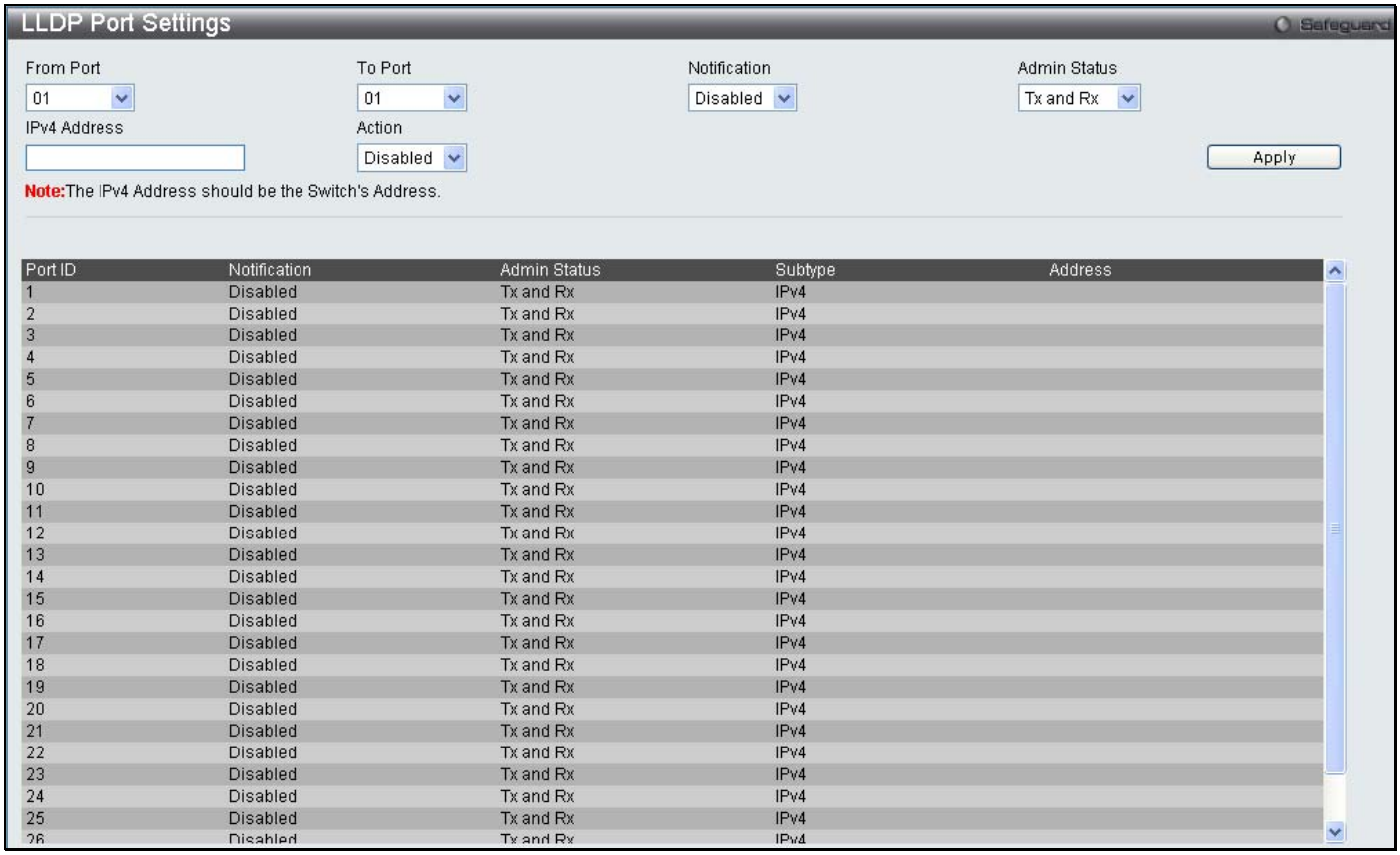


Figure 7- 47. LLDP Port Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Notification	Use the pull-down menu to Enable or Disable the status of the LLDP notification.
Admin Status	Select the status of the notification, use the drop-down menu to choose between *TX, RX, TX And RX or Disabled.*
IPv4 Address	Enter the management address or the address of the entity you wish to advertise to.
Action	Used to *Enable* or *Disable* the advertise management address function base port.

Click **Apply** to implement changes made.

LLDP Management Address List

To view this window, Click **L2 Features** > **LLDP** > **LLDP Management Address List**

Figure 7- 48. LLDP Management Address List window

The following parameters can be set:

Parameter	Description
IPv4 Address	Enter the management ip address or the ip address of the entity you wish to advertise to. IPv4 will ensure the message is sent by the router to ask for the advertisements.

Click **Find** to implement changes made.

LLDP Basic TLVs Settings

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

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

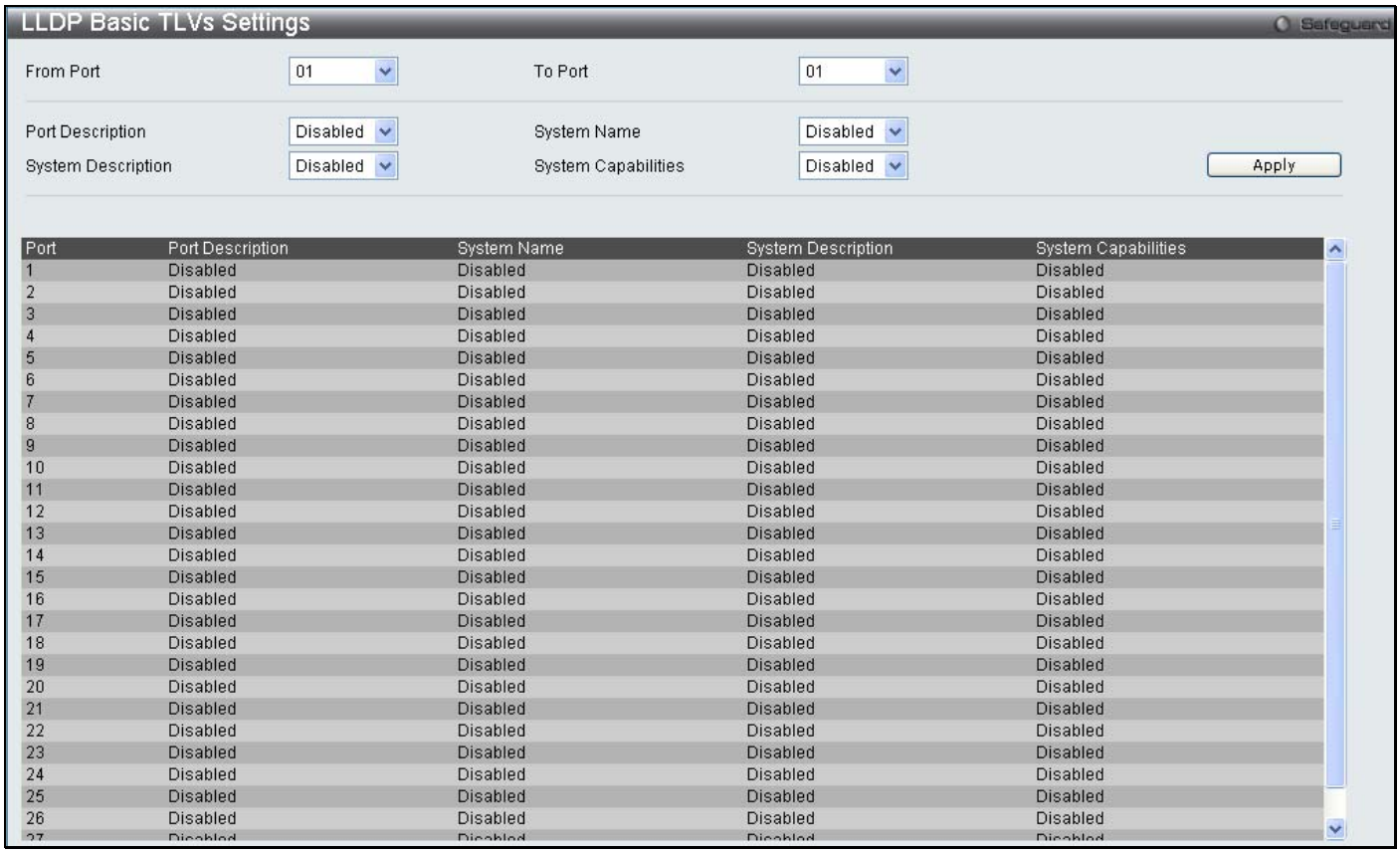


Figure 7- 49. LLDP Basic TLVs Settings window

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

The following parameters can be set:

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

Click **Apply** to implement changes made.

LLDP Dot1 TLVs Settings

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

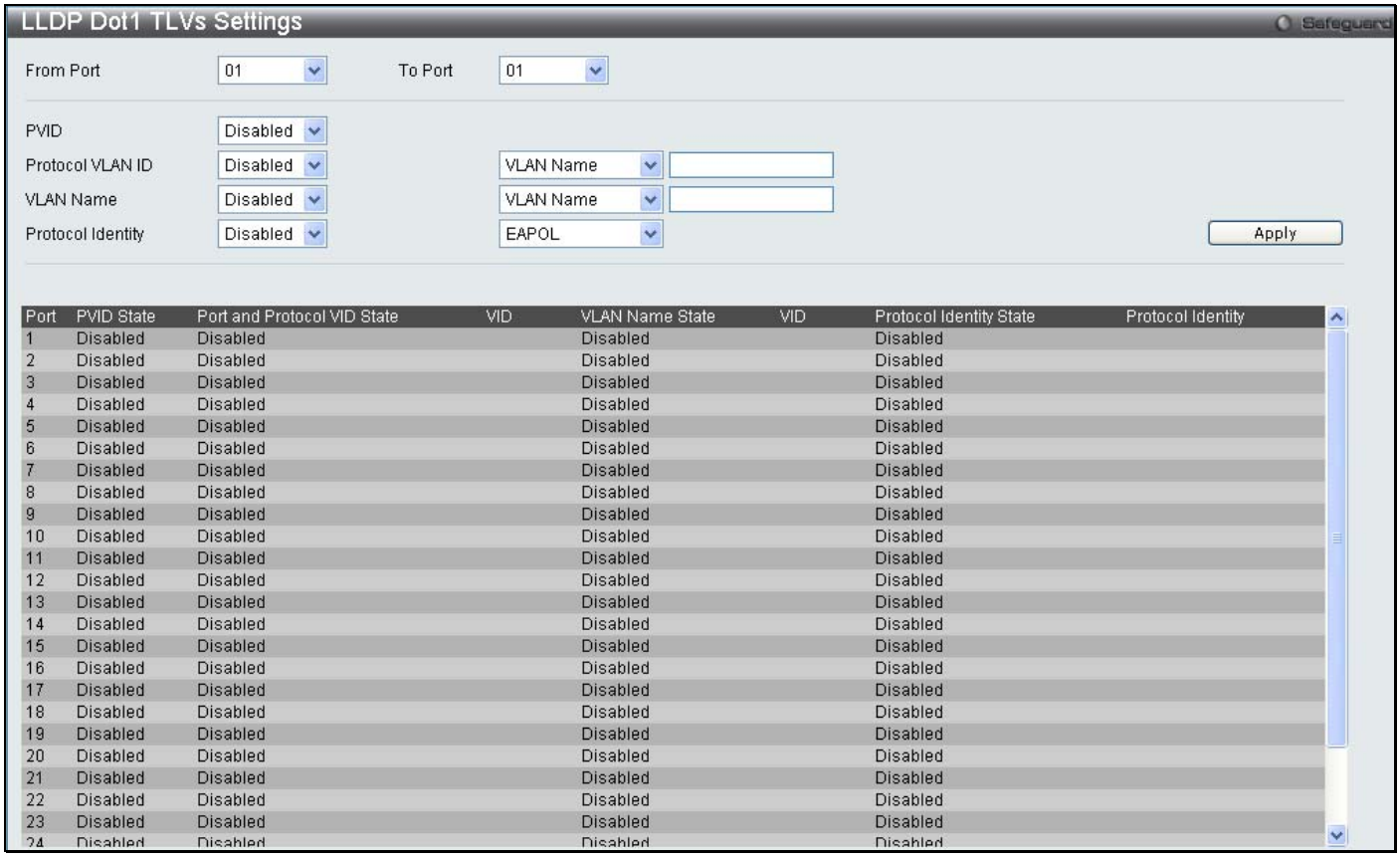


Figure 7- 50. LLDP Dot1 TLVs Settings window

The following parameters can be set:

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

Click **Apply** to implement changes made.

LLDP Dot3 TLVs Settings

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

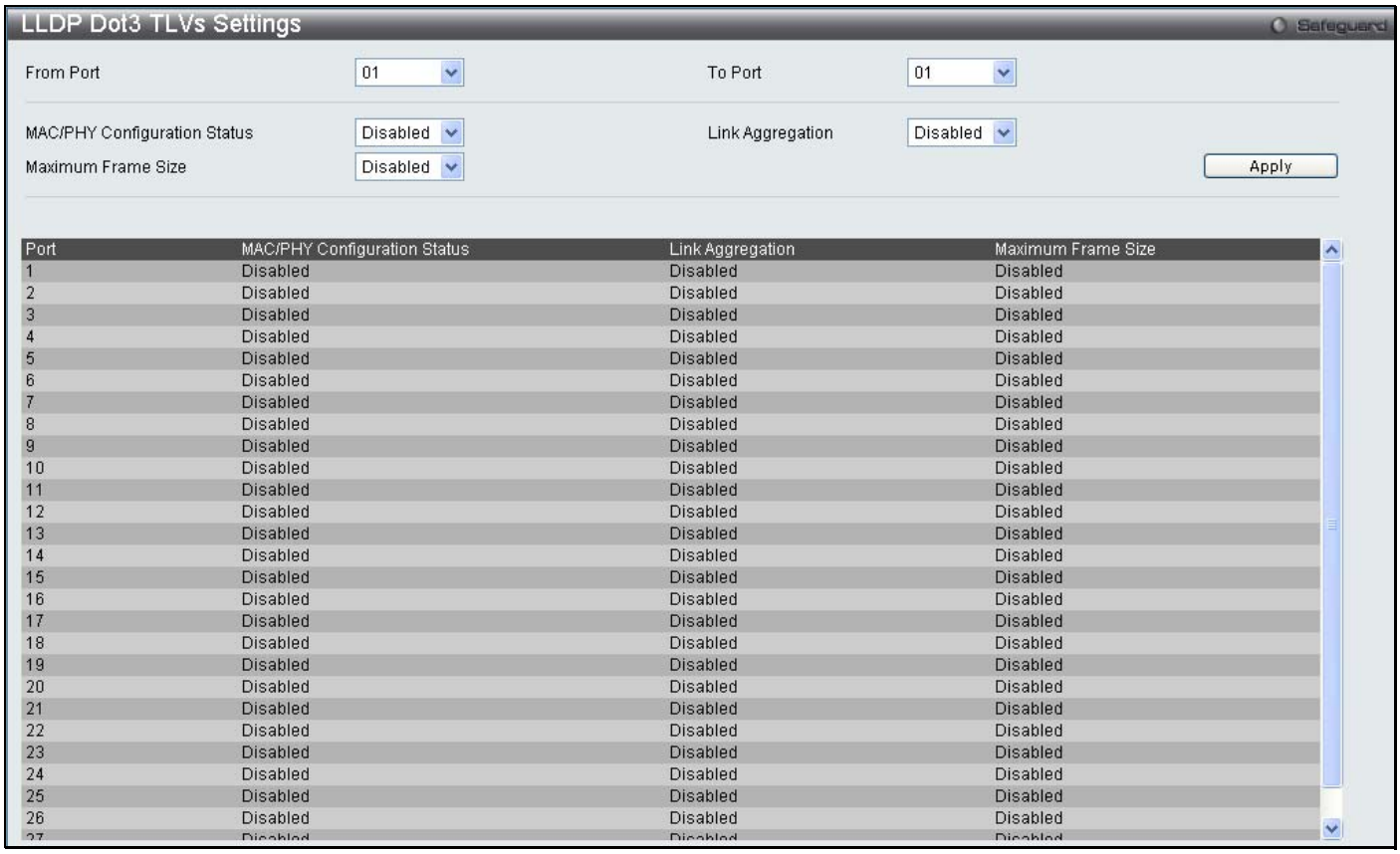


Figure 7- 51. LLDP Dot3 TLVs Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the drop-down menu to select a range of ports to be configured.
MAC/PHY Configuration Status	Use the drop-down menu to configure the advertise MAC or PHY status of the switch.
Link Aggregation	Use the drop-down menu to enable or disable the advertise link aggregation state on the Switch.
Maximum Frame Size	Use the drop-down menu to enable or disable the advertise Maximum Frame Size.

Click **Apply** to implement changes made.

LLDP Statistics System

LLDP Statistics System allows you to view the LLDP Stastics on the Switch and also the settings for individual ports. 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**

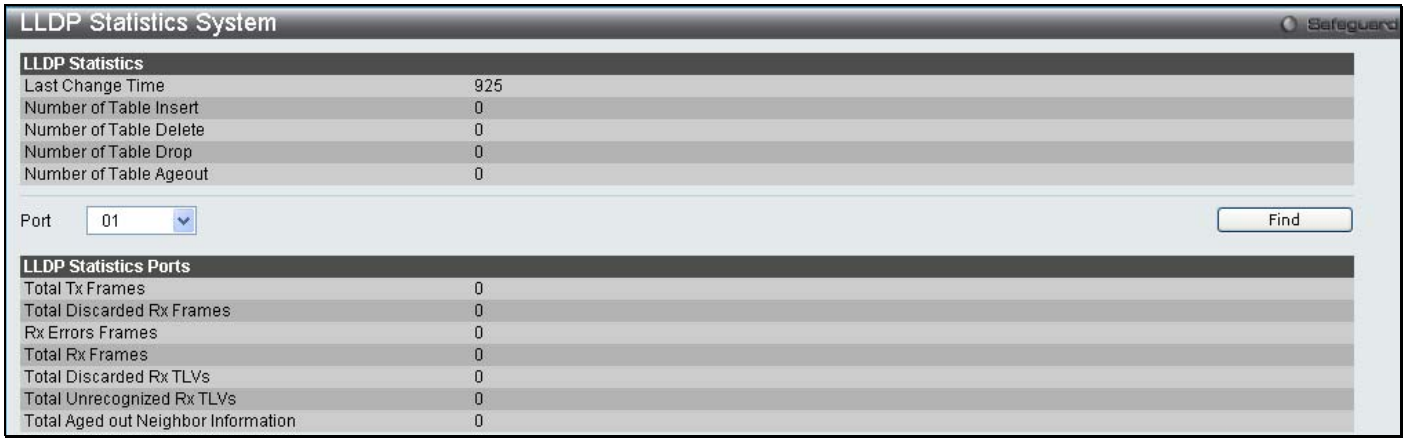


Figure 7- 52. LLDP Statistics System window

LLDP Local Port Information

LLDP Local Port Information window displays the information on a per port basis in the local port brief table shown below.

To view this window, Click **L2 Features** > **LLDP** > **LLDP Local Port Information**

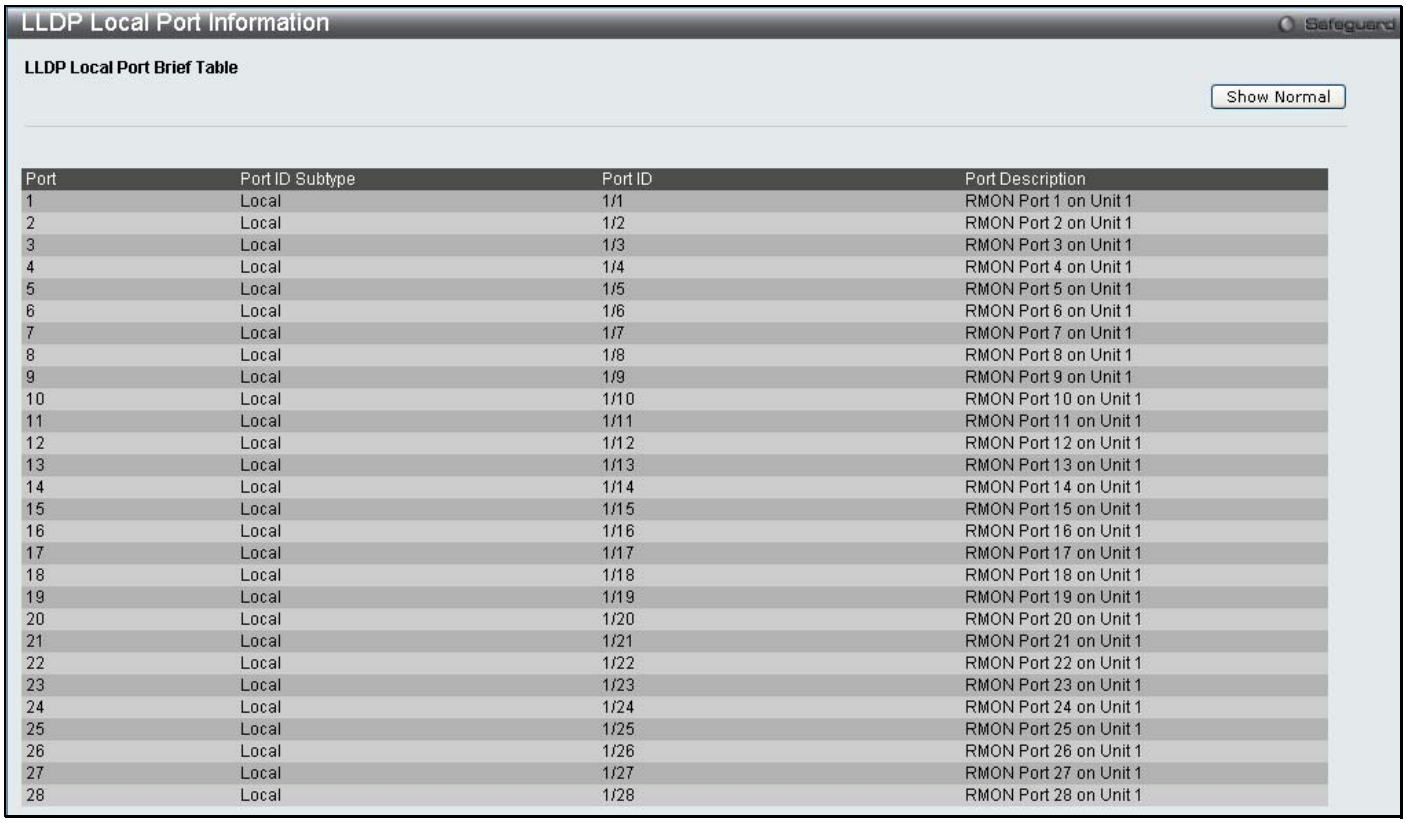


Figure 7- 53. LLDP Local Port Information window

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

Figure 7- 54. 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.

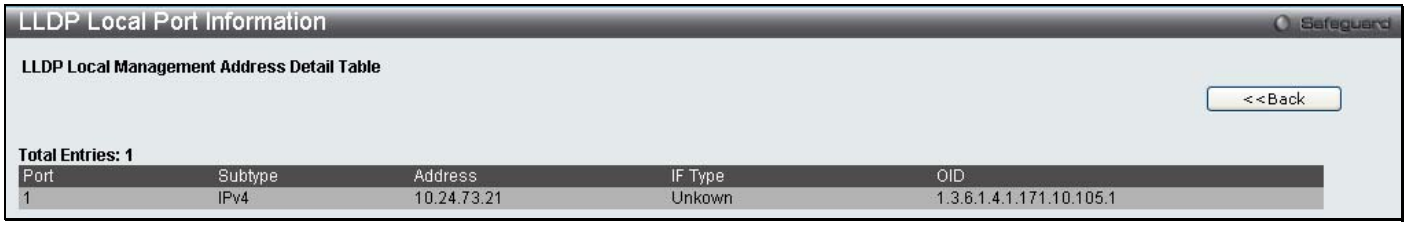


Figure 7- 55. LLDP Local Port Information (Show Detail) window

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

LLDP Remote Port Information

To view this window, Click **L2 Features** > **LLDP** > **LLDP Remote Port Information**

Figure 7- 56. 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.

Figure 7- 57. LLDP Remote Port Information (Show Normal) window

Section 8

QoS

HOL Blocking Prevention

Bandwidth Control

Traffic Control

802.1p Default Priority

802.1p User Priority

QoS Scheduling Mechanism

SRED

The DES-3528 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 DES-3528 implements 802.1P priority queuing.

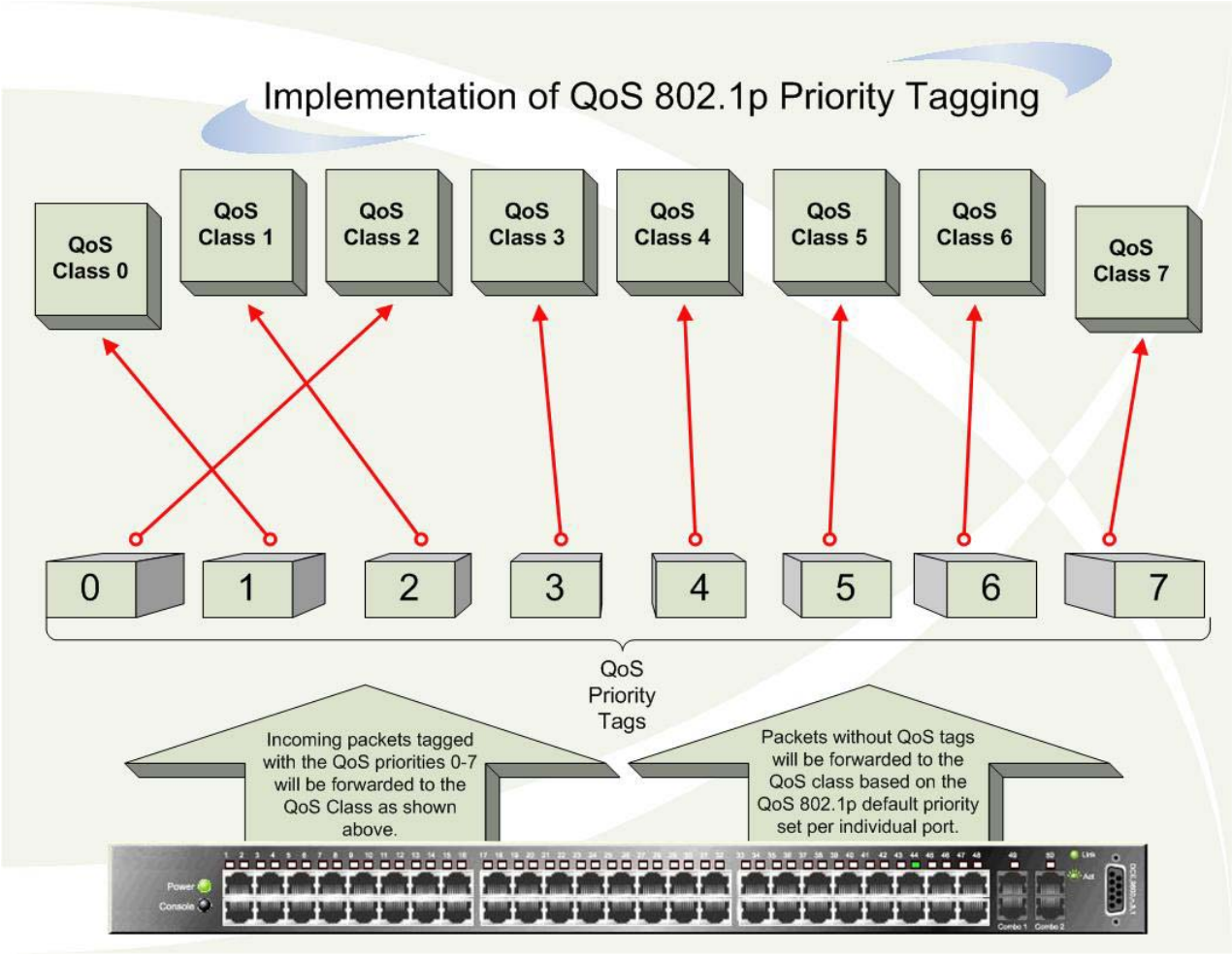


Figure 8- 1. Mapping QoS on the Switch

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, lets 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 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 Q6 queue.

NOTE: In the DES-3500 Series, the Q7 is reserved for future use.

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, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

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

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

Remember that the xStack DES-3528 has eight priority queues (and eight Classes of Service) for each port on the Switch.

HOL Blocking Pevention

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

To view this table Click **QoS** > **HOL Prevention Settings**

Figure 8- 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 table Click **QoS** > **Bandwidth Control**

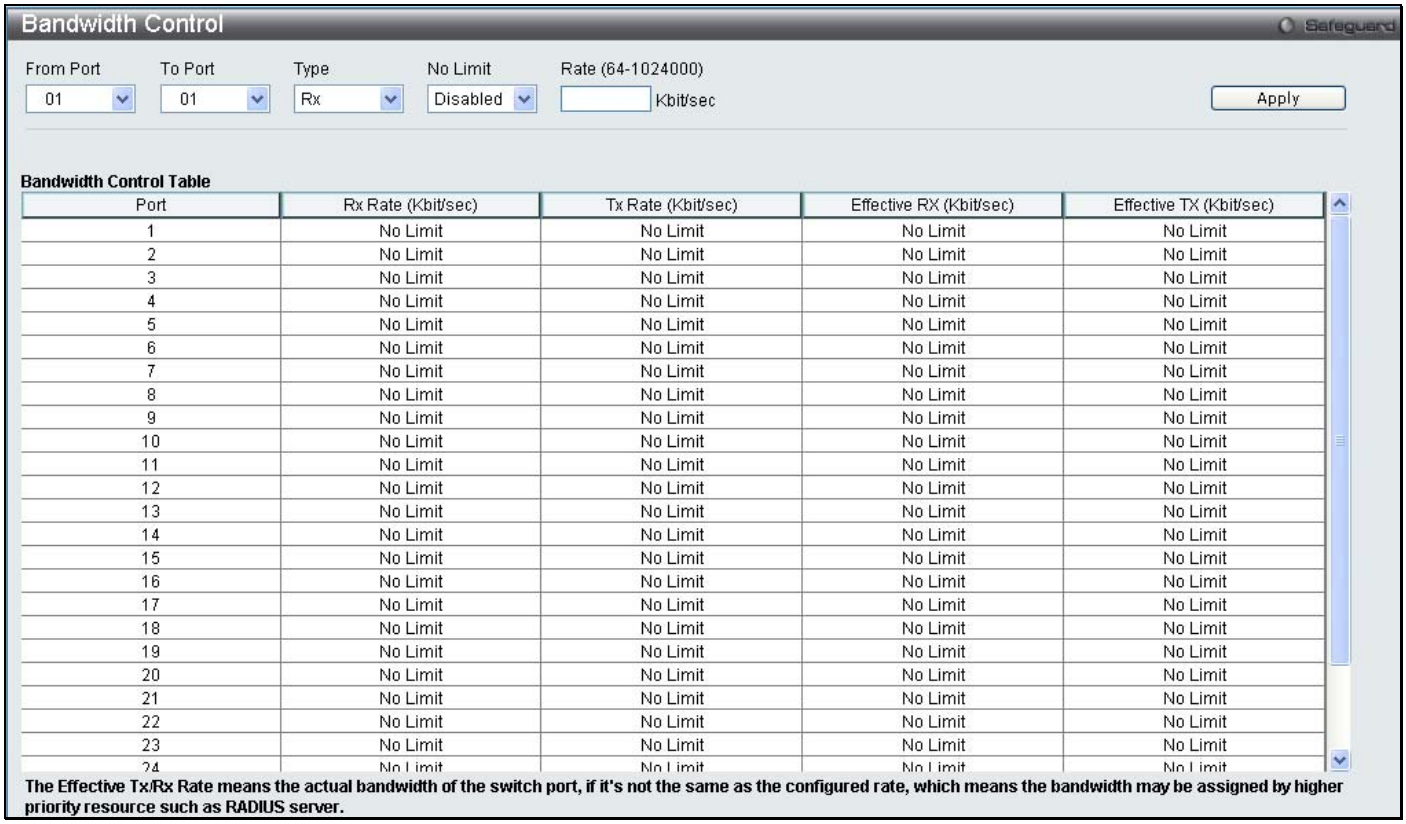


Figure 8- 3. Bandwidth Control window

The following parameters can be set or are displayed:

Parameter	Description
From port/To port	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.
Rate	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 do 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 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 recoup it using the **Port Configuration** window in the **Administration** 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 table Click **QoS** > **Traffic Control**

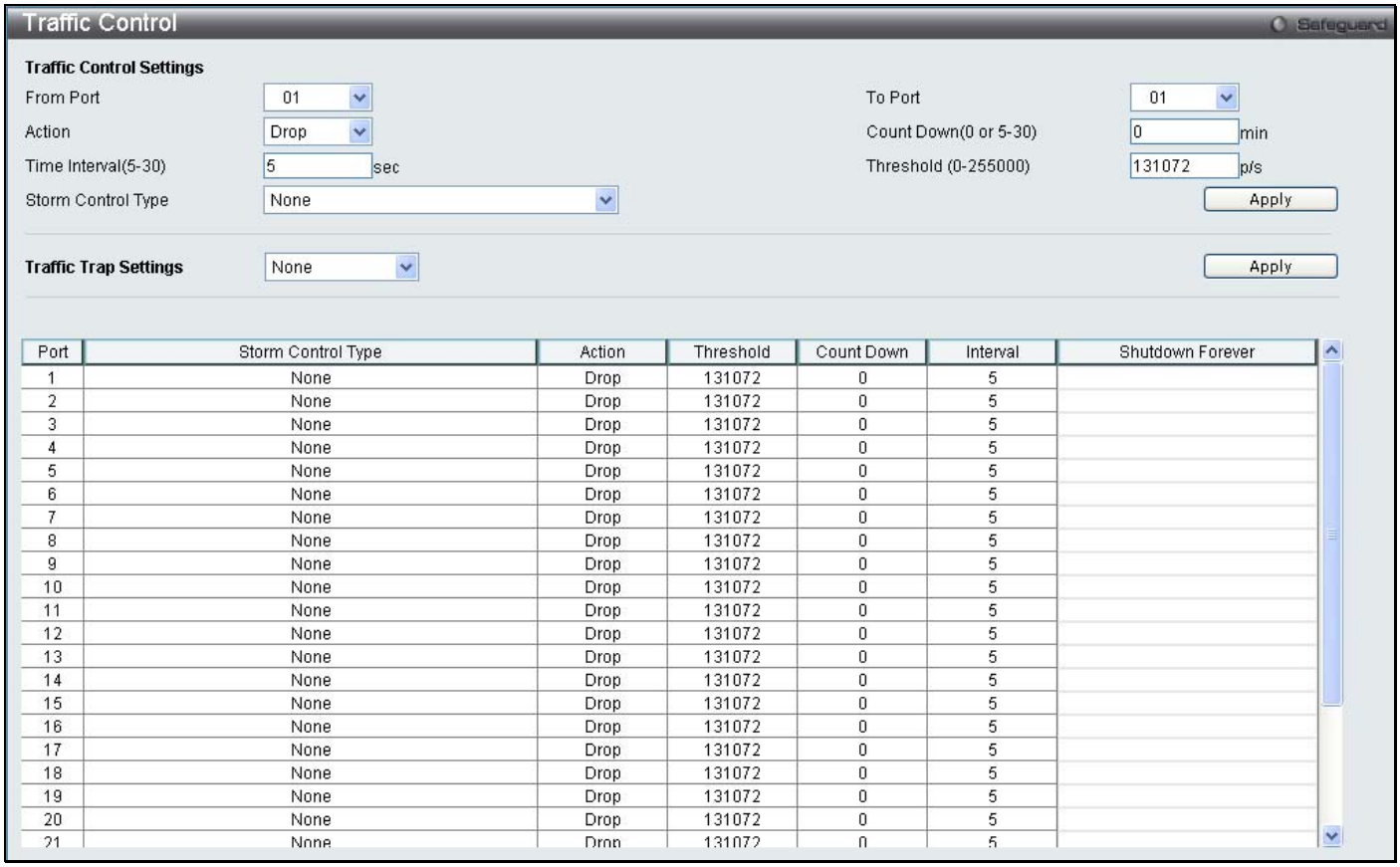


Figure 8- 4. Traffic Control window

Parameter	Description
Traffic Control Settings	
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Action	Select the method of traffic Control from the pull-down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *Shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Count Down	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are *0*, *5-30* minutes. 0 is disable forever state, port will not enter to shut down forever.
Time Interval	The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Interval may be set between *5* and *30* seconds with the default setting of *5* seconds.
Threshold	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from *0* to *255000* with a default setting of *131072*.
Storm Control Type	Select the type of Storm Type to detect, either Broadcast Multicast or Unicast. Once selected, use the pull-down menu to enable or disable this storm detection.
Traffic Trap Setting	
Storm Trap	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: • *None* – Will not send Storm trap warning messages regardless of action taken by the Traffic Control mechanism. • *Storm Occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. • *Storm Cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. • *Both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. This function cannot be implemented in the Hardware mode. (When Drop is chosen in the Action field.

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

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

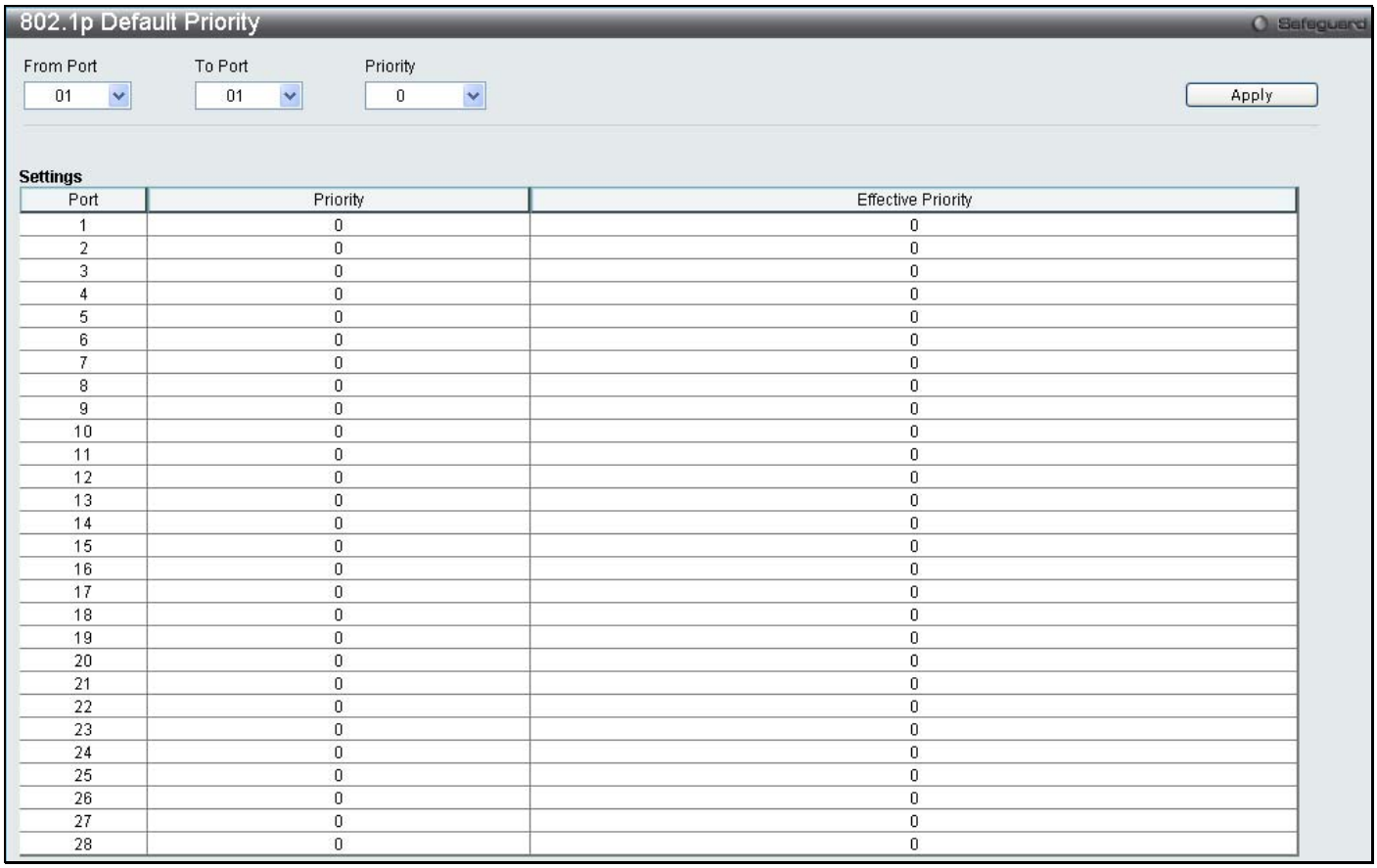
NOTE: Ports that are in the Shutdown forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

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

802.1p Default Priority

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

To view this window click **QoS** > **802.1p Default Priority**.



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

Figure 8- 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**.

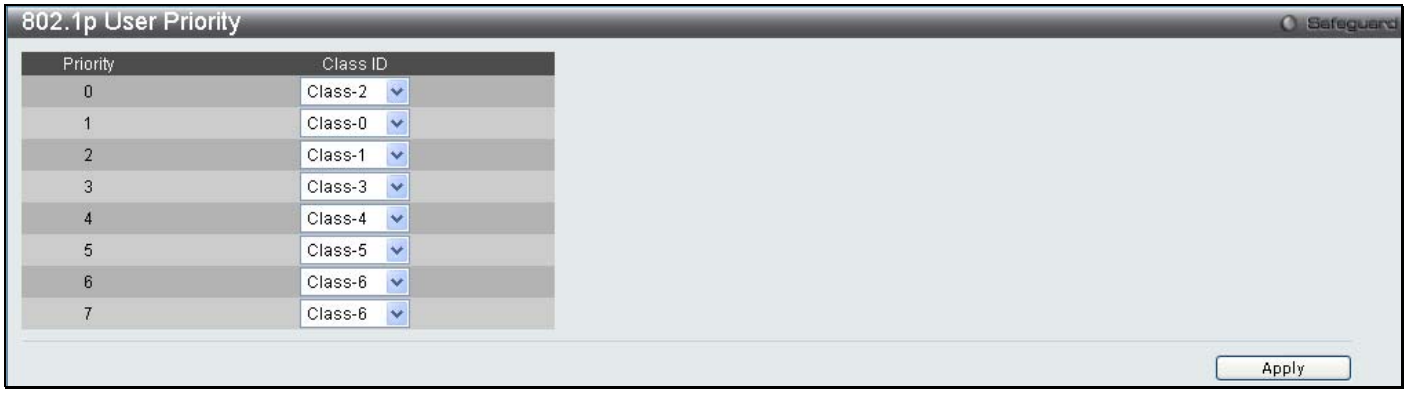


Figure 8- 6. 802.1p User Priority window

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**

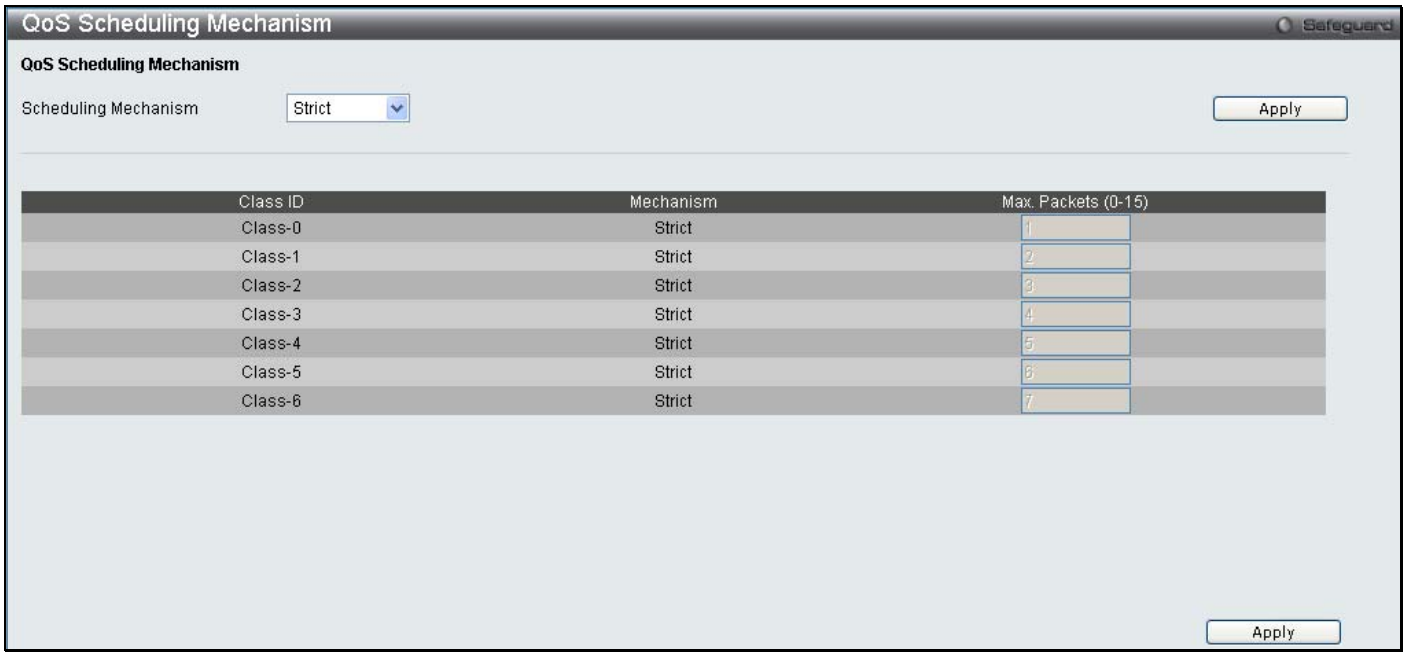


Figure 8- 7. QoS Scheduling Mechanism

The **Scheduling Mechanism** has the following parameters.

Parameter	Description
Strict	The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.

WRR	Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority classes of service.

Click **Apply** to implement changes made.

NOTE: The settings you assign to the queues, numbers 0-7, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

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**

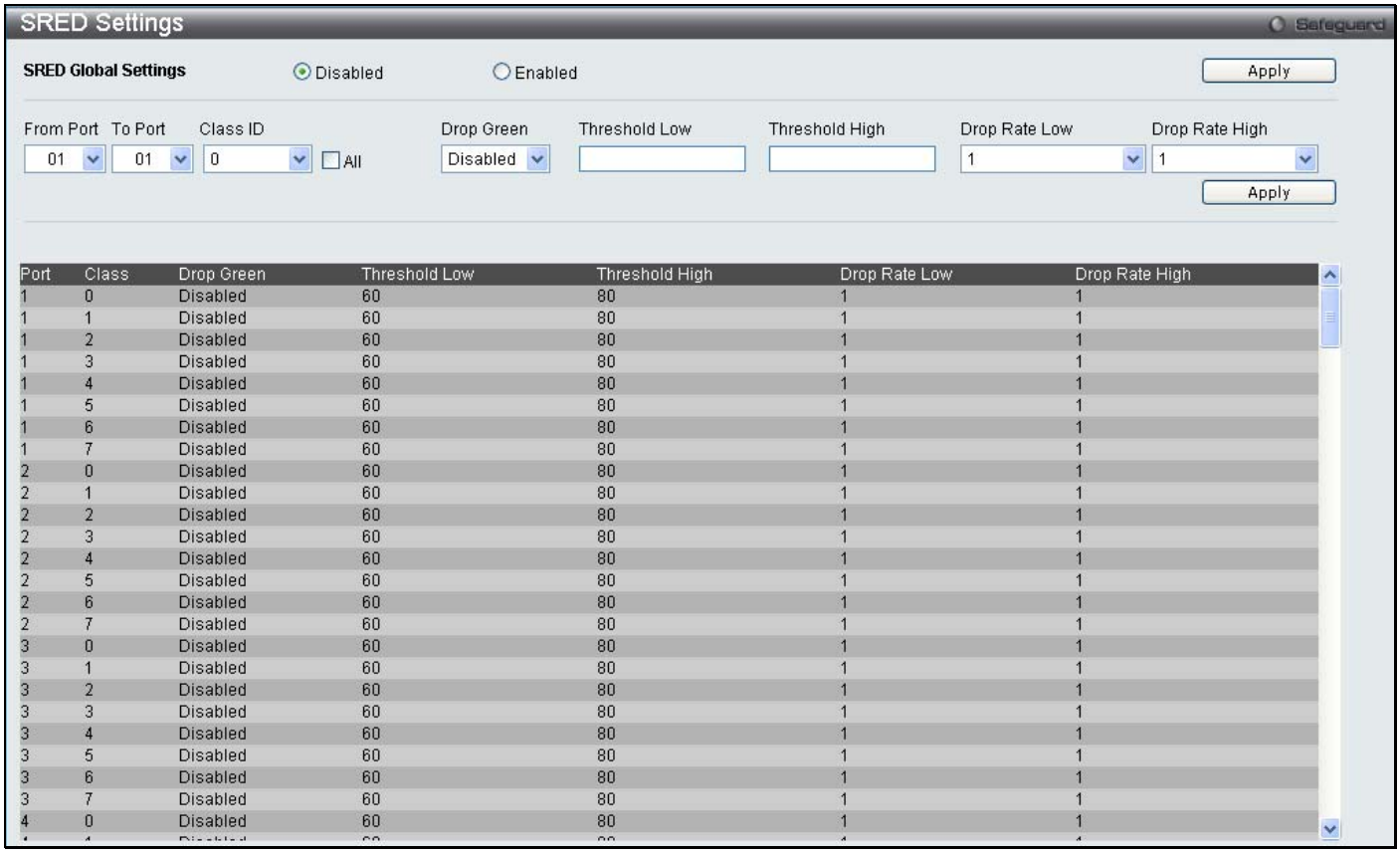


Figure 8- 8. SRED Settings window

The following parameters may be set:

Parameter	Description
From port/To port	A consecutive group of ports may be configured starting with the selected port.
Class ID	Select the Class ID, from *0*-7, to configure for the SRED parameters. Selecting *all* will set the parameters configured here for all CoS queues.
Drop Green	*Enabled:* 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. *Disabled*: 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.
Threshold Low	Threshold Low refers to the drop red packets it might also include yellow packets.
Threshold High	Threshold High refers to the drop yellow or green packets depending on the drop mode.
Drop Rate Low **Drop Rate High**	There are eight drop rates as shown below, the user may determine the drop rate for the expected packet. **Configure Value — Drop rate for expected packet** **1 — 100%** **2 — 6.25%** **3 — 3.125%** **4 — 1.5625%** **5 — 0.78125%** **6 — 0**.390625% **7** — 0.1953125% **8** — 0.09765625%

SRED Drop Counter

To view this window click **QoS** > **SRED** > **SRED Drop Counter**

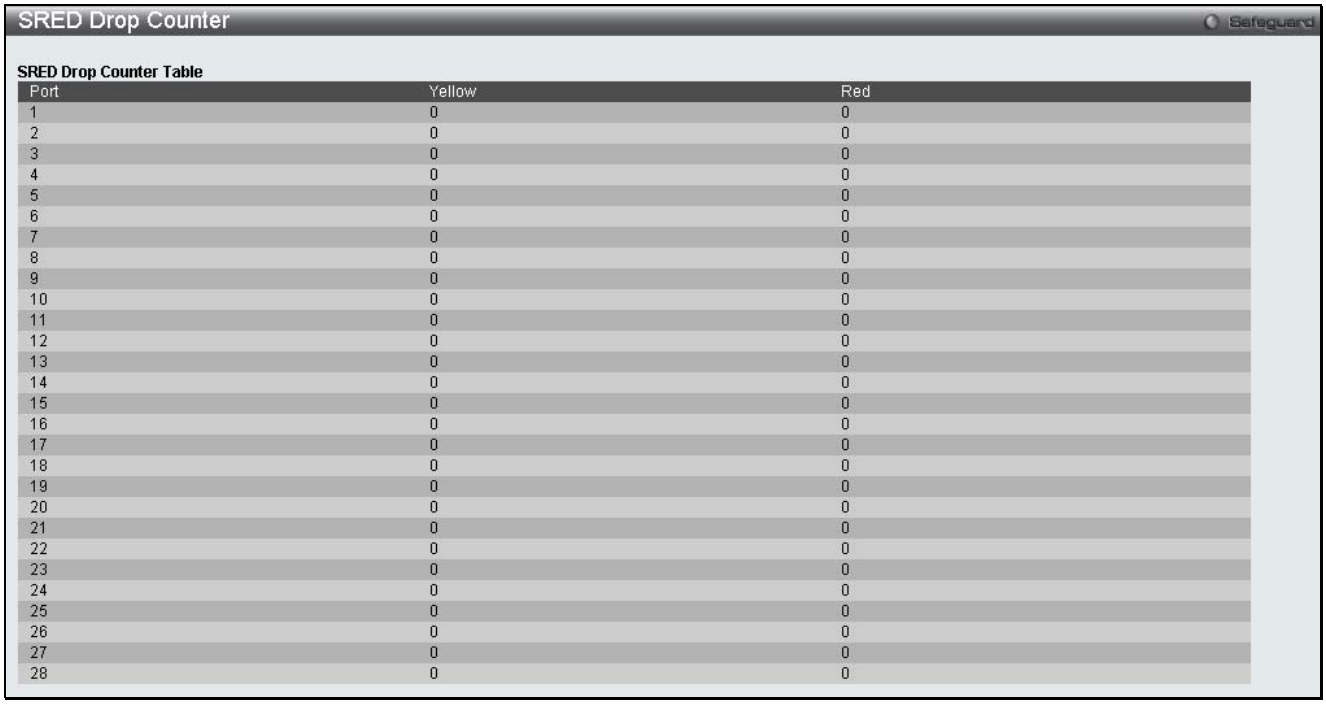


Figure 8- 9. SRED Drop Counter window

DSCP Trust Settings

This window is used to enable DSCP Trust Settings.

To view this window click **QoS** > **SRED** > **DSCP Trust Settings**

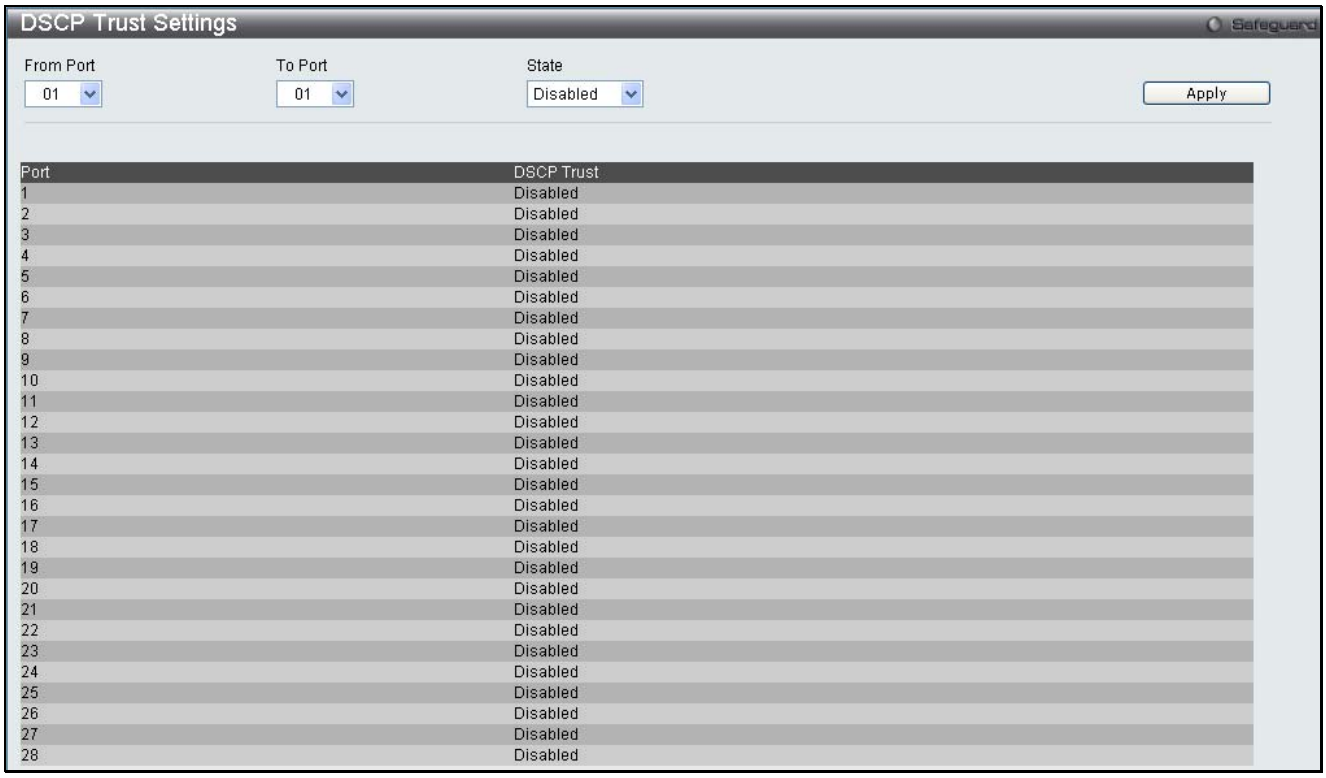
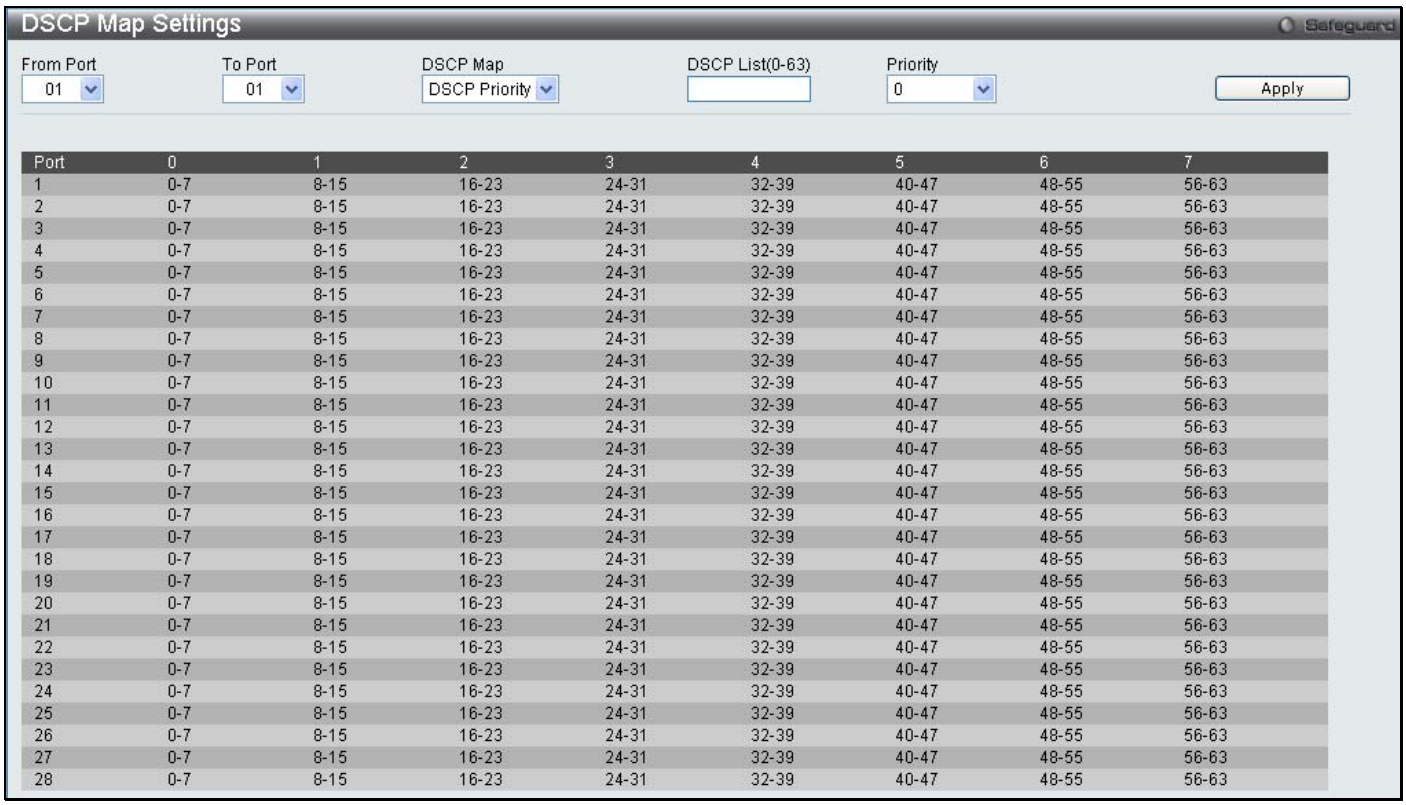


Figure 8- 10. DSCP Trust Settings window

DSCP Map Settings

This window is used to enable DSCP Map Settings.

To view this window click **QoS** > **SRED** > **DSCP Map Settings**



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
13	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
14	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
15	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
16	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
17	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
18	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
19	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
20	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
21	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
22	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
23	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
24	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
25	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
26	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
27	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
28	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Figure 8- 11. DSCP Map Settings window

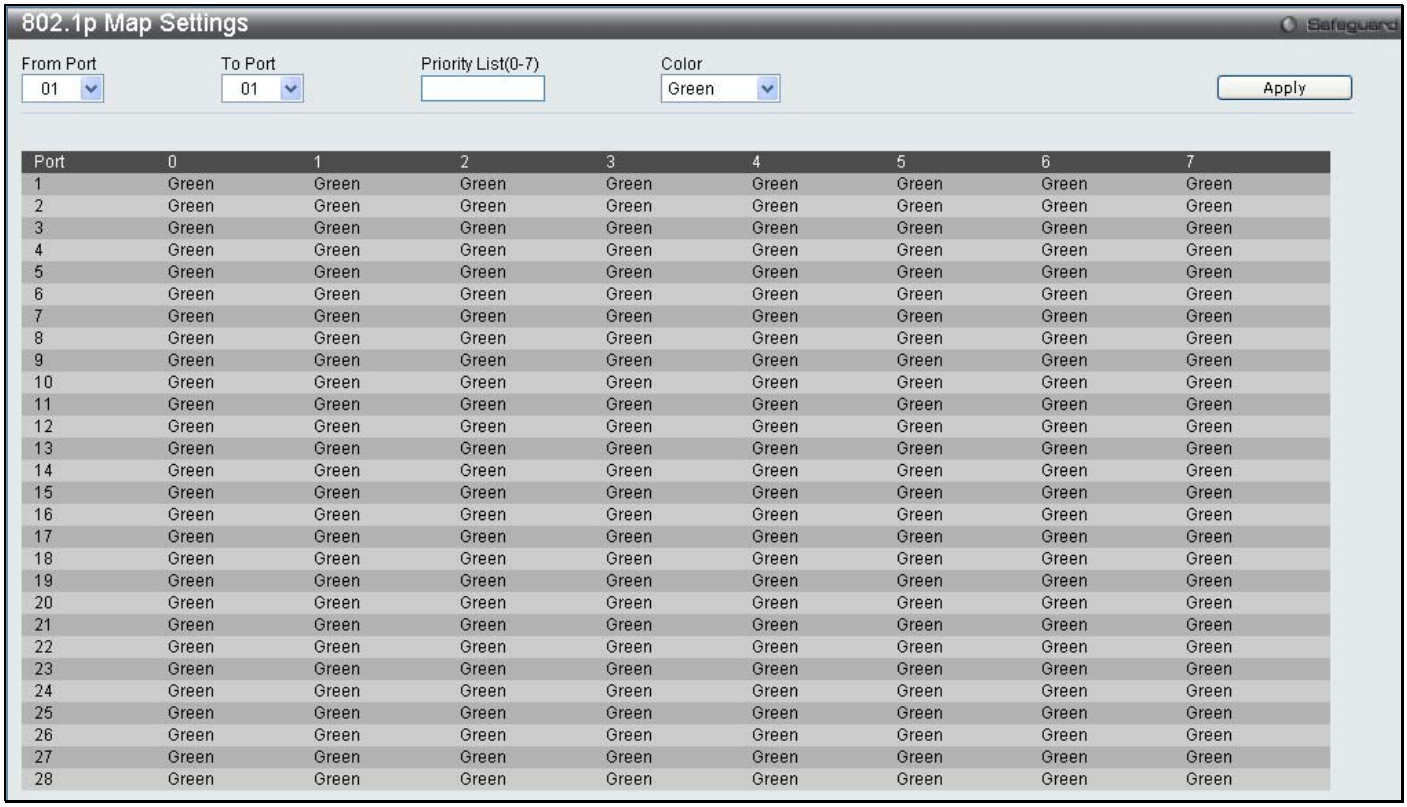
The following parameters may be set:

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

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**



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
13	Green	Green	Green	Green	Green	Green	Green	Green
14	Green	Green	Green	Green	Green	Green	Green	Green
15	Green	Green	Green	Green	Green	Green	Green	Green
16	Green	Green	Green	Green	Green	Green	Green	Green
17	Green	Green	Green	Green	Green	Green	Green	Green
18	Green	Green	Green	Green	Green	Green	Green	Green
19	Green	Green	Green	Green	Green	Green	Green	Green
20	Green	Green	Green	Green	Green	Green	Green	Green
21	Green	Green	Green	Green	Green	Green	Green	Green
22	Green	Green	Green	Green	Green	Green	Green	Green
23	Green	Green	Green	Green	Green	Green	Green	Green
24	Green	Green	Green	Green	Green	Green	Green	Green
25	Green	Green	Green	Green	Green	Green	Green	Green
26	Green	Green	Green	Green	Green	Green	Green	Green
27	Green	Green	Green	Green	Green	Green	Green	Green
28	Green	Green	Green	Green	Green	Green	Green	Green

Figure 8- 12. DSCP Map Settings window

The following parameters may be set:

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

Section 9

Security

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

JWAC

NetBIOS Filtering Settings

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may 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, [0]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.

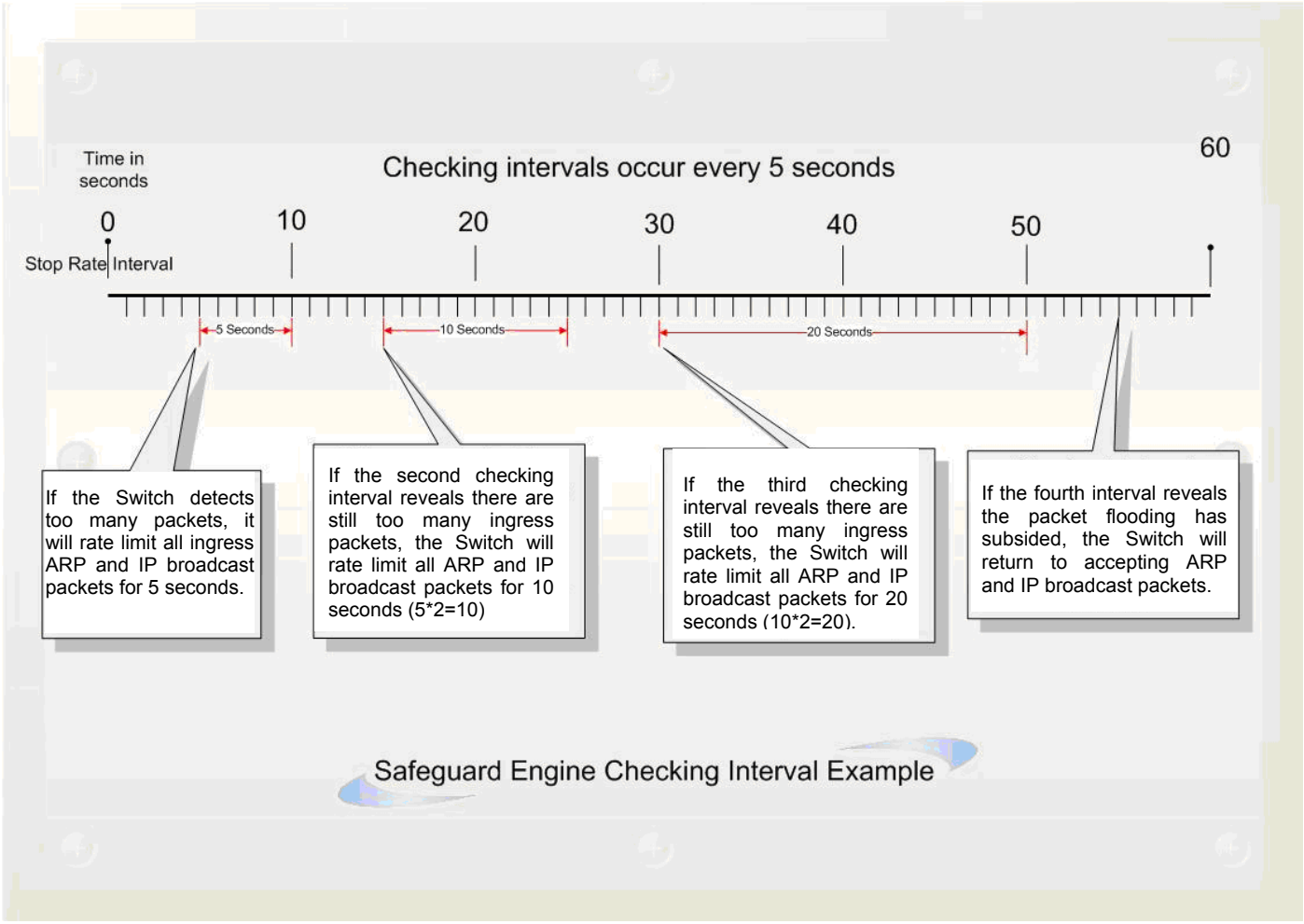


Figure 9- 1. Mapping QoS on the Switch

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

Figure 9- 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 windown, next to Safeguard. To set the Safeguard Engine for the Switch, complete the following fields:

Parameter	Description
Rising Threshold	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into the Exhausted state.
Falling Threshold	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Exhausted state and returns to normal mode.
Trap/log	Use the pull-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Toggle the State field to either *Strict* or *Fuzzy* for the Safeguard Engine of the Switch.

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

Trusted Host

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

To view this window click **Security > Trusted Host**

Figure 9- 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. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the xStack DES-3528 switch, 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.

IMP 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 Global Settings**

Figure 9- 4. IMP Global Settings window

The following parameters can be set:

Parameter	Description
ACL Mode	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 *Enabled* can only be automatically installed if the Access Profile table has two entries available of the possible six entries allowed.
Trap / Log	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.
DHCP Snoop State	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 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 Port Settings**

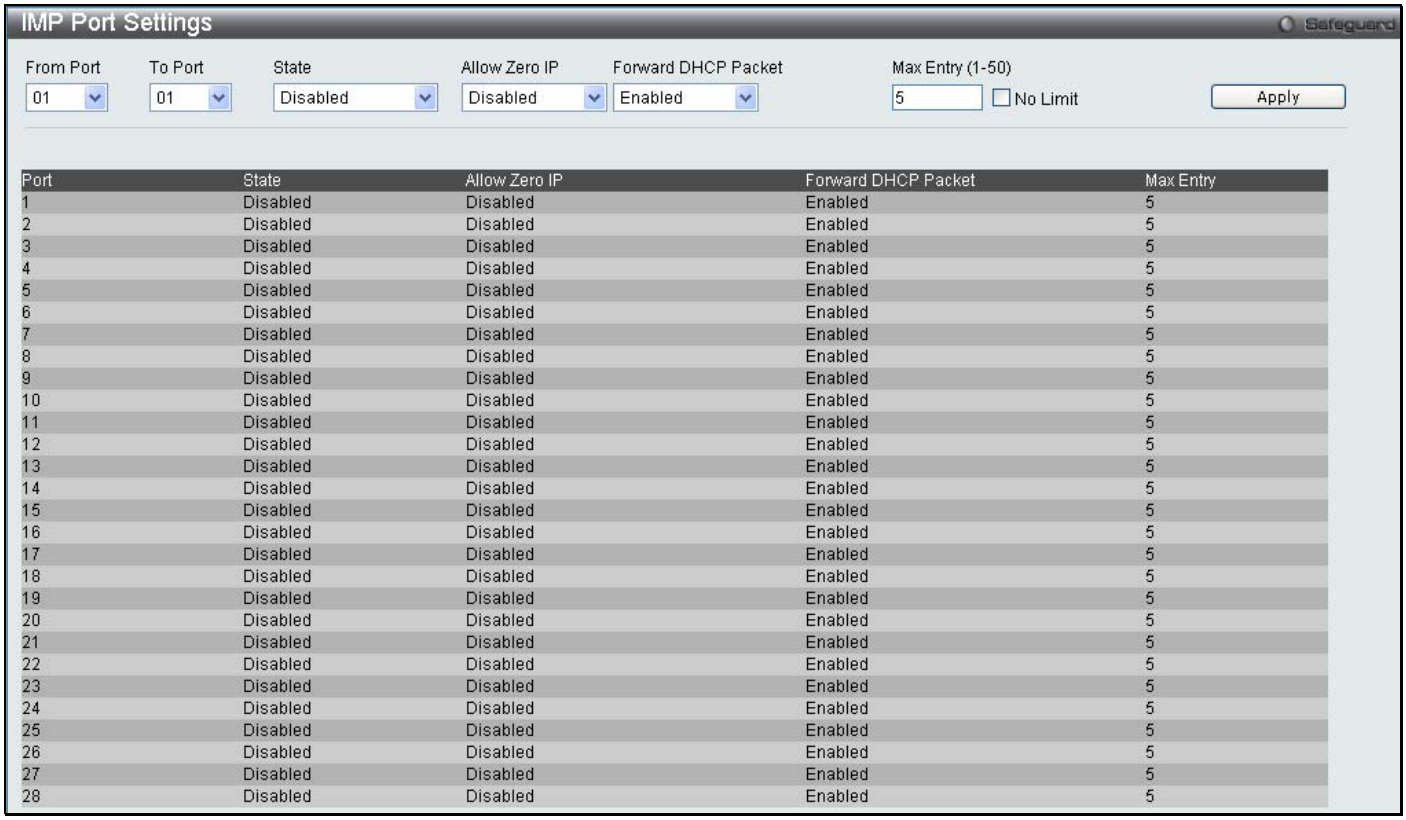


Figure 9- 5. IMP Port Settings window

The following fields can be set or modified:

Parameter	Description
From Port…To Port	Select a port or range of ports to set for IP-MAC Binding.
State	Use the pull-down menu to enable or disable these ports for IP-MAC Binding.
Strict	This mode provides a stricter method of control. If the user selects this mode, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the S/W learns the entries for the ports. The port will check ARP packets and IP packets by IP-MAC-PORT Binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. 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.
Loose	This mode provides a looser way of control. If the user selects loose mode, ARP packets and IP Broadcast packets will be sent to the CPU. The packets will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-PORT Binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.
Allow Zero IP	Use the 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.
Forward DHCP Packet	By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded. 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.
Max Entry	Specifies the maximum number of IP-MAC-Port Binding entries. By default, per port max entry is 5.

IMP 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 Entry Settings**

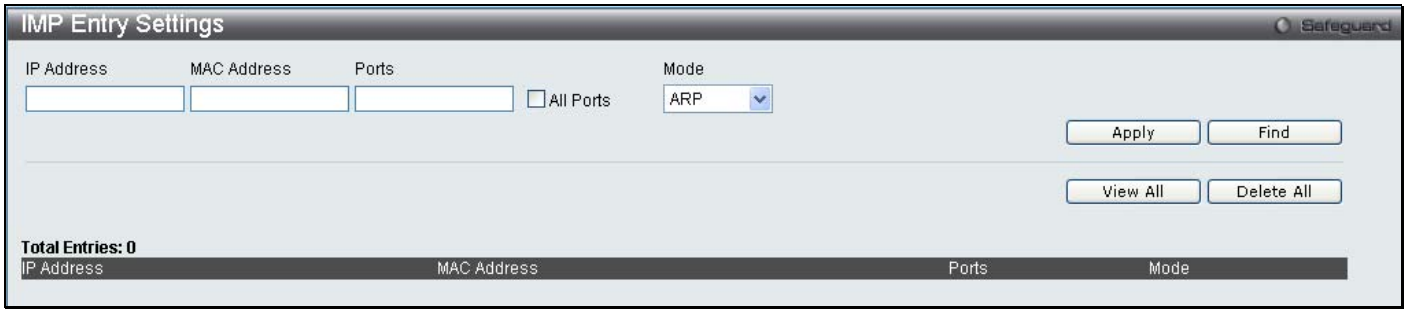


Figure 9- 6. IMP Entry Settings window

The following fields can be set or modified:

Parameter	Description
IP Address	Enter the IP address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Mode	The user may set the IP-MAC Binding Mode here by using the pull-down menu. The choices are: *ARP* – 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. *ACL* – 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.
Ports	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click the All check box to configure this entry for all ports on the Switch.

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

DHCP Snooping Entries

This 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**

Figure 9- 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**

Figure 9- 8. MAC Blocked List window

Port Security

Port Security 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 can not be changed once the port lock is enabled. Using 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 the following window click, **Security** > **Port Security** > **Port Security Settings**

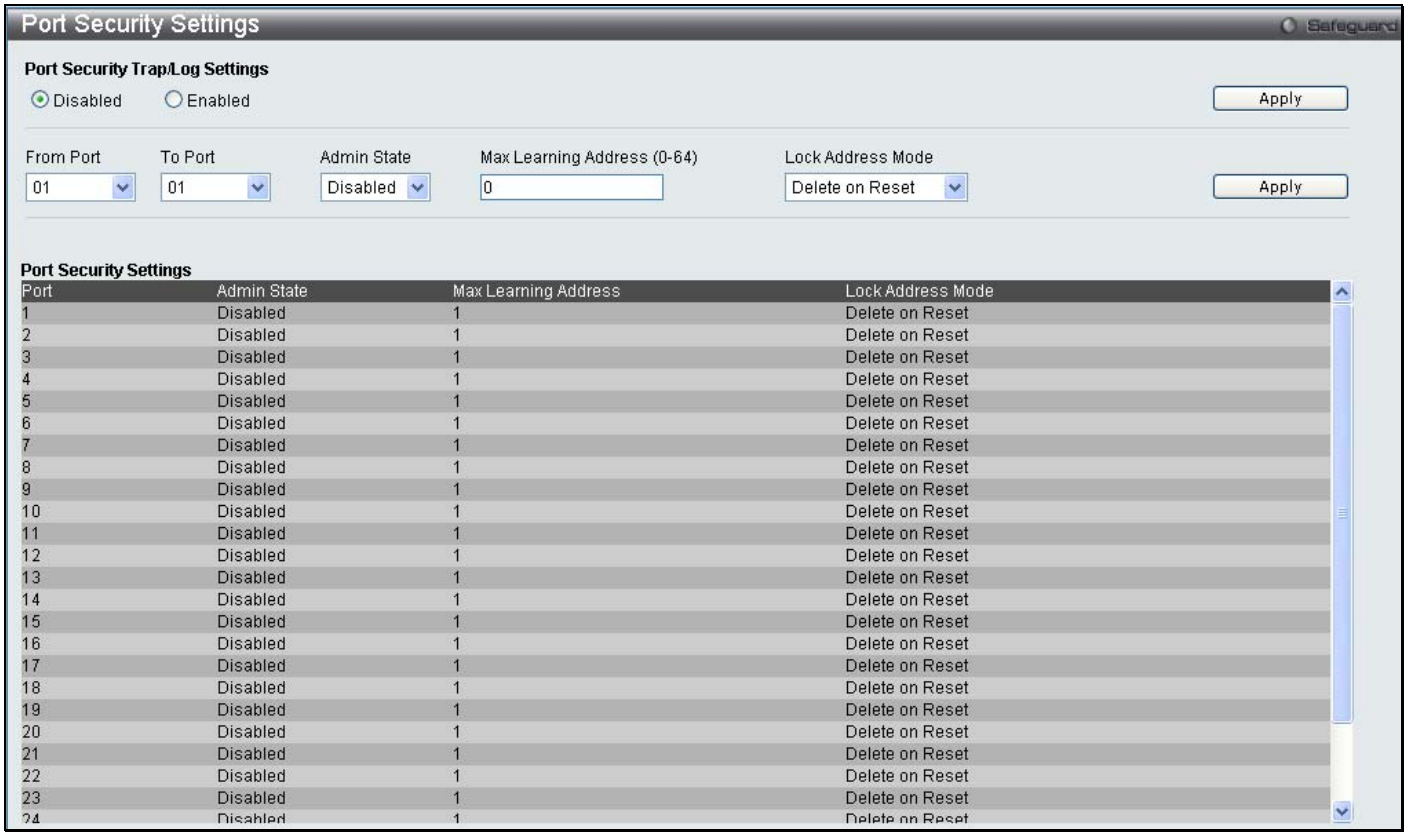


Figure 9- 9. Port Security Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Learning Address (0-64)	The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.
Lock Address Mode	This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: *Permanent* – The locked addresses will not age out after the aging timer expires. *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

Port Security FDB Entries

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

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

Figure 9- 10. Port Security FDB Entries window

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.

DHCP Screening Port Settings

The following window will allow users to enable ports on the switch to be used in DHCP Server Screening. To view this window, click **Security > DHCP Server Screening > DHCP Screening Port Settings**:

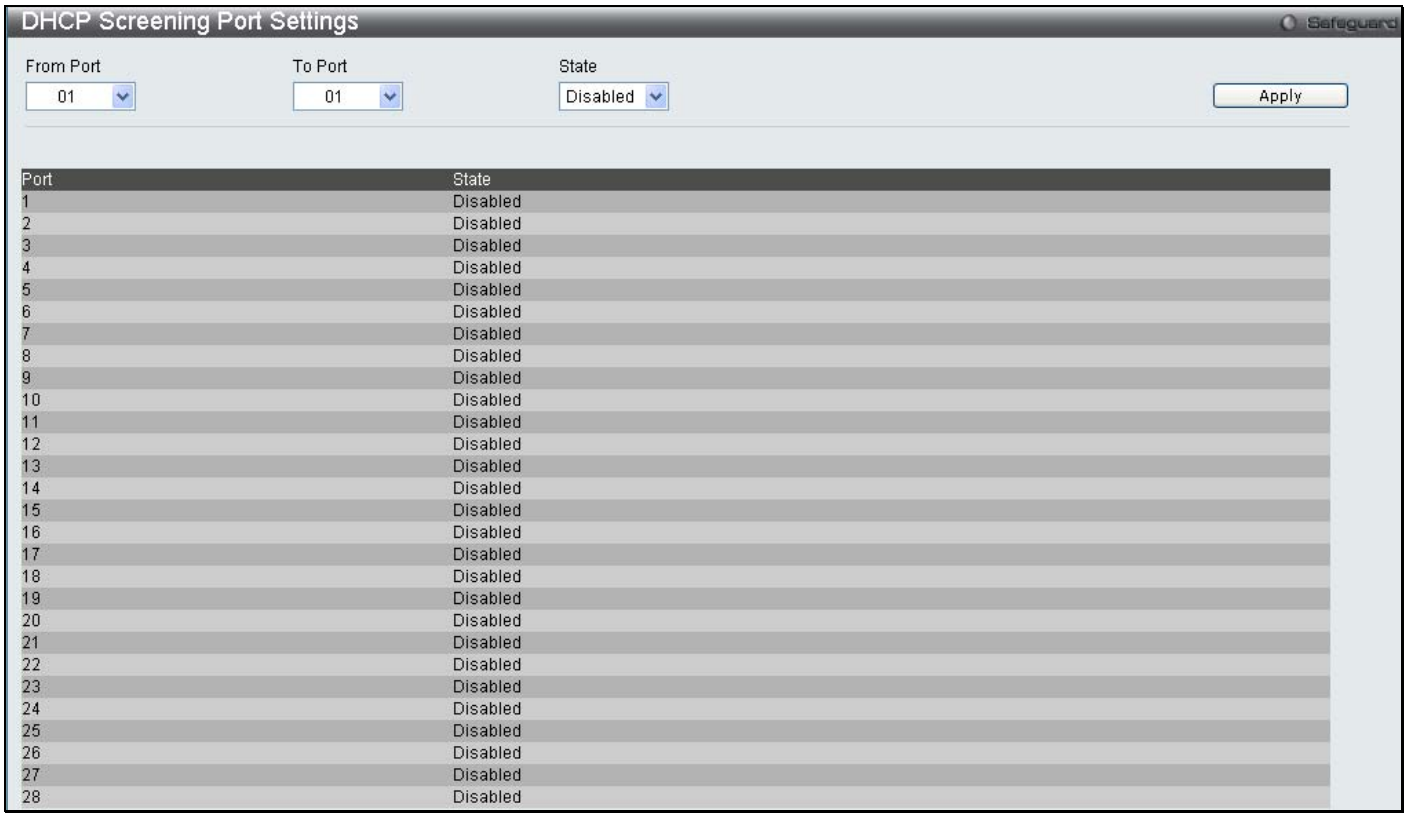


Figure 9- 11. DHCP Screening Port Settings window

The user may set the following parameters:

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

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

DHCP Offer Filtering

The following window will allow users to configure the DHCP Server Settings on the switch. To view this window, click **Security > DHCP Server Screening > DHCP Offer Filtering**:

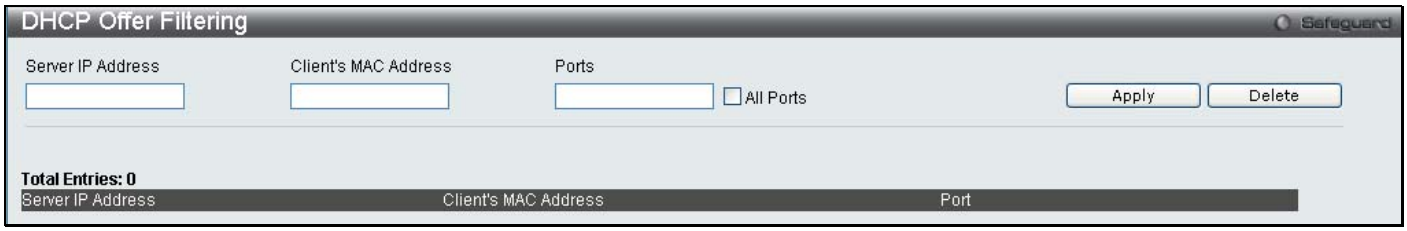


Figure 9- 12. DHCP Offer Filtering window

The user may set the following parameters:

Parameter	Description
Server IP Address	The IP address of the DHCP server.
Client's MAC Address	The MAC address of the Client.
Ports	Choose the range of ports that you want to use as the DHCP server, or check the *All Ports* box if you wish to use all the ports on the switch.

After setting the previous parameters, click **Apply** to allow your changes to be implemented.

802.1X

802.1x Port-Based and MAC-Based Access Control

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

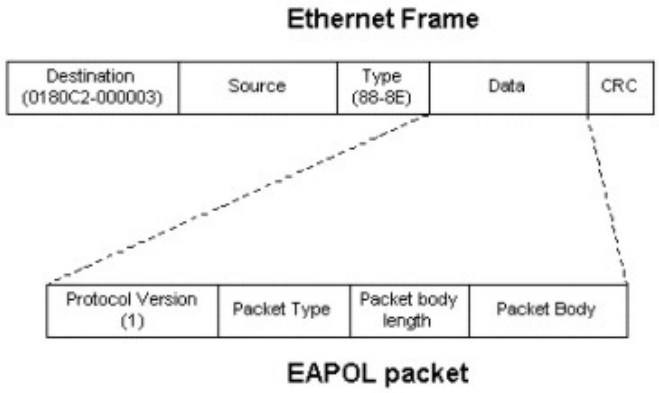


Figure 9- 13. The EAPOL Packet

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.

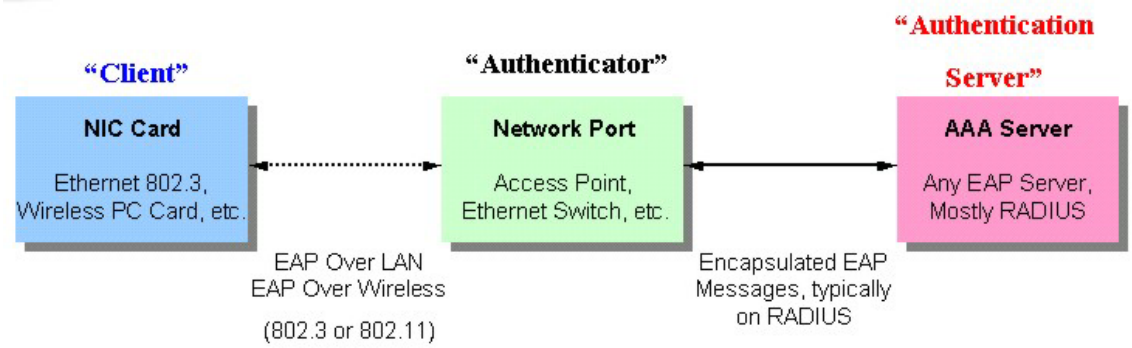


Figure 9- 14. The three roles of 802.1x

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

Authentication Server

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

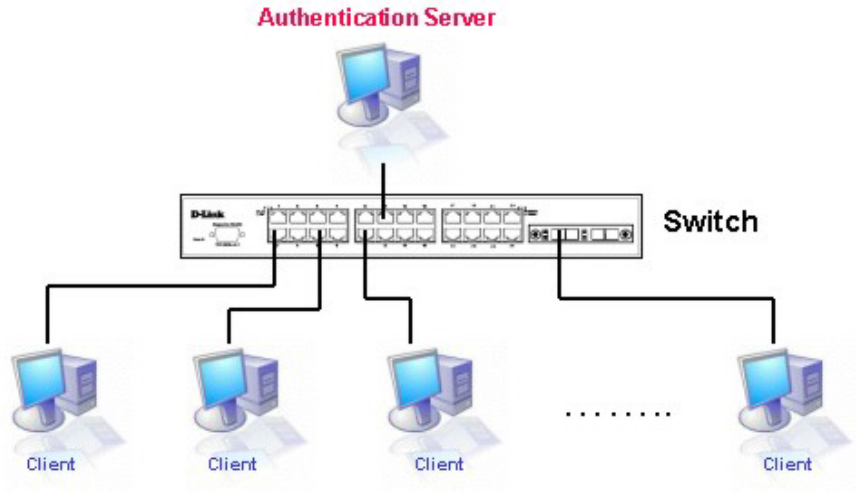


Figure 9- 15.The Authentication Server

Authenticator

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

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

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

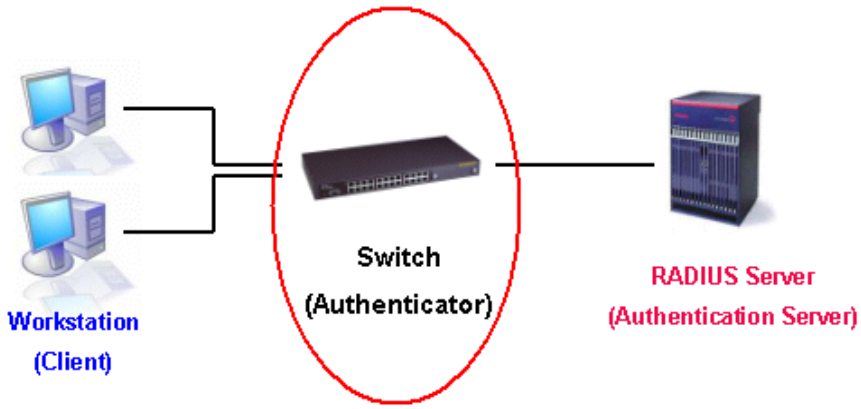


Figure 9- 16.The Authenticator

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, that software is included within the operating system. All other users are required to attain 802.1x client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

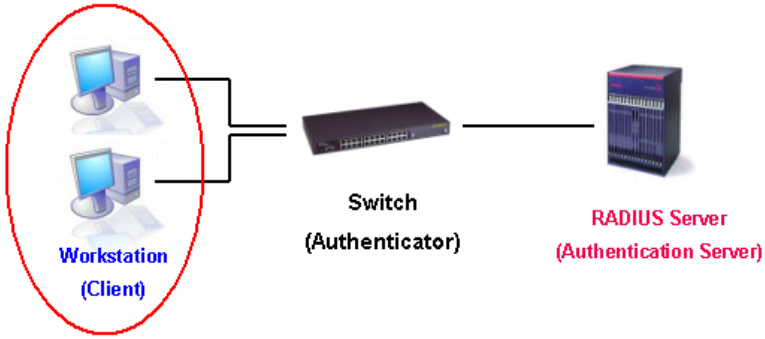


Figure 9- 17.The Client

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.

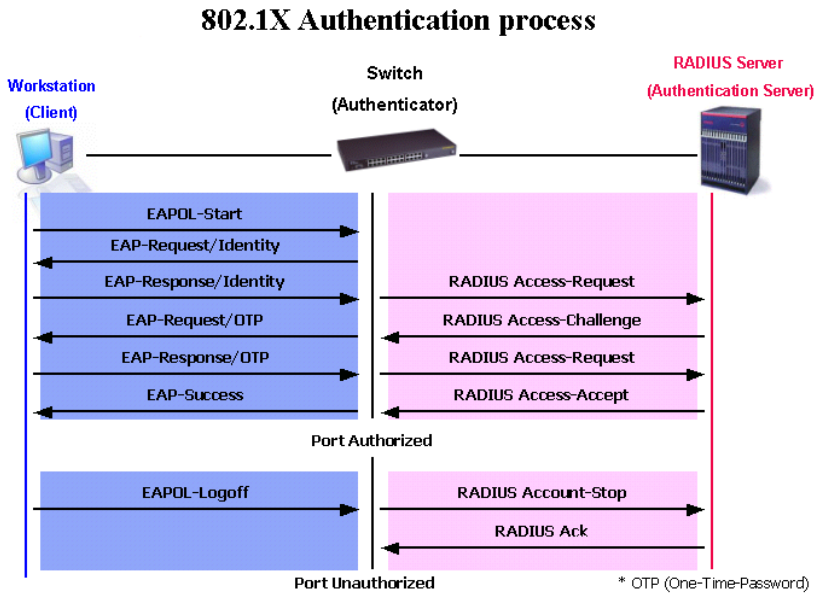


Figure 9- 18. The 802.1x Authentication Process

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. MAC-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 MAC-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

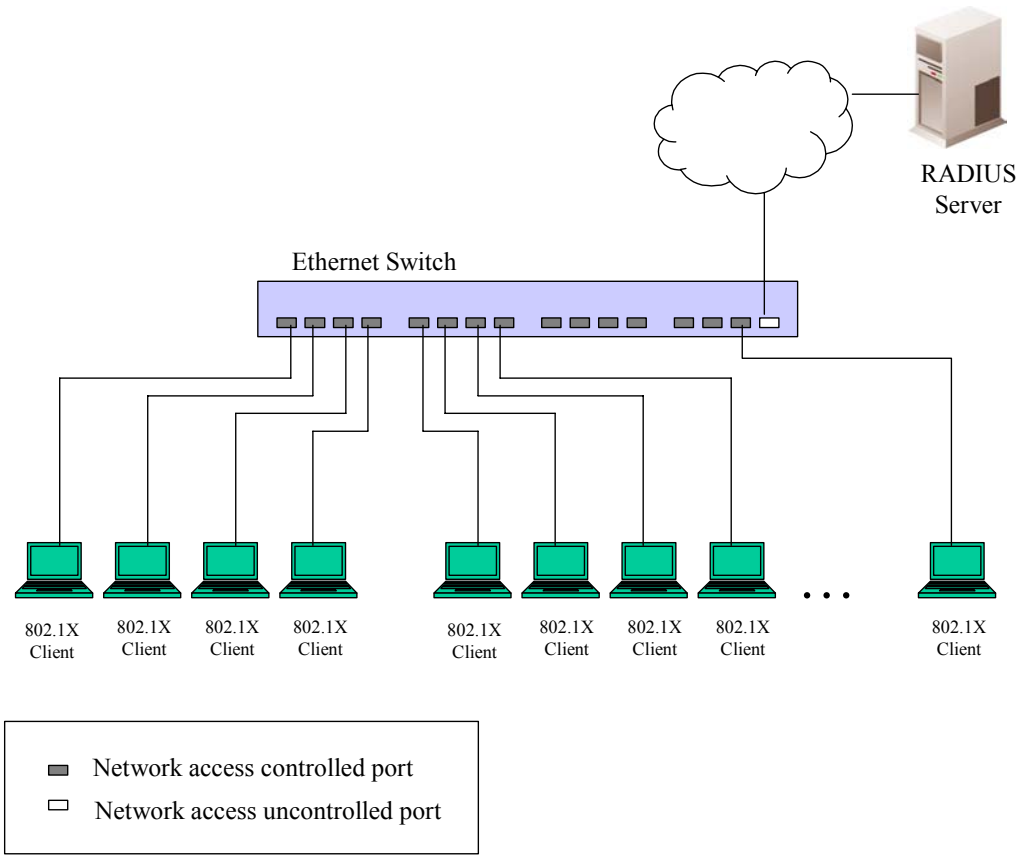


Figure 9- 19. Example of Typical Port-Based Configuration

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.

MAC-Based Network Access Control

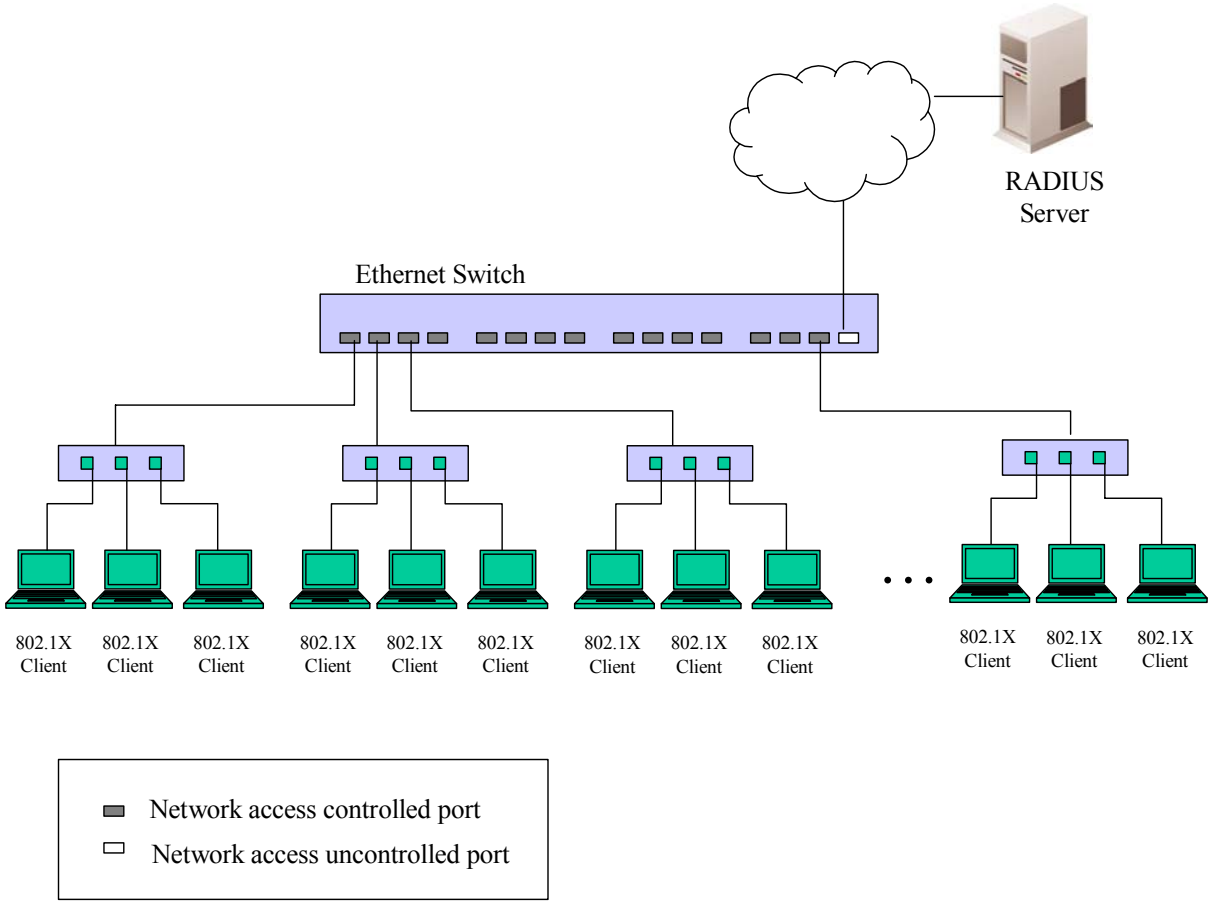


Figure 9- 20. Example of Typical MAC-Based Configuration

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 Force Disconnect

To configure the 802.1X Force Disconnect, click **Security** > **802.1X** > **802.1X Force Disconnect**

Figure 9- 21. 802.1X Force Disconnect window

Use the drop down menu to select either Port or MAC Address and enter the corresponding information, click **Force Disconnect** for the changes to take effect.

802.1X Settings

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

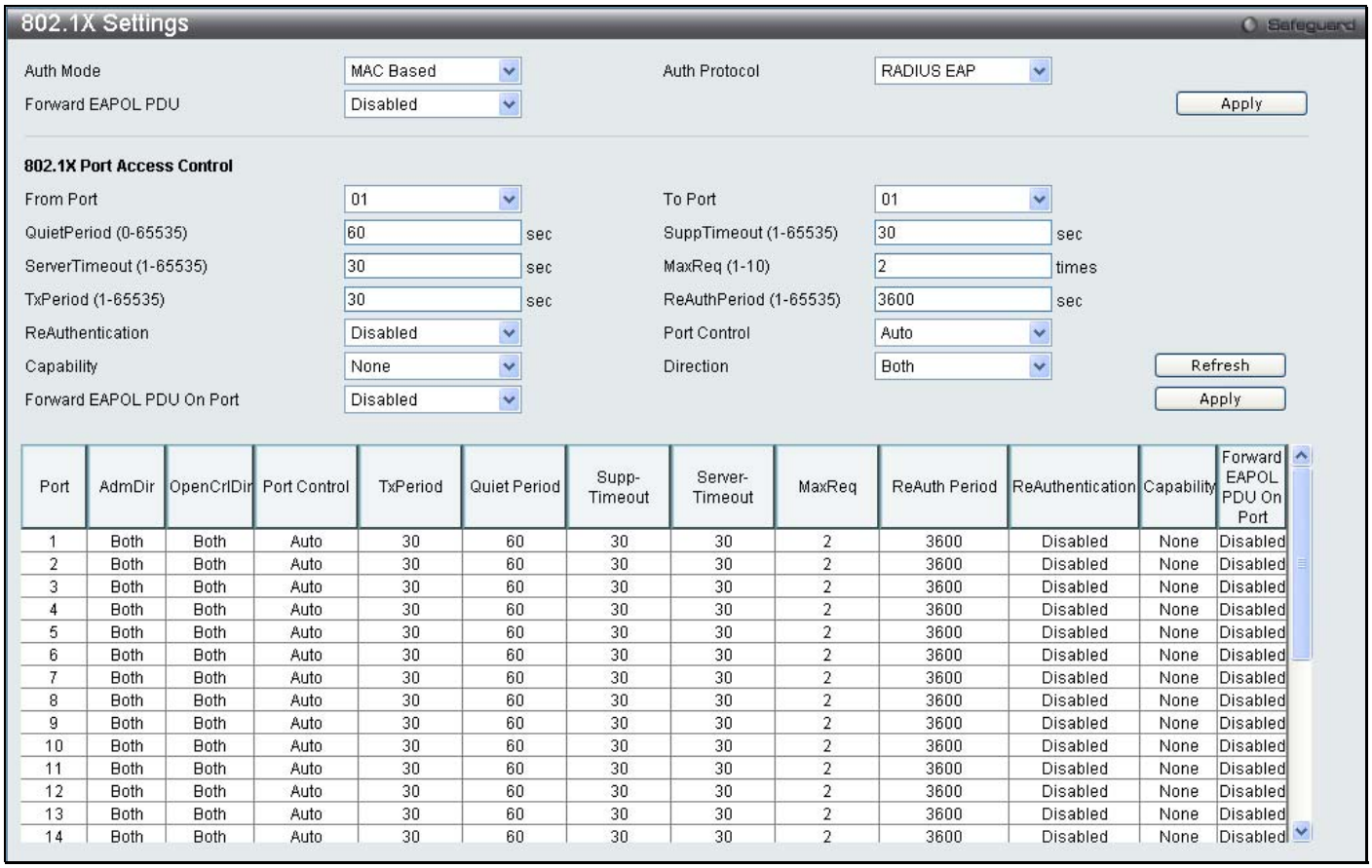


Figure 9- 22. 802.1X Settings window

This window allows you to set the following features:

Parameter	Description
Auth Mode	The Auth Mode allows the user to choose among, *Disabled*, *Port Based* or *MAC Based* Authentication Mode.
Auth Protocol	Choose the Auth Protocol either *RADIUS EAP* or *Local*.
Forward EAPOL PDU	This enables or disables the Switch retransmit EAPOL PDU Request.
From Port/To Port	Enter the port or ports to be set.

QuietPeriod (0-65535)	This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2*.
TxPeriod (1-65535)	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.
ReAuthEnabled	Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.
PortControl	This allows you to control the port authorization state. Select *forceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *forceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
Capability	This allows the 802.1x Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated A user must pass the authentication process to gain access to the network. Select *None* disable 802.1x functions on the port.
Direction	Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* are selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
Forward EAPOL PDU On Port	This enables or disables the Switch retransmit EAPOL PDU Request on a per port basis.

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

802.1X User

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

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

Figure 9- 23. 802.1X User window

Authentication RADIUS Server

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

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

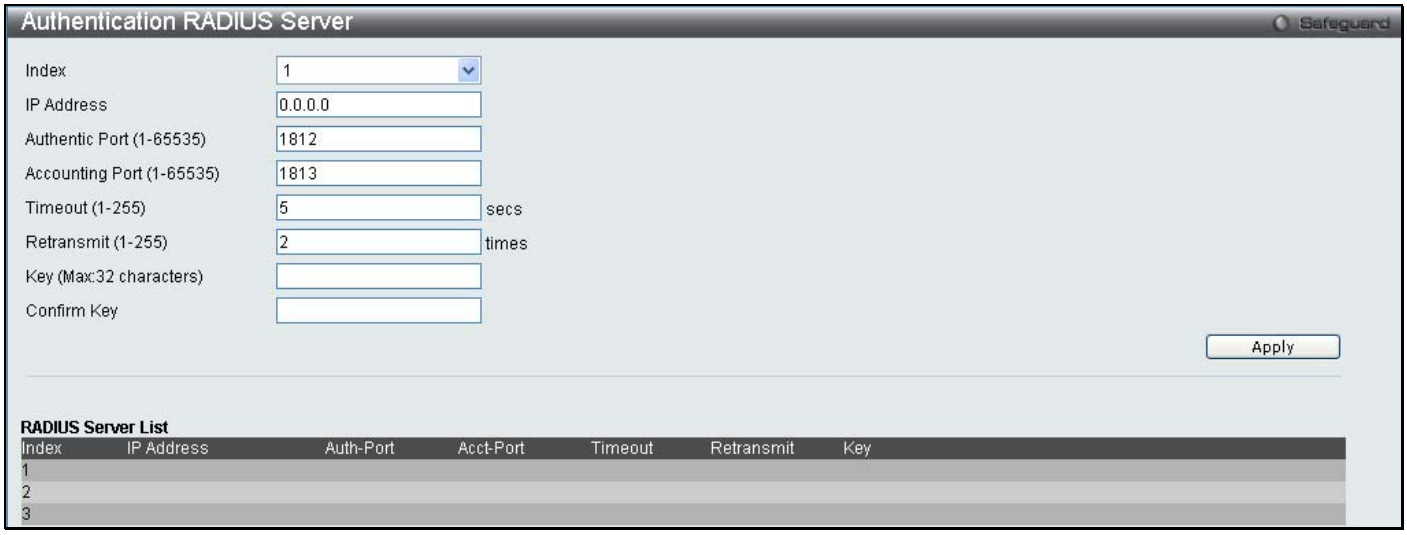


Figure 9- 24. Authentic RADIUS Server window

This window displays the following information:

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

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.

To initialize ports, click **Security** > **802.1X** > **Initialize Port(s)**

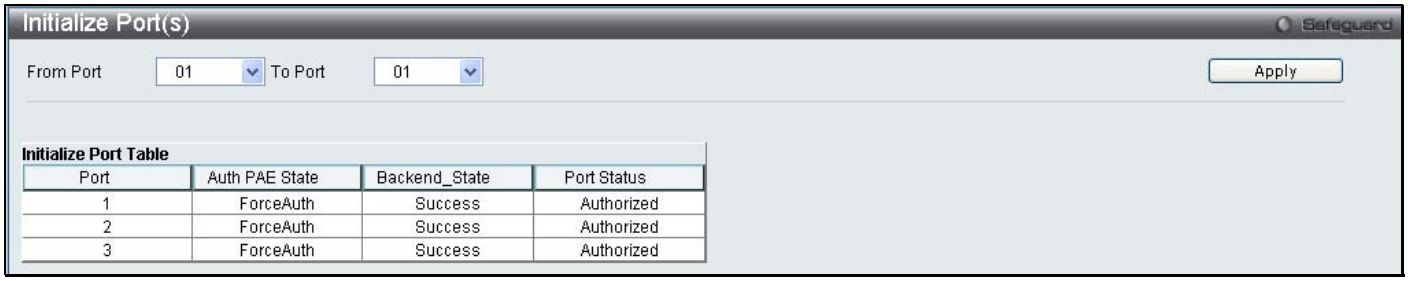


Figure 9- 25. Initialize Port(s) window

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.

To reauthenticate ports, click **Security** > **802.1X** > **Reauthenticate Port(s)**

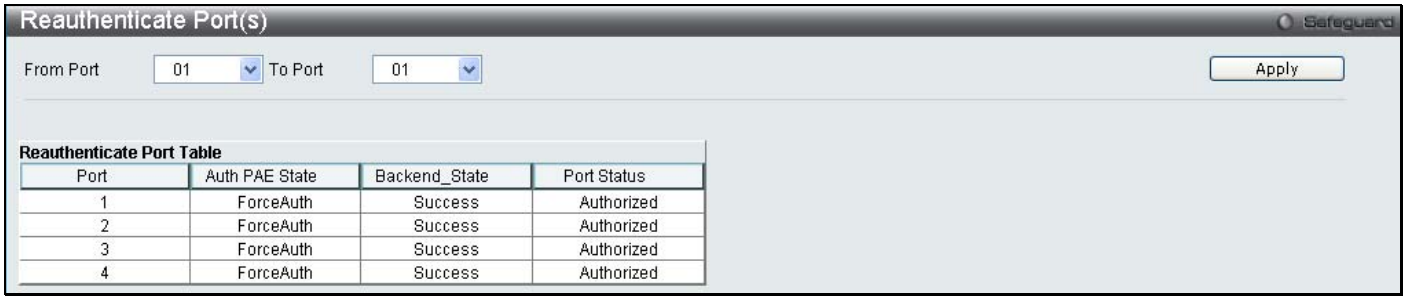


Figure 9- 26. Reauthenticate Port(s) window

To reauthenticate port(s), use the drop down menu to select the port(s) and click **Apply**.

Guest VLAN

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 posseses 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.

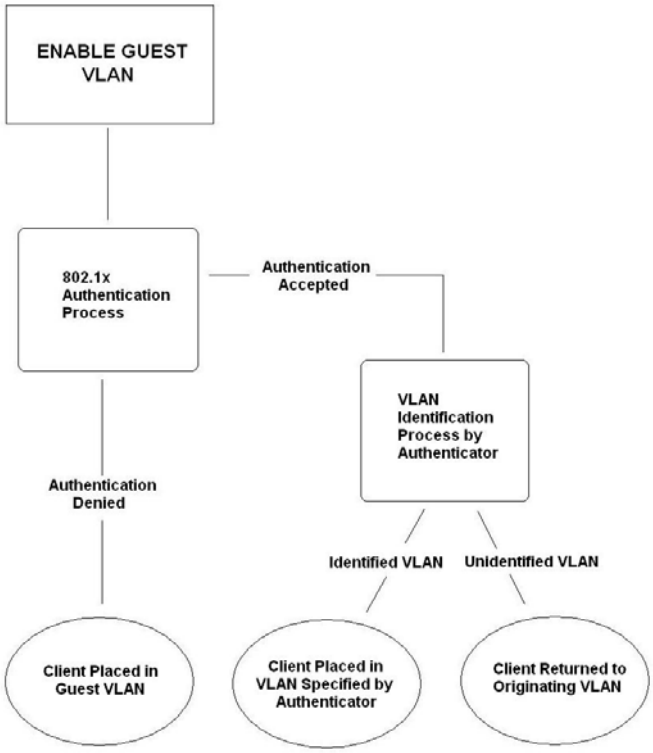


Figure 9- 27. Guest VLAN Authentication Process

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.
5. If a port is a member of multiple VLANs, it cannot become a member of the Guest VLAN.

Guest VLAN Configuration

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

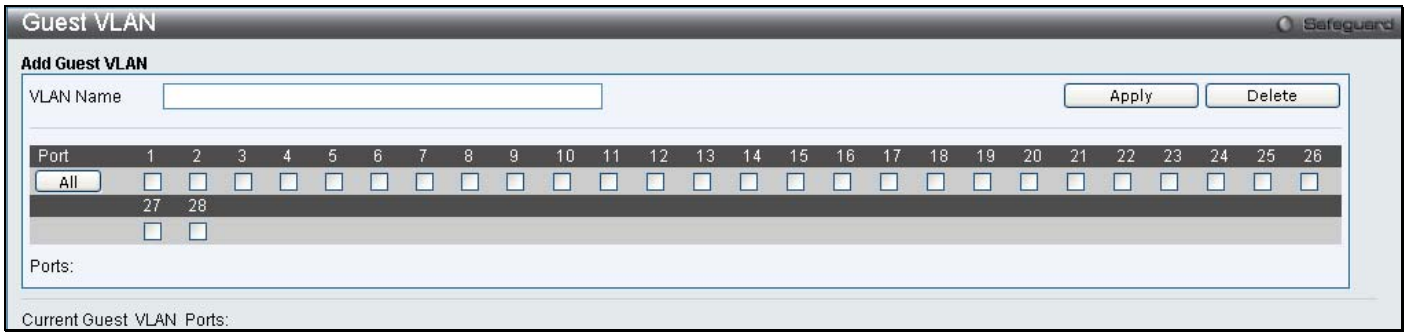


Figure 9- 28. Guest VLAN window

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

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as an 802.1x Guest VLAN.
Port List	Set the port list of ports to be enabled for the 802.1x Guest VLAN using the pull down menus.

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**:

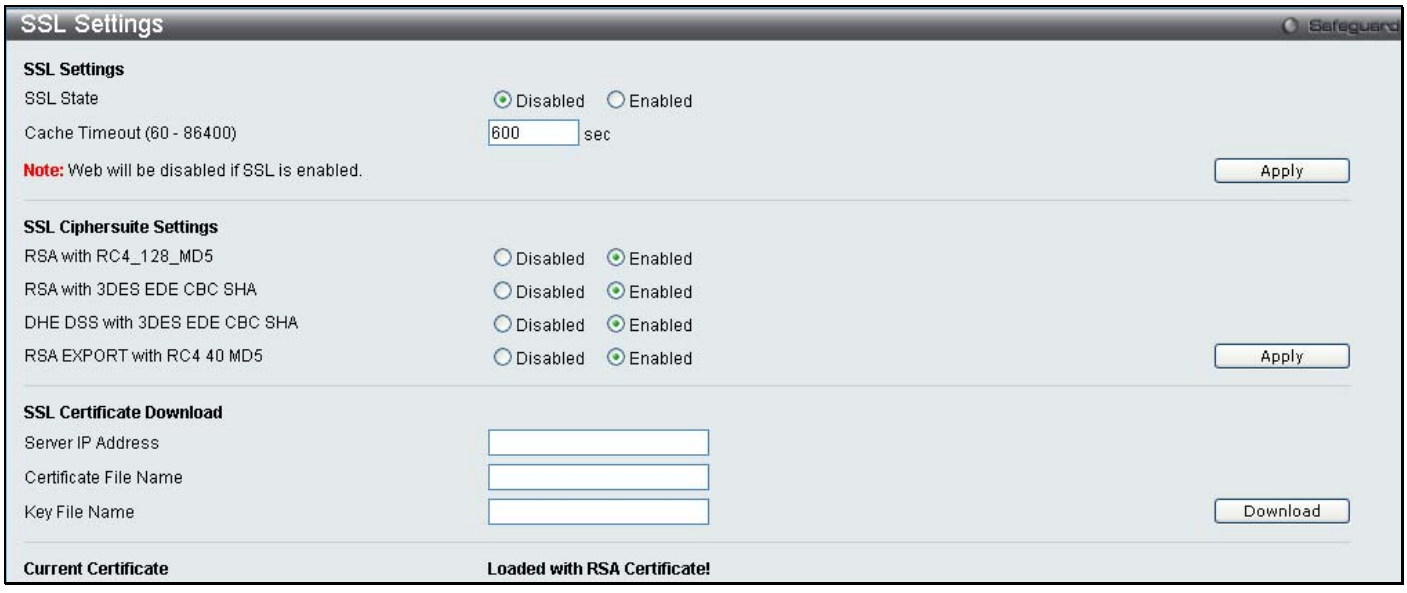


Figure 9- 29. SSL Settings

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

Parameter	Description
SSL Settings	
SSL Status	Use the pull-down menu to enable or disable the SSL status on the switch. The default is disabled.

Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.
SSL Ciphersuite Settings	
RSA with RC4_128_MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
DHE DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
SSL Certificate Download	
Server IP	Enter the IP address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

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

SSH

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

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

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

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

SSH Settings

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

To view this screen click, **Security > SSH > SSH Settings**

Figure 9- 30. SSH Settings window

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

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

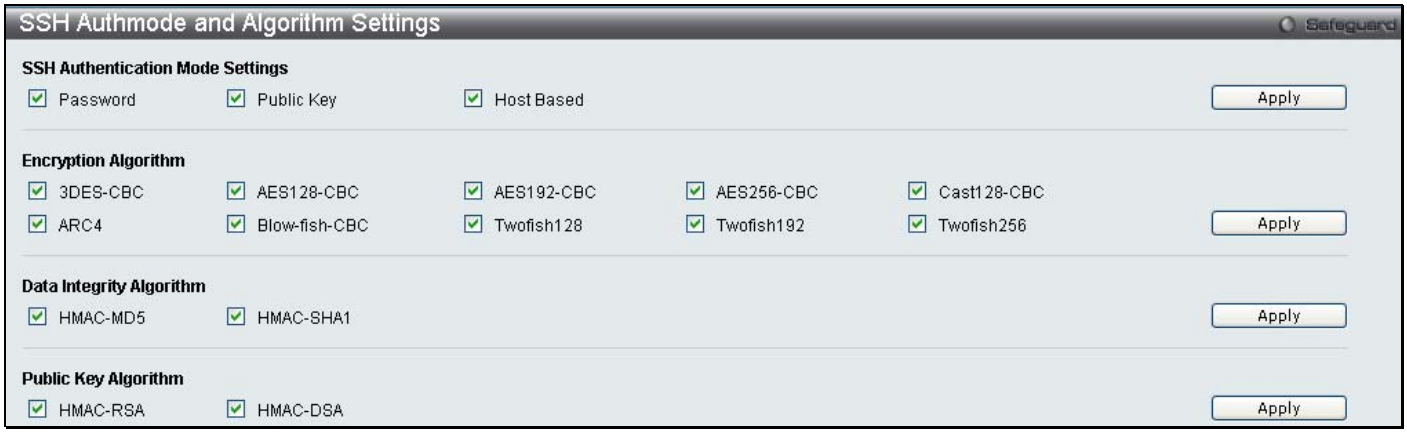


Figure 9- 31. SSH Authmode and Algorithm Settings window

The following algorithms may be set:

Parameter	Description
SSH Authentication Mode Settings	
Password	This parameter may be enabled if the administrator wishes to use a locally configured password for authentication on the Switch. The default is enabled.
Public Key	This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch. The default is enabled.
Host-based	This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. The default is enabled.
Encryption Algorithm	
3DES-CBC	Use the pull-down to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish CBC	Use the pull-down to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Use the pull-down to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.

Cast128-CBC	Use the pull-down to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Use the pull-down to enable or disable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Use the pull-down to enable or disable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Use the pull-down to enable or disable the twofish256 encryption algorithm. The default is enabled.
Data Integrity Algorithm	
HMAC-SHA1	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.
HMAC-MD5	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.
Public Key Algorithm	
HMAC-RSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. The default is enabled.

Click **Apply** to implement changes made.

SSH User Authentication Lists

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

To access the following window, click **Security > SSH > SSH User Authentication Mode**.

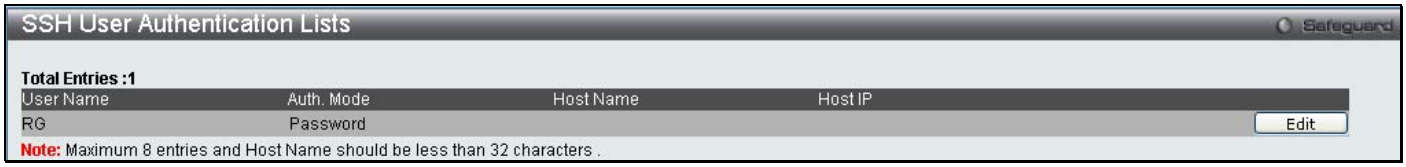


Figure 9- 32. SSH User Authentication Lists window

In the example aboveright, 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.

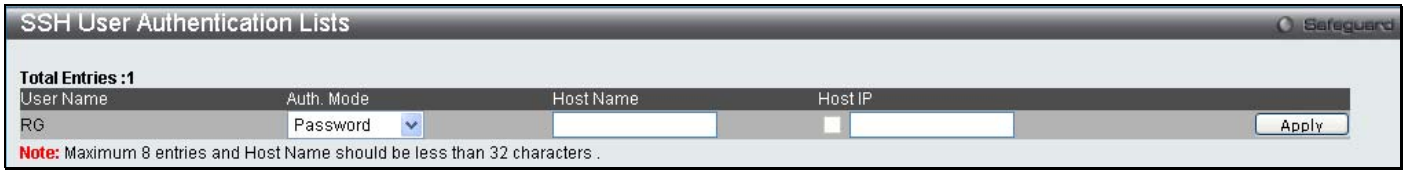


Figure 9- 33. SSH User Authentication Lists - Edit window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Auth. Mode	The administrator may choose one of the following to set the authorization for users attempting to access the Switch. *Host Based* – This parameter should be chosen if the administrator wishes to use a remote

	SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *Host Name* – Enter an alphanumeric string of no more than 31 characters to identify the remote SSH user. *Host IP* – Enter the corresponding IP address of the SSH user. *Password* – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation. *Public Key* – This parameter should be chosen if the administrator wishes to use the publickey on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.

Click **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 logins to the device successfully through [0]TACACS/XTACACS/TACACS+server or none method, the “user” priviledge level is the only level assigned. If the user wants to get the administration privilege level, the user must use the “enable admin” command to promote his privilege level. However when the user logins to the device successfully through the RADIUS server or through the local method, 3 kinds of privilege levels can be assigned to the user and the user can not use the “enable admin” command to promote to the admin privilege level.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Authentication Policy Settings

This 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 access the following window, click **Security > Access Authentication Control > Authentication Policy Settings**:

Figure 9- 34. Authentication Policy Settings window

The following parameters can be set:

Parameters	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

Click **Apply** to implement changes made.

Application Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (Enable Admin**)** utilizing a previously configured method list.

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

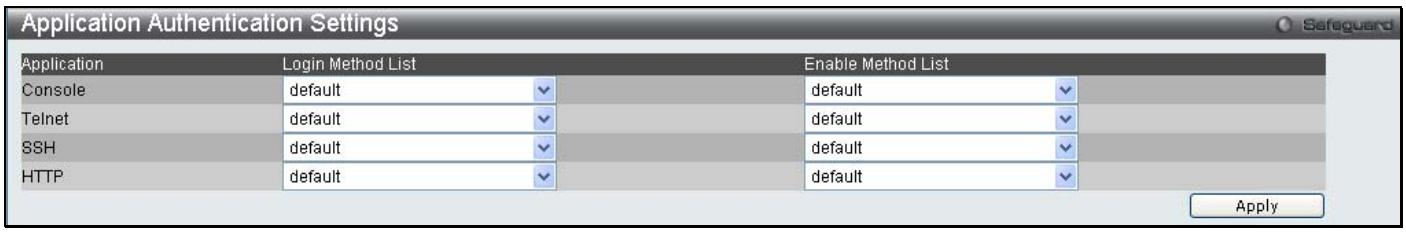


Figure 9- 35 Application's Authentication Settings window

The following parameters can be set:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH, and the WEB (HTTP) application.

Login Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Login Method Lists** window, in this section, for more information.
Enable Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Enable Method Lists** window, in this section, for more information

Click **Apply** to implement changes made.

Authentication Server Group

This window will allow users to set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentications server hosts may be added to any particular group.

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

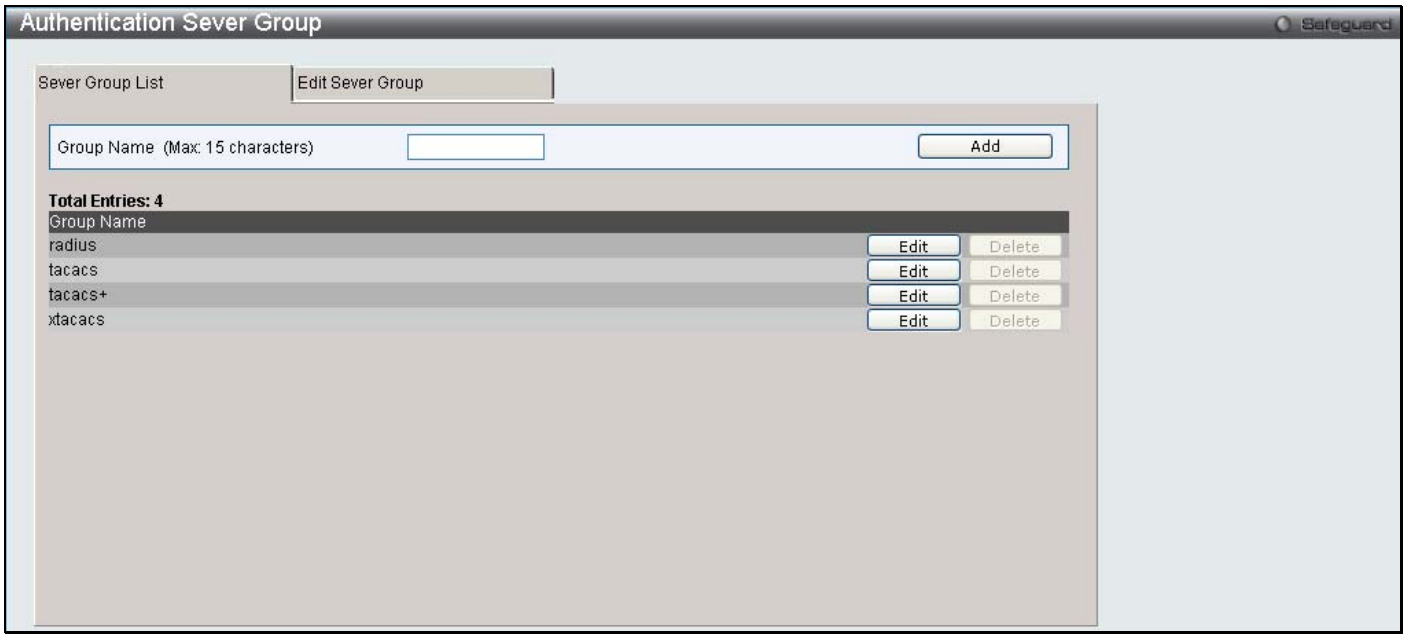


Figure 9- 36. Authentication Server Group Settings window

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.

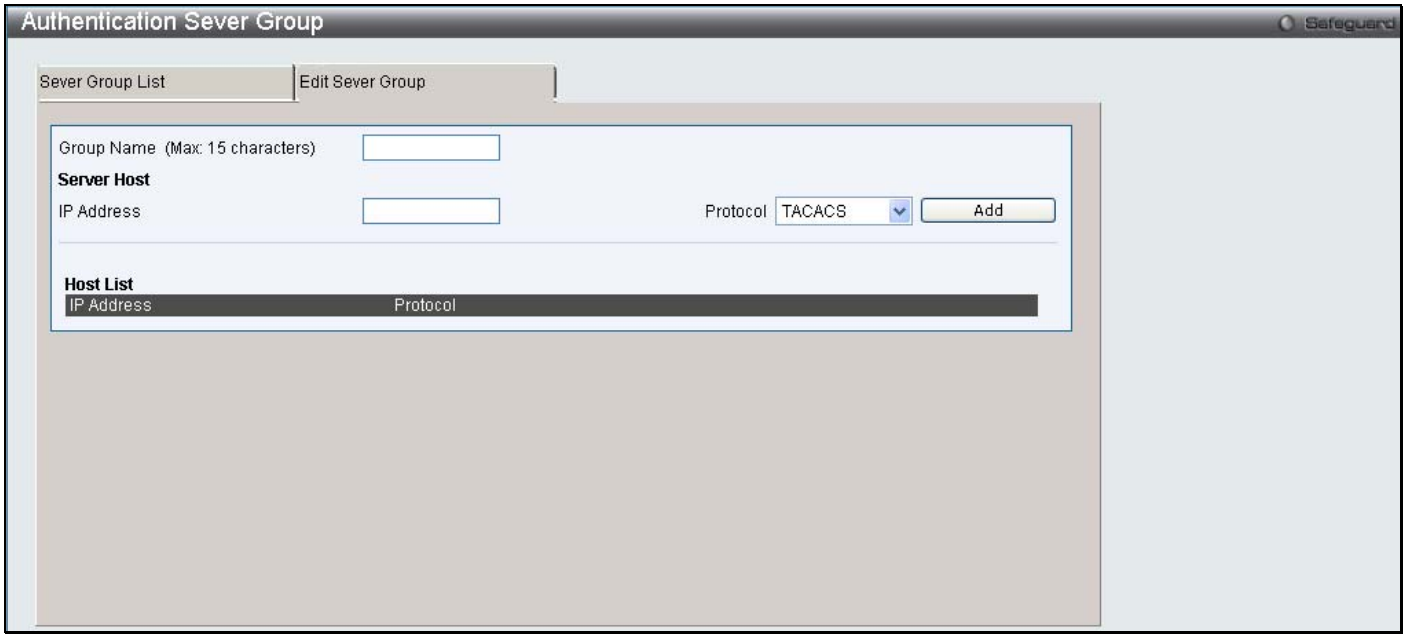


Figure 9- 37. Authentication Server Group Settings Edit window

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

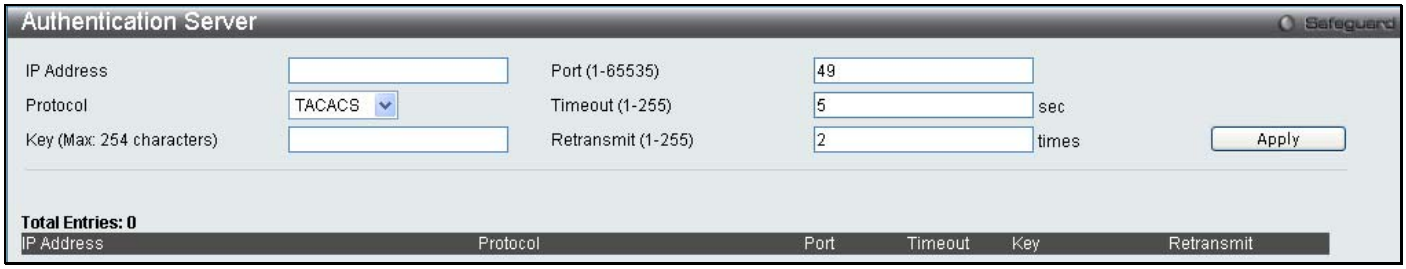


Figure 9- 38. Authentication Server Settings window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host the user wishes to add.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Protocol	The protocol used by the server host. The user may choose one of the following: *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS 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.

[0]When the user logins to the device successfully through [0]TACACS/XTACACS/TACACS+server or none method, the “user” privilege level is assigned only. If the user wants to get admin privilege level, the user must use the **Enable Admin** window to promote his privilege level. (See the Enable Admin part of this section for more detailed information.) But when the user logins to the device successfully through RADIUS server or local method, 3 kinds of privilege levels can be assigned to the user and the user can not use the **Enable Admin** window to promote to admin privilege level.

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

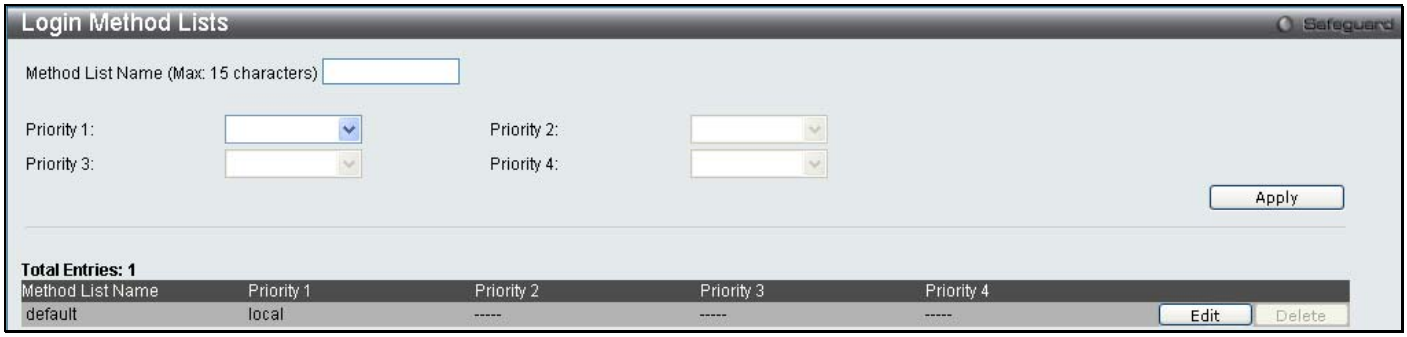


Figure 9- 39. Login Method Lists window

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 corressponding **Delete** button. To modify a Login Method List, click on its corresponding **Edit** button.

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

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *server_group* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. *none* - Adding this parameter will require no authentication to access the Switch.

Enable Method Lists

The **Enable Method List Settings** window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.

NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following table, click **Security > Access Authentication Control > Enable Method Lists**:

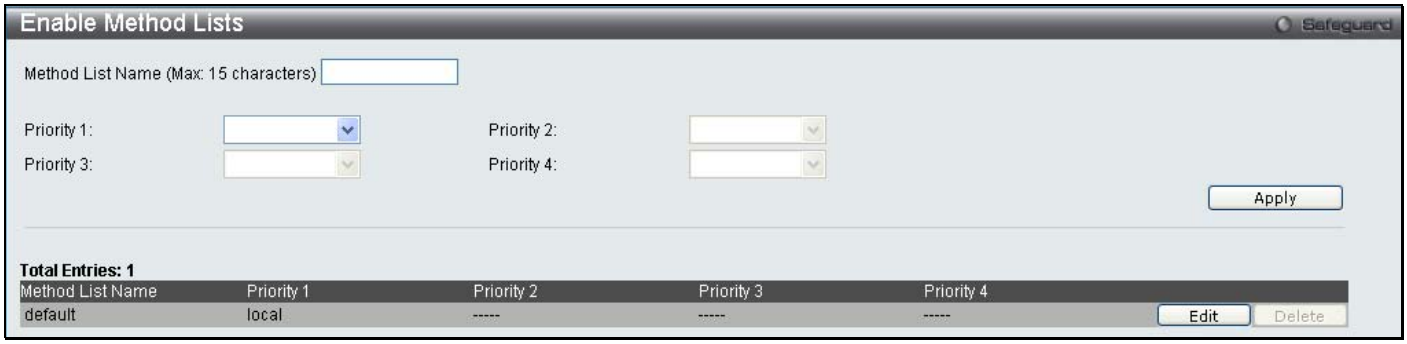


Figure 9- 40. Enable Method List window

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

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

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *local_enable* - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The user in the next section entitled Local Enable Password must set the local enable password. *none* - Adding this parameter will require no authentication to access the Switch. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. server_group - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.

Local Enable Password Settings

This window will configure the locally enabled password for the Enable Admin command. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security > Access Authentication Control > Local Enable Password Settings**:

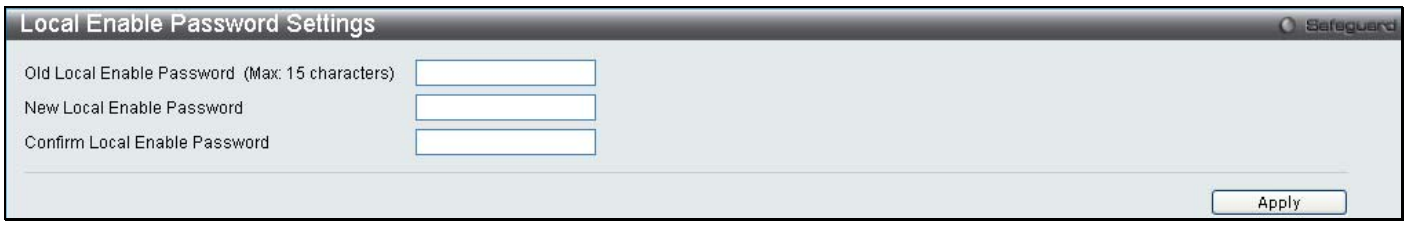


Figure 9- 41. Configure Local Enable Password window

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

Parameter	Description
Old Local Enable Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

RADIUS Accounting Services

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 Authentic
- 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 enable the RADIUS Accounting Settings on the switch, click **Security > Access Authentication Control > RADIUS Accounting Settings**

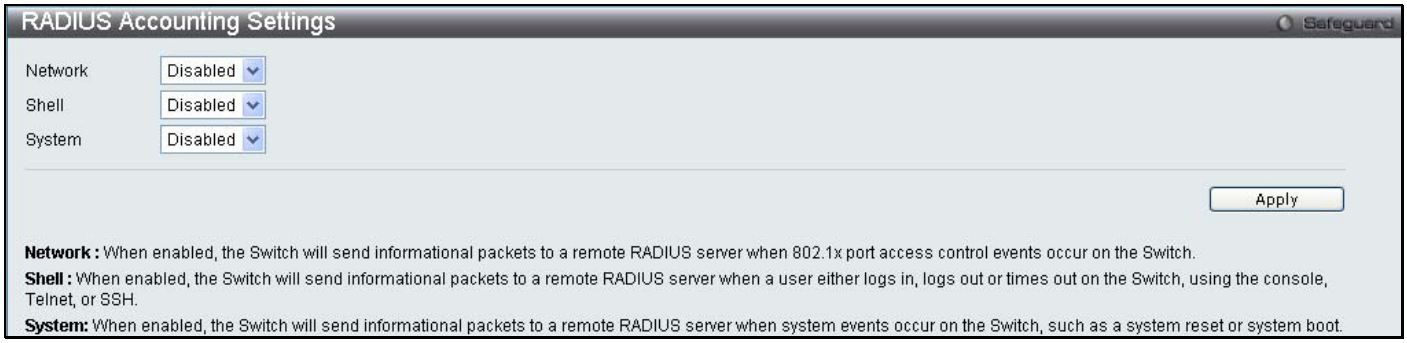


Figure 9- 42. RADIUS Accounting Setting

MAC-Based Access Control

The MAC-Based Access Control feature will allow users to configure a list of MAC addresses, either locally or on a remote RADIUS server, to be authenticated by the Switch and given access rights based on the configurations set on the Switch of the target VLAN where these authenticated users are placed.

The Switch will learn MAC addresses of a device through the receipt of ARP packets or DHCP packets and then attempt to match them on the authenticating list. If the client has not been configured for DHCP or does not have an IP configuration in static mode, then MAC addresses cannot be discovered and the client will not be authenticated. Ports and MAC addresses awaiting authentication are placed in the Guest VLAN where the Switch administrator can assign limited rights and privileges.

For local authentication on the Switch, the user must enter a list of MAC addresses to be accepted through this mechanism using the MAC-Based Access Control Local Database Settings window, as seen below. The user may enter up to 1024 MAC addresses locally on the Switch but only sixteen MAC addresses can be accepted per physical MAC-Based Access Control enabled port. Once a MAC addresses has been authenticated by the Switch on the local side, the port where that MAC address resides will be placed in the previously configured target VLAN, where the rights and privileges are set by the switch administrator. If the VLAN Name for the target VLAN is not found by the Switch, the Switch will return the port containing that MAC address to the originating VLAN. If the MAC address is not found and the port is in the Guest VLAN, it will remain in the Guest VLAN, with the associated rights. If the port is not in the guest VLAN, this MAC address will be blocked by the Switch.

For remote RADIUS server authentication, the user must first configure the RADIUS server with a list of MAC addresses and relative target VLANs that are to be authenticated on the Switch. Once a MAC address has been discovered by the Switch through ARP or DHCP packets, the Switch will then query the remote RADIUS server with this potential MAC address, using a RADIUS Access Request packet. If a match is made with this MAC address, the RADIUS server will return a notification stating that the MAC address has been accepted and is to be placed in the target VLAN. If the VID for the target VLAN is not found, the Switch will return the port containing the MAC address to the original VLAN. If the MAC address is not found, and if the port is in the Guest VLAN, it will remain in the Guest VLAN, with the associated rights. If the port is not in the guest VLAN, this MAC address will be blocked by the Switch.

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. MAC-Based Access Control is its own entity and is not dependant on other authentication functions on the Switch, such as 802.1X, Web-Based authentication etc…
4. 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.
5. 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 enable the MAC Based Access Control Global Settings on the switch, click **Security > MAC Based Access Control > MAC Based Access Control Settings**

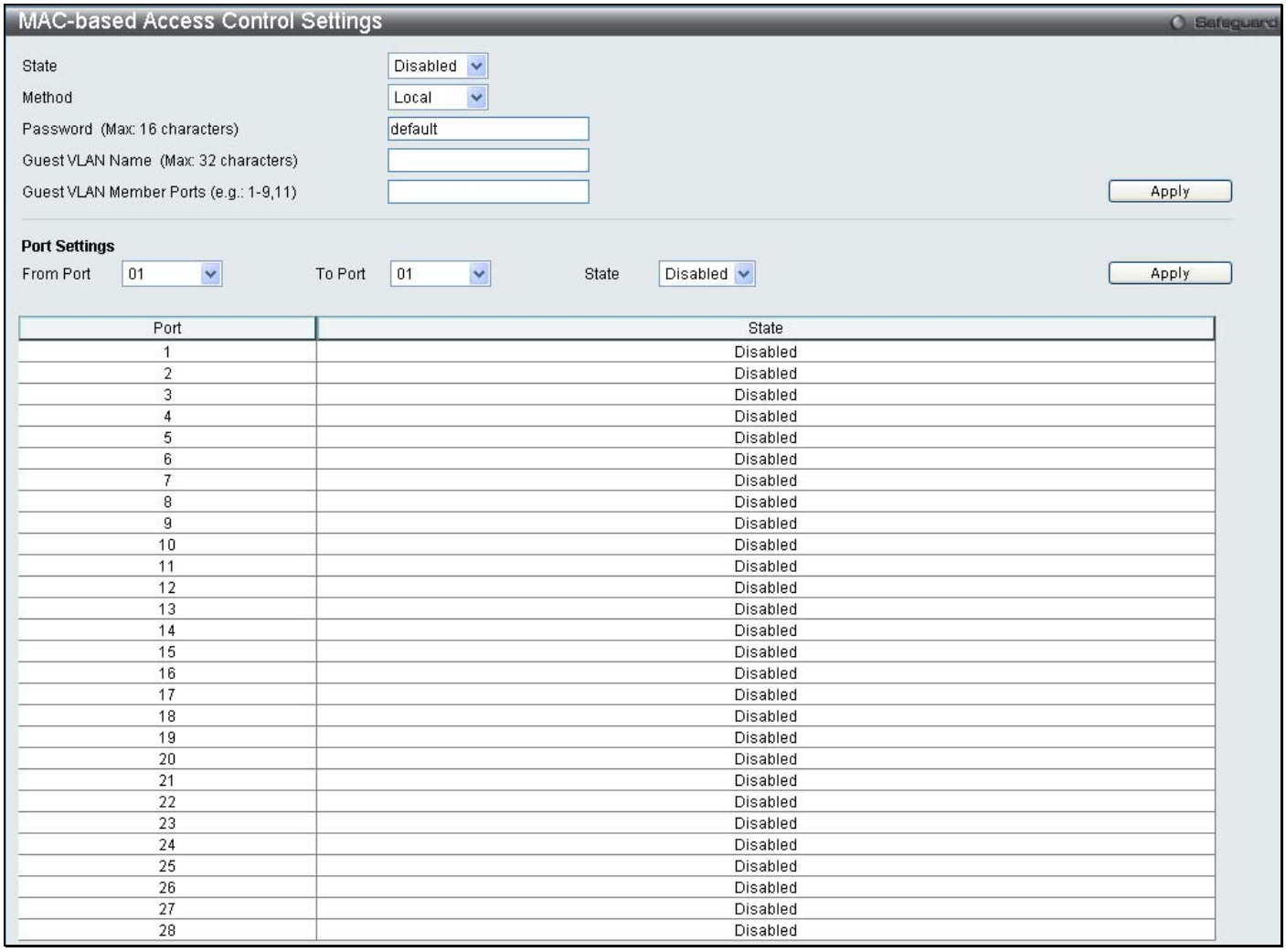


Figure 9- 43. MAC Based Access Control Settings

The following parameters may be viewed or set:

Parameter	Description
Settings	
State	Use the pull-down menu to globally enable or disable the MAC-Based Access Control function on the Switch.
Method	Use the pull-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-Based Access Control. This MAC address list can be configured in the MAC-Based Access Control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-Based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
Guest VLAN	Displays the name of the previously configured Guest VLAN being used for this function. Clicking the hyperlinked name will send the web manager to Guest VLAN configuration screen for MAC-Based Authentication.

Guest VLAN Member Ports	Displays the list of ports that have been configured for the Guest VLAN.
Port Settings	
From Port/To Port	Enter the Port range.
State	Use the pull-down menu to enable or disable the MAC-Based Access Control function on individual ports.

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 1024 MAC addresses to be authenticated using the local method configured here. To enable the MAC Based Access Control Local MAC Settings on the switch, click **Security > MAC Based Access Control > MAC Based Access Control Local Settings**

Figure 9- 44. 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**.

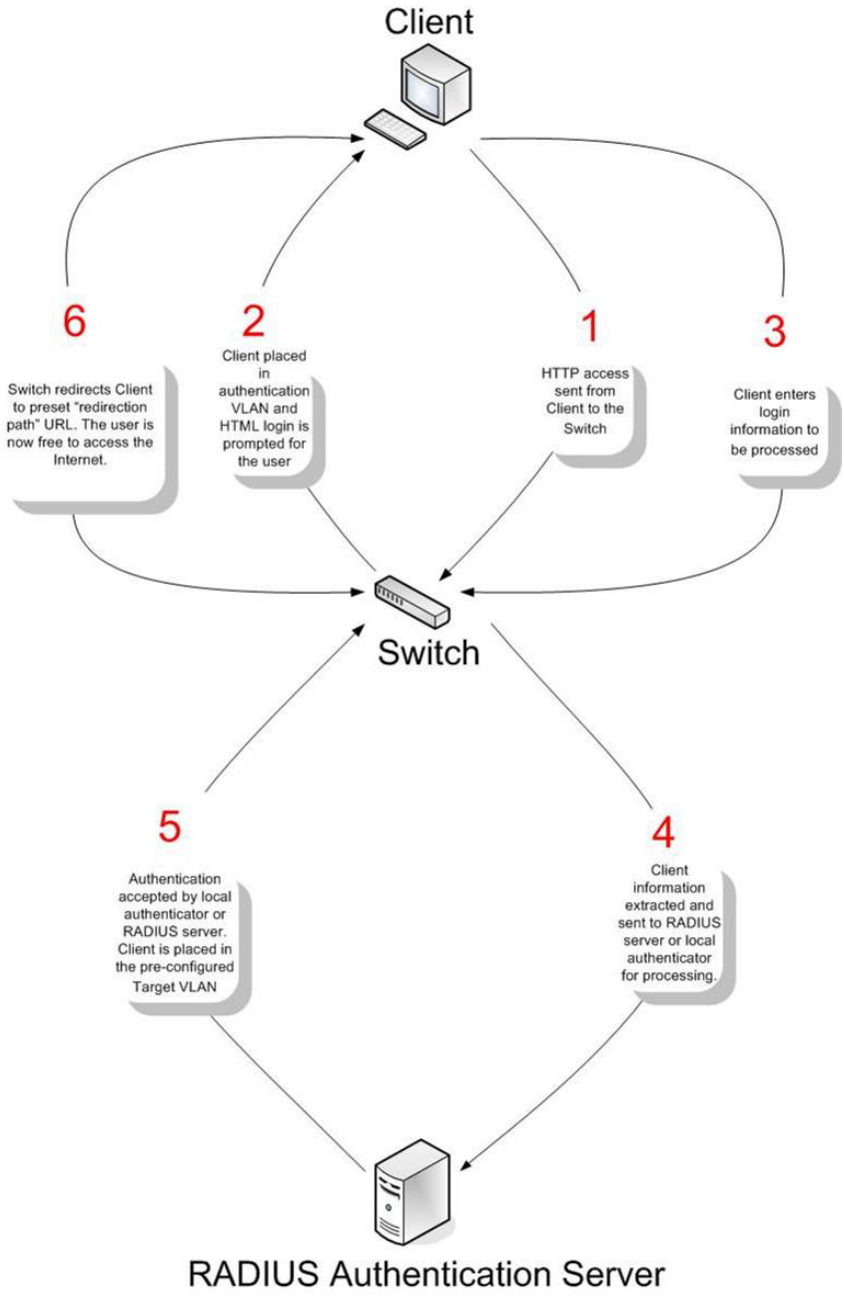
Web Authentication

Web-based Access Control is another port based access control method implemented similarily 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.

To the right there 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

To configure the Switch for Web Authentication Settings, open the **Security** > **Web Authenication** > **Web-based Access Control Settings**

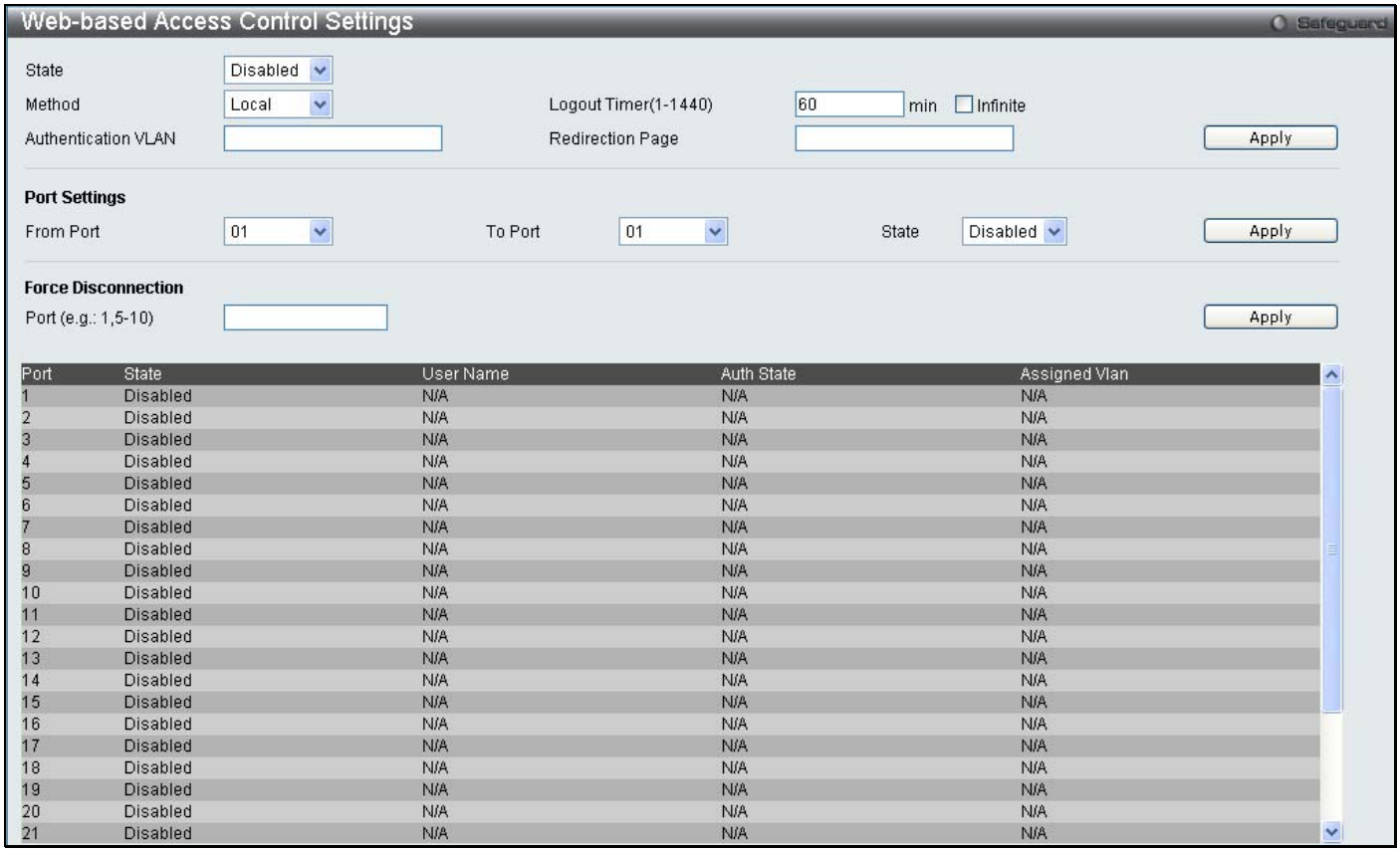


Figure 9- 45. Web-based Access Control Settings

To set the Web-based Access Control for the Switch, complete the following fields:

Parameter	Description
State	Toggle the State field to either *Enable* or *Disable* for the Web-based Access Control settings of the Switch.
Method	Use the pull-down menu to choose the authenticator for Web-based Access Control. The user may choose: *local* – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch configured using the User Account Creation screen seen below. *radius* – Choose this parameter to use a remote RADIUS server as the authenticating method for users trying to access the network via the switch. This RADIUS server must have already been pre-assigned by the administrator using the RADIUS Server window located in the 802.1x section.
Logout Timer (1-1440)	The logout time in displayed in minutes, enter a value between *1* and *1440*.
VLAN	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

	RADIUS server. This VLAN should be pre-configured to have limited access rights to web based authenticated users.
Redirection Page	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.
Port List	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

To configure the Switch for Web Authentication Settings, open the **Security** > **Web Authenication** > **Web-based Access Control User Settings**

Figure 9- 46. Web-based Access Control User Settings window

Parameter	Description
Create User	
User Name	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 *local* as their web based authenticator.
Password	Enter the password the administrator has chosen for the selected user. This field is case sensitive and must be a complete alphanumeric string. This field is for administrators who

	have selected *local* as their web based authenticator.
Confirmation	Re-enter the password.
User-VLAN Mapping	
User Name	Enter the user name of a guest authenticated through this process, to be mapped to a previously configured VLAN with limited rights.
VLAN Name	Enter the VLAN name of a previously configured VLAN to which successfully authenticated web user will be mapped.

JWAC (Japanese Web-based Access Control)

The **JWAC** folder contains three windows: **JWAC Global Settings**, **JWAC Port Settings**, **JWAC User Settings.**

JWAC Global Settings

Use this window to enable and configure Japanese Web-based Access Control on the Switch. Please note that JWAC and Web Authentication are mutually exclusive functions. That is, they cannot be enabled at the same time. To use the JWAC feature, computer users need to pass through two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the Switch. For the second stage, the authentication is similar to Web Authentication, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.

To view this window, click **Security** > **JWAC** > **JWAC Global Settings**

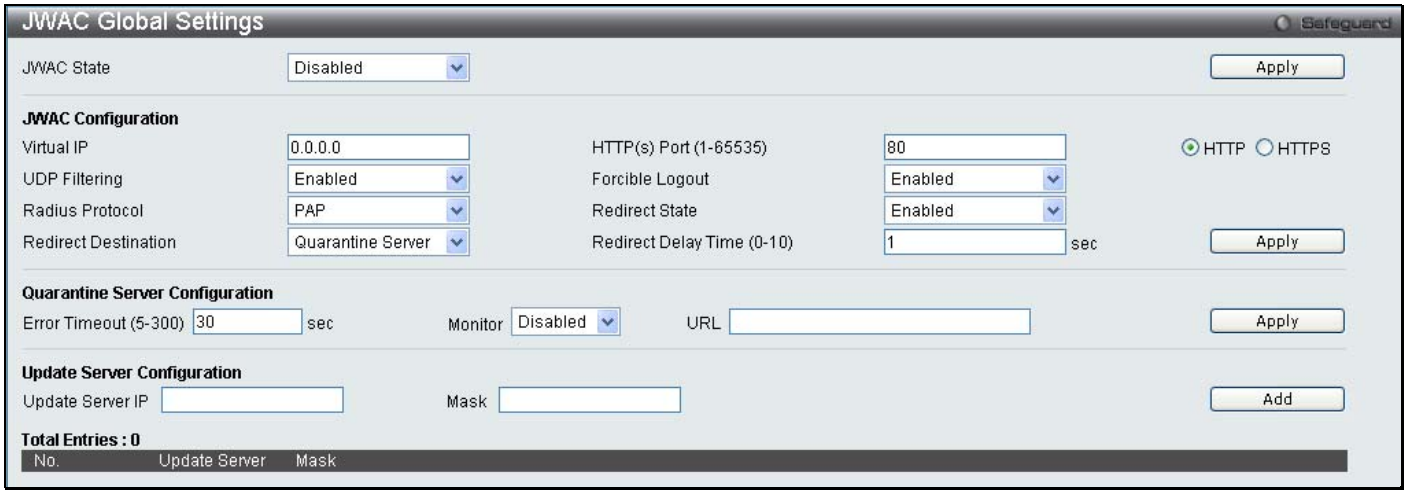


Figure 9- 47. JWAC Global Settings

To set the Web Authentication for the Switch, complete the following fields:

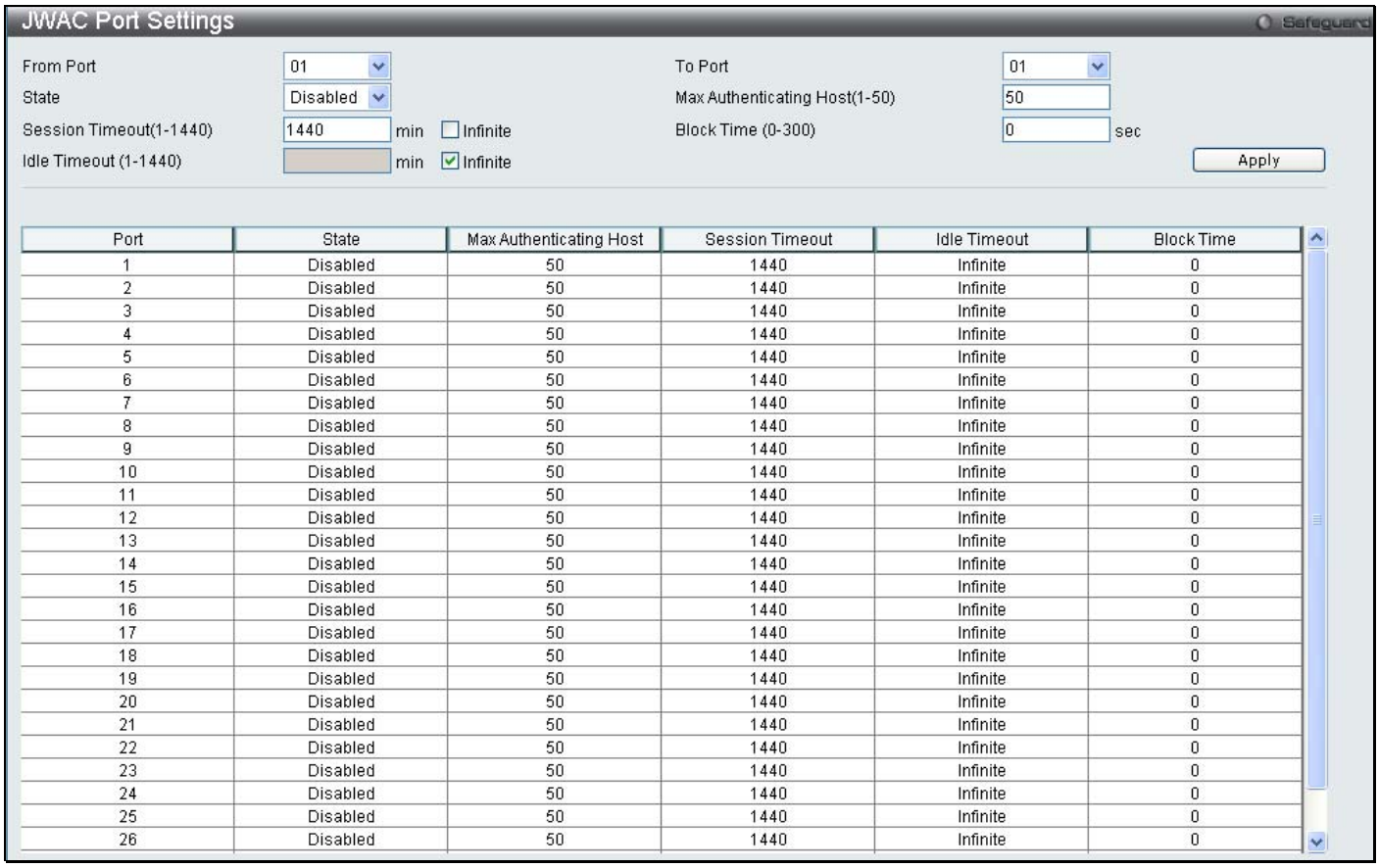
Parameter	Description
JWAC Settings	
JWAC State	Use this drop-down menu to either enable or disable JWAC on the Switch.
JWAC Configuration	
Virtual IP	This parameter specifies the JWAC Virtual IP address that is used to accept authentication requests from an unauthenticated host. Only requests sent to this IP will get a correct response. NOTE: This IP does not respond to ARP requests or ICMP packets.

HTTPs Ports (1-65535)	This parameter specifies the TCP port that the JWAC Switch listens to and uses to finish the authentication process.
UDP Filtering	This parameter enables or disables JWAC UDP Filtering. When UDP Filtering is *Enabled*, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped
Forcible Logout	This parameter enables or disables JWAC Forcible Logout. When Forcible Logout is *Enabled*, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will move back to the unauthenticated state.
RADIUS Protocol	This parameter specifies the RADIUS protocol used by JWAC to complete a RADIUS authentication. The options include *Local*, *EAP MD5*, *PAP*, *CHAP*, *MS CHAP*, and *MS CHAPv2*.
Redirect State	This parameter enables or disables JWAC Redirect. When the redirect quarantine server is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When the redirect JWAC login page is enabled, the unauthenticated host will be redirected to the JWAC login page in the Switch to finish authentication. When redirect is disabled, only access to the quarantine server and the JWAC login page from the unauthenticated host are allowed, all other web access will be denied. NOTE: When enabling redirect to the quarantine server, a quarantine server must be configured first.
Redirect Destination	This parameter specifies the destination before an unauthenticated host is redirected to either the *Quarantine Server* or the *JWAC Login Page*.
Redirect Delay Time (0-10)	This parameter specifies the Delay Time before an unauthenticated host is redirected to the Quarantine Server or JWAC Login Page. Enter a value between *0* and *10* seconds. A value of *0* indicates no delay in the redirect.
Quarantine Server Configuration	
Error Timeout (5-300)	This parameter is used to set the Quarantine Server Error Timeout. When the Quarantine Server Monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from the Quarantine Server during the configured Error Timeout, the Switch then regards it as not working properly. Enter a value between *5* and *300* seconds.
Monitor	This parameter enables or disables the JWAC Quarantine Server Monitor. When *Enabled*, the JWAC Switch will monitor the Quarantine Server to ensure the server is okay. If the Switch detects no Quarantine Server, it will redirect all unauthenticated HTTP access attempts to the JWAC Login Page forcibly if the Redirect is enabled and the Redirect Destination is configured to be a Quarantine Server.
Quarantine Server URL	This parameter specifies the JWAC Quarantine Server URL. If the Redirect is enabled and the Redirect Destination is the Quarantine Server, when an unauthenticated host sends the HTTP request packets to a random Web server, the Switch will handle this HTTP packet and send back a message to the host to allow it access to the Quarantine Server with the configured URL. When a computer is connected to the specified URL, the quarantine server will request the computer user to input the user name and password to complete the authentication process.
Update Server Configuration	
Update Server IP	This parameter specifies the Update Server IP address.
Mask	This parameter specifies the Server IP net mask.

Click **Apply** to implement changes made.

JWAC Port Settings

To view JWAC port settings for the Switch, click **Security** > **JWAC** > **JWAC Port Settings**.



Port	State	Max Authenticating Host	Session Timeout	Idle Timeout	Block Time
1	Disabled	50	1440	Infinite	0
2	Disabled	50	1440	Infinite	0
3	Disabled	50	1440	Infinite	0
4	Disabled	50	1440	Infinite	0
5	Disabled	50	1440	Infinite	0
6	Disabled	50	1440	Infinite	0
7	Disabled	50	1440	Infinite	0
8	Disabled	50	1440	Infinite	0
9	Disabled	50	1440	Infinite	0
10	Disabled	50	1440	Infinite	0
11	Disabled	50	1440	Infinite	0
12	Disabled	50	1440	Infinite	0
13	Disabled	50	1440	Infinite	0
14	Disabled	50	1440	Infinite	0
15	Disabled	50	1440	Infinite	0
16	Disabled	50	1440	Infinite	0
17	Disabled	50	1440	Infinite	0
18	Disabled	50	1440	Infinite	0
19	Disabled	50	1440	Infinite	0
20	Disabled	50	1440	Infinite	0
21	Disabled	50	1440	Infinite	0
22	Disabled	50	1440	Infinite	0
23	Disabled	50	1440	Infinite	0
24	Disabled	50	1440	Infinite	0
25	Disabled	50	1440	Infinite	0
26	Disabled	50	1440	Infinite	0

Figure 9- 48. JWAC Port Settings window

To set the JWAC on individual ports for the Switch, complete the following fields:

Parameter	Description
From Port / To Port	Lists the range of Ports that will be configured in this window.
Aging Time (1-1440 Minutes)	This parameter specifies the period of time a host will keep in authenticated state after it successes to authenticate. Enter a value between *1* and *1440* minutes. The default setting is *1440* minutes. To maintain a constant Port Configuration tick the Infinite check box in the JWAC configuration window.
MAX Authenticating Host	This parameter specifies the maximum number of host process authentication attempts allowed on each port at the same time.
Idle Time (1-1440 Minutes)	This parameter specifies the period of time during which there is no traffic for an authenticated host and the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. A value of Infinite indicates the Idle state of the authenticated host on the port will never be checked. The default setting is Infinite.
Block Time (0-300 Seconds)	This parameter specifies the period of time a host will keep in a blocked state after it fails to authenticate. Enter a value between *0* and *300* seconds. The default setting is *0* seconds.
State	This parameter specifies the state of the configured ports.

Click **Apply** to implement changes made.

JWAC User Account

To view JWAC user settings for the Switch, go to the **Security** > **JWAC** > **JWAC User Account**

Figure 9- 49. JWAC User Settings window

Parameter	Description
User Name	Enter a username of up to 15 alphanumeric characters.
Password	Enter the password of the user. This field is case-sensitive and must be a complete alphanumeric string.
Confirm Password	Retype the password entered in the previous field.
VID (1-4094)	Enter a VLAN ID up to 4094.

Click **Apply** to implement changes made.

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

To view NetBIOS Settings on the Switch, go to the **Security** > **NetBIOS Filtering Settings**

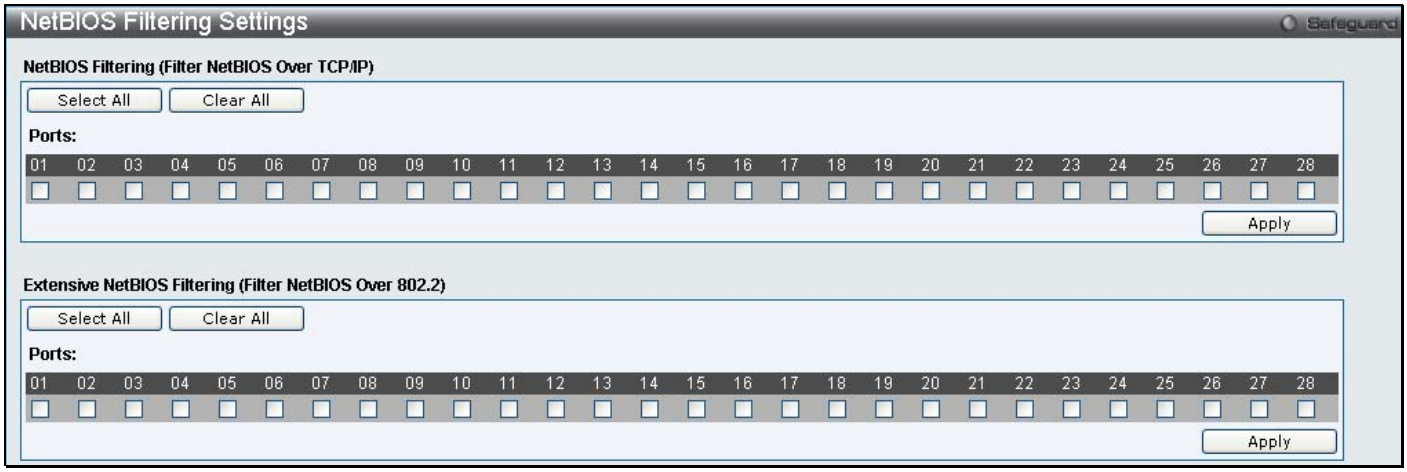


Figure 9- 50. NetBIOS Filtering Settings window

Section 10

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 6 access profiles. The rules used to define the access profiles are limited to a total of 768 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**

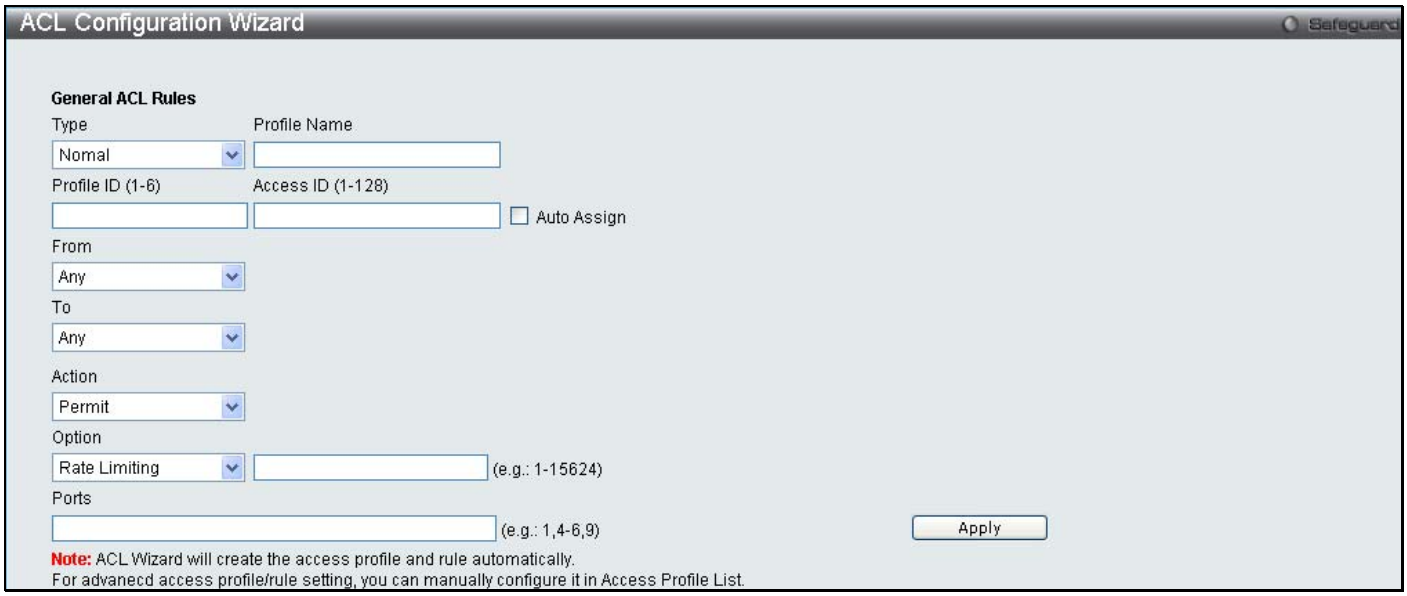


Figure 10- 1. ACL Configuration Wizard

The following parameters can be configured.

Parameter	Description
Type	Select the type of ACL you wish to create, either normal or CPU.
Profile Name	Select a unique Profile Name for this profile set.
Profile ID (1-6)	Enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.

From	Use the drop-down menu to select from MAC Address, IPv4 Address or IPv6.
To	Use the drop-down menu to select from MAC Address, IPv4 Address or IPv6. When IPv6 is selected the user can only enter the IPv6 source address or the IPv6 destination address at any one time.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Option	Use the pull down menu to select an option, the user can choose between *Rate Limiting*, *Change 1P Priority*, *Replace DSCP* and *Replace ToS Precedence*.
Ports	Enter a range of ports to be configured.

Click **Apply** to implement changes made.

Access Profile List

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts. To display the currently configured Access Profiles on the Switch, open the **ACL** folder and click the **Access Profile Lists** link. This will open the **Access Profile Table** page, as shown below.

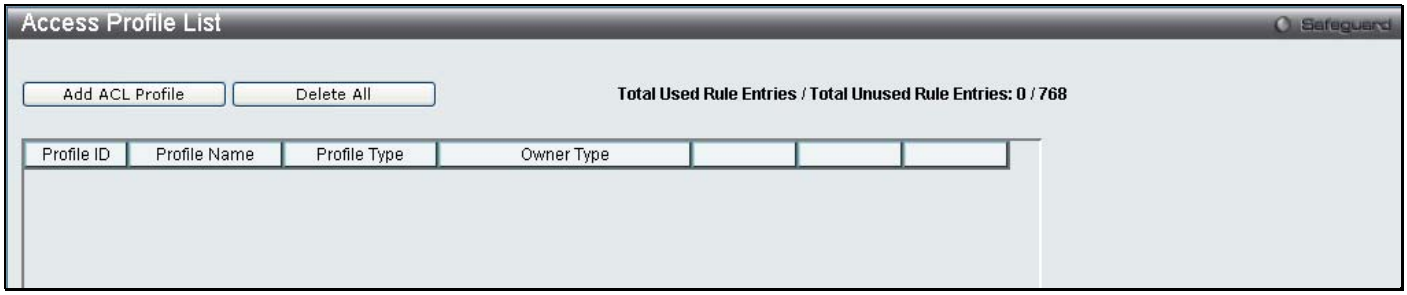


Figure 10- 2. Access Profile Lists

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 **Clear 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.

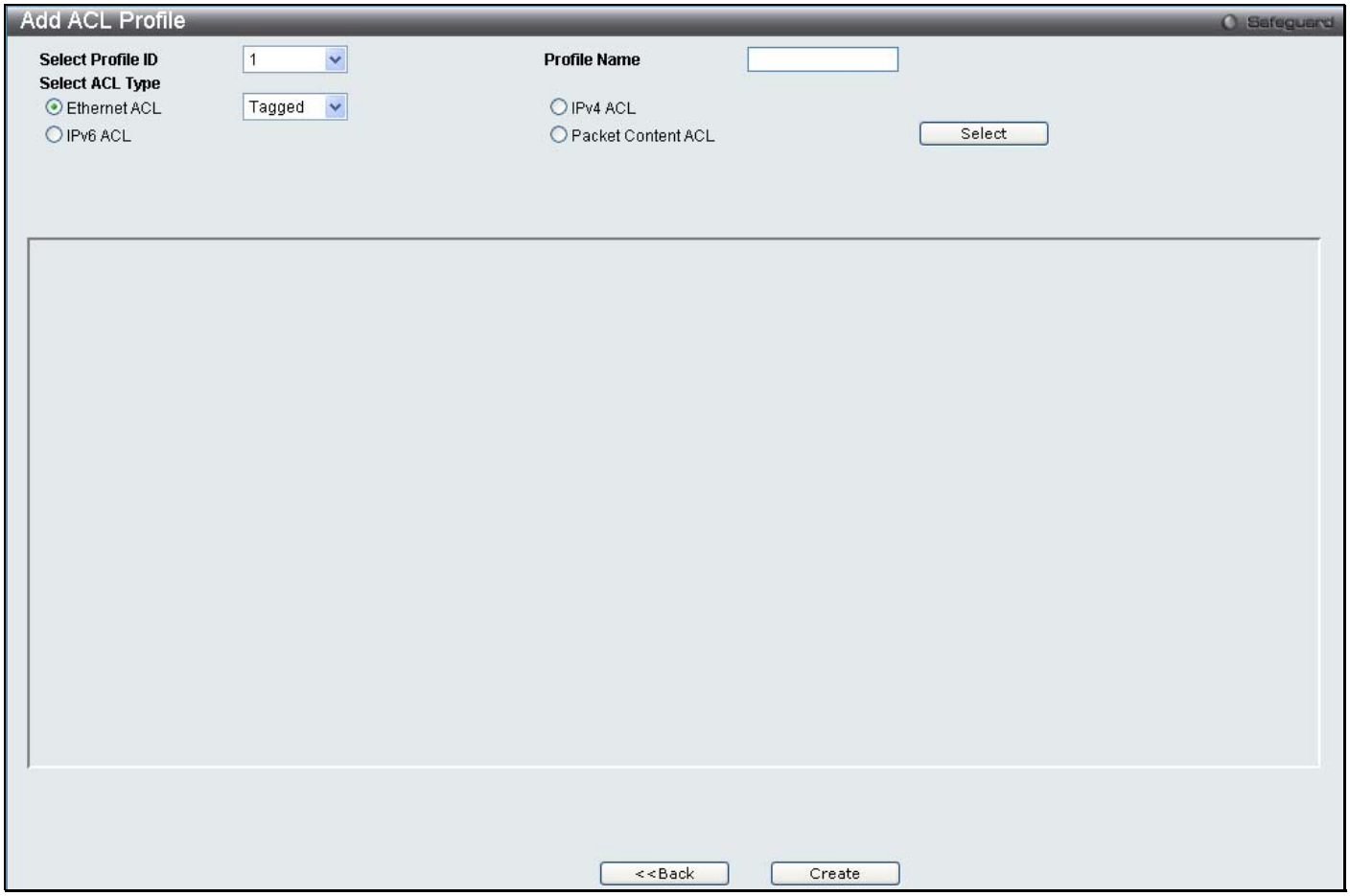


Figure 10- 3. Add Access Profile (Ethernet)

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

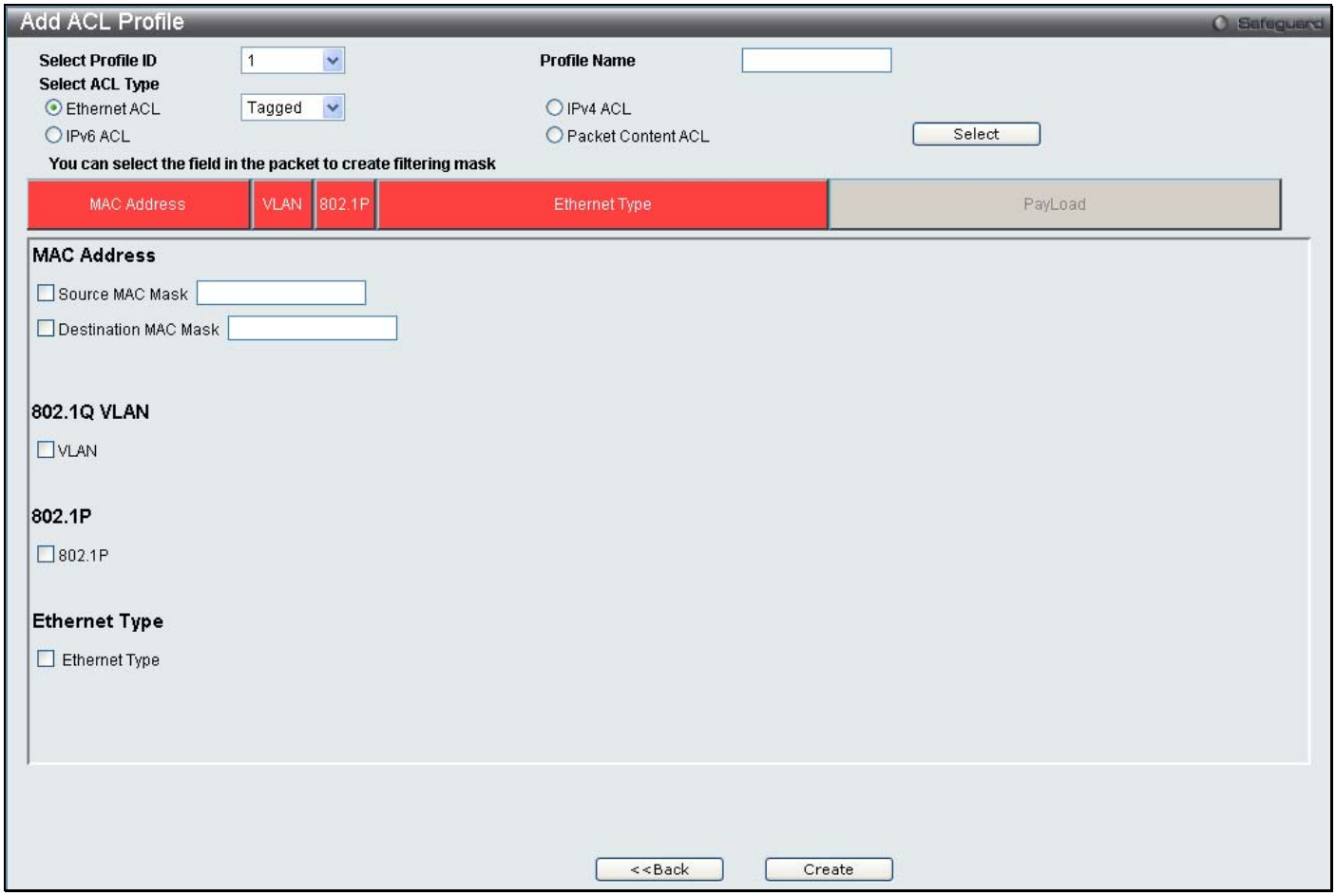


Figure 10- 4. Add Ethernet ACL Profile window

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
Ethernet ACL	To configure this profile select the Ethernet ACL, and use the drop down menu to choose between *tagged* or *untagged*.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
Select ACL Type	Select profile based on Ethernet (MAC Address), IP 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 hide the content of the packet header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.

802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

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

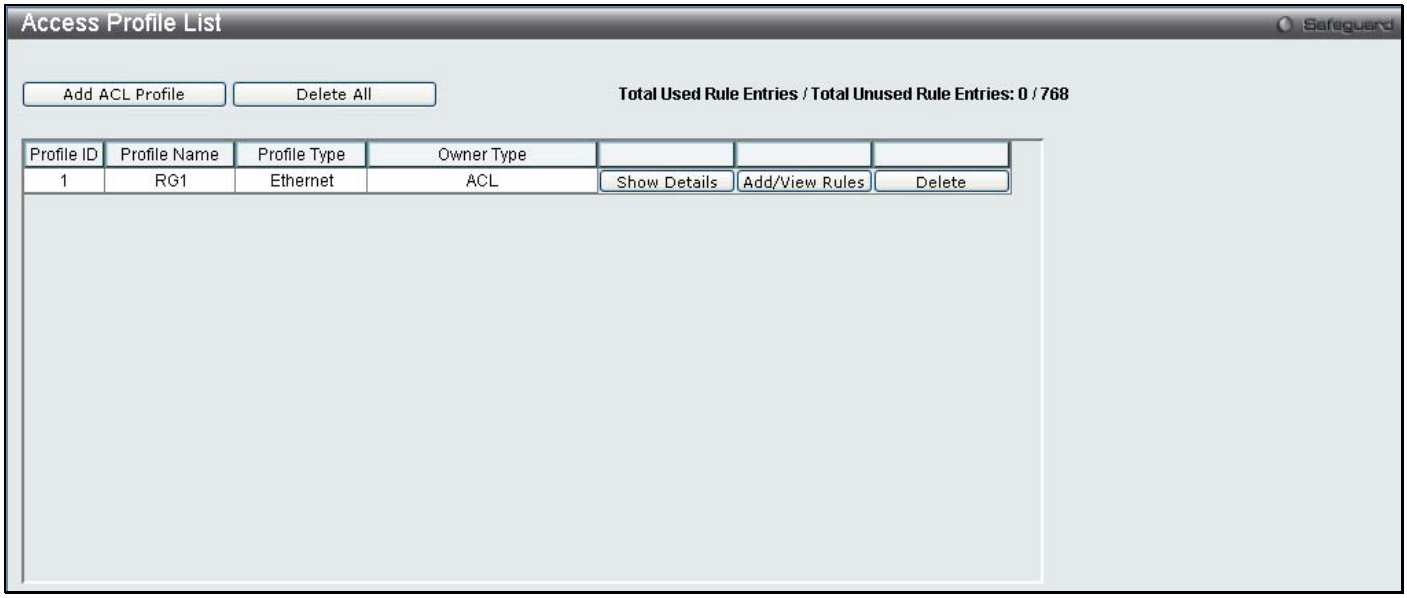


Figure 10- 5. Access Profile List (Ethernet)

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

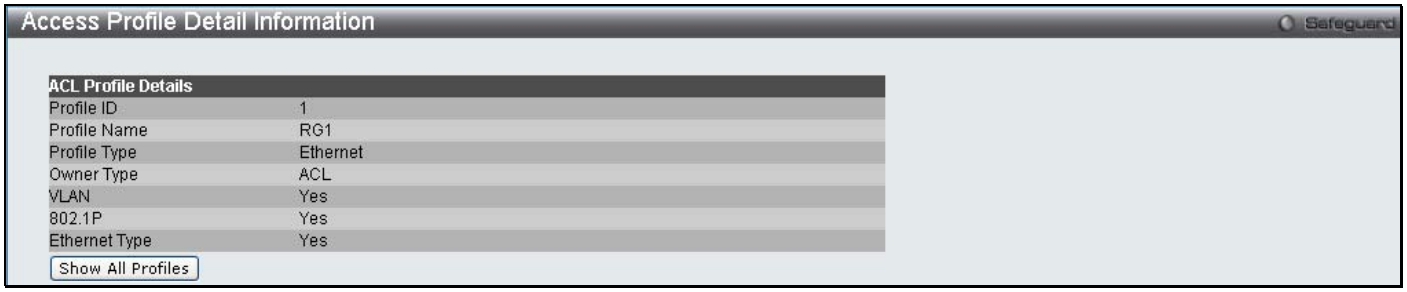


Figure 10- 6. Access Profile Details (Ethernet)

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.

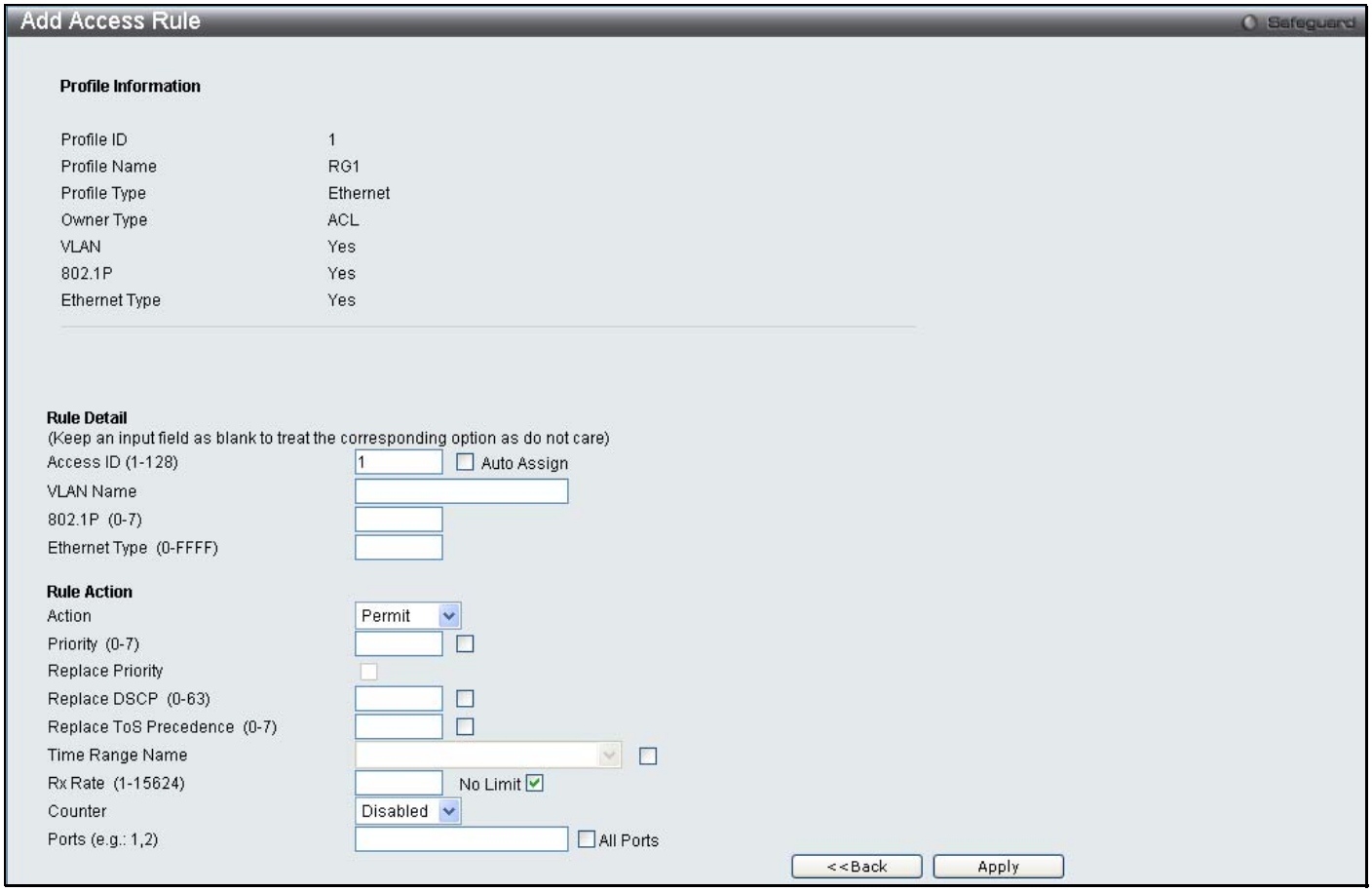


Figure 10- 7. Access Profile Ethernet

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

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Replace ToS	Select this option to instruct the Switch to replace the Type of Service as part of the packet

Precedence	header.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type (0-FFFF)	Specifies that the Switch will examine the Ethernet type value in each frame's header. Example: Ethernet type=0x0800 is IPv4 packets. Ethernet type=0x86DD is IPv6 packet.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Specifies whether counter feature will be enabled/disabled This is optional, the default is disabled. If the rule is not binded with flow_meter, then all packet matched will be countered. If the rule is binded with flow_meter, then "counter" here will be overrided.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.

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

Figure 10- 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.

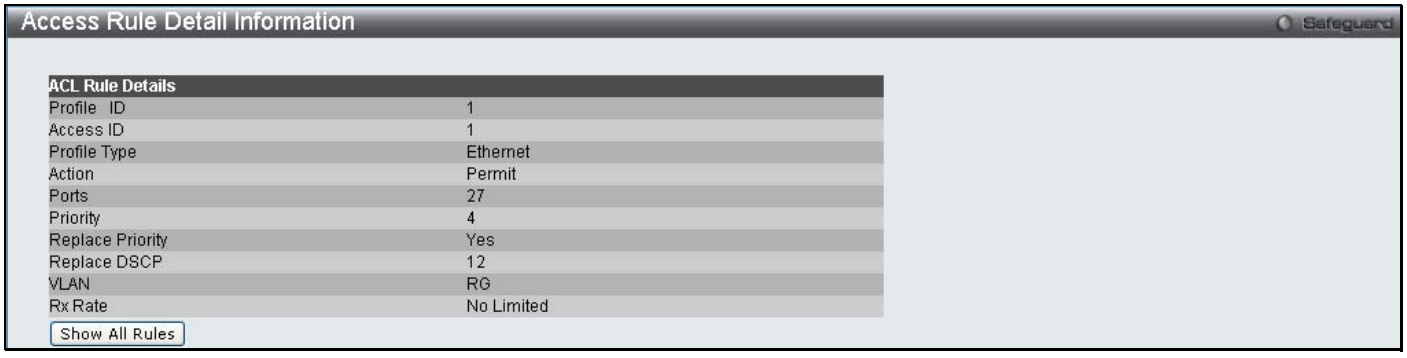


Figure 10- 9. Access Rule Detail Information (Ethernet)

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.

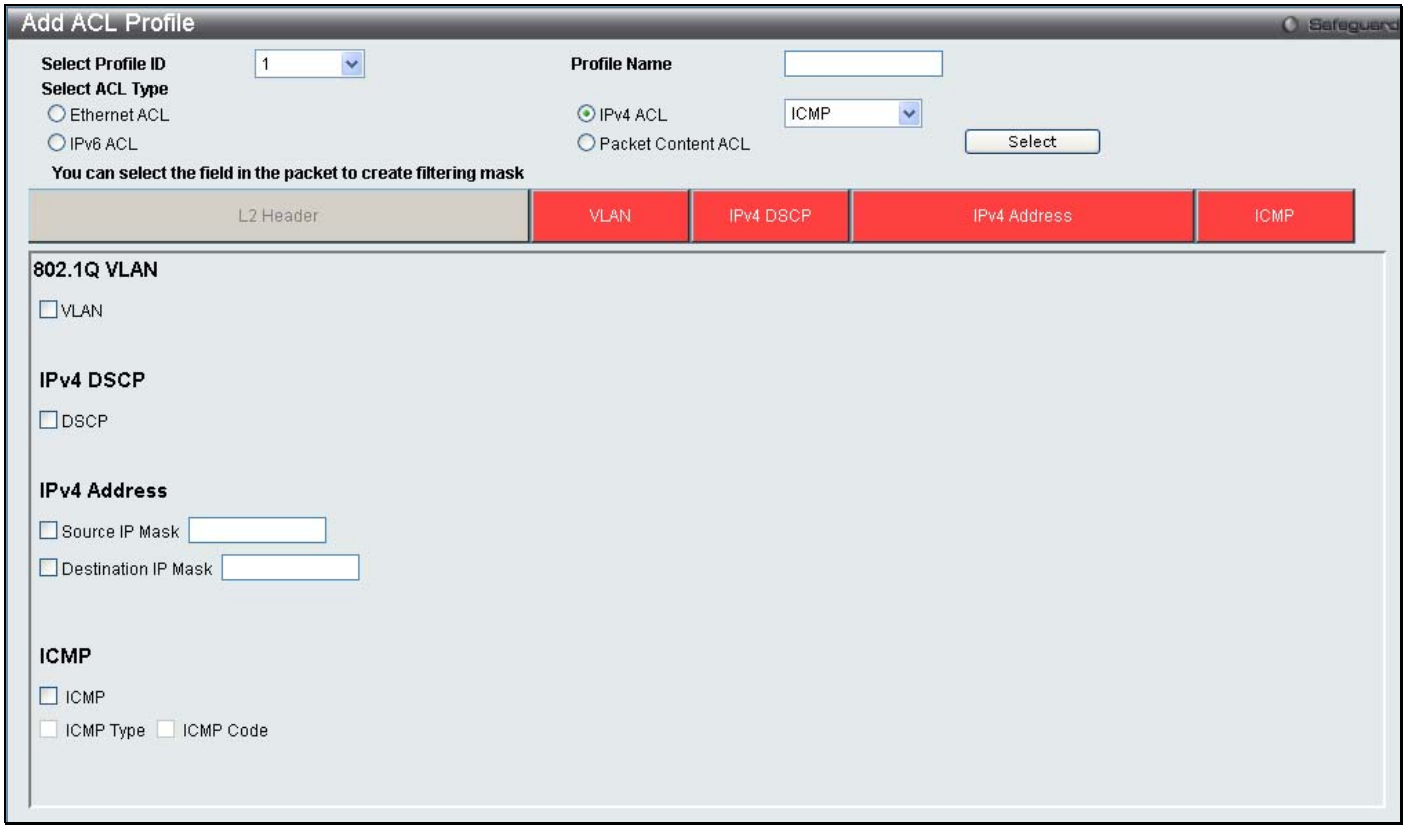


Figure 10- 10. Add IPv4 ACL Profile

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
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
ICMP Type	• *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet. • *type <value 0-65535>* – Specifies that the access profile will apply to this ICMP type value. • *code <value 0-255>* – Specifies that the access profile will apply to this ICMP code.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select **ICMP** to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select **Type** to further specify that the access profile will apply an ICMP type value, or specify **Code** to further specify that the access profile will apply an ICMP code value. Select **IGMP** to instruct the Switch to examine the Internet Group Management Protocol

	(IGMP) field in each frame's header. Select **Type** to further specify that the access profile will apply an IGMP type value Select **TCP** to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize), **fin** (finish). **src port mask** - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. **dst port mask** - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. Select **UDP** to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. **src port mask** - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff). **dst port mask** - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff). ***Protocol_id <0x0-0xff>*** – Enter a value defining the protocol ID in the packet header to mask. ***user_define_mask <hex 0x0-0xffffffff>*** – Enter a value defining the mask options behind the IP header.

Click **Apply** to implement changes made.

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

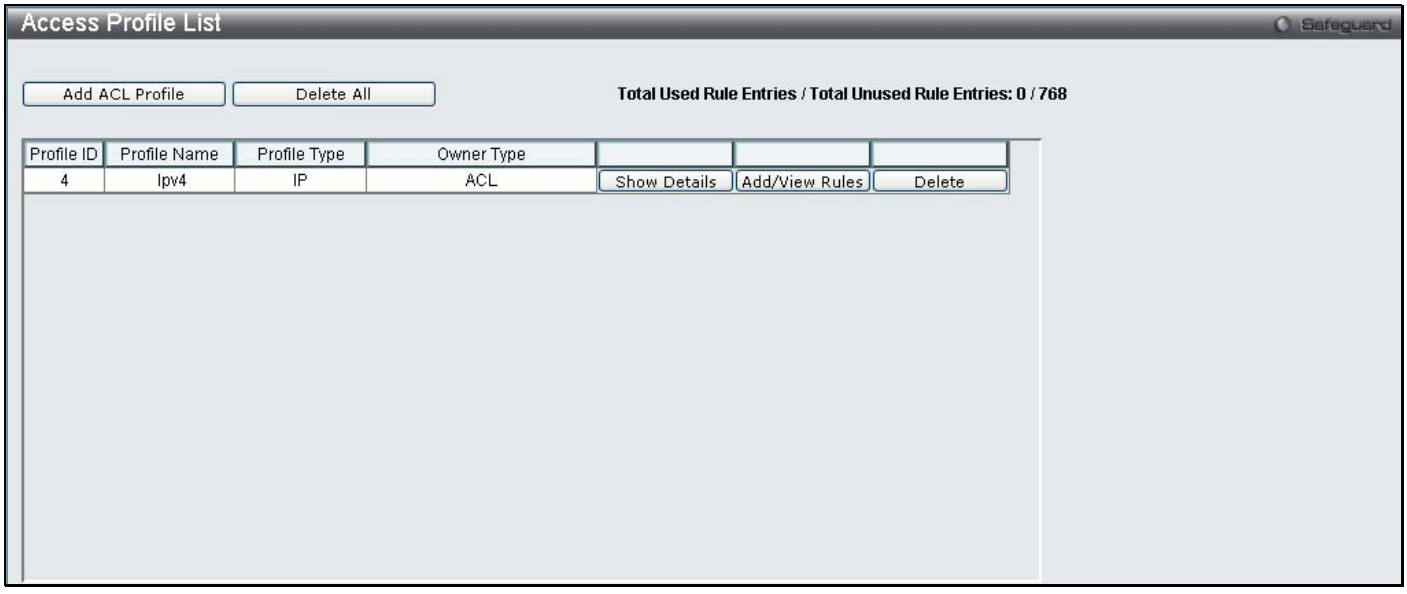


Figure 10- 11. Access Profile List (IPv4)

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

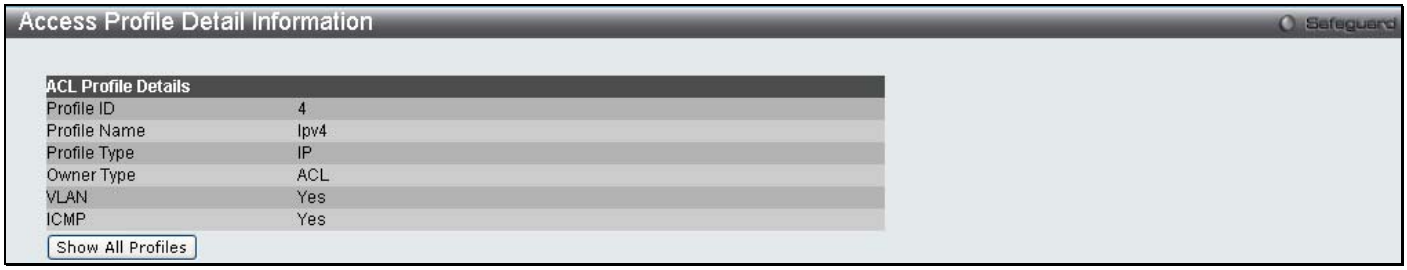


Figure 10- 12. Access Profile Details (IPv4)

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.

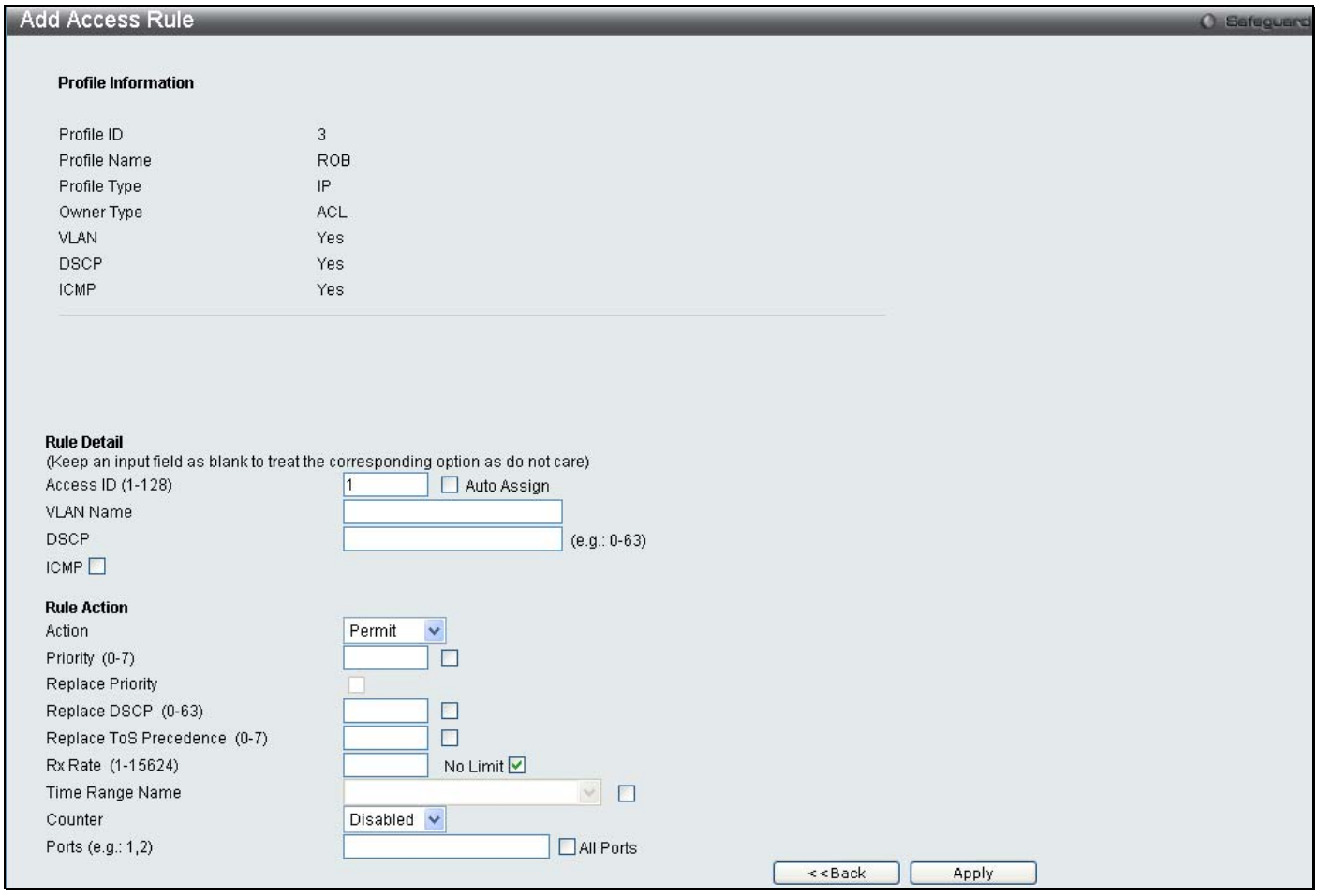


Figure 10- 13. Access Profile (IPv4)

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

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have

	its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace Priority	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Replace ToS Precedence	Select this option to instruct the Switch to replace the Type of Service as part of the packet header.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Enable or disable the counter settings.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.

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

Figure 10- 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.

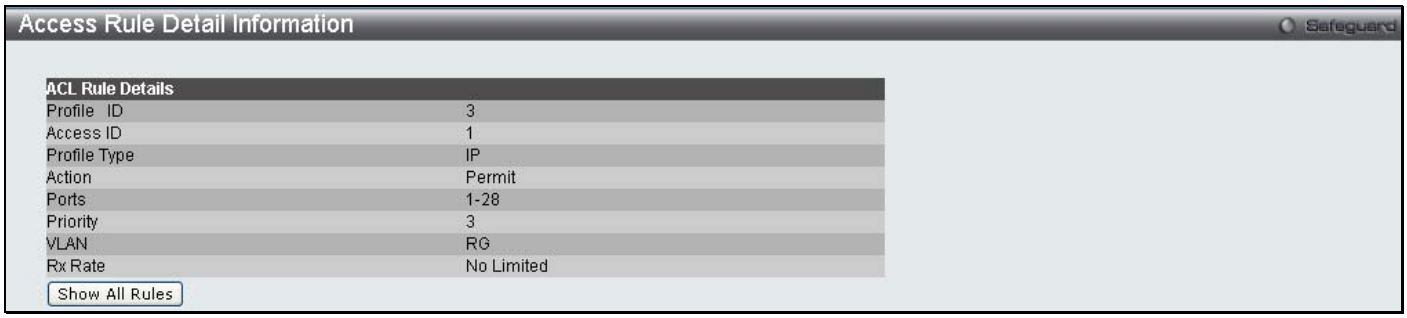


Figure 10- 15. Access Rule Detail Information

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.

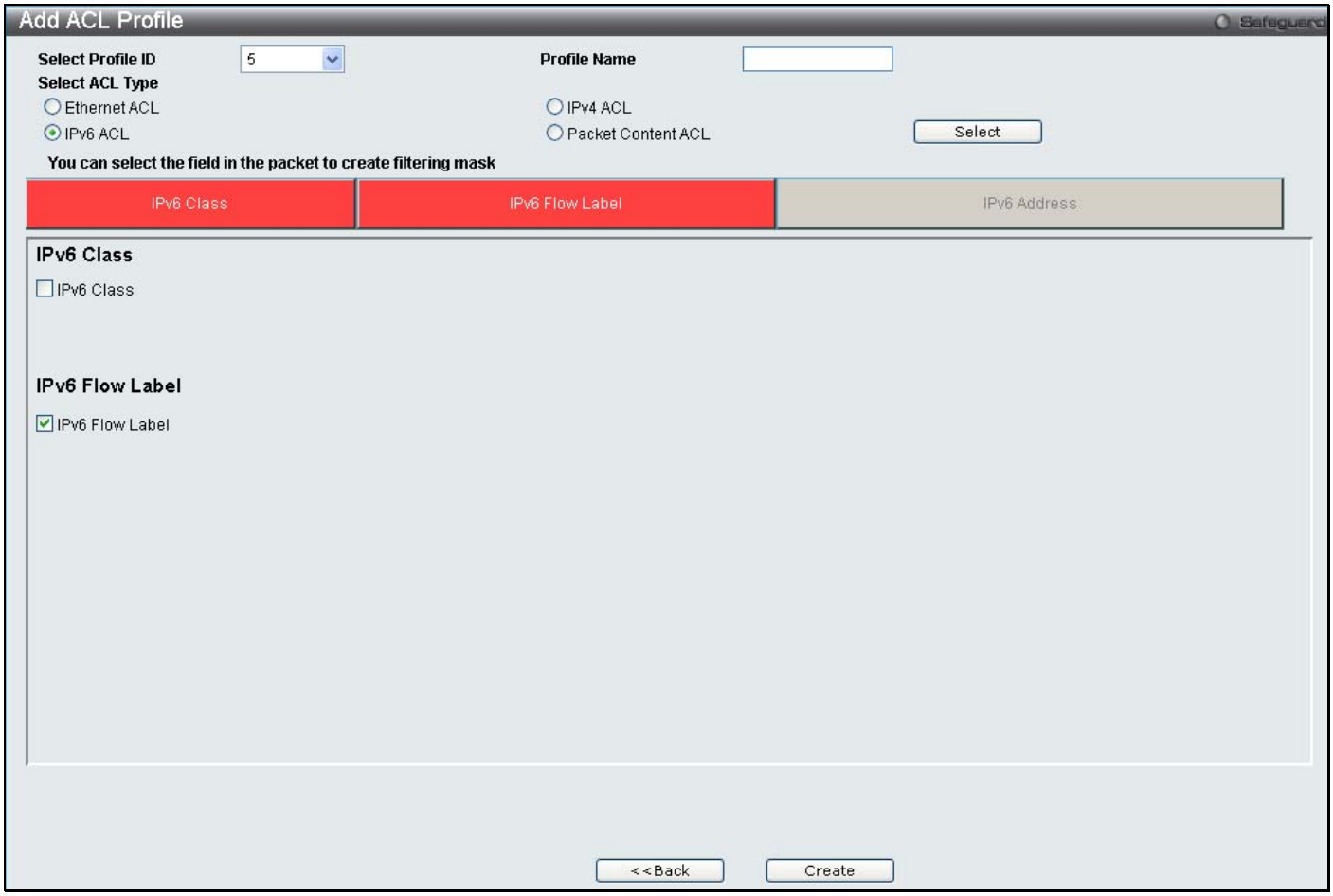


Figure 10- 16. Add IPv6 ACL Profile

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
IPv6 Class	Ticking this check box will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 Address	*IPv6 Source Address* – Enter an IPv6 address to be used as the source address. *IPv6 Destination Address* – Enter an IPv6 address that will be used as the destination address. **NOTE:** At any one time the user can only choose IPv6 class and IPv6 Flow Label together or IPv6 Address by itself.

Click **Apply** to implement changes made.

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

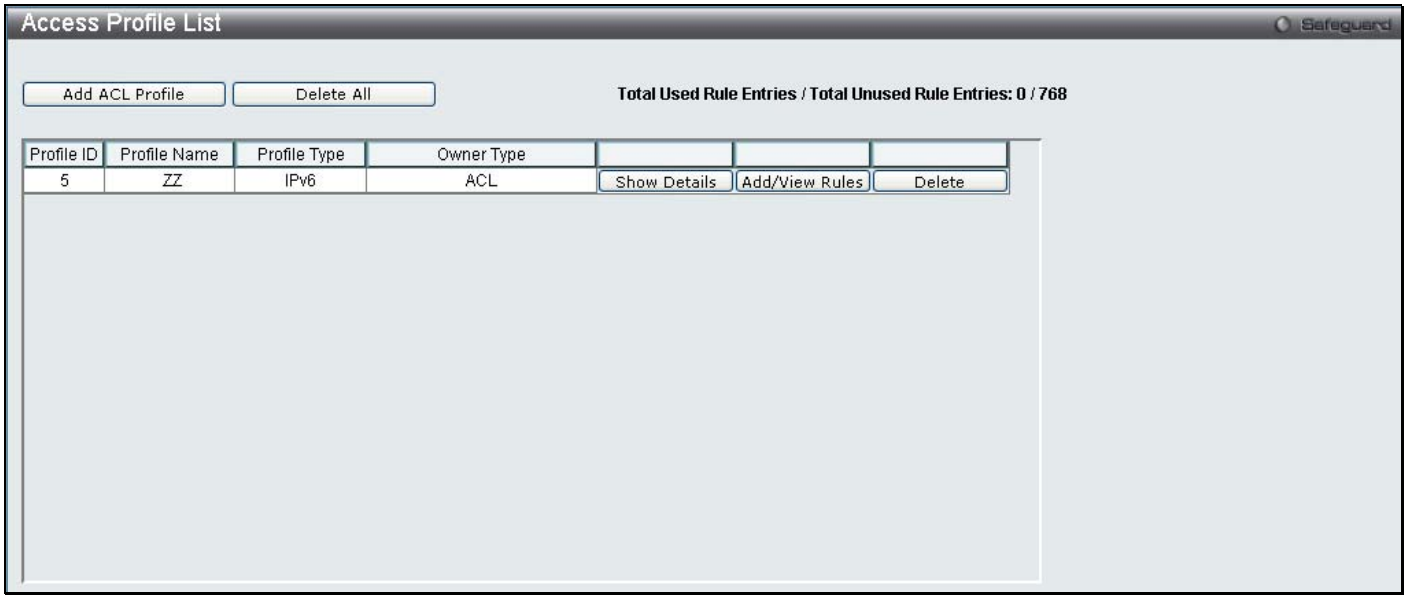


Figure 10- 17. Access Profile List (IPv6)

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

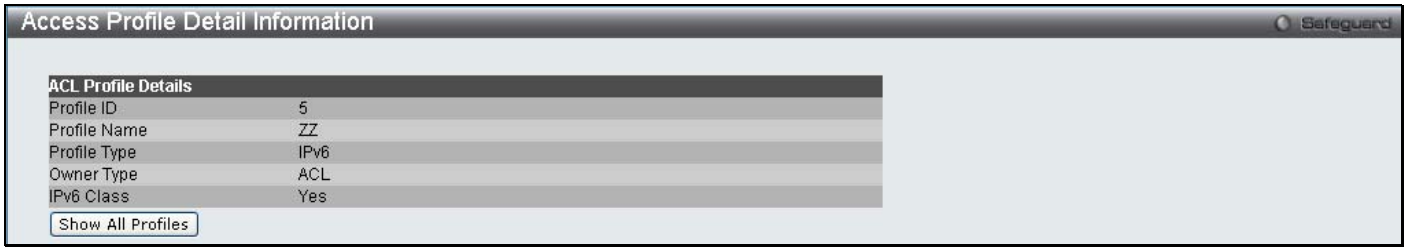


Figure 10- 18. Access Profile Details (IPv6)

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.

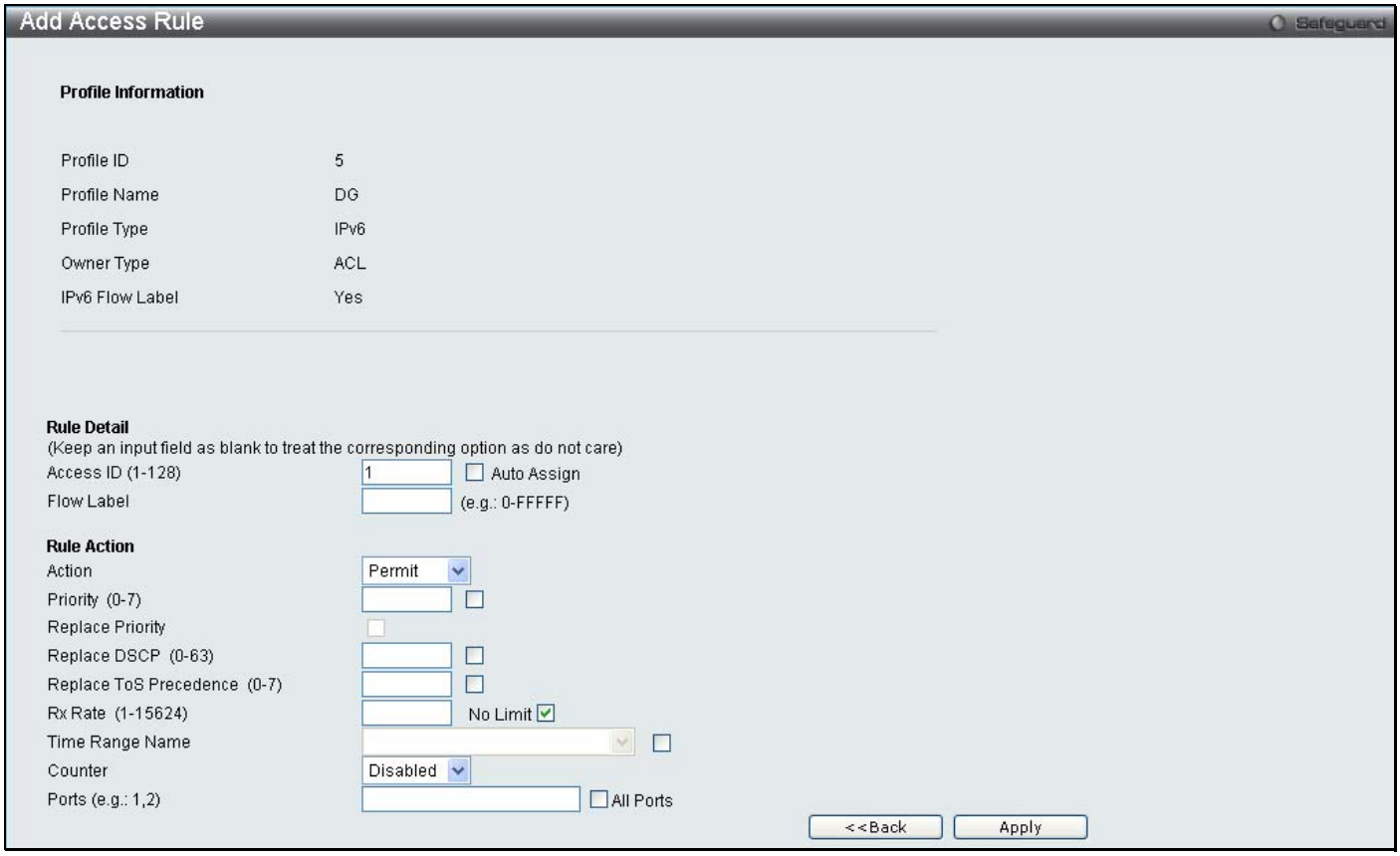


Figure 10- 19. Access Profile (IPv6)

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

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace Priority	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Replace ToS Precedence	Select this option to instruct the Switch to replace the Type of Service as part of the packet header.
Class	Entering a class will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or

	Precedence bits field in IPv4.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *15624* or tick the No Limit check box. The default setting is No Limit.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Enable or disable the counter settings.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.

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

Figure 10- 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.

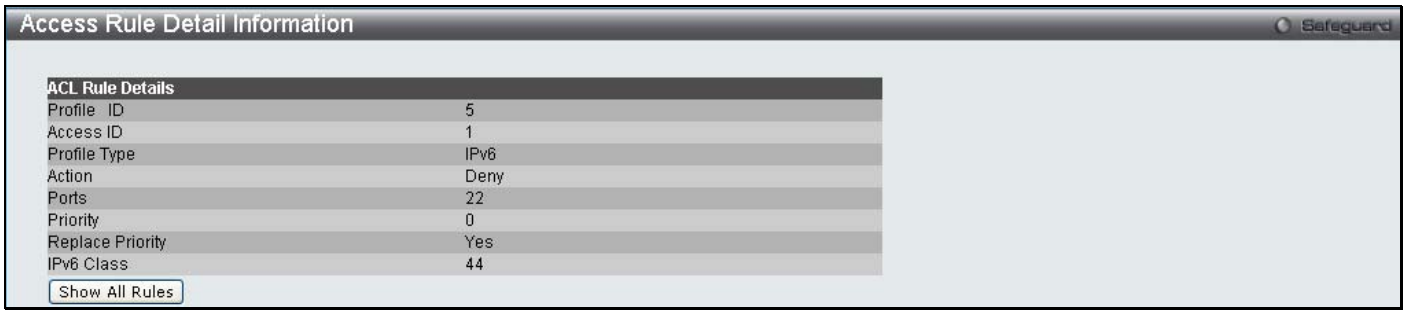


Figure 10- 21. Access Rule Detail Inforamtion (Ipv6)

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

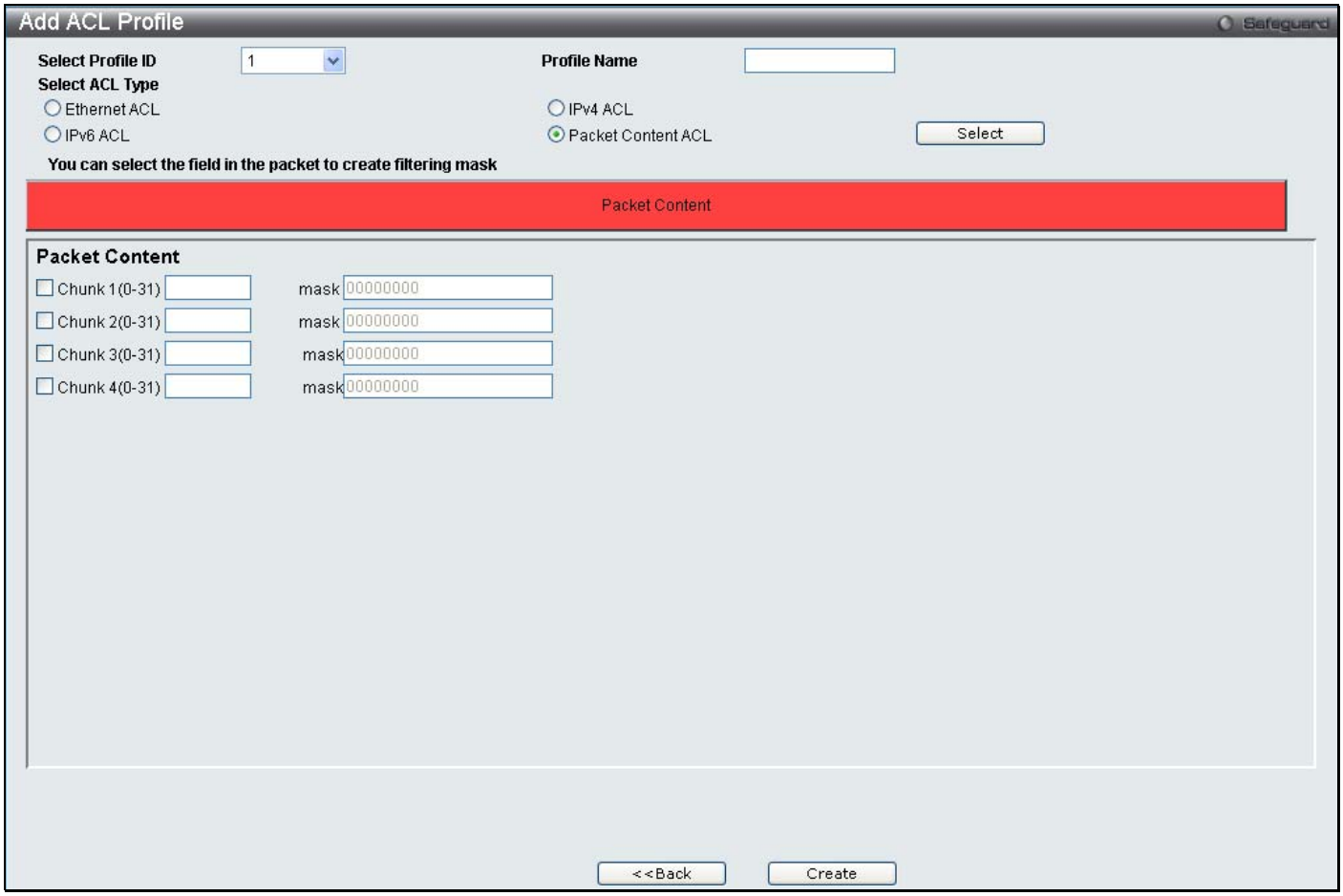


Figure 10- 22. Add Packet Content ACL Profile

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
Chunk	Allows users to examine up to 4 specified offset_chunks within a packet at one time and specifies the frame content offset and mask. There are 4 chunk offsets and masks that can be configured. A chunk mask presents 4 bytes. 4 offset_chunks can be selected from a possible 32 predefined offset_chunks as described below: offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4. chunk0: B126, B127, B0, B1 chunk1: B2, B3, B4, B5 chunk2: B6, B7, B8, B9 …… chunk29: B114, B115, B116, B117 chunk30: B118, B119, B120, B121 chunk31: B122, B123, B124, B125 Example: offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1

	offset_chunk_1 0 0x0000ffff will match packet byte offset,0,1 Note: 1. Only one packet_content_mask profile can be created. With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link xStack switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click **Apply** to implement changes made.

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

Figure 10- 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.

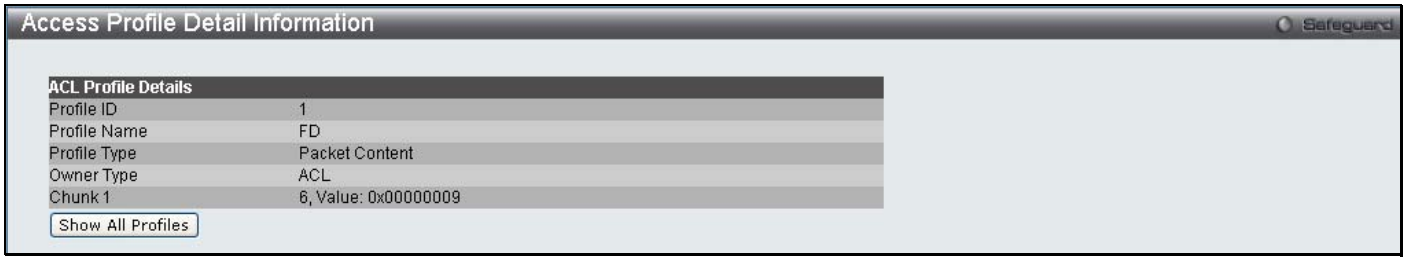


Figure 10- 24. Access Profile Details (Packet Content)

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.

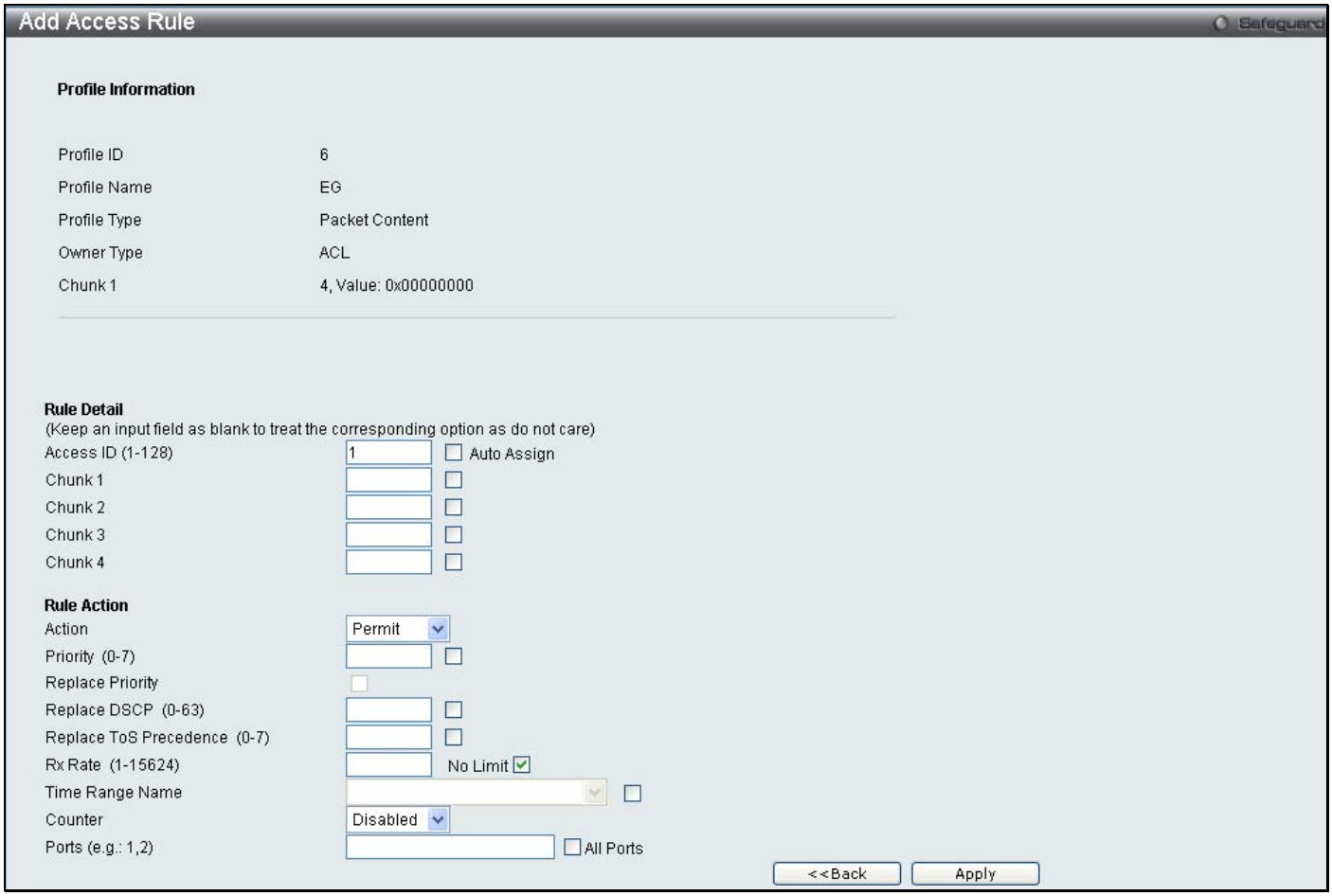


Figure 10- 25. Access Profile (Packet Content)

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

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Replace ToS Precedence	Select this option to instruct the Switch to replace the Type of Service as part of the packet header.
Chunk	This field will instruct the Switch to mask the packet header beginning with the offset value specified.
Rx Rate (1-15624)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of *10* then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *15624* or

	tick the No Limit check box. The default setting is No Limit.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Enable or disable the counter settings.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.

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

Figure 10- 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.

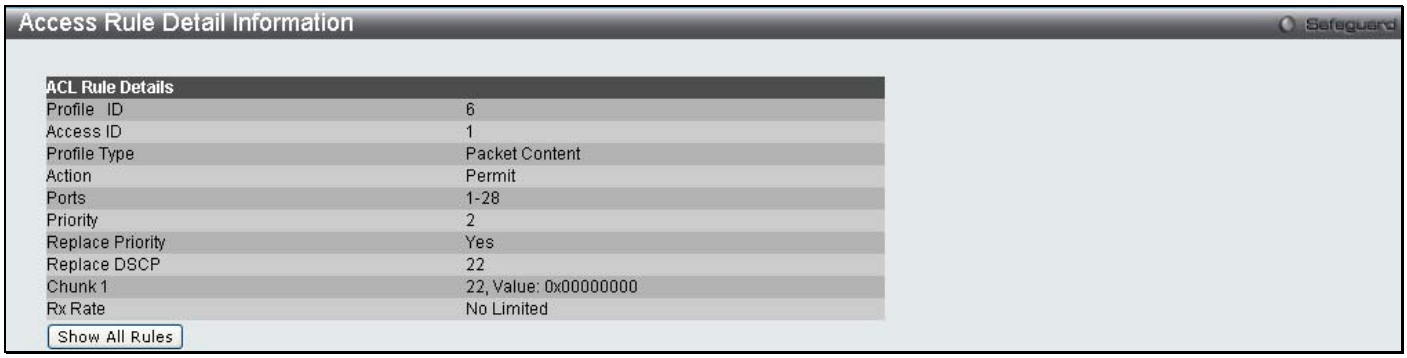


Figure 10- 27. Access Rule Detail Information (Packet Content)

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 access this window, click **ACL > CPU Access Profile List**.

Choose Enabled to enable CPU packets to be scrutinized by the Switch and Disabled to disallow this scrutiny.

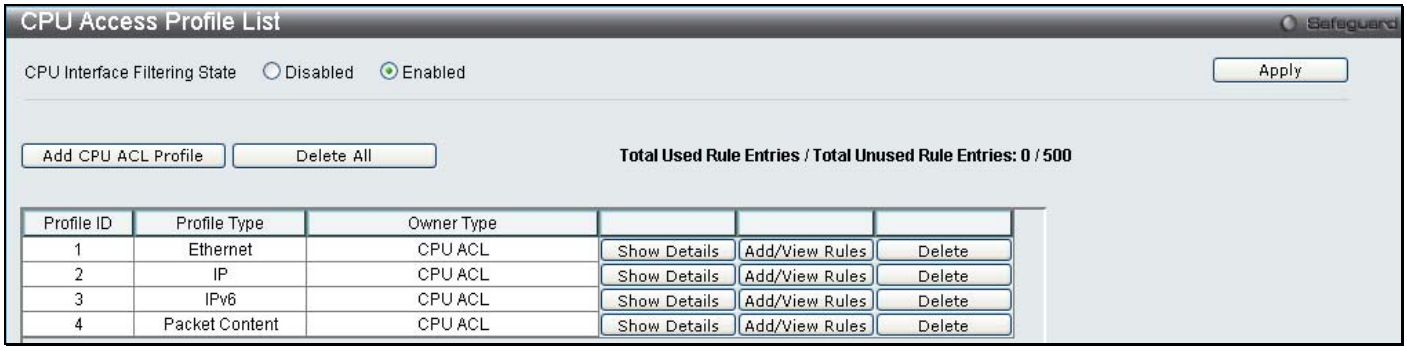


Figure 10- 28. CPU Access Profile List window

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 Acces 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.

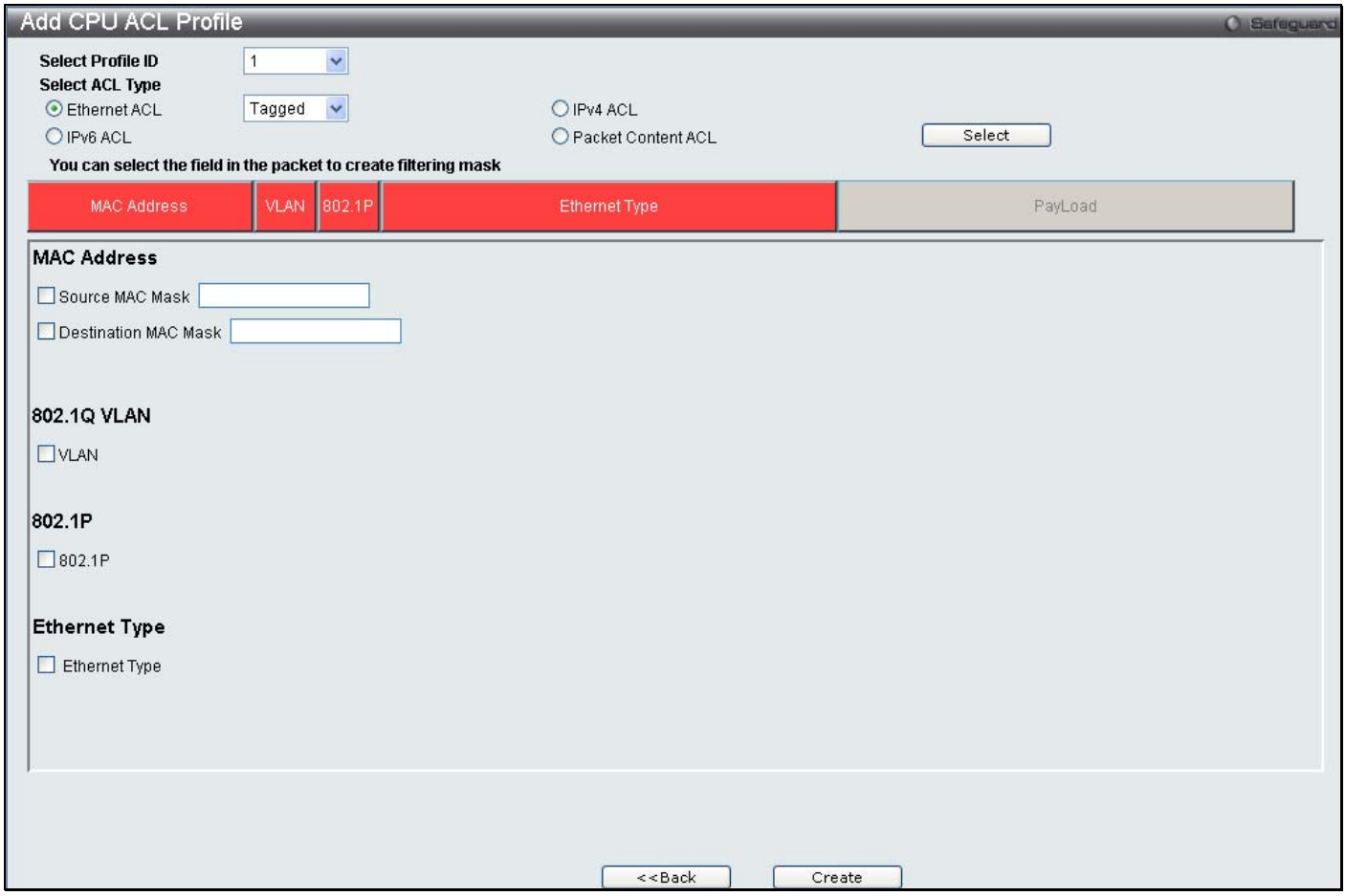


Figure 10- 29. Add CPU ACL Profile window for Ethernet

Parameter	Description
Select Profile ID (1-5)	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from *1* to *5*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IP 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 IP to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **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:

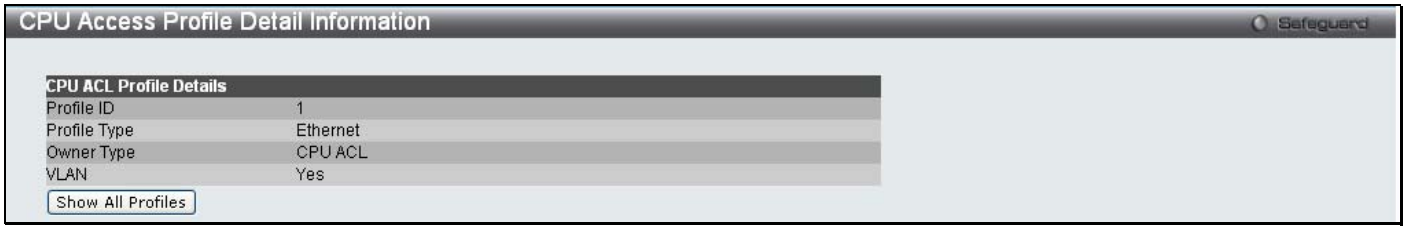


Figure 10- 30. CPU Access Profile Detail Information window for Ethernet

The window shown below is the **Add CPU ACL Profile** window for IP (IPv4).

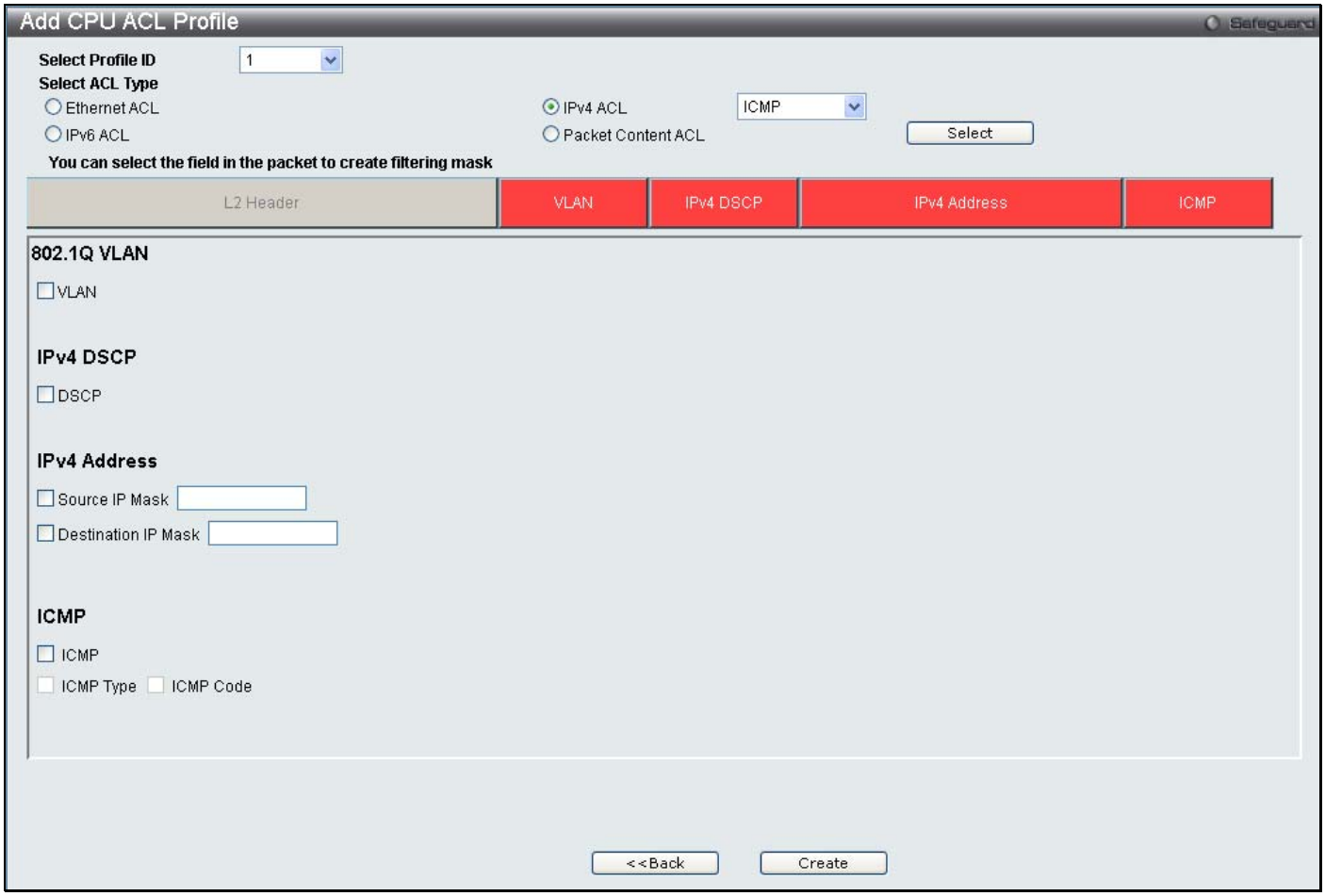


Figure 10- 31. Add CPU ACL Profile window for IP (IPv4)

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

Parameter	Description
Select Profile ID	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from *1* to *5*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IP 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 IP to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.

Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify *Code* to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires a source port mask and/or a destination port mask is to be specified. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). *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 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:

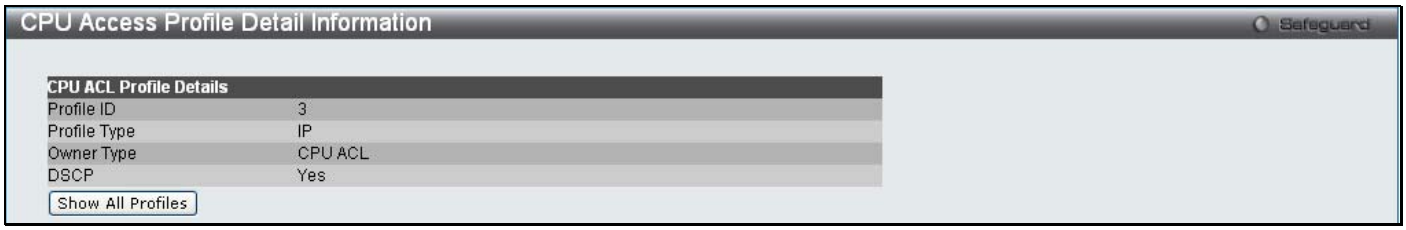


Figure 10- 32. CPU Access Profile Detail Information window for IP (IPv4)

The window shown below is the **Add CPU ACL Profile** window for IPv6.

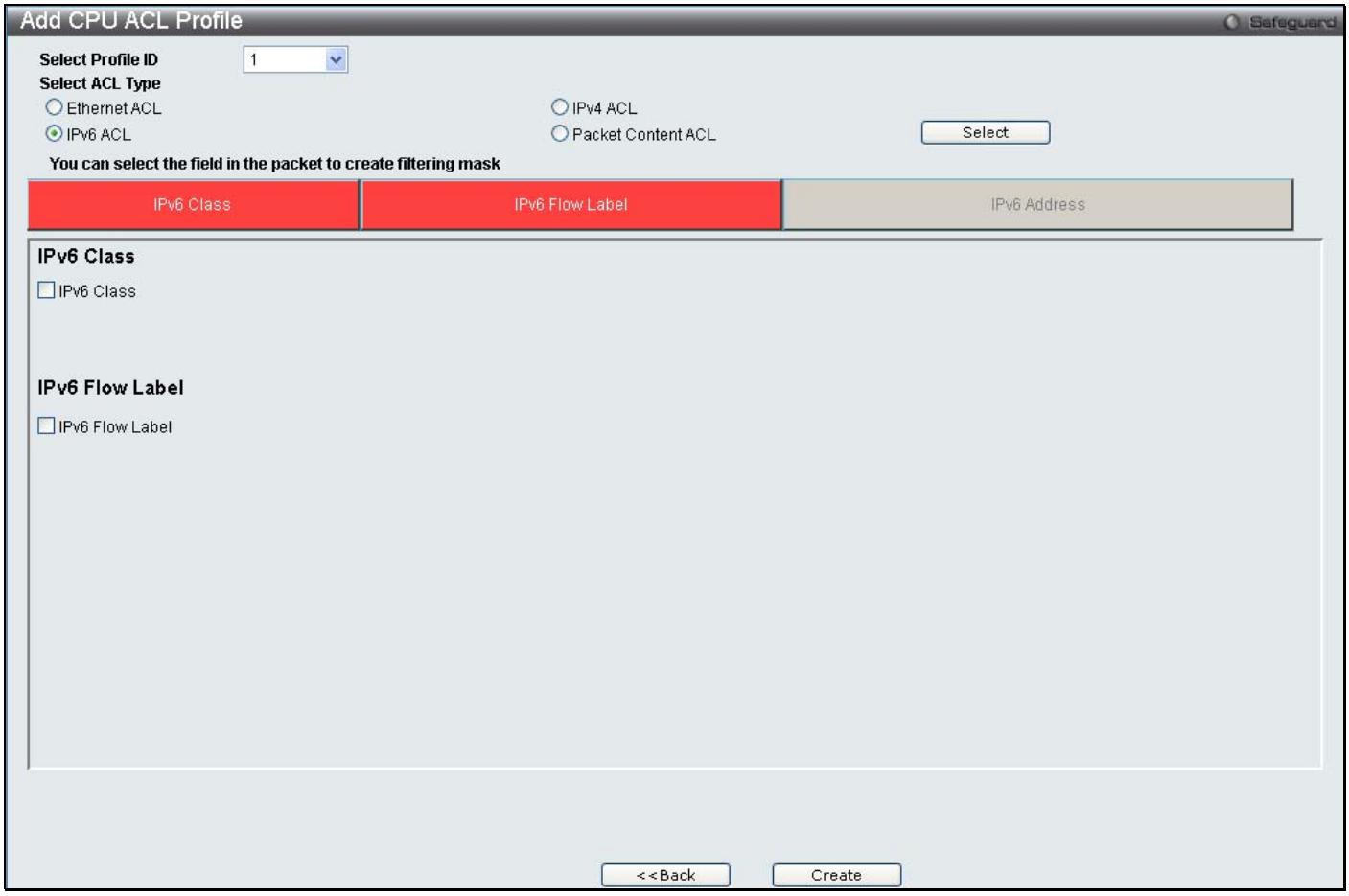


Figure 10- 33. Add CPU ACL Profile window for IPv6

The following parameters may be configured for the IPv6 filter.

Parameter	Description
Select Profile ID	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from *1* to *5*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IP 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 IP to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
IPv6 Class	Checking this field will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Checking this field will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 Address	*IPv6 Source Address* – Enter an IPv6 address to be used as the source address. *IPv6 Destination Address* – Enter an IPv6 address that will be used as the destination address.  **NOTE:** At any one time the user can only choose IPv6 class and IPv6 Flow Label together or IPv6 Address by itself.

Click **Apply** to 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:

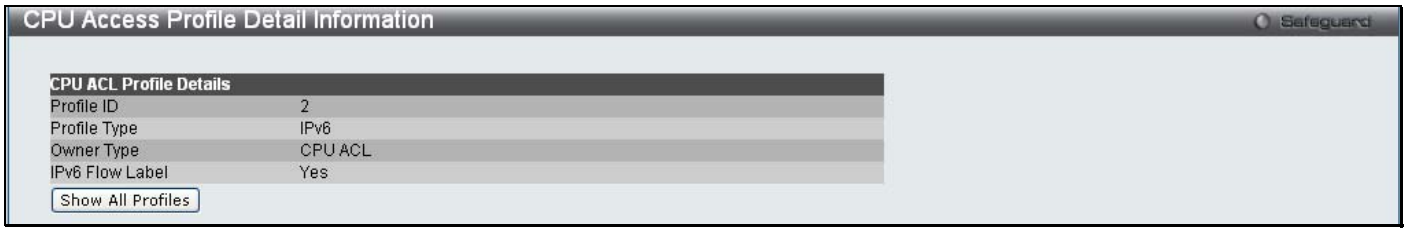


Figure 10- 34. CPU Access Profile Detail Information window for IPv6

The window shown below is the **Add CPU ACL Profile** window for Packet Content.

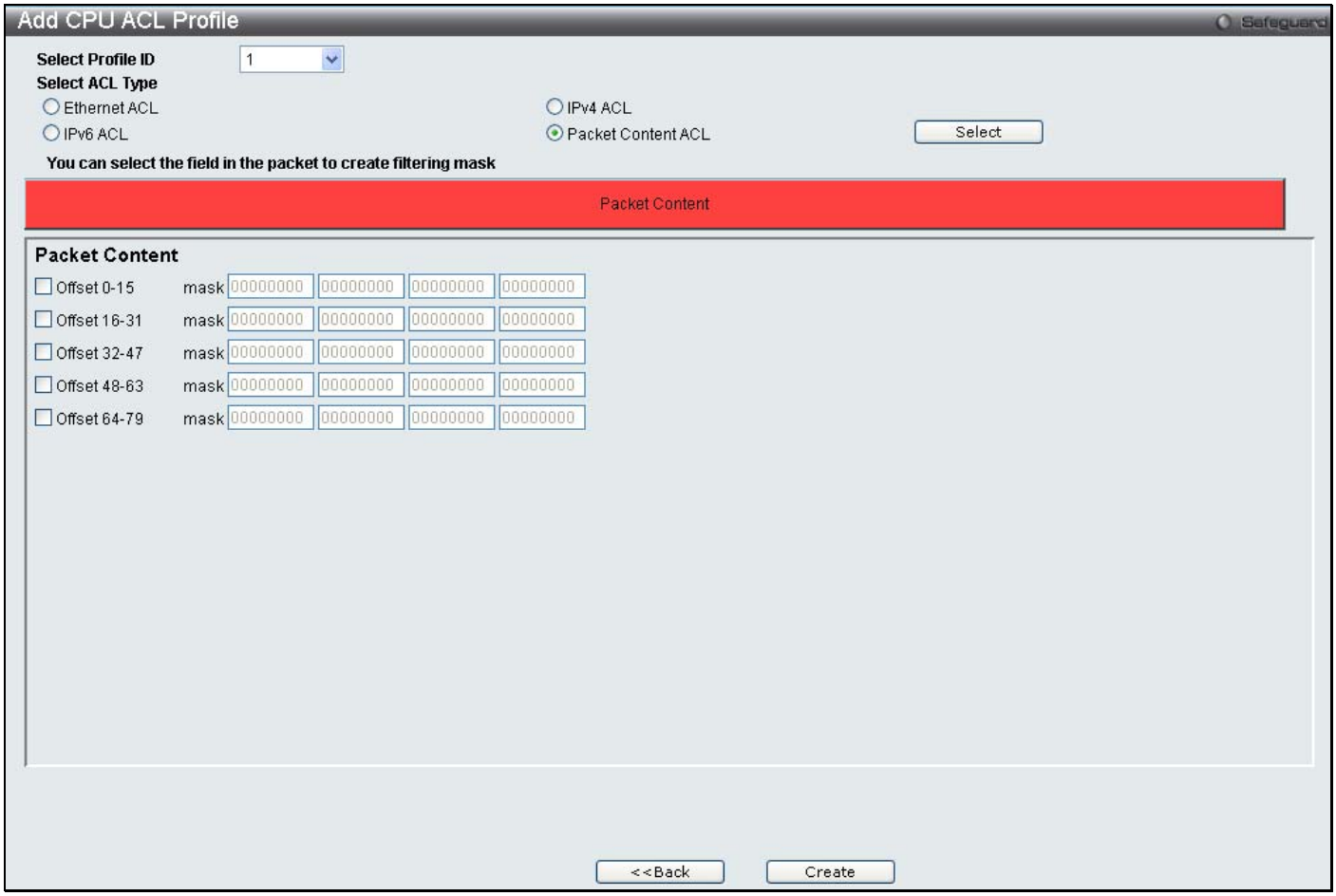


Figure 10- 35. Add CPU ACL Profile window for Packet Content

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

Parameter	Description
Select Profile ID	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from *1* to *5*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IP 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 IP to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.

Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: • *0-15* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • *16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. • *32-47* – Enter a value in hex form to mask the packet from byte 32 to byte 47. • *48-63* – Enter a value in hex form to mask the packet from byte 48 to byte 63. • *64-79* – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click **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:

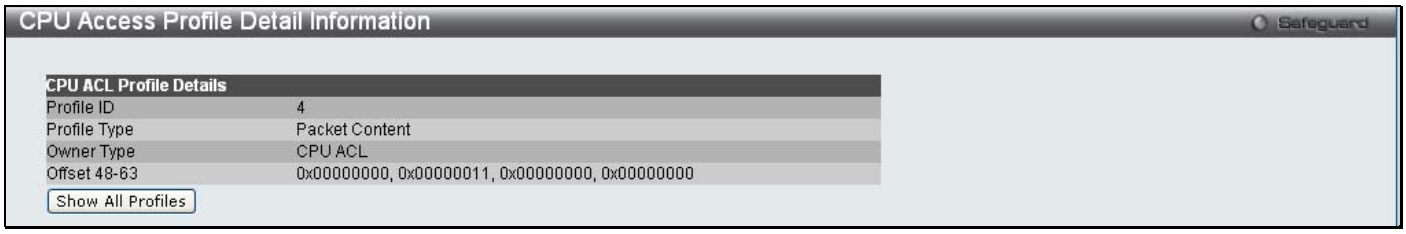


Figure 10- 36. CPU Access Profile Detail Information window for Packet Content

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 10- 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:

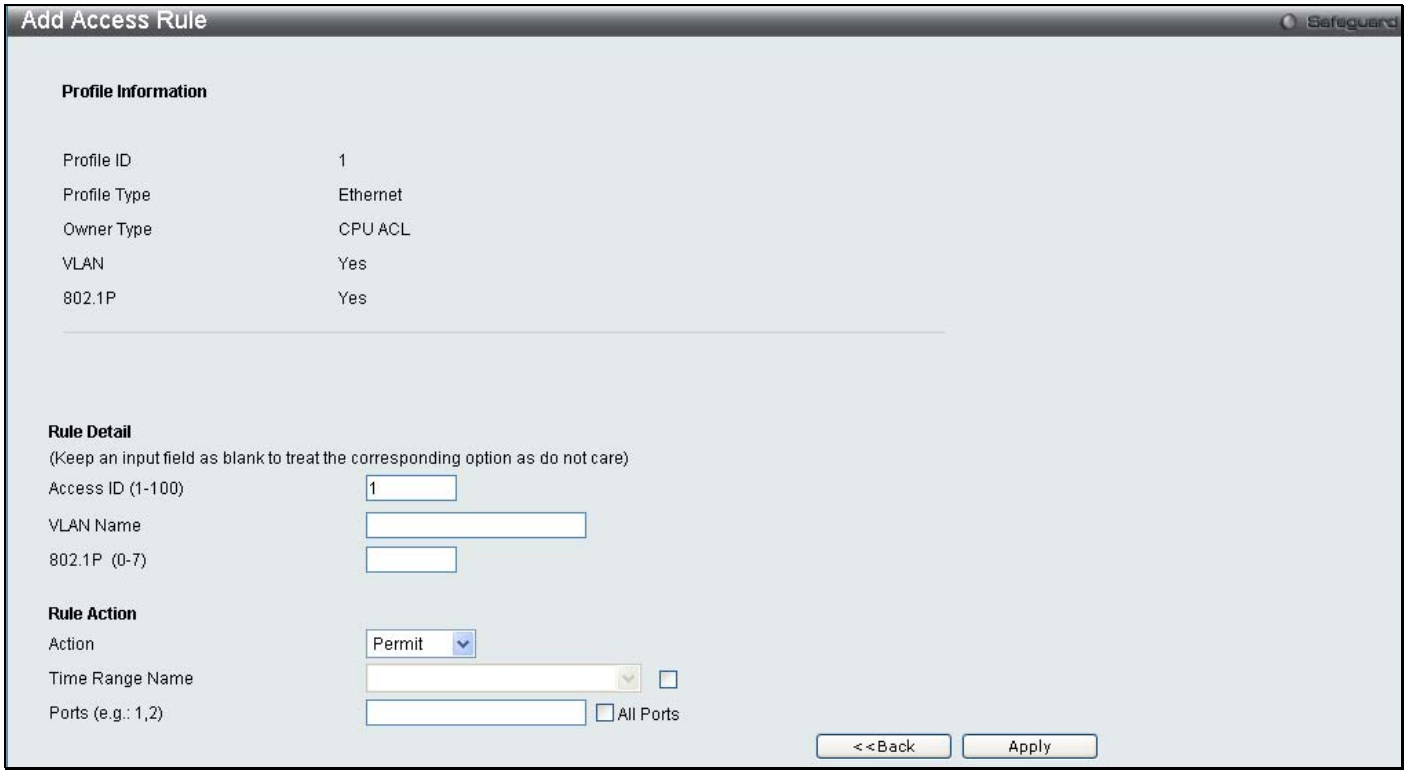


Figure 10- 38. Add Access Rule window for Ethernet

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

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Ethernet Type (0-FFFF)	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

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:

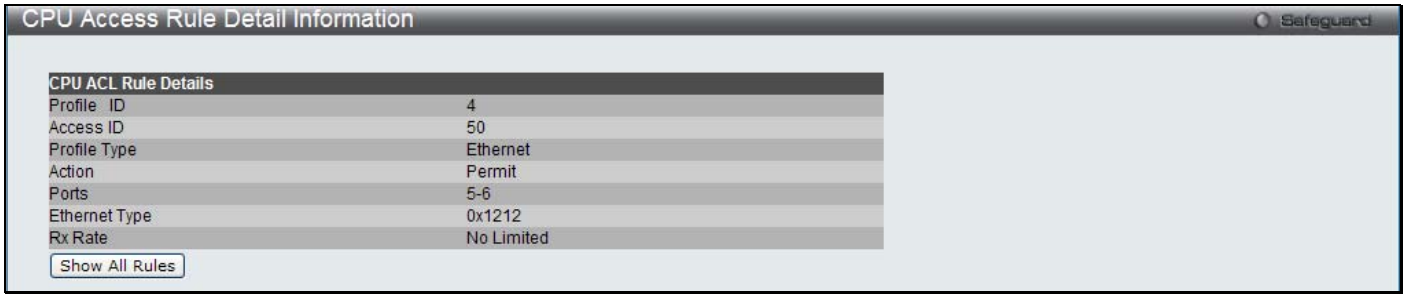


Figure 10- 39. CPU Access Rule Detail Information window for Ethernet

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 10- 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:

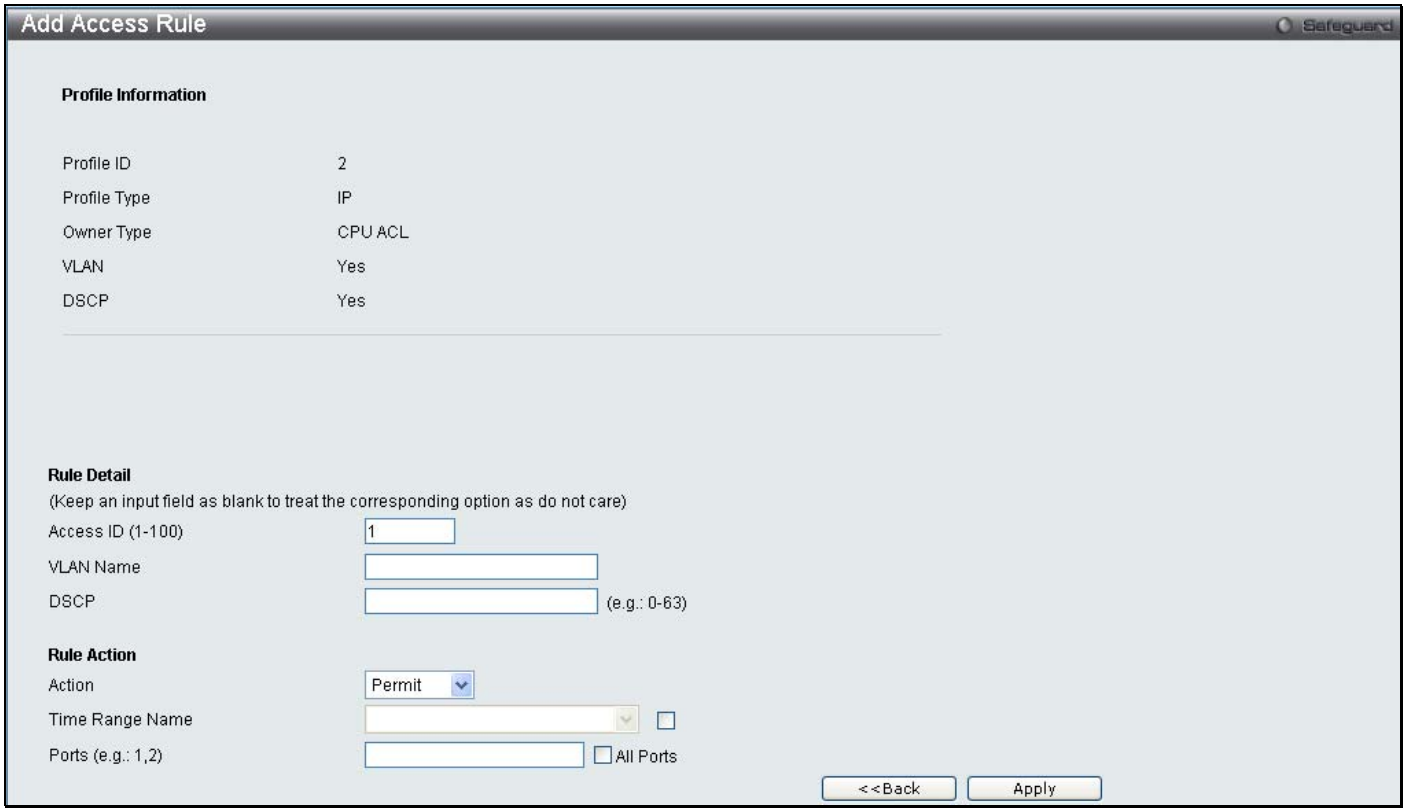


Figure 10- 41. Add Access Rule window for IP

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

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

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:

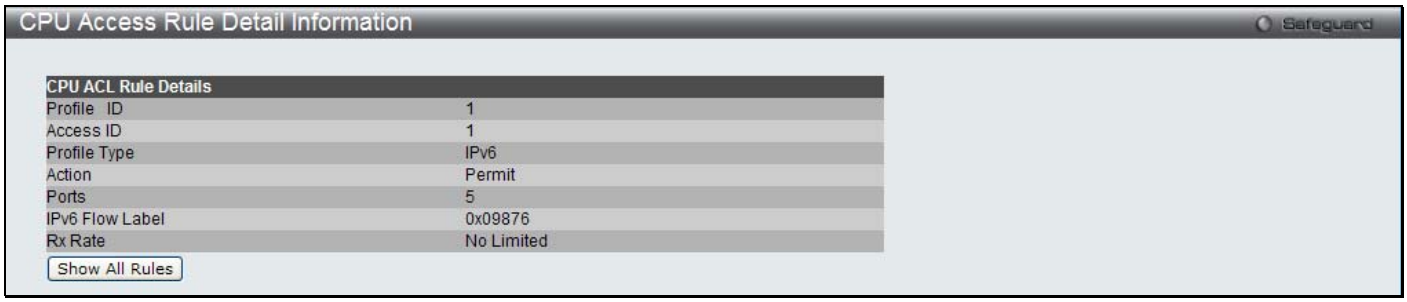


Figure 10- 42. CPU Access Rule Detail Information window for IP

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 10- 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:

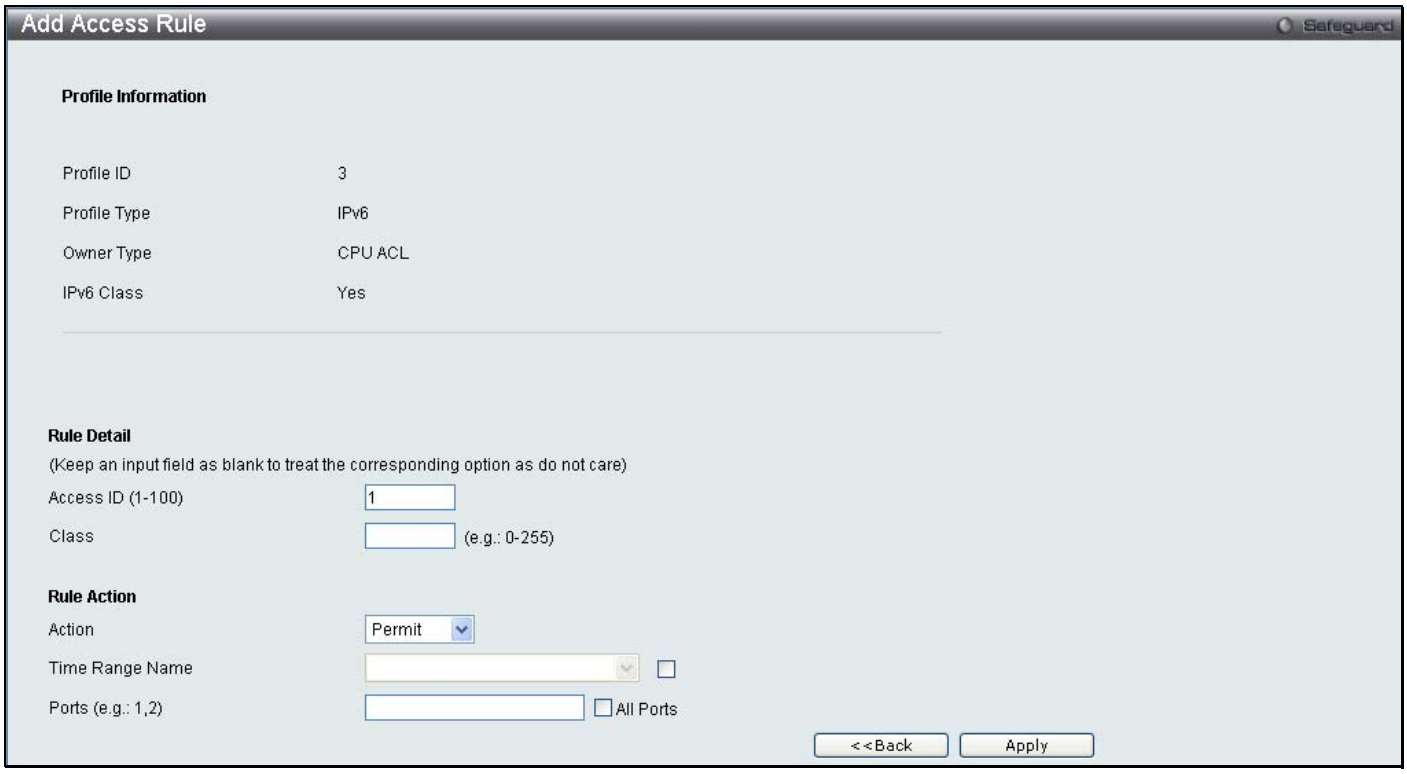


Figure 10- 44. Add Access Rule window for IPv6

To set the Access Rule for IPv6, adjust the following parameters and click **Apply**.

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

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:

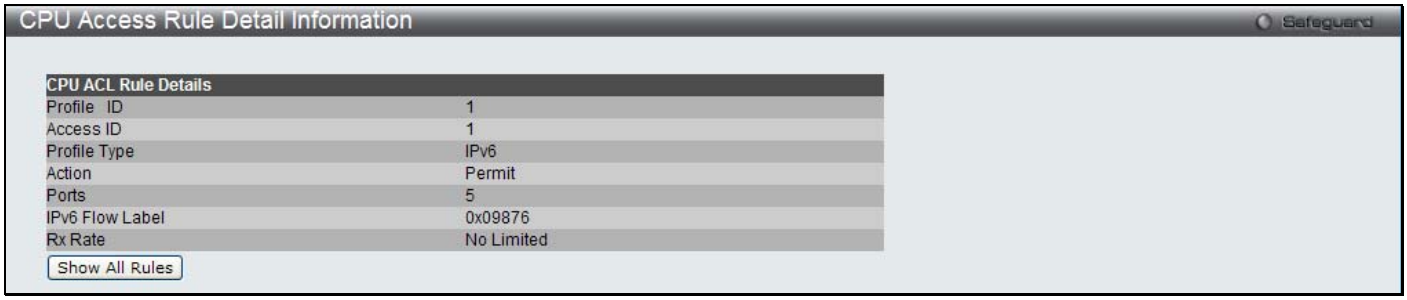


Figure 10- 45. CPU Access Rule Detail Information window for IPv6

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 10- 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:

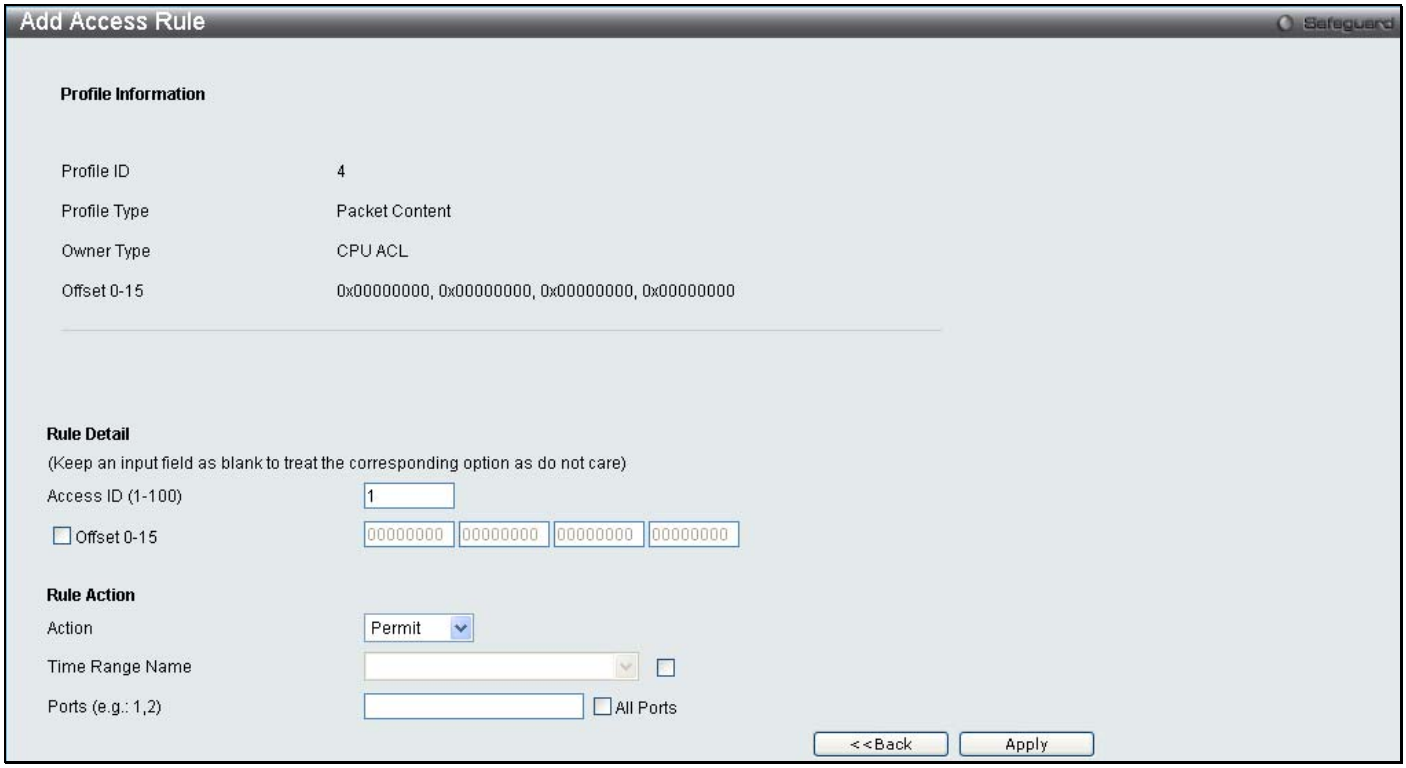


Figure 10- 47. Add Access Rule window for Packet Content

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

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: Offset 0-15 - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. Offset 16-31 - Enter a value in hex form to mask the packet from byte 16 to byte *31*. Offset 32-47 - Enter a value in hex form to mask the packet from byte 32 to byte 47. Offset 48-63 - Enter a value in hex form to mask the packet from byte 48 to byte 63. Offset 64-79 - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

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:

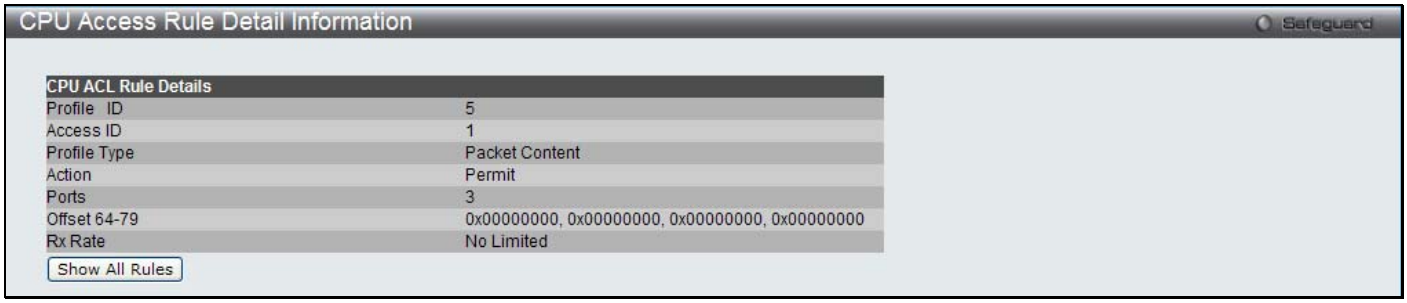


Figure 10- 48. CPU Access Rule Detail Information window for Packet Content

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 open this window, click **ACL > ACL Finder**:

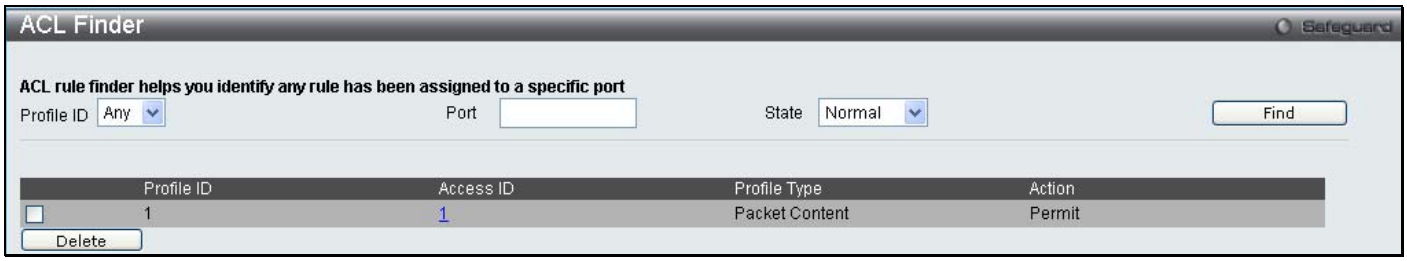


Figure 10- 49. ACL Finder window

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 open this window, click **ACL > ACL Flow Meter**:

Figure 10- 50. ACL Flow Meter window

The following fields may be configured:

Parameter	Description
Profile ID	The pre-configured Profile ID for which to configure the Flow Metering parameters.
Access ID	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.

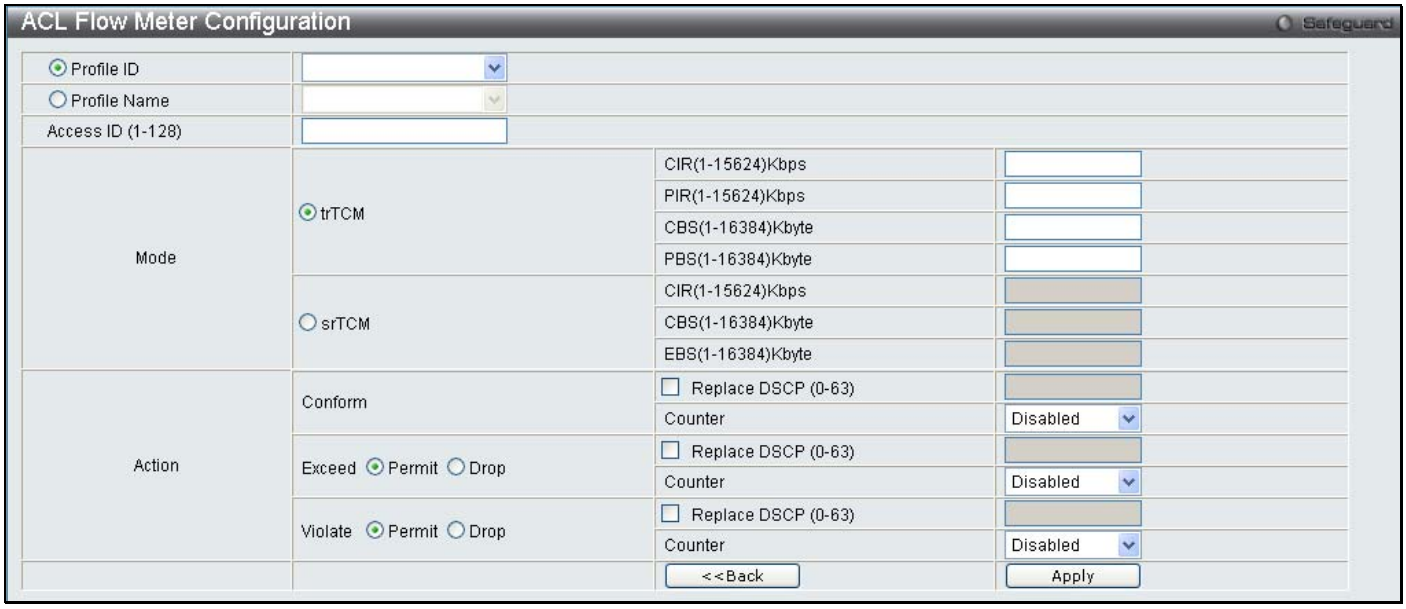


Figure 10- 51. ACL Flow Meter - Add window

The following fields may be configured:

Parameter	Description
Profile ID	Use the drop down menu to select the pre-configured Profile ID that will be used to configure the Flow Metering parameters.
Profile Name	Use the drop down menu to select the pre-configured Profile Name.
Access ID (1-128)	Enter the Access ID that will be used to configure the Flow Metering parameters, enter a value between *1* and *128*.
Mode	Select the mode to be used either *trTCM* or *srTCM* and enter the corresponding information. **trTCM –** 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. • **CIR(1-15624)Kbps** – Specifies the Committed Information Rate of the packet. The unit is 64Kbps. That is to say, 1 means 64Kbps. • **PIR(1-15624)Kbps** – Specifies the Peak Information Rate of the packet. The unit is 64Kbps. That is to say, 1 means 64Kbps. • **CBS(1-16384)Kbyte** – Specifies the Committed Burst Size of the packet. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is optional and the default value is 4*1024. The max value is 16*1024. • **PBS(1-16384)Kbyte** – Specifies the Peak Burst Size of the packet. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is optional and the default value is 4*1024. The max value is 16*1024. **srTCM** – 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. • **CIR(1-15624)Kbps** – Specifies the Committed Information Rate of the packet. The unit is 64Kbps. That is to say, 1 means 64Kbps. • **CBS(1-16384)Kbyte** – Specifies the Committed Burst Size of the packet. The unit is Kbytes. That is to say, 1 means 1Kbytes. The maximum value is 16*1024. • **EBS(1-16384)Kbyte** – Specifies the Excess Burst Size of the packet. The unit is Kbytes. That is to say, 1 means 1Kbytes. The maximum value is 16*1024.

Action	**Conform** – Specifies the action when the packet is in “green color” mode. • **Permit** – Permits the packet. • **Replace dscp** – Change the dscp of the packet **Exceed** – Specifies the action when the packet is in “yellow color” mode. • **Permit** – Permits the packet. • **Replace DSCP** – Allows you to change the DSCP of the packet. • **Drop** – Drops the packet. **Violate** – Specifies the action when the packet is in “red color” mode. • **Permit** – Permits the packet. • **Replace DSCP** – Change the DSCP of the packet. • **Drop** – Drops the packet.

Click **Apply** to implement changes made, click **Back** to return to the ACL Flow Meter.

Section 11

Monitoring

Device Status
CPU Utilization
Port Utilization
Packet Size
Packets
Errors
Port Access Control
Browse ARP Table
Browse VLAN
Show VLAN Ports
Browse Router Port
Browse MLD Router Port
Browse Session Table
IGMP Snooping Group
MLD Snooping Group
JWAC Host Table
MAC Address Table
System Log

Device Status

The Device Status window displays status information for Internal Power and External Power.

To open this window, click **Monitoring > Device Status**:

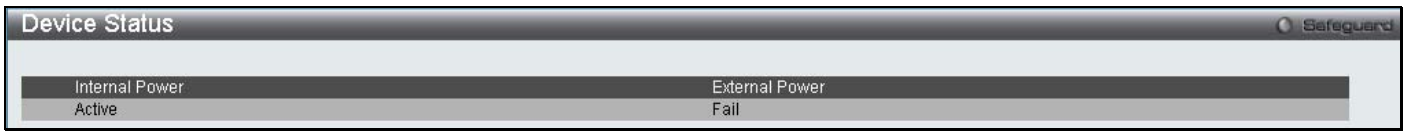


Figure 11- 1. Device Status window

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**

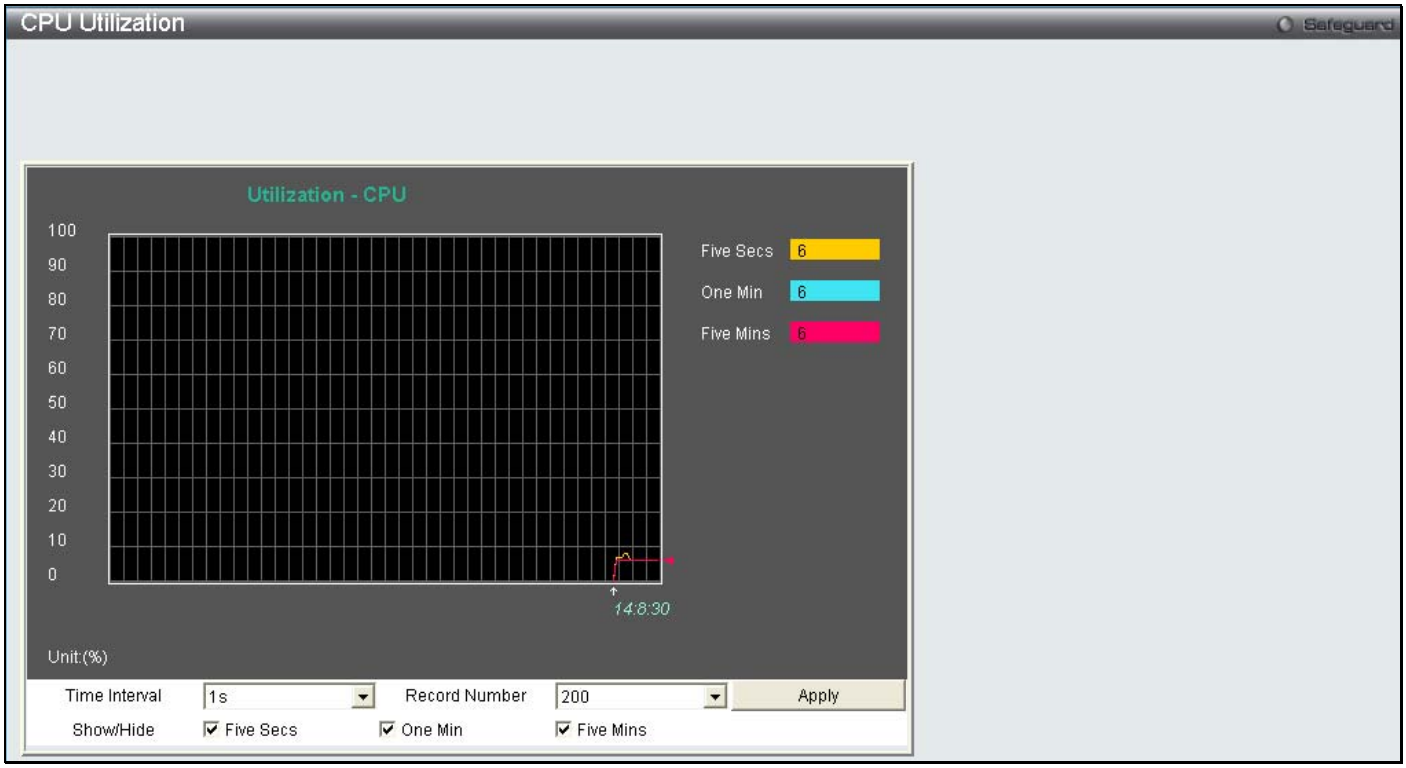


Figure 11- 2. CPU Utilization window

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
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Five Secs, One Min, and Five Mins.

Port Utilization

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

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

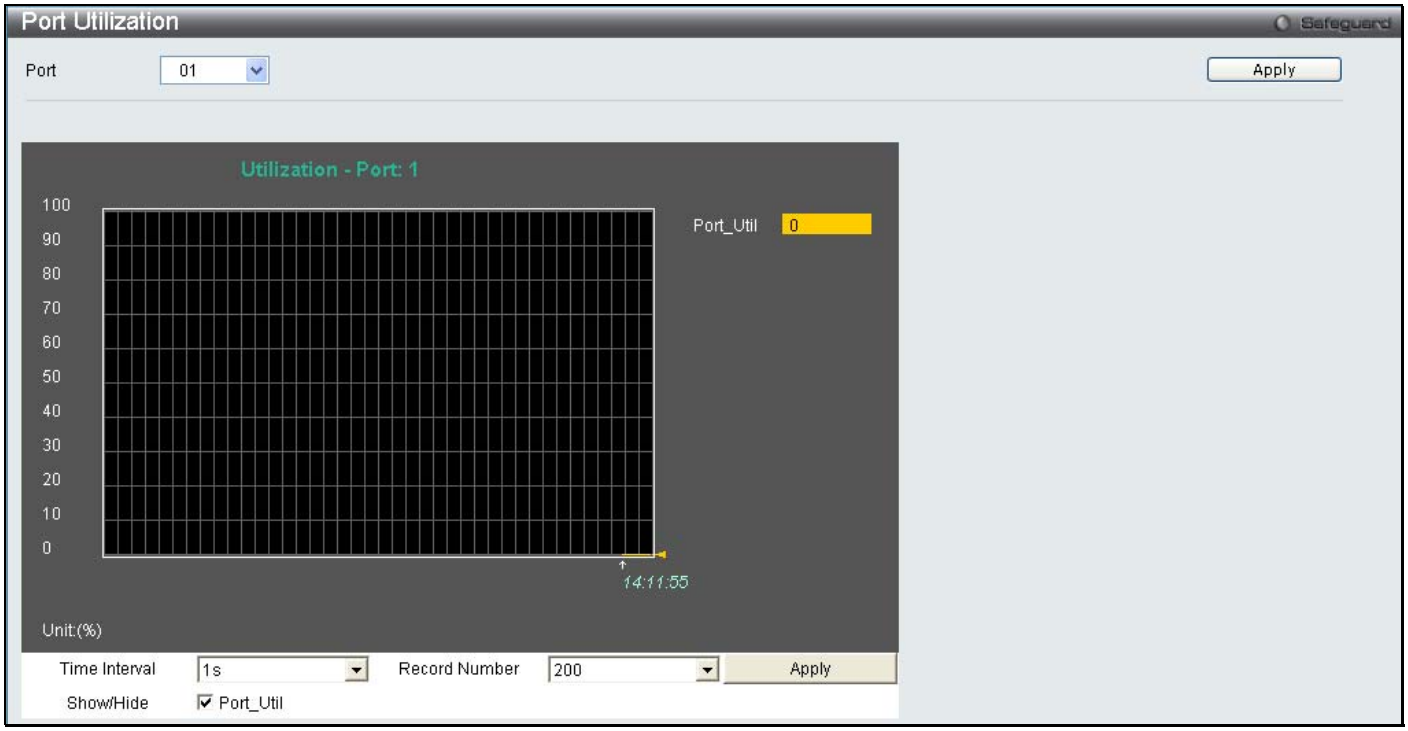


Figure 11- 3. Port Utilization window

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

Change the view parameters as follows:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Port Util.

Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the packet size windows, click **Monitoring** > **Packet Size**:

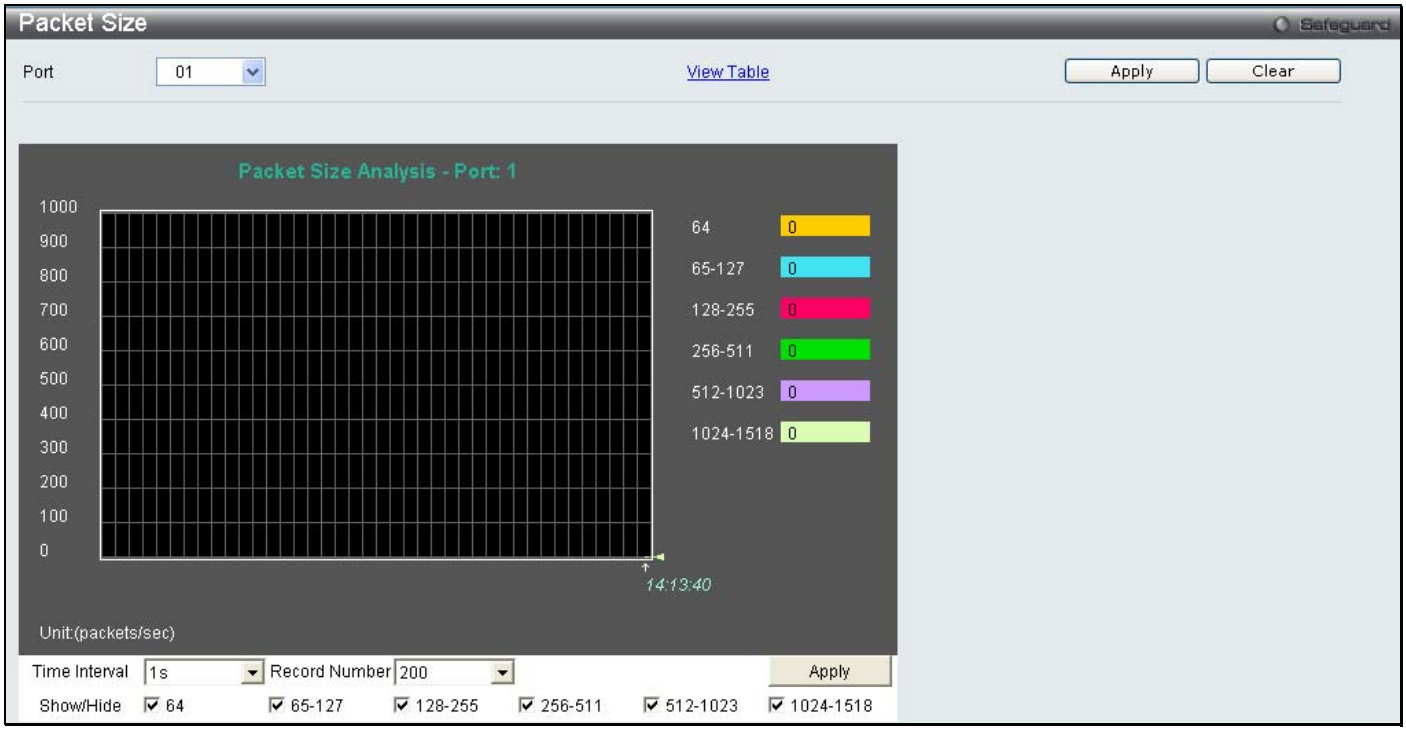


Figure 11- 4. Packet Size window

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

Figure 11- 5. Packet Size Table window

The following fields can be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.

64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

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 the following graph of packets received on the Switch Click **Monitoring > Packets > Received (RX)**.

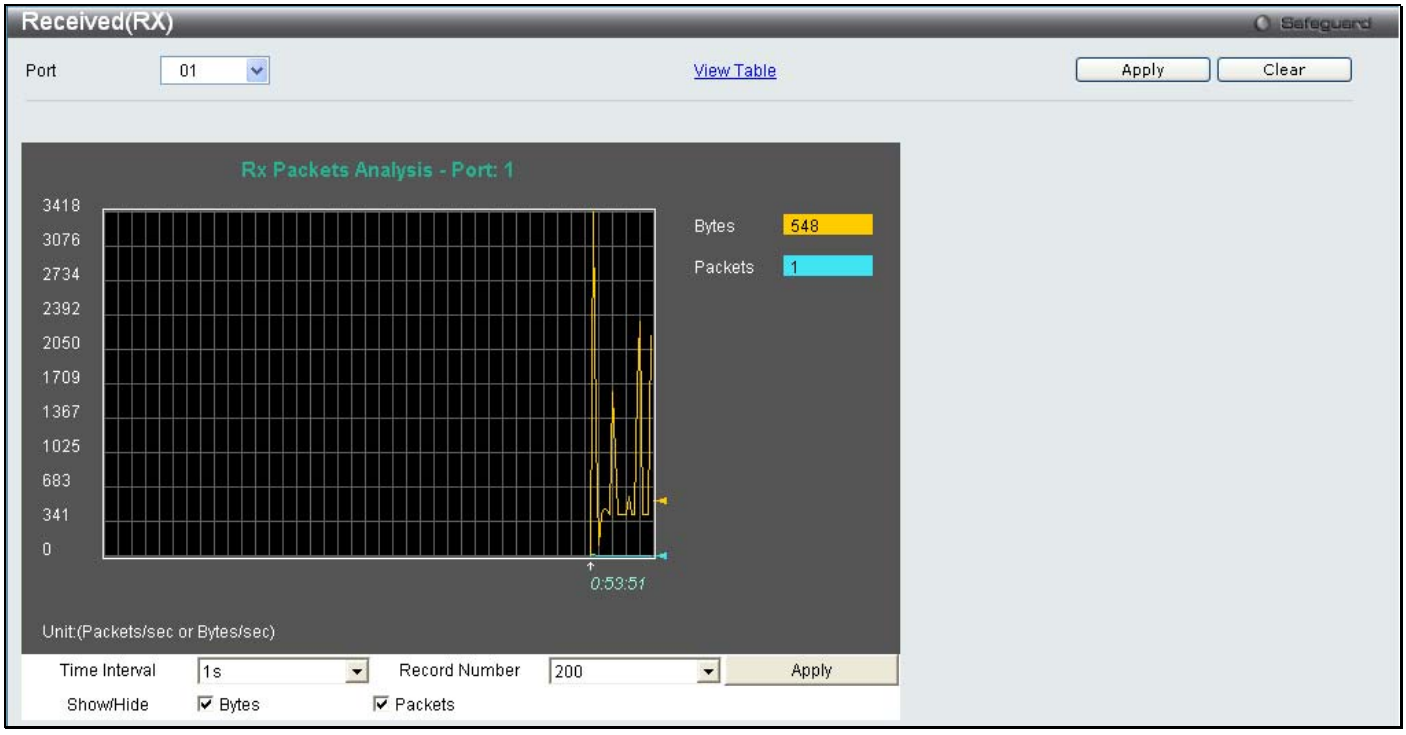


Figure 11- 6. Received (RX) window (for Bytes and Packets)

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

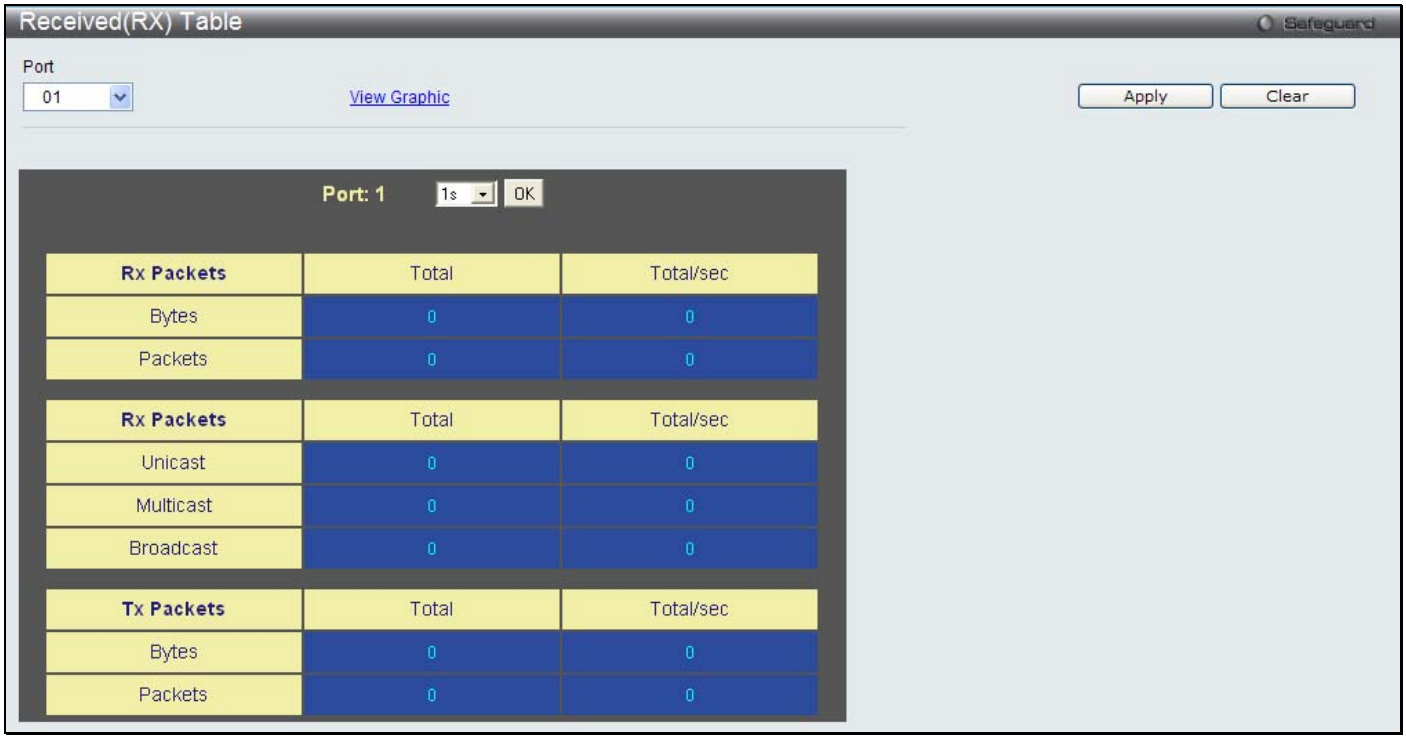


Figure 11- 7. Received (RX) Table window (for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.

	value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB_cast (RX)

This table displays the UMB_cast RX Packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following graph of UMB cast packets received on the Switch, click **Monitoring > Packets > UMB_cast (RX)**.

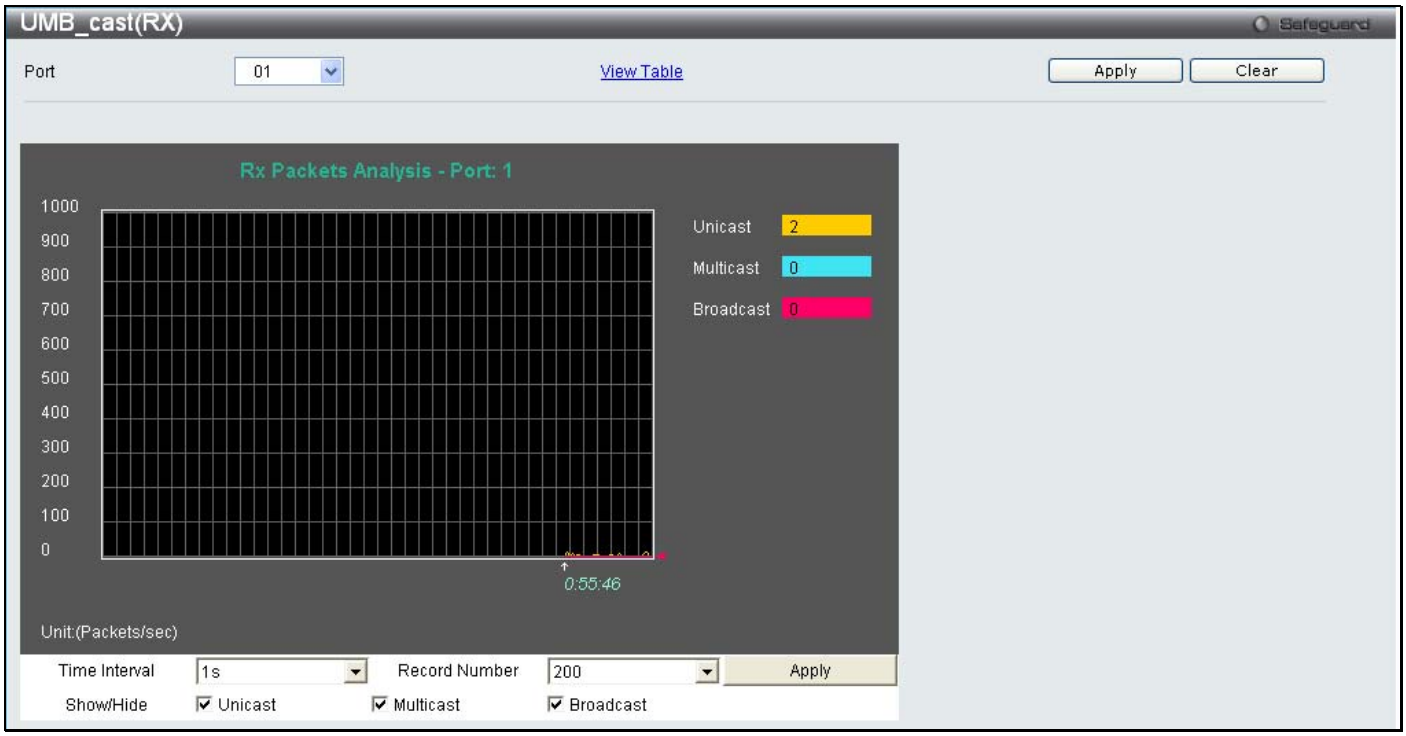


Figure 11- 8. UMB_cast (RX) window (for Unicast, Multicast, and Broadcast Packets)

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

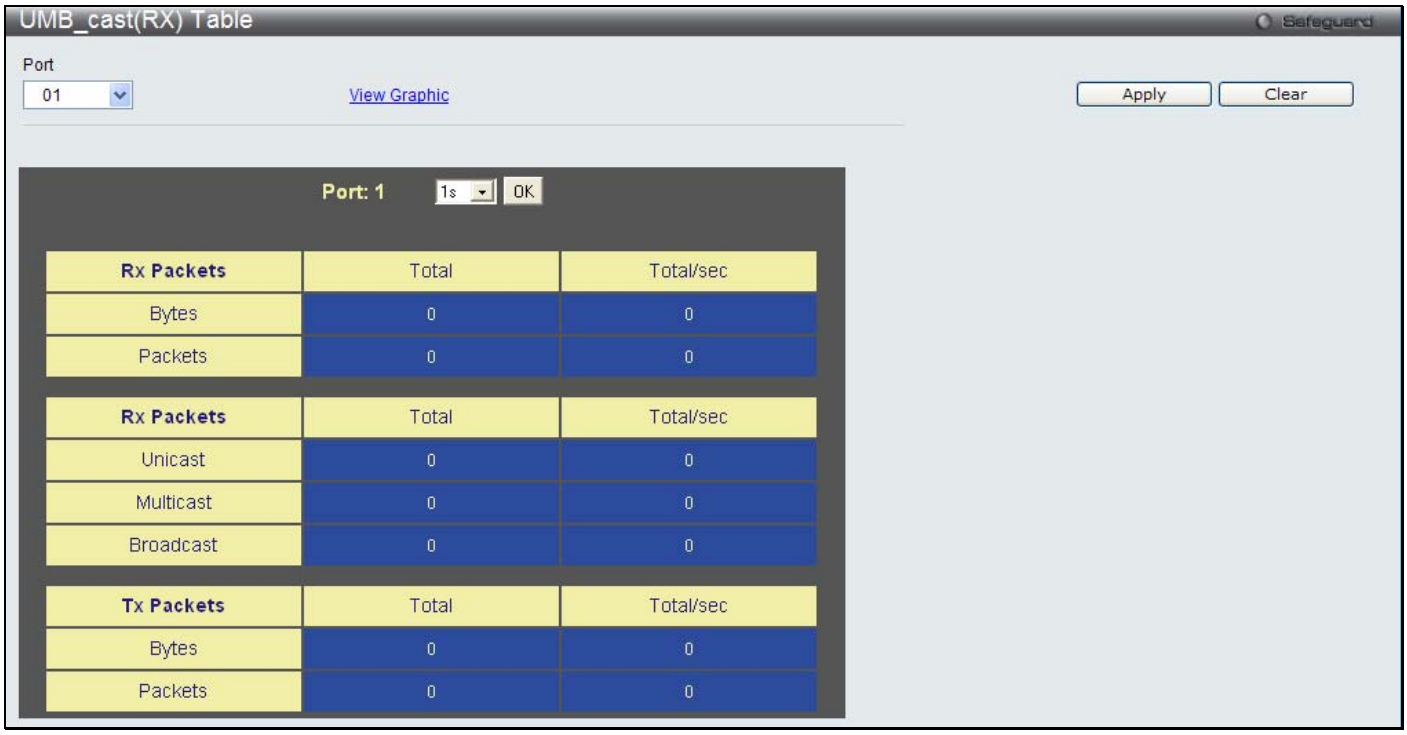


Figure 11- 9. UMB_cast (RX) Table window (for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following graph of packets transmitted from the Switch Click **Monitoring** > **Packets** > **Transmitted (TX)**.

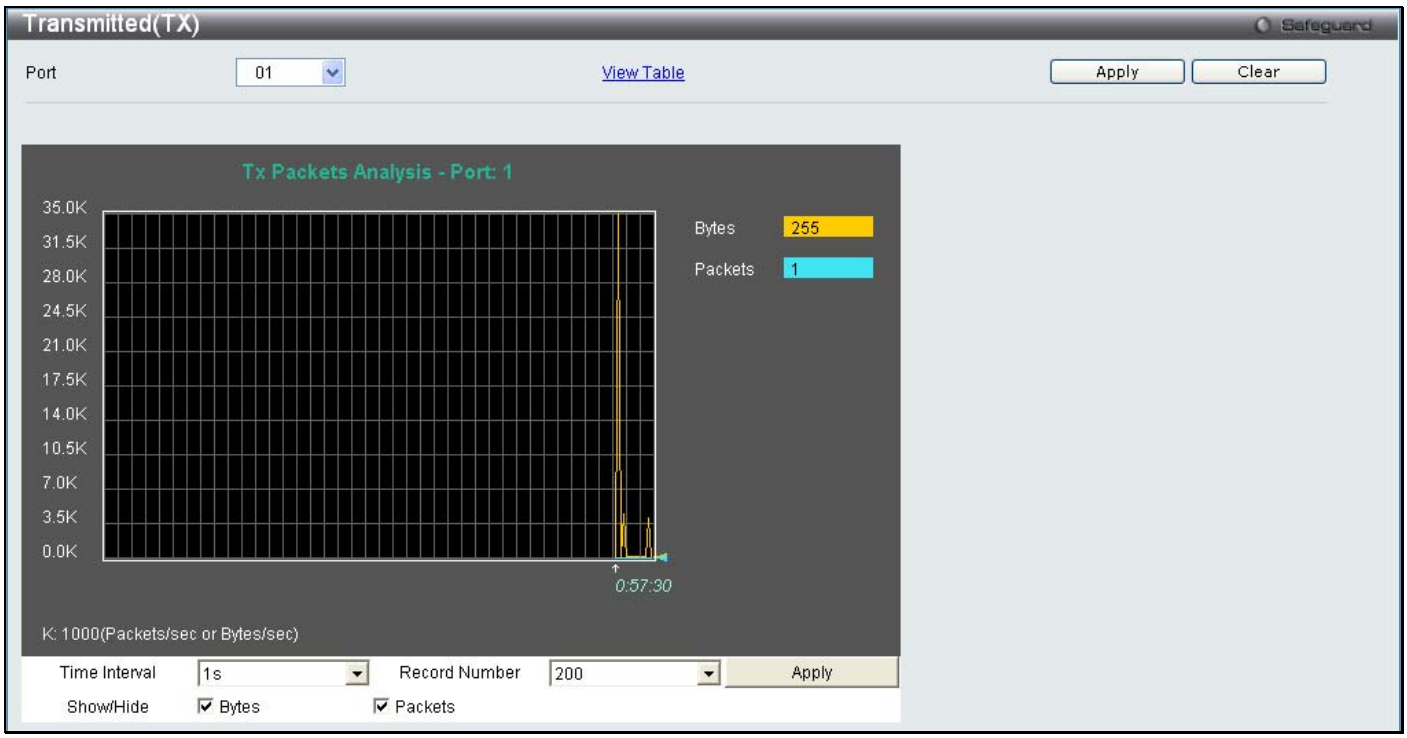


Figure 11- 10. Transmitted (TX) window (for Bytes and Packets)

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

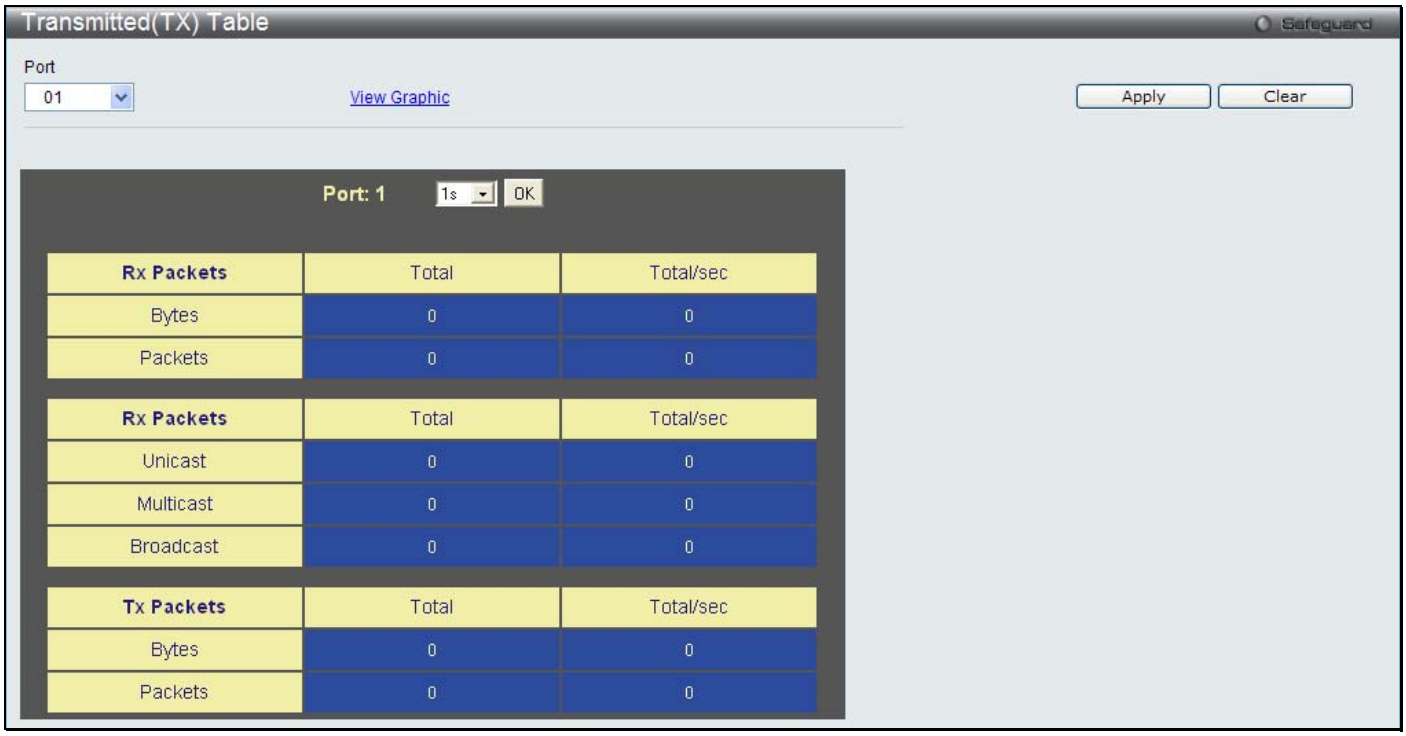


Figure 11- 11. Transmitted (TX) Table window (for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following graph of error packets received on the Switch Click **Monitoring** > **Errors** > **Received (RX)**.

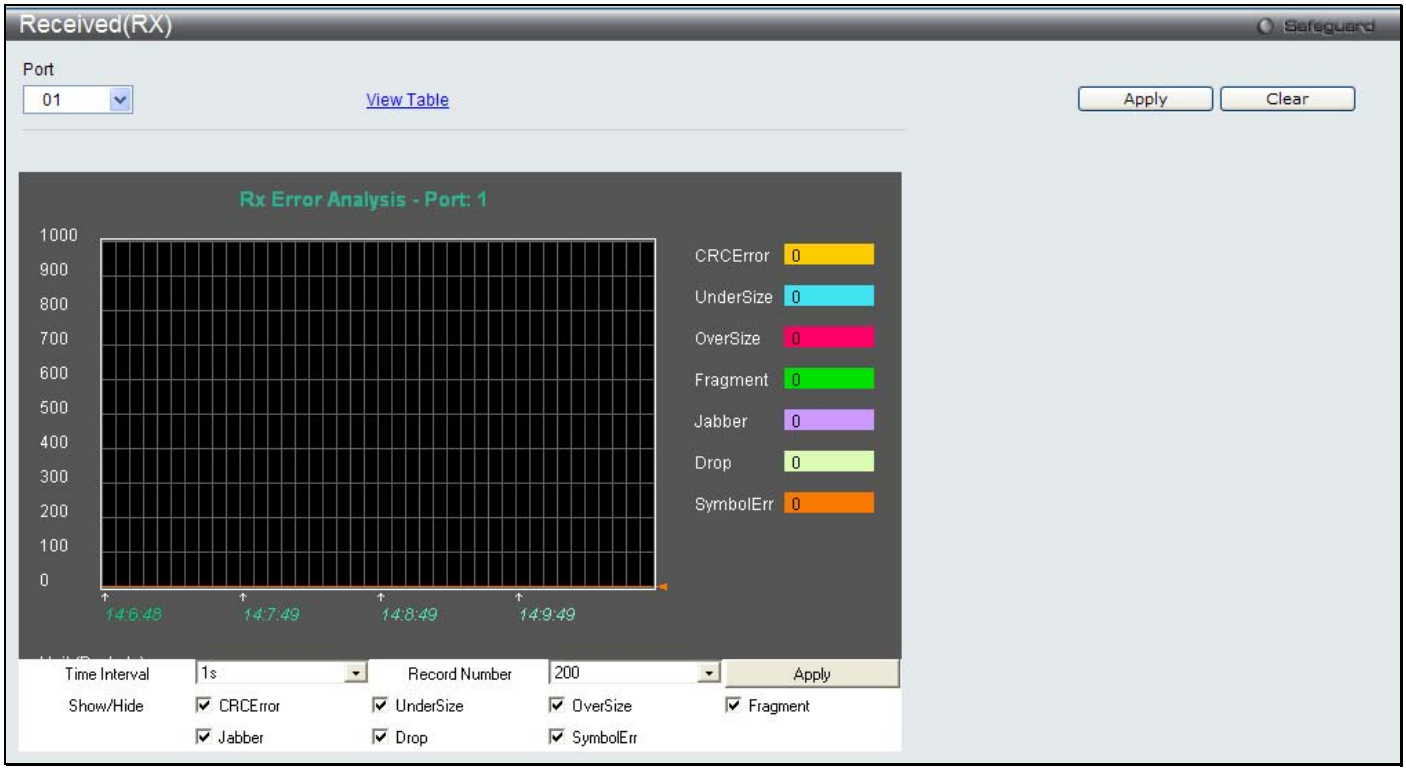


Figure 11- 12. Received (RX) window (for errors)

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

Figure 11- 13. Received (RX) Table window (for errors)

The following fields can be set:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Symbol	Counts the number of packets received that have errors received in the symbol on the physical labor.
Show/Hide	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.
Clear	Clicking this button clears all statistics counters on this window.

View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view the following graph of error packets received on the Switch Click the **Monitoring** > **Errors** > **Transmitted (TX)**

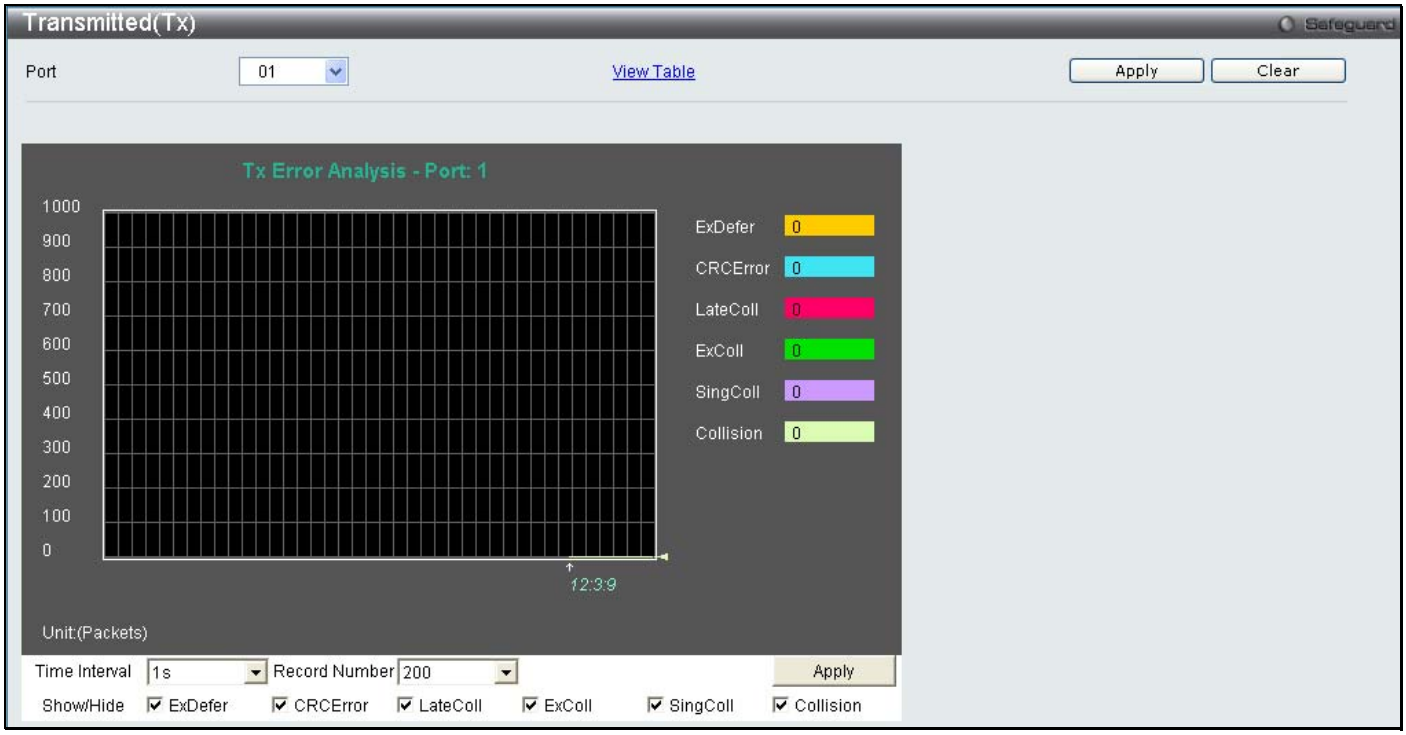


Figure 11- 14. Transmitted (TX) window (for errors)

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

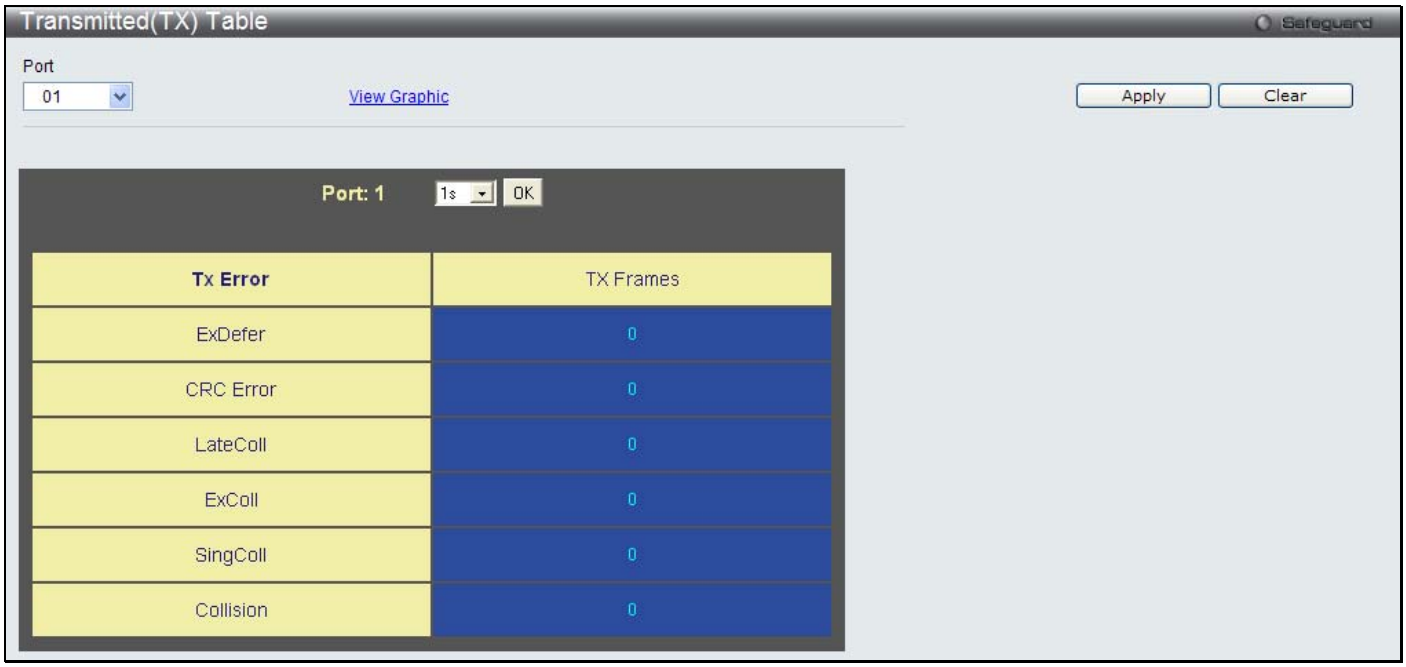


Figure 11- 15. Transmitted (TX) Table window (for errors)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Port Access Control

The following windows are used to monitor 802.1X statistics of the Switch, on a per port basis. To view the **Port Access Control** windows, open the **Monitoring** folder and click **Port Access Control**. There are seven monitoring windows in this section.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view the **RADIUS Authentication** window, click **Monitoring > Port Access Control > RADIUS Authentication**.

Figure 11- 16. RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following information is displayed:

Parameter	Description
InvalidServerAddresses	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or

	Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

RADIUS Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view the **RADIUS Account Client** window, click **Monitoring > Port Access Control > RADIUS Account Client**.

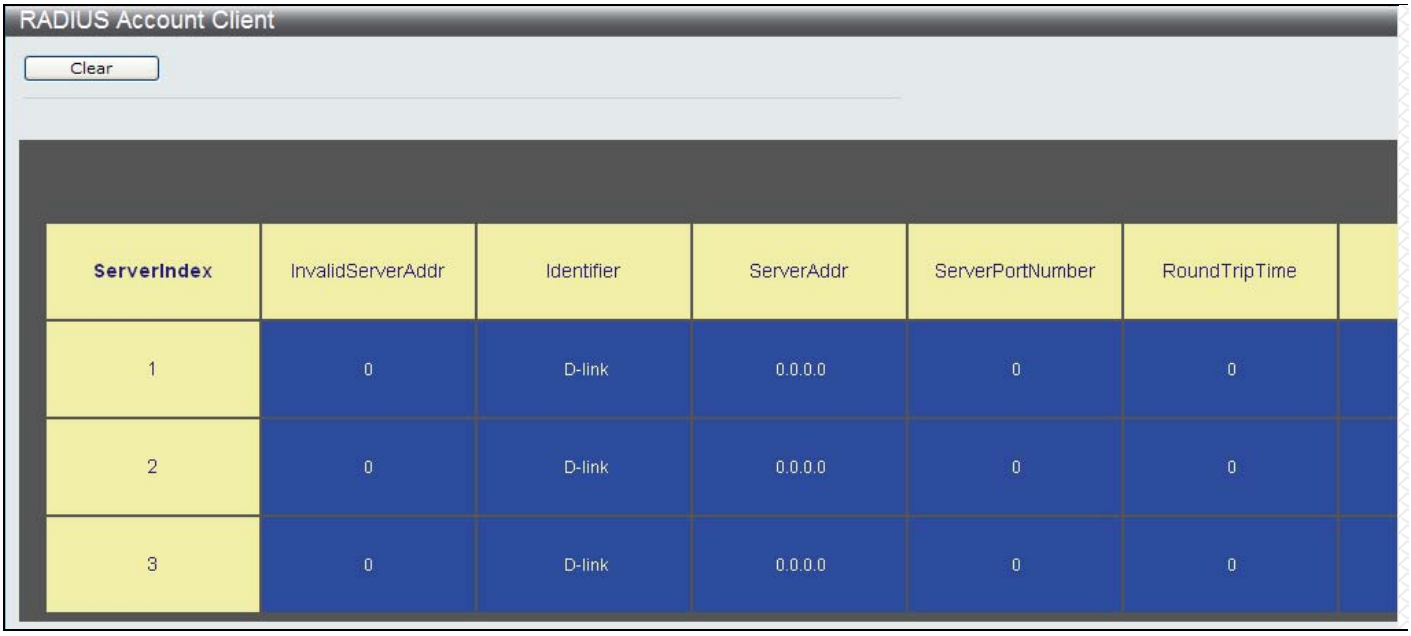


Figure 11- 17. RADIUS Account Client window

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
ClientInvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
ClientIdentifier	The NAS-Identifier of the RADIUS accounting client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
ServerAddress	The (conceptual) table listing the RADIUS accounting servers with which the client

	shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
ClientRoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
ClientRequests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
ClientRetransmissions	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.
ClientResponses	The number of RADIUS packets received on the accounting port from this server.
ClientMalformedResponses	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.
ClientBadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
ClientPendingRequests	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.
ClientTimeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
ClientUnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
ClientPacketsDropped	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 the Authenticator State, click **Monitoring > Port Access Control > Authenticator State**.

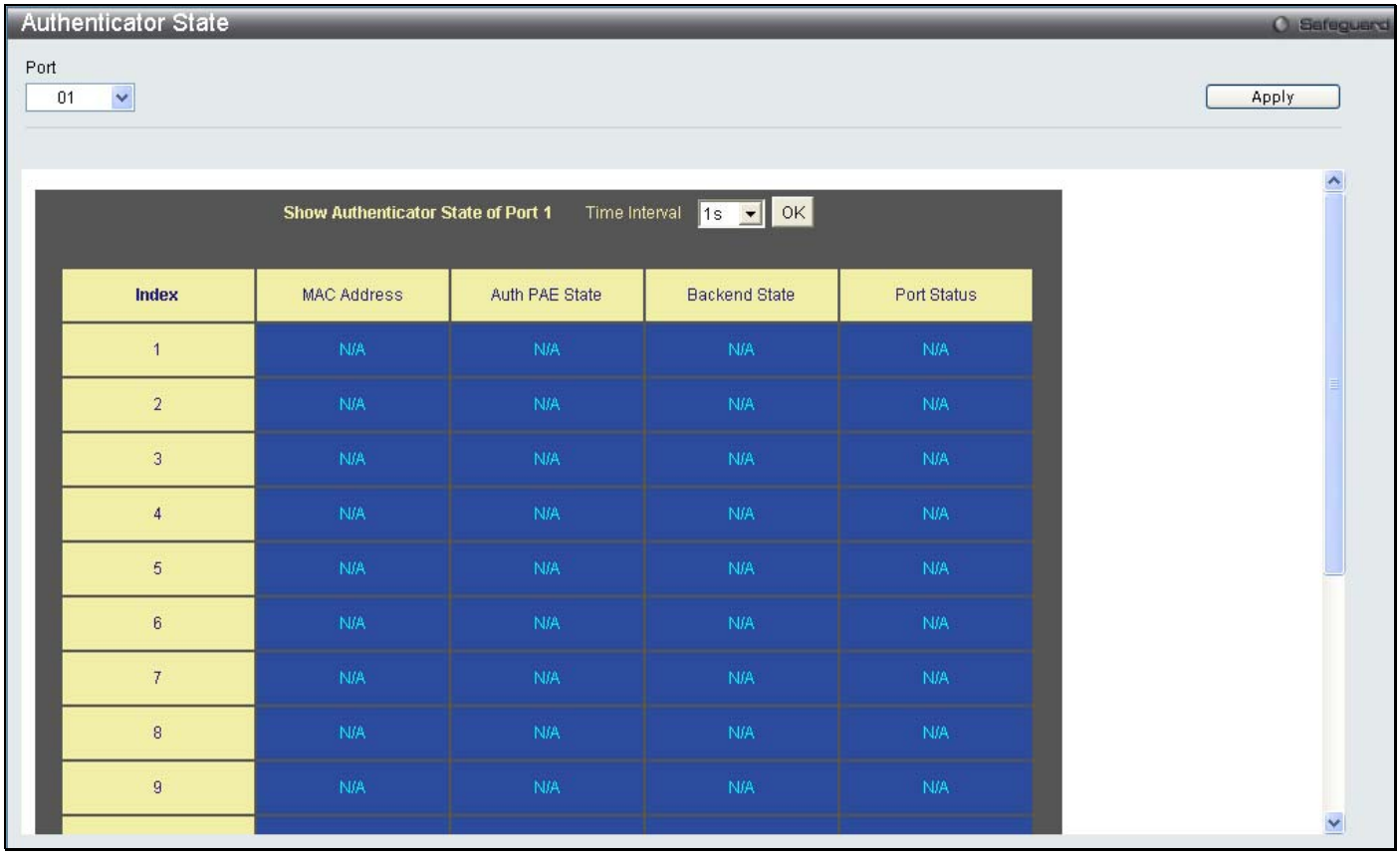


Figure 11- 18. Authenticator State window (for MAC-based 802.1X)

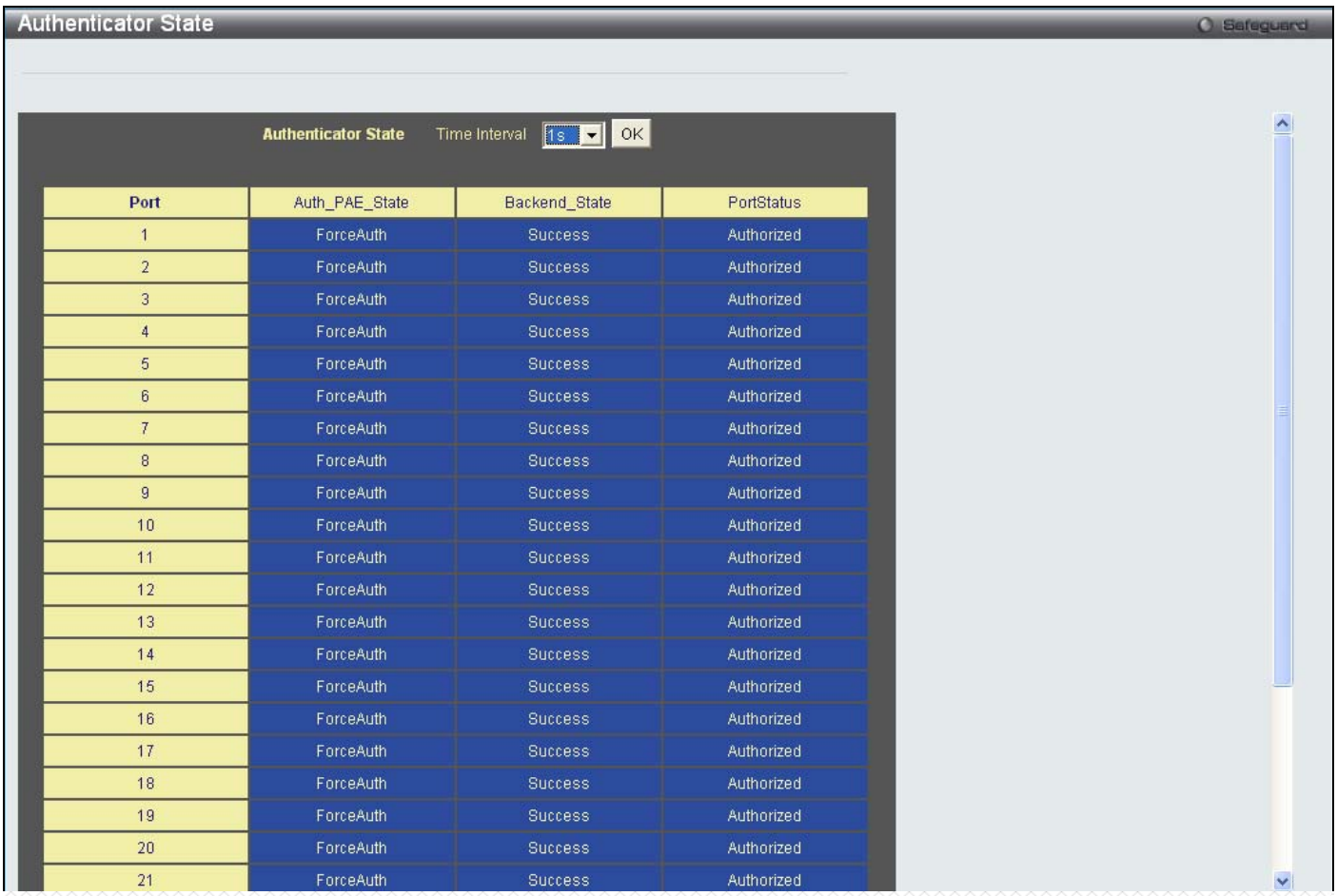


Figure 11- 19. Authenticator State window (for Port-based 802.1X)

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
MAC Address	The MAC Address of the device of the corresponding index number.
Auth PAE State	The Authenticator PAE State value can be: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Backend State	The Backend Authentication State can be Request, Response, Success, Fail, Timeout, Idle, Initialize, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be Authorized, Unauthorized, or N/A.

Authenticator Statistics

This window contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the Authenticator Statistics, click **Monitoring > Port Access Control > Authenticator Statistics**:

Figure 11- 20. Authenticator Statistics window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of valid EAPOL frames that have been received by this Authenticator.
Frames Tx	The number of EAPOL frames that have been transmitted by this Authenticator.
Rx Start	The number of EAPOL Start frames that have been received by this Authenticator.
TxReqId	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
RxLogOff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Tx Req	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Rx RespId	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx Resp	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx Error	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Last Version	The protocol version number carried in the most recently received EAPOL frame.
Last Source	The source MAC address carried in the most recently received EAPOL frame.

Authenticator Session Statistics

This window contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Session Statistics** window, click **Monitoring > Port Access Control > Authenticator Session Statistics**.

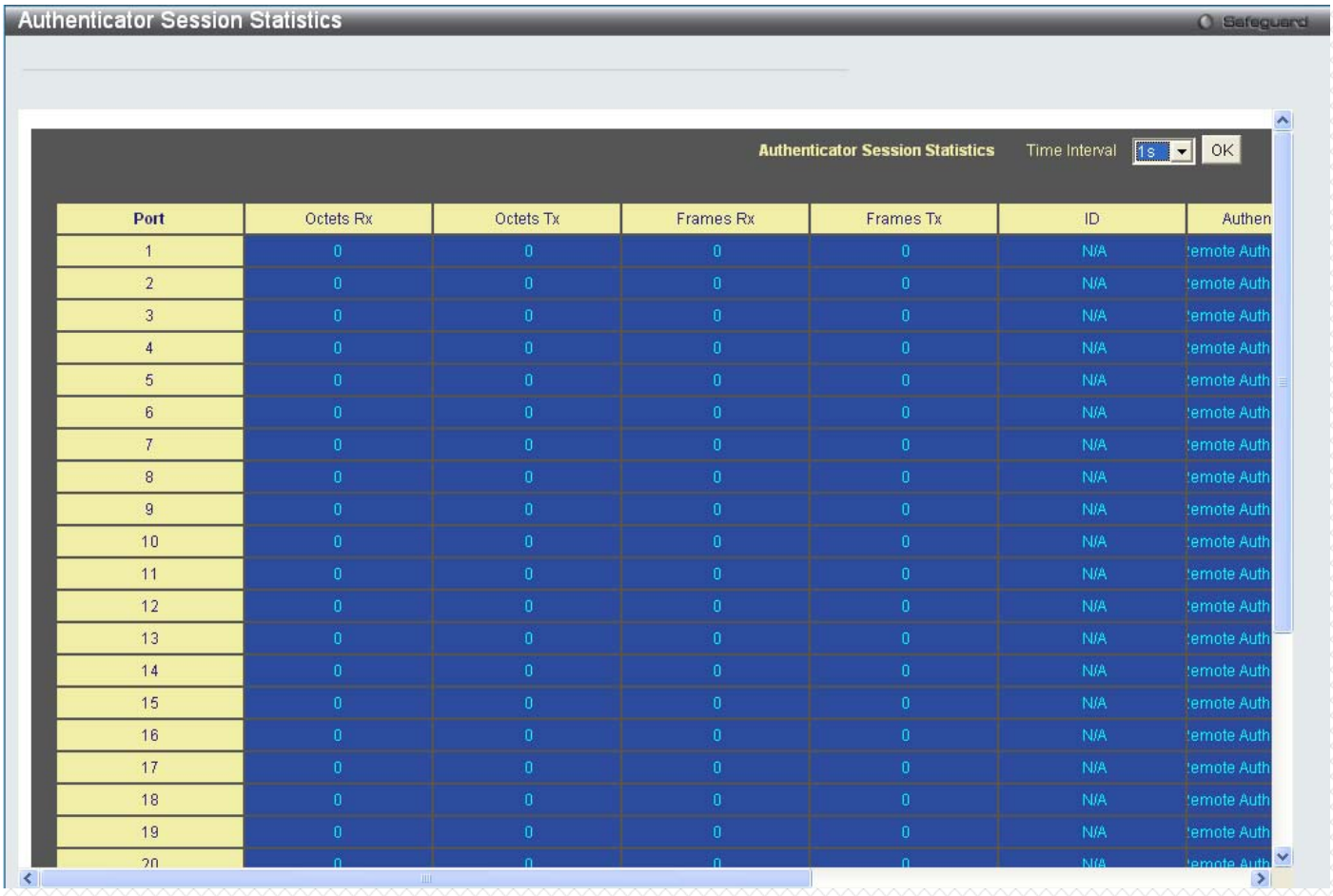


Figure 11- 21. Authenticator Session Statistics window

The user may select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Octets Rx	The number of octets received in user data frames on this port during the session.
Octets Tx	The number of octets transmitted in user data frames on this port during the session.
Frames Rx	The number of user data frames received on this port during the session.
Frames Tx	The number of user data frames transmitted on this port during the session.
ID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
Authentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server - The Authentication Server is external to the Authenticator's System. (2) Local Authentic Server - The Authentication Server is located within the Authenticator's

	System.
Time	The duration of the session in seconds.
Terminate Cause	The reason for the session termination. There are eight possible reasons for termination. 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
UserName	The User-Name representing the identity of the Supplicant PAE.

Authenticator Diagnostics

This window contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Diagnostics** window, click **Monitoring > Port Access Control > Authenticator Diagnostics**.

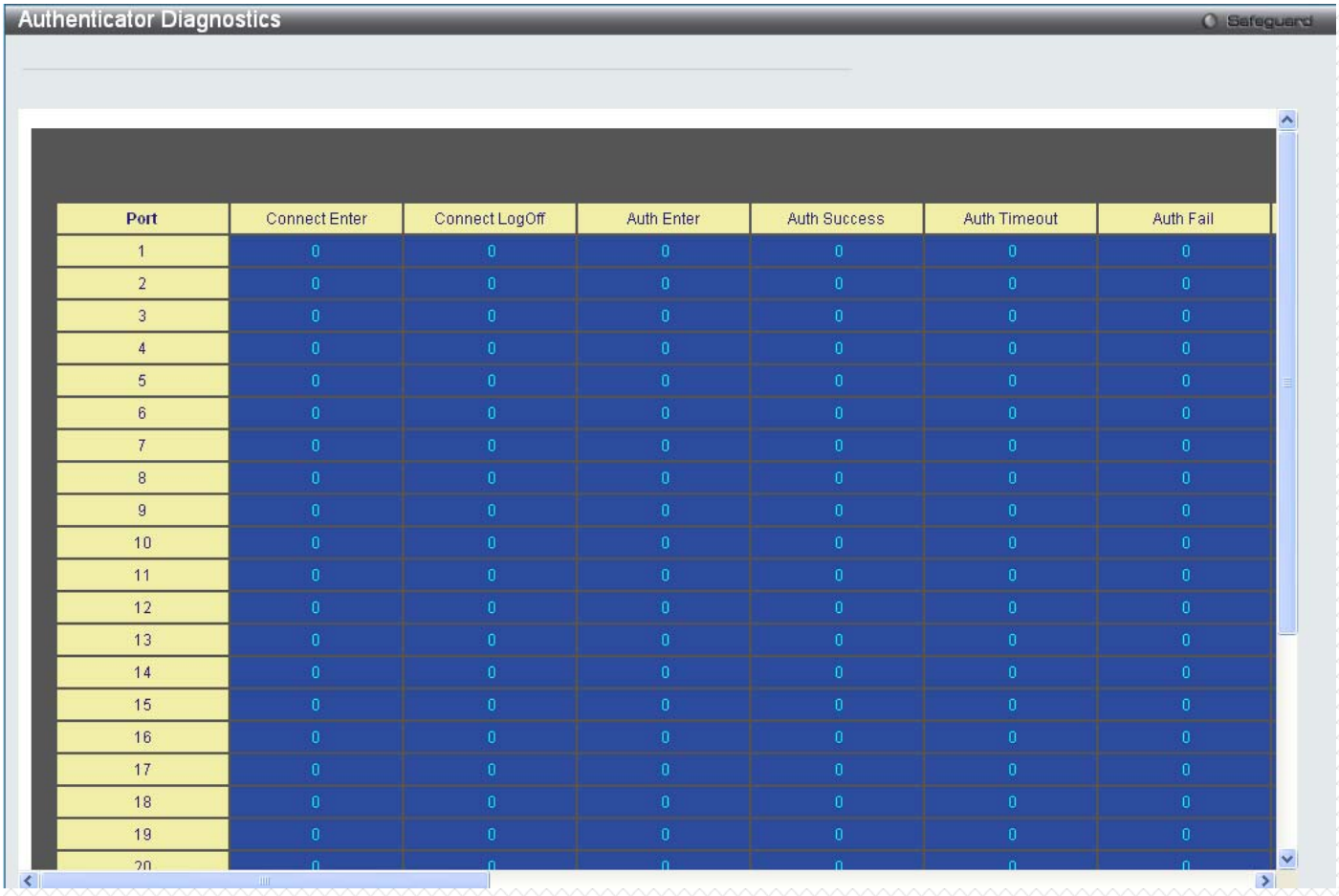


Figure 11- 22. Authenticator Diagnostics window

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Connect Enter	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
Connect LogOff	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
Auth Enter	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
Auth Success	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
Auth Timeout	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
Auth Fail	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).
Auth Reauth	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Auth Start	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
Auth LogOff	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
Authed Reauth	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Authed Start	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
Authed LogOff	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
Responses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
AccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
OtherReqToSupp	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
NonNakRespFromSup	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.

Bac Auth Success	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
Bac Auth Fail	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

Browse ARP Table

This window displays current ARP entries on the Switch. To search a specific ARP entry, enter an Interface Name or an IP Address at the top of the window and click **Find**. Click the **Show Static** button to display static ARP table entries. To clear the ARP Table, click **Clear All**.

The view the **Browse ARP Table** window, click **Monitoring** > **Browse ARP Table**.

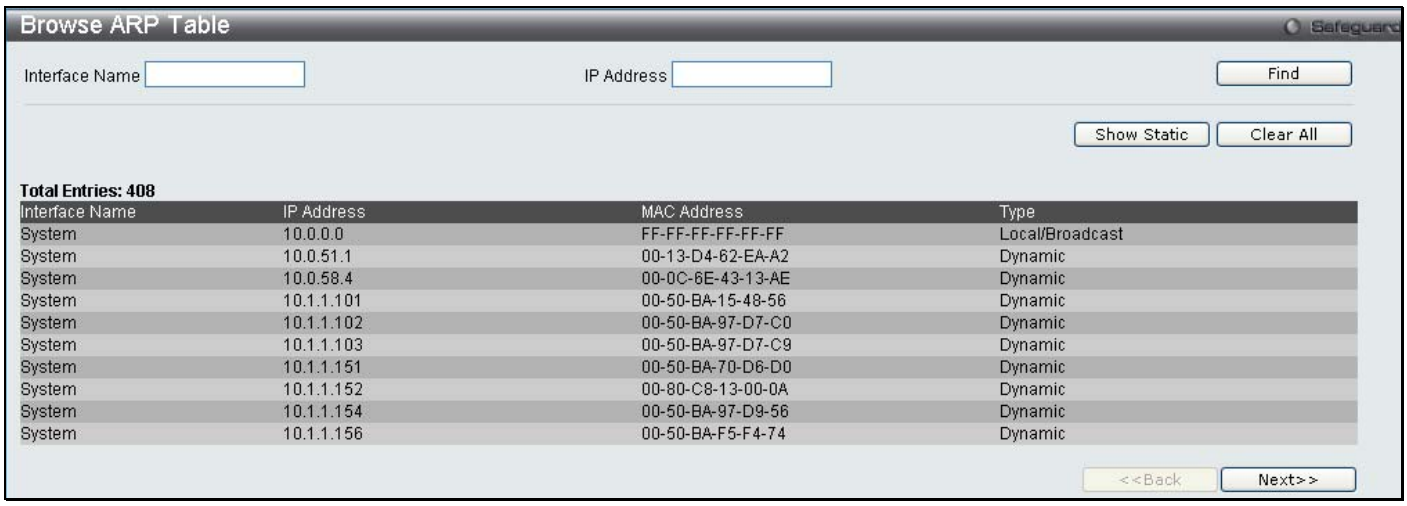


Figure 11- 23. Browse ARP Table window

Browse VLAN

This window allows the VLAN status for each of the Switch's ports to be viewed by VLAN. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button.

To view the **Browse VLAN** click, **Monitoring** > **Browse VLAN**.

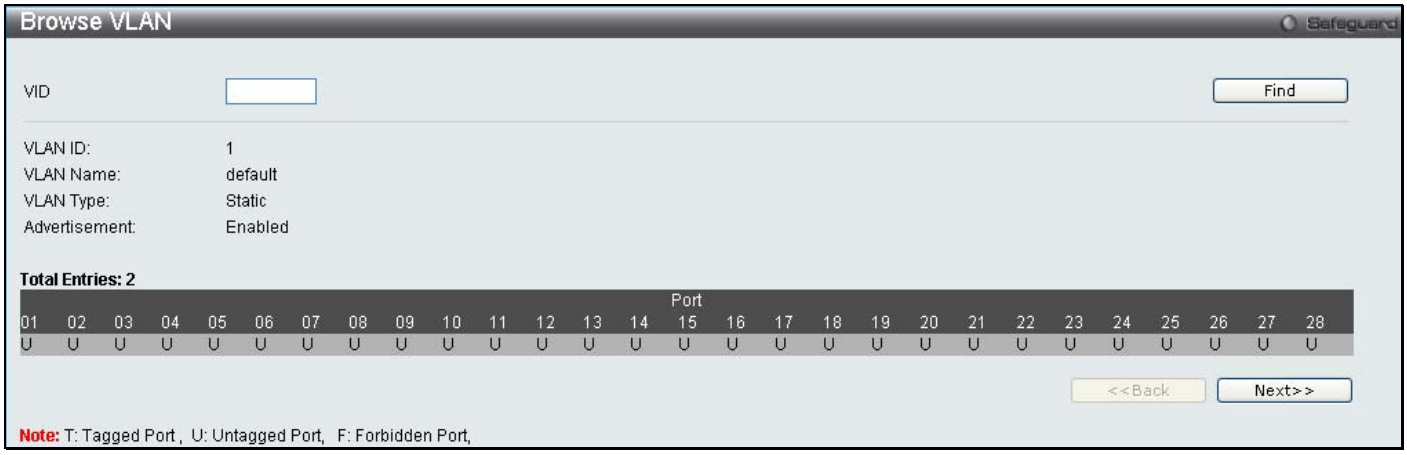


Figure 11- 24. Browse VLAN window

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 the **Browse VLAN** click, **Monitoring** > **Show VLAN Ports.**

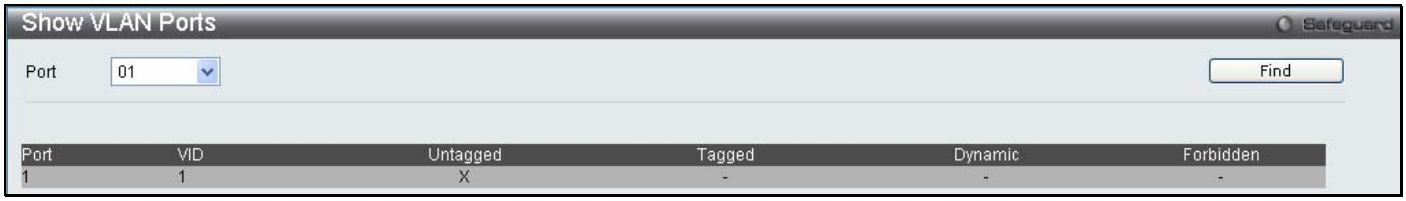


Figure 11- 25. Browse VLAN window

Browse 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 the **Browse Router Port** window, click, **Monitoring** > **Browse Router Port**.

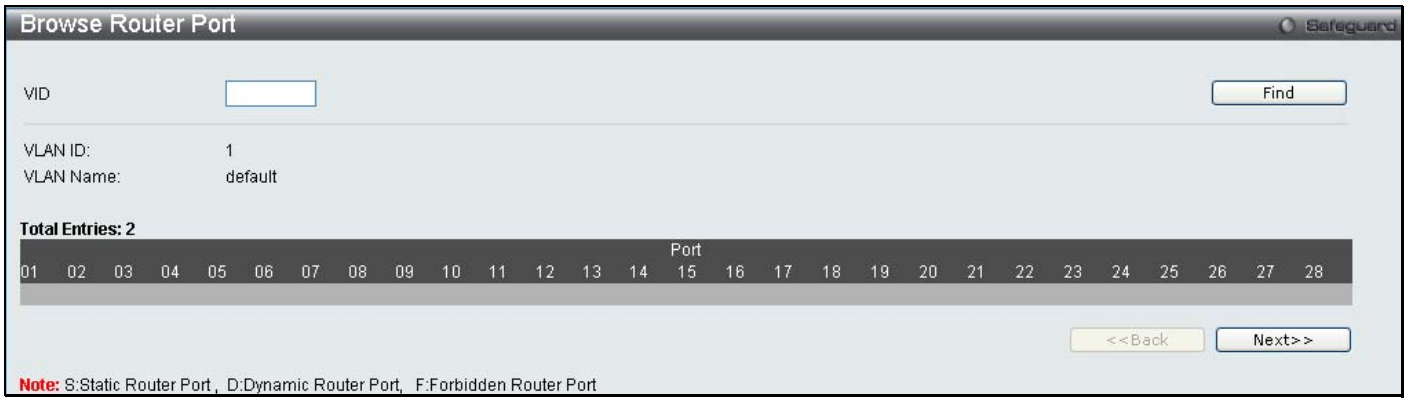


Figure 11- 26. Browse Router Port window

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 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 the **Browse MLD Router Port** window, click **Monitoring** > **Browse MLD Router Port**.

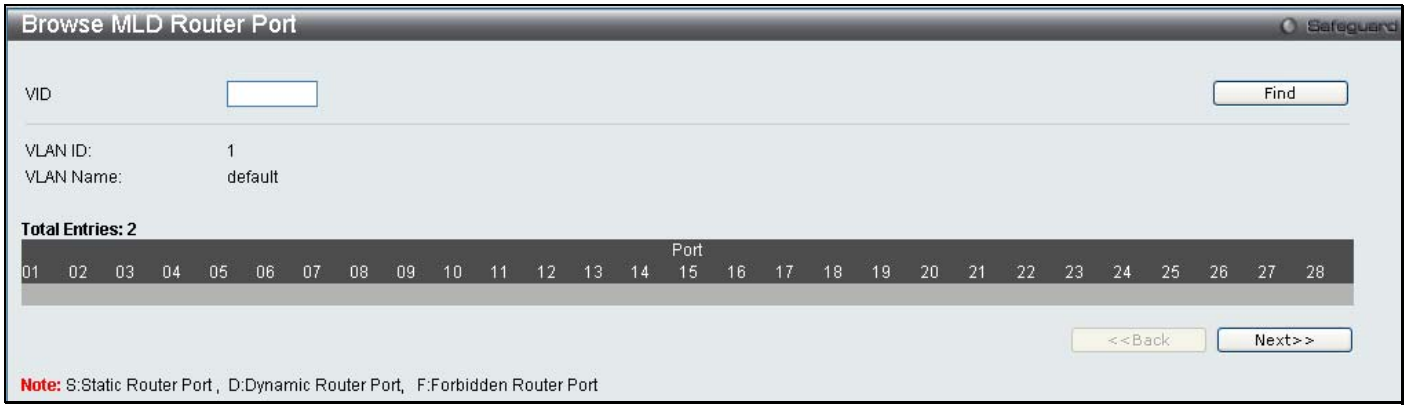


Figure 11- 27. Browse MLD Router Port window

Browse Session Table

This window displays the management sessions since the Switch was last rebooted.

To view the **Browse Session Table** window, click **Monitoring** > **Browse Session Table**.

Figure 11- 28. Browse Session Table 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 the **IGMP Snooping Group** window, click **Monitoring** > **IGMP Snooping Group**.

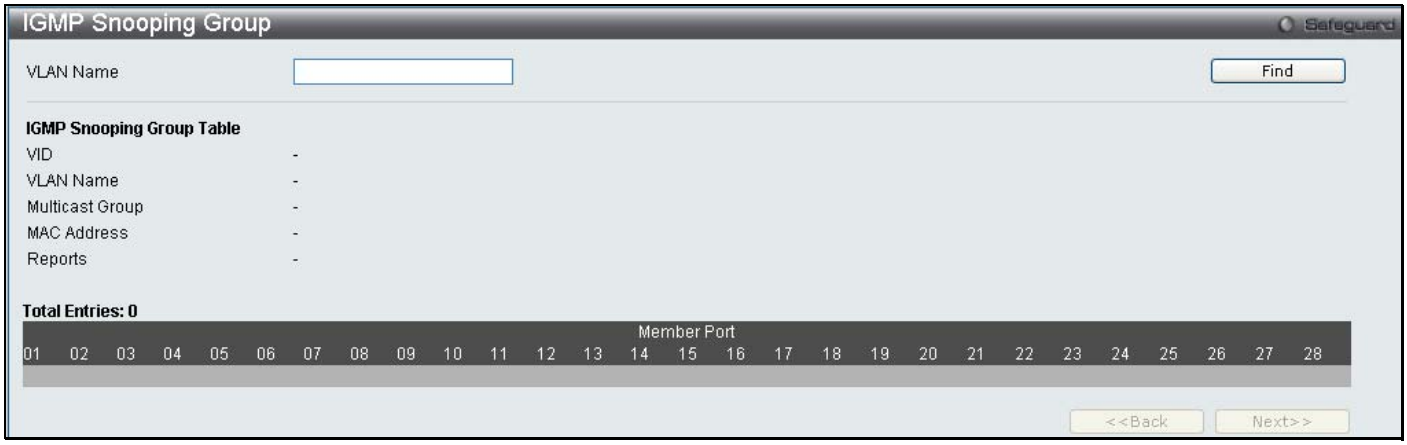


Figure 11- 29. IGMP Snooping Group window

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

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN ID of the multicast group.
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Reports	The total number of reports received for this group.

NOTE: To configure IGMP snooping for the Switch, go to the **L2 Features** folder and select **IGMP Snooping** > **IGMP Snooping Settings**.

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 the **MLD Snooping Group** window, click **Monitoring** > **MLD Snooping Group**.

Figure 11- 30. MLD Snooping Group window

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN name of the MLD multicast group.
Multicast Group	The IP address of the MLD multicast group.
MAC Address	The MAC address of the MLD multicast group.
Reports	The total number of reports received for this group.

NOTE: To configure MLD snooping for the Switch, go to the **L2 Features** folder and select **MLD Snooping** > **MLD Snooping Settings**.

JWAC Host Table

To view the **JWAC Host Table** window, click, **Monitoring** > **JWAC Host Table**.

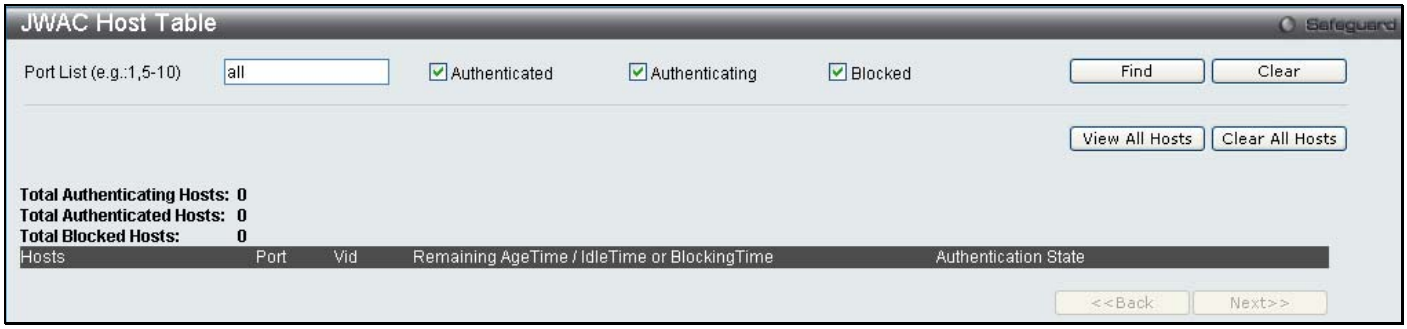


Figure 11- 31. JWAC Host Table window

MAC Address Table

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

To view the **MAC Address Table** window, click **Monitoring** > **MAC Address Table**.

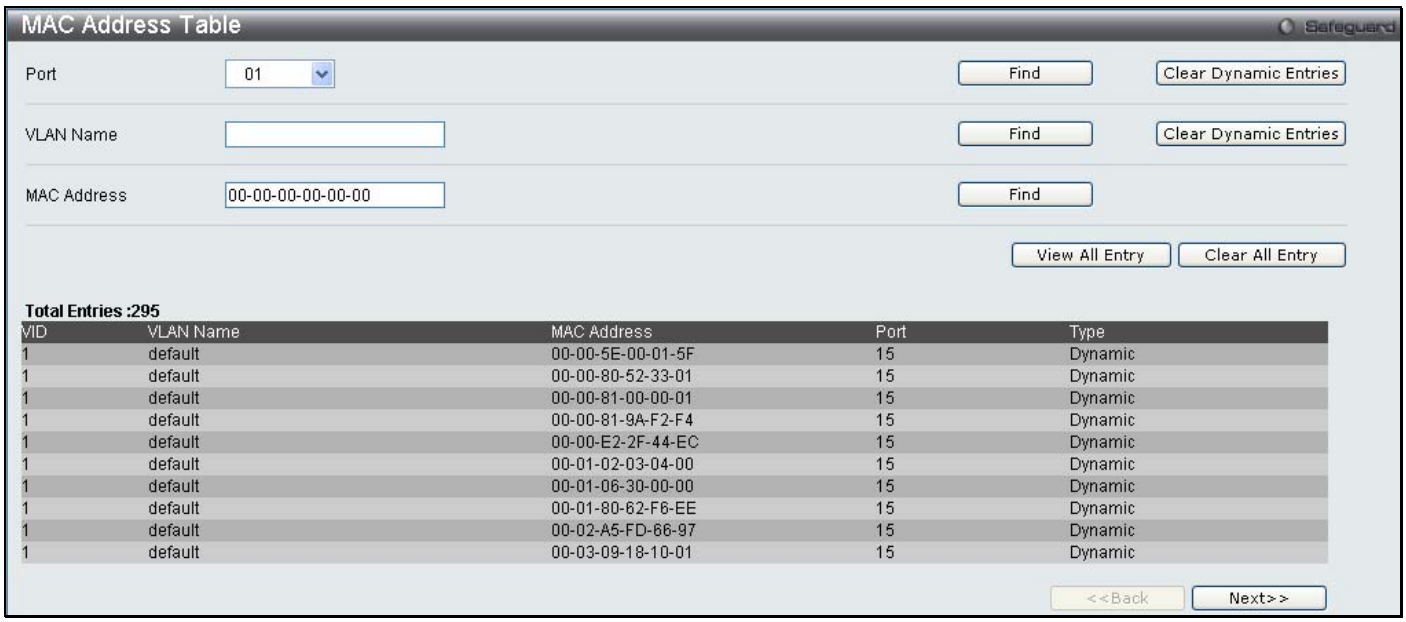


Figure 11- 32. MAC Address Table window

The functions used in the MAC address table are described below:

Parameter	Description
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
Clear Dynamic Entries	Clicking this button will allow the user to delete alll dynamic entries of the address table.
View All Entry	Clicking this button will allow the user to view all entries of the address table.
Clear All Entry	Clicking this button will allow the user to delete all entries of the address table.

System Log

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

To view the Switch history log, Click **Monitoring** > **System Log**:

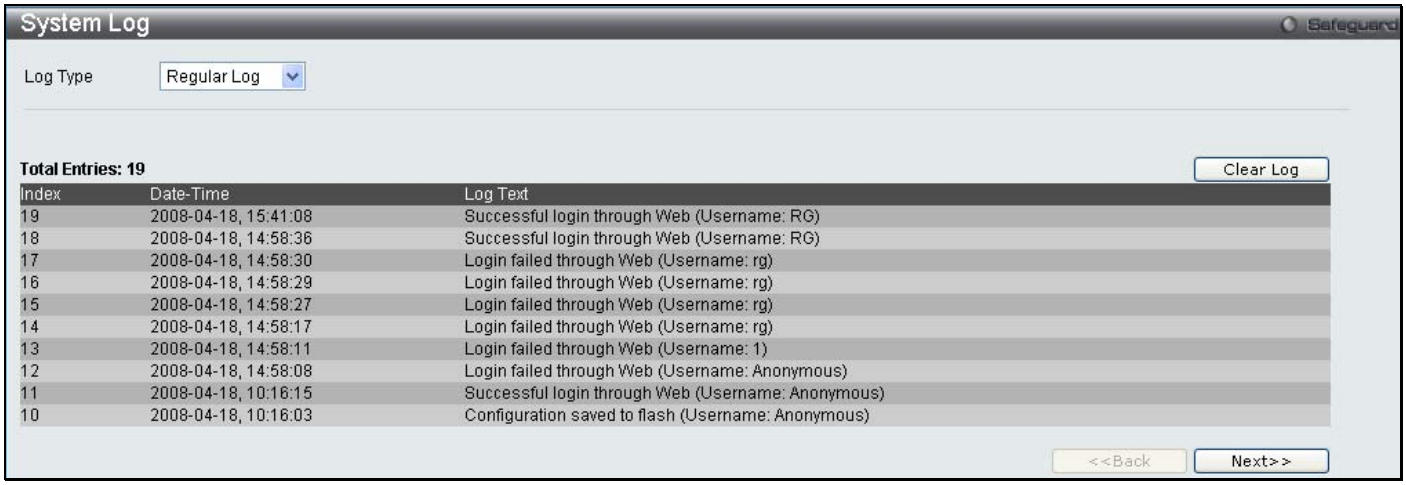


Figure 11- 33. System Log window

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** will allow the user to clear the Switch History Log.

The information in the table is categorized as:

Parameter	Description
Type	Choose the type of log to view. There are two choices: *Regular Log* – Choose this option to view regular switch log entries, such as logins or firmware transfers. *Attack Log* – Choose this option to view attack log files, such as spoofing attacks.
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Date-Time	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

Section 12

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:

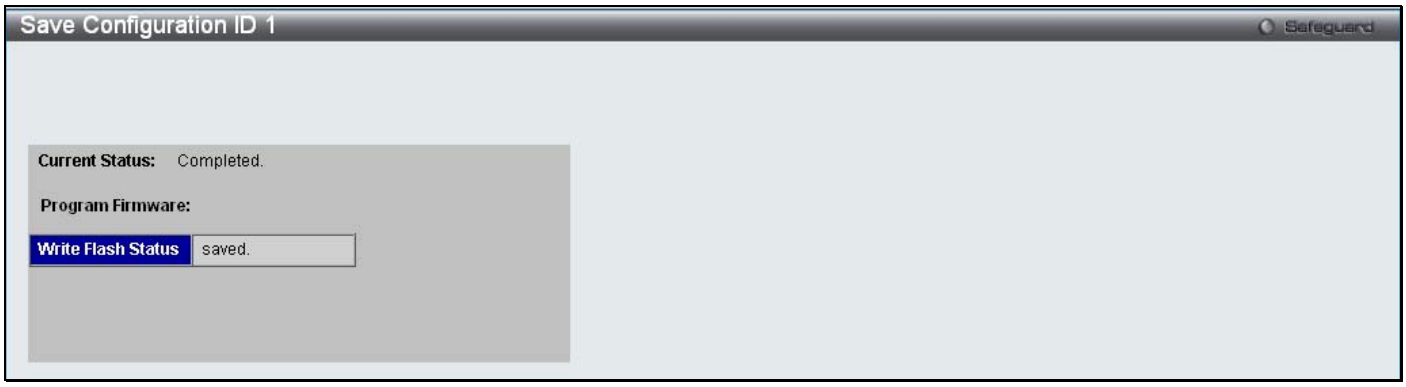


Figure 12- 1. Save Configuration ID 1 window

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:

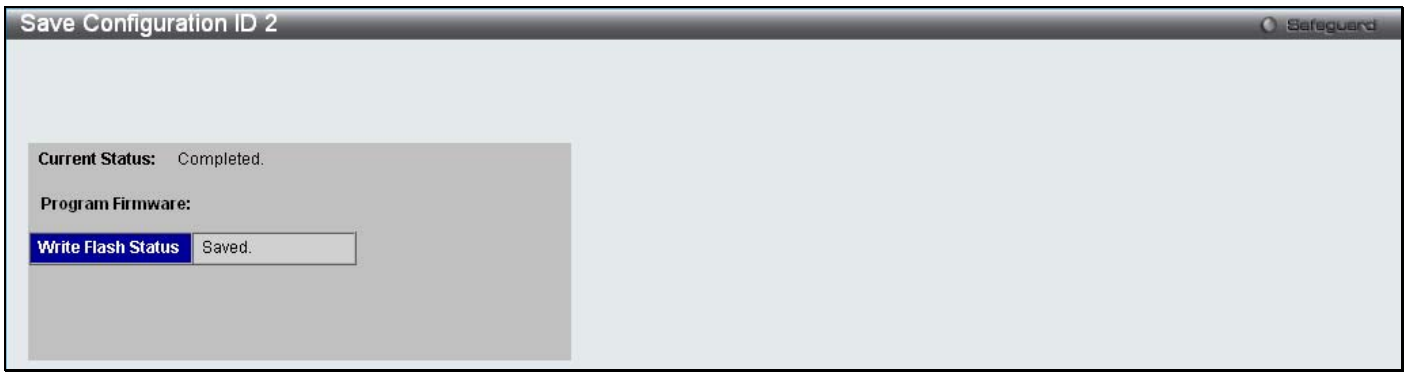


Figure 12- 2. Save Configuration ID 2 window

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 12- 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:

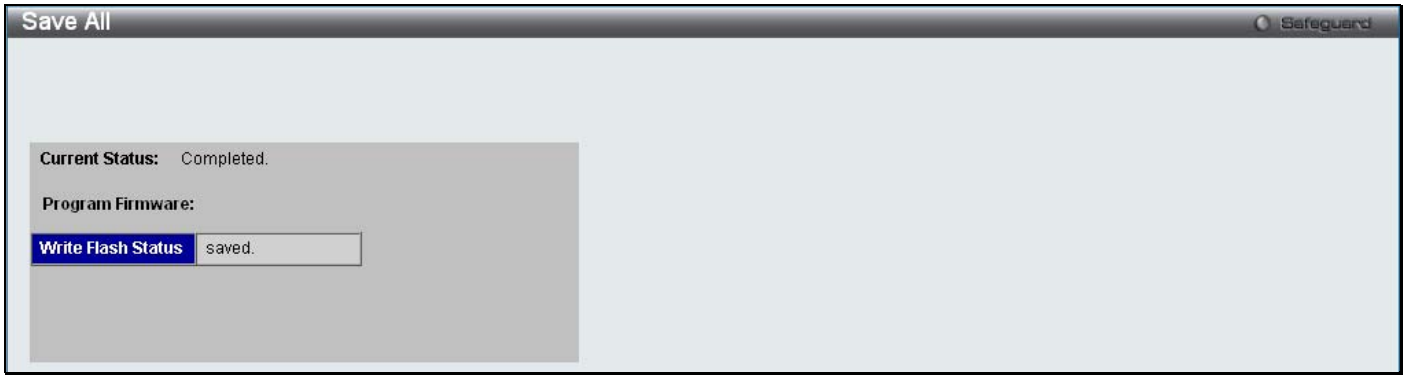


Figure 12- 4. Save All window

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, file/path name, desired Configuration ID, and click **Backup**.

To restore the configuration file, enter the Server IP, file/path name, desired Configuration ID, and click **Restore**.

Figure 12- 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 and file/path name and then click **Upload** or **Upload Attack Log**.

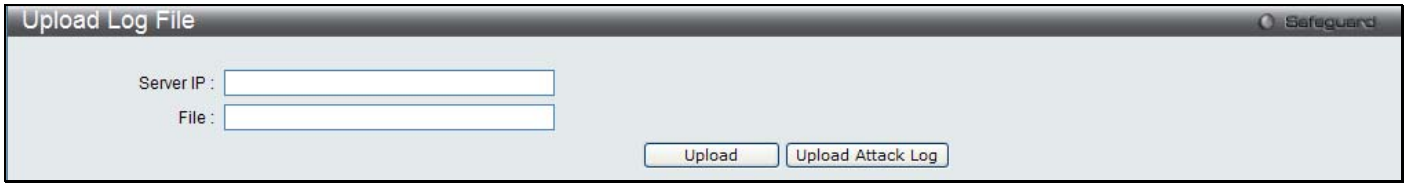


Figure 12- 6. Upload Log File window

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.

Figure 12- 7. Reset System window

Download Firmware

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

Figure 12- 8. Download Firmware window

Enter the Server IP address in the first field and and specify the path/file name of the firmware in the second field. Click **Download** to initiate the file transfer.

Reboot System

The following window is used to restart the Switch.

Figure 12- 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

Technical Specifications

General	
Protocols	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Gibabit Ethernet. (SFP “Mini GBIC”) IEEE 802.1D Spanning Tree IEEE 802.1D/S/W Spanning Tree IEEE 802.1Q VLAN IEEE 802.1p Priority Queues IEEE 802.1X Port Based Network Access Control IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 NWay auto-negotiation
Fiber-Optic	SFP Support: DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX) DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DEM-312GT2 (1000BASE-LX) DEM-210 (Single Mode 100BASE-FX) DEM-211 (Multi Mode 100BASE-FX) WDM Transceivers Supported: DEM-330T (TX-1550/RX-1310nm), up to 10km, Single-Mode DEM-330R (TX-1310/RX-1550nm), up to 10km, Single-Mode DEM-331T (TX-1550/RX-1310nm), up to 40km, Single-Mode DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode
Standards	CSMA/CD
Data Transfer Rates: **Ethernet** **Fast Ethernet** **Gigabit Ethernet**	Half-duplex Full-duplex 10 Mbps 20Mbps 100Mbps 200Mbps n/a 2000Mbps
Topology	Star
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports	24 x 10/100Base-T Ports 2 x 1000Base-T/SFP Combo Ports 2 x 1000Base-T ports

Physical and Environmental	
Internal Power Supply	Input: 100~240V, AC/1.5A, 50~60Hz Output: 12V, 5A (Max)
Power Consumption	Max. 20.5 watts
Operating Temperature	0 - 45°C
Storage Temperature	-40 - 70°C
Humidity	Operation Relative Humidity: 20 - 80% non-condensing. Storage Relative Humidity: 10 – 90% non-condensing.
Dimensions	441(W) x 210(D) x 44(H) mm
Weight	2.51kg (5.53lbs)
EMI	CE Class A, FCC Class A, C-Tick, VCCI
Safety	CB Report, UL

LED indicators

Location	LED Indicative	Color	Status	Description
Per Device	**Power**	Green	Solid Light	Power On
			Light off	Power Off
	Console	Green	Solid Light	Console on
			Blinking	POST is in progress.
			Light off	Console off
	RPS	Green	Solid Light	RPS is in Use
			Light Off	RPS Off
	Master(MS)	Green	Solid Light	When the device is the stacking master.
			Light Off	Not the Stacking Master.
	Stacking ID	Green	Capable 1-8	The Box ID is assigned either by the user (static mode) or by the system (automatic mode). When the box becomes a primary master the 7 segment works as bu-function. That is box ID and “H” indicate as primary Master and the display will be shown by turn. That is boxID- > H -> boxID -> H…
LED Per 10/100 Mbps Port	**Link/Act/Speed**	Green/Amber	Solid Green	When there is a secure 100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a Fast Ethernet connected port.
			Solid Amber	When there is a secure 10Mbps Ethernet connection (or link) at any of the ports.

			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at an Ethernet connected port.
			Light off	No link
LED Per GE Port	**Link/Act/Speed mode for 1000BASE-T ports**	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 10/100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 10/100Mbps Fast Ethernet connected port.
			Light off	No link
	Link/Act/Speed mode for SFP ports	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 100Mbps connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at the ports.
			Light off	No link

Performance

Feature	Detailed Description
Wire speed on all FE/GE ports	Full-wire speed (full-duplex) operation on all FE/GE ports
Forwarding Mode	Store and Forward
Switching Capacity	12.8Gbps for DES-3528
64 Byte system packet forwarding rate	9.5 million packets per second for DES-3528
Priority Queues	8 Priority Queues per port
MAC Address Table	Supports 16K MAC address
Transmission Method	Store-and-forward
Packet Buffer	1 MB per device
Packet Filtering/Forward Rate	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1 Gbps port)
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

Port Functions

Feature	Detailed Description
Console Port	DCE RS-232 DB-9 for out-of-band configuration of the software features.
24 x 10/100BaseT ports	Compliant to following standards: • IEEE 802.3 compliance • IEEE 802.3u compliance • Support Half/Full-Duplex operations • All ports support Auto MDI-X/MDI-II cross over • IEEE 802.3x Flow Control support for Full-Duplex mode, Back Pressure when Half-Duplex mode, and Head-of-line blocking prevention. • Compliant IEEE802.3af standard(only for PoE)
2 Combo ports in the front panel	2 combo 1000BASE-T/SFP ports 1000BASE-T ports compliant to following standards: • IEEE 802.3 compliance • IEEE 802.3u compliance • IEEE 802.3ab compliance • Support Full-Duplex operations • IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention SFP Transceivers Supported: • DEM-310GT (1000BASE-LX) • DEM-311GT (1000BASE-SX) • DEM-314GT (1000BASE-LH) • DEM-315GT (1000BASE-ZX) • DEM-312GT2 (1000BASE-LX) • DEM-210 (Single Mode 100BASE-FX) • DEM-211 (Multi Mode 100BASE-FX) WDM Transceiver Supported: • DEM-330T (TX-1550/RX-1310nm),up to 10km,Single-Mode • DEM-330R (TX-1310/RX-1550nm), up to 10km,Single-Mode • DEM-331T (TX-1550/RX-1310nm), up to 40km, Single-Mode • DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode Compliant to following standards: • IEEE 802.3z compliance • IEEE 802.3u compliance

2 1000BASE-T ports in the rear panel	1000BASE-T ports compliant to following standards: • IEEE 802.3 compliance • IEEE 802.3u compliance • IEEE 802.3ab compliance • Support Full-Duplex operations • IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention

FE Port Pin Assignment for Data/Power Pairs: (alternative A MDI-X)

PIN#	Signal	Descriptions
1	Receive+	Positive Receive signal
2	Receive-	Negation Receive signal
3	Transmit+	Positive Transmit signal
4		
5		
6	Transmit-	Negation Transmit signal
7		
8		

Appendix B

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.

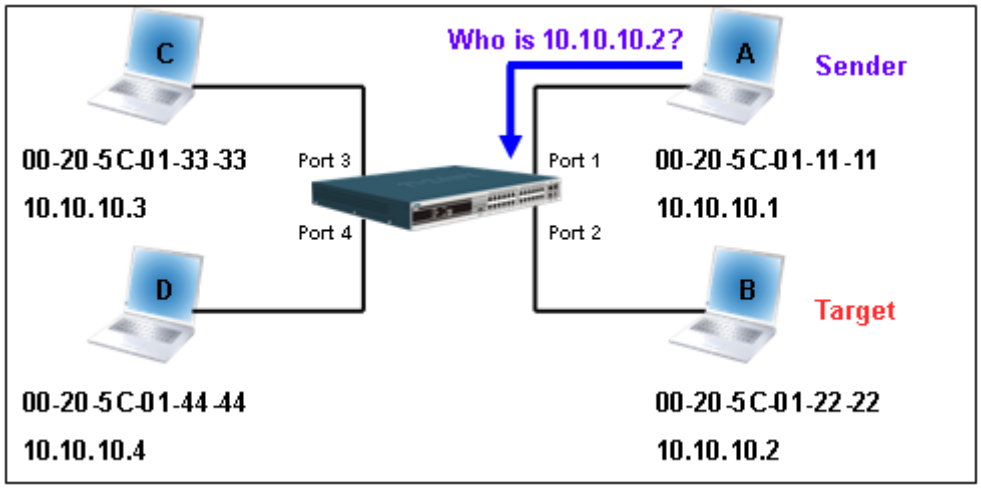


Figure-1

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	***10.10.10.1***	***00-00-00-00-00-00***	***10.10.10.2***

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 address	Source address	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	***00-20-5C-01-11-11***			

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.

Forwarding Table

Port1 00-20-5C-01-11-11

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).

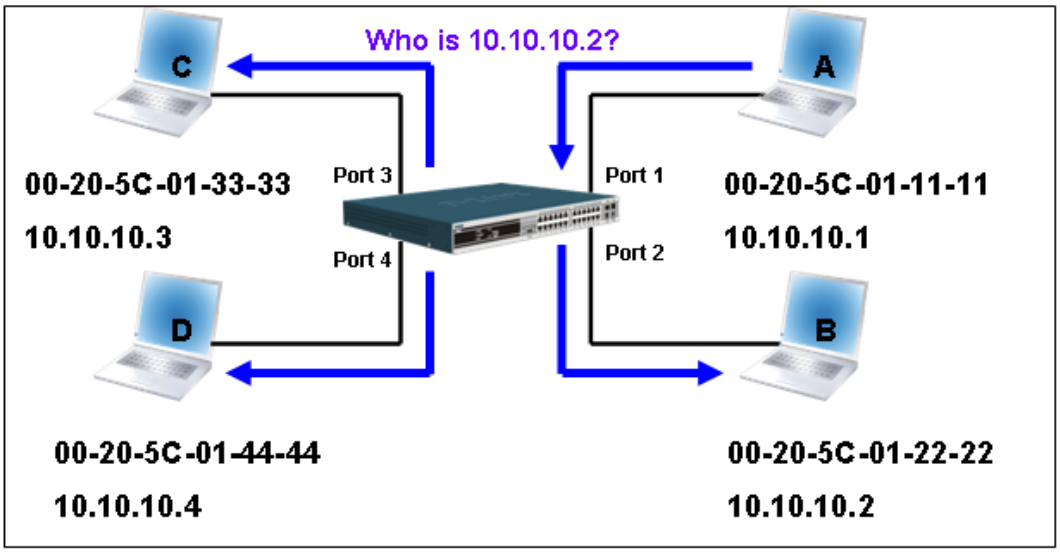


Figure - 2

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).

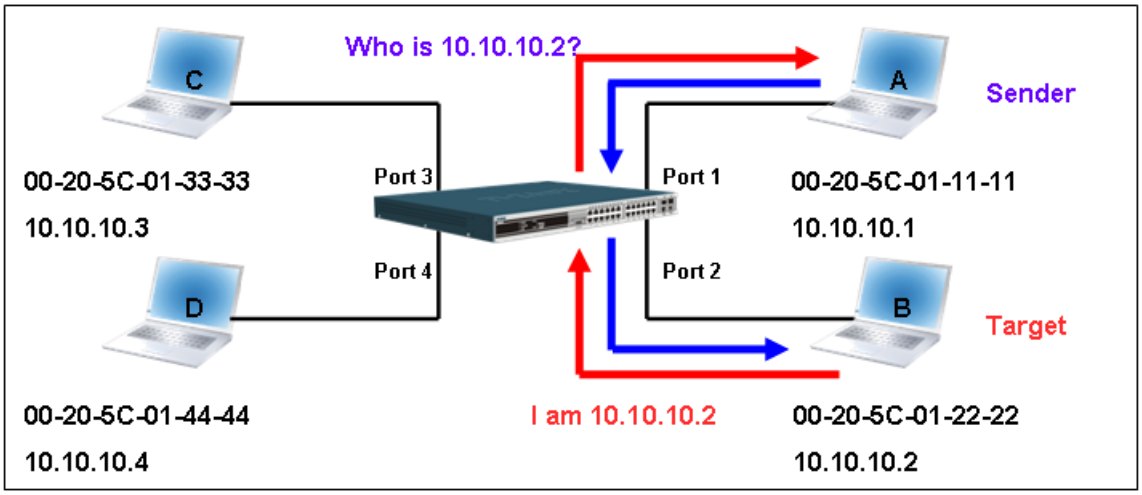


Figure-3

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	***00-20-5C-01-11-11***	***10.10.10.1***	***00-20-5C-01-22-22***	***10.10.10.2***

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
00-20-5C-01-11-11	***00-20-5C-01-22-22***			

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.

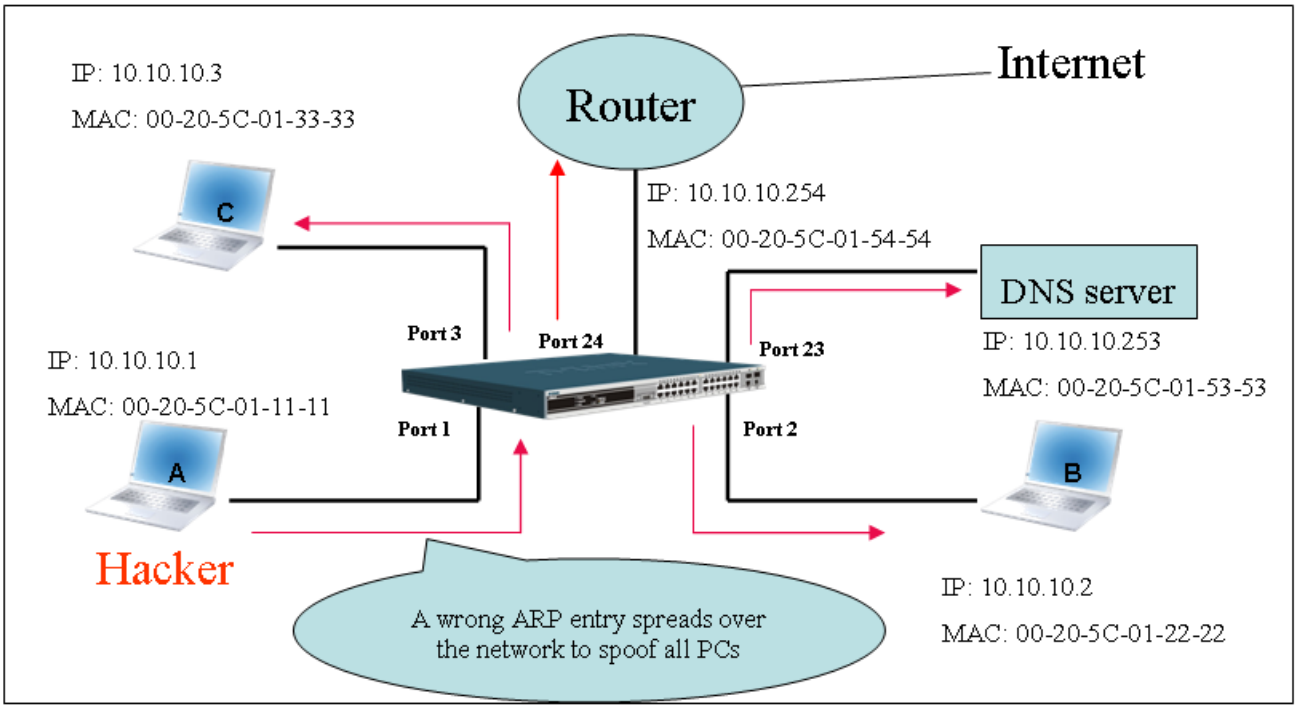


Figure-4

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 Header			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	***00-20-5C-01-11-11***	***10.10.10.254***	***00-20-5C-01-11-11***	***10.10.10.254***

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.

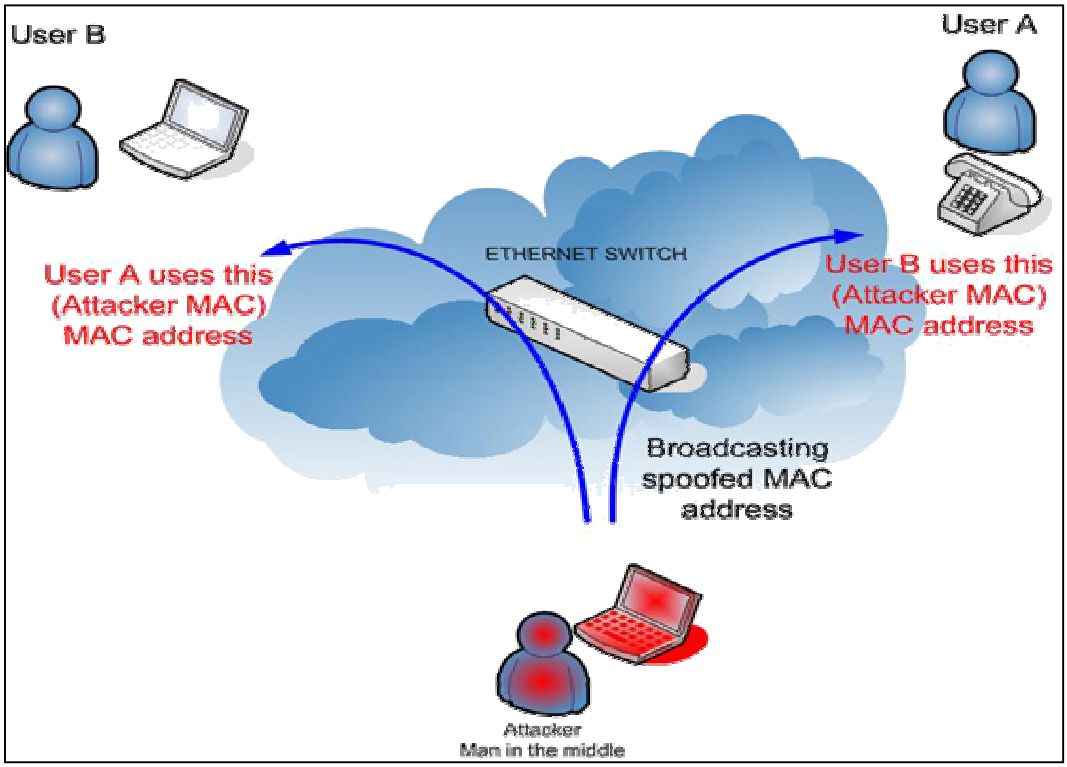
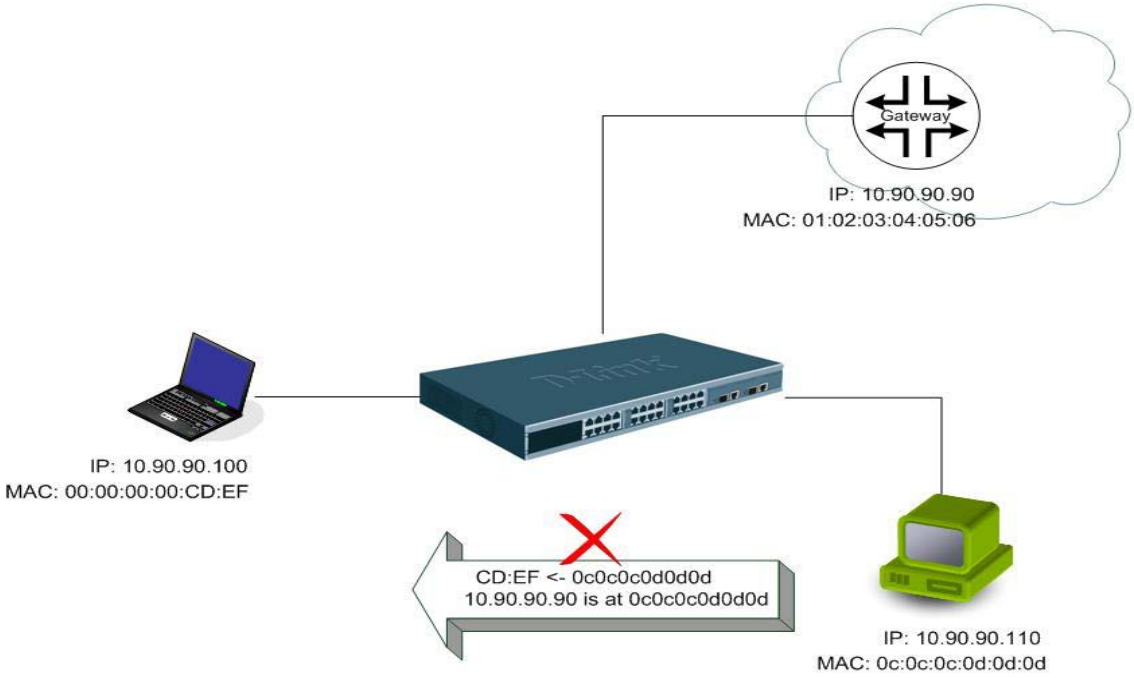


Figure-5

- **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 DES-3528 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 DES-3528 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 128th 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	Chunk5	Offset Chunk6	Offset Chunk7	Chunk8	Offset Chunk9	Offset Chunk10	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 Chunk129	Offset Chunk30
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
	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.

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)
	01 02 03 04 05 06	0806							0a5a5a5a (10.90.90.90)		

Table-7: A completed ARP packet contained in Ethernet frame

	Command	Description
Step1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	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 Source MAC in Ethernet frame can pass through the switch.
Step3	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 Ethernet Type (Blue in Table-6: 13th & 14th bytes) - The second Chunk starts from Chunk 7: mask for Sender IP (First 2-byte) in ARP packet (Green in Table-6: 29th & 30th bytes) - The third Chunk starts from Chunk 8: mask for Sender IP (Last 2-byte) in ARP packet (Brown in Table-6: 31st & 32nd bytes)
Step4	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 Sender IP claim they are the gateway's IP will be dropped.
Step5	Save	- Save config

Appendix C

System Log Entries

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

Category	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
Upload/ Download	Firmware upgraded successfully	Firmware upgraded by console successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded by console(Username: <username>)	Informational
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>)	Informational
	Configuration upload was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>)	Warning
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>)	Informational

	Log message upload was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>)	Warning
Interface	Port link up	Port <unitID:portNum> link up, <link state>	Informational
	Port link down	Port <unitID:portNum> link down	Informational
Console	Successful login through Console	Unit <unitID>, Successful login through Console (Username: <username>)	Informational
	Login failed through Console	Unit <unitID>, Login failed through Console (Username: <username>)	Warning
	Logout through Console	Unit <unitID>, Logout through Console (Username: <username>)	Informational
	Console session timed out	Unit <unitID>, 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>)	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational
STP	Topology changed	Topology changed	Informational
	New Root selected	New Root selected	Informational

	BPDU Loop Back on port	BPDU Loop Back on Port <unitID:portNum>	Warning
	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
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning

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

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

	user due to AAA server timeout or improper configuration.	configuration (Username: <username>,MAC: <mac>)	
	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 wron	Warning
	AAA doesn't support this functionality	AAA doesn't support this functionality	Informational
Port Security	Port security has exceeded its maximum learning size and will not learn any new addresses	Port security violation mac addrss <macaddr> on locking address full port <unitID:portNum>	Warning
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational
	Safeguard Engine is in filtering packet mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast strom occurrence	Port <portNum> Broadcast storm is occurring	Warning
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shut down due to a packet storm	Port <portNum> is currently shut down due to a packet storm	Warning

IP-MAC-PORT Binding	Unauthenticated ip address and discard by ip mac port binding	Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Unauthenticated IP address encountered and discarded by ip IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IP-MAC port binding (IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Warning
CTP	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
	Age out	JWAC host aged out (Username: %s, MAC: %s, Port: %s)	Information

Appendix D

Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

Standard	Media Type	Maximum Distance
SFP	1000BASE-LX, Single-mode fiber module 1000BASE-SX, Multi-mode fiber module 1000BASE-LHX, Single-mode fiber module 1000BASE-ZX, Single-mode fiber module	10km 550m 40km 80km
1000BASE-T	Category 5e UTP Cable	100m
100BASE-TX	Category 5 and Category 5e UTP Cable (100 Mbps)	100m
10BASE-T	Category 3, 4, 5, and 5e UTP Cable (10 Mbps)	100m

Appendix E

Glossary

1000BASE-SX: A short laser wavelength on multimode fiber optic cable for a maximum length of 2000 meters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

line speed: See baud rate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

D-Link®
Building Networks for People

Limited Warranty (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

Limited Lifetime Warranty for the product is defined as follows:

- Hardware: For as long as the original customer/end user owns the product, or five (5) years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power supplies and fans: Three (3) Year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Software Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping

charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

CE Mark Warning: This is a Class A product. In a residential environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures**:**

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration

Register your D-Link product online at http://support.dlink.com/register/

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

D-Link Europe Limited Lifetime Warranty

Dear Customer,

Please read below to understand the details of the warranty coverage you have.

Warranty terms for D-LINK xStack products:

All D-Link xStack products* are supplied with a 5 year warranty as standard. To enable the Limited Lifetime Warranty on this product you must register the product, within the first three months of purchase**, on the following website: **http://www.dlink.biz/productregistration/**

D-Link will then provide you with a Limited Lifetime Warranty reference number for this product. Please retain your original dated proof of purchase with a note of the serial number, and Limited Lifetime Warranty reference number together with this warranty statement and place each document in a safe location. When you make a warranty claim on a defective product, you may be asked to provide this information.

Nothing in this Limited Lifetime Warranty affects your statutory rights as a consumer. The following are special terms applicable to your Limited Lifetime hardware warranty.

Warranty beneficiary

The warranty beneficiary is the original end user. The original end user is defined as the person that purchases the product as the first owner.

Duration of Limited Lifetime Warranty

As long as the original end-user continues to own or use the product with the following conditions:

- fan and power supplies are limited to a five (5) year warranty only
- in the event of discontinuance of product manufacture, D-Link warranty support is limited to five (5) years from the announcement of discontinuance. If a product is no longer available for replacement, D-Link will issue a product comparable or better to the one originally purchased.

Replacement, Repair or Refund Procedure for Hardware

D-Link or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the RMA request. Actual delivery times may vary depending on customer location. D-Link reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number, please visit: http://service.dlink.biz and for Italy and Spain, please use: http://rma.dlink.es or http://rma.dlink.it.

D-Link Limited Lifetime Warranty

Hardware: D-Link warrants the D-Link hardware named above against defects in materials and workmanship for the period specified above. If D-Link receives notice of such defects during the warranty period, D-Link will, at its option, either repair or replace products proving to be defective. Replacement products may be either new or like-new.

***Software*.** D-Link warrants that D-Link software will not fail to execute its programming instructions, for the period specified above, due to defects in material and workmanship when properly installed and used. If D-Link receives notice of such defects during the warranty period, D-Link will replace software media that does not execute its programming instructions due to such defects.

Warranty exclusions

This warranty does not apply if the software, product or any other equipment upon which the software is authorized to be used (a) has been altered, except by D-Link or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by D-Link (improper use or improper maintenance), (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed, for beta, evaluation, testing or demonstration purposes for which D-Link does not charge a purchase price or license fee or (e) defects are caused by force majeure (lightning, floods, war, etc.), soiling, by extraordinary environmental influences or by other circumstances of which D-Link is not responsible.

Disclaimer of warranty

Please note, some countries do not allow the disclaimer of implied terms in contracts with consumers and the disclaimer below may not apply to you.

To the extend allowed by local law, the above warranties are exclusive and no other warranty, condition or other term, whether written or oral, is expressed or implied. D-Link specifically disclaims any implied warranties, conditions and terms of merchantability, satisfactory quality, and fitness for a particular purpose.

To the extent allowed by local law, the remedies in this warranty statement are customer's sole and exclusive remedies. Except as indicated above, in no event will D-Link or its suppliers be liable for loss of data or for indirect, special, incidental, consequential (including lost profit or data), or other damage, whether based in a contract, tort, or otherwise.

To the extent local law mandatorily requires a definition of "Lifetime Warranty" different from that provided here, then the local law definition will supersede and take precedence.

Valid law

The warranty is subject to the valid laws in the country of purchase and is to be interpreted in the warranty terms with the said laws. You may have additional legal rights that are not restricted by this warranty. Nothing in this Limited Lifetime Warranty affects your statutory rights as a consumer.

* DES-6500 series is excluded from the Limited Lifetime Warranty offering and will be supplied with a standard 5 year warranty.

** Failure to register this product within the first three months of purchase [by the first user only] will invalidate the Limited Lifetime Warranty.

LIMITED WARRANTY

D-Link provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor. D-Link would fulfill the warranty obligation according to the local warranty policy in which you purchased our products.

Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period") if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

Product Type	***Warranty Period***
Product (including Power Supplies and Fans)	One (1) Year
Spare parts and pare kits	Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion may replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:

Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same. The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided. After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The packaged product shall be insured and shipped to Authorized D-Link Service Office with all shipping costs prepaid. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

This limited warranty provided by D-Link does not cover:

Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed;

Initial installation, installation and removal of the product for repair, and shipping costs;

Operational adjustments covered in the operating manual for the product, and normal maintenance;

Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage;

and

Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER,

WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks

Copyright Statement

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Tech Support

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the service period, and warranty confirmation service, during the warranty period on this product. U.S. and Canadian customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 354-6555

Monday to Friday 8:00am to 5:00pm PST

D-Link Technical Support over the Internet:

http://support.dlink.com

email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

1-800-361-5265

Monday to Friday 7:30am to 9:00pm EST

D-Link Technical Support over the Internet:

http://support.dlink.com

email: support@dlink.ca

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link websites.

If you require product support, we encourage you to browse our FAQ section on the Web Site before contacting the Support line. We have many FAQ's which we hope will provide you a speedy resolution for your problem.

D-Link UK & Ireland Technical Support over the Telephone:

United Kingdom

08456 12 0003

BT 3ppm peak, 1.5ppm off peak, 0.5ppm weekends. (UK Pence per mintue). Other carriers could be lower.

Times Mon-Fri 9.00am - 6.00pm Sat 10.00am - 2.00pm

Ireland

+1890 886 899

€0.05ppm peak, €0.045ppm off peak

Times Mon-Fri 9.00am - 6.00pm Sat 10.00am - 2.00pm

D-Link UK & Ireland Technical Support over the Internet:

Web: http://www.dlink.co.uk

E-mail: ftp://ftp.dlink.co.uk

D-Link®

Building Networks for People

Technische Unterstützung

Aktualisierte Versionen von Software und Benutzerhandbuch finden Sie auf der Website von D-Link.

D-Link bietet kostenfreie technische Unterstützung für Kunden innerhalb Deutschlands, Österreichs, der Schweiz und Osteuropas.

Unsere Kunden können technische Unterstützung über unsere Website, per E-Mail oder telefonisch anfordern.

Telefon: +49 (1805)2787

0,14€ pro Minute

Web: http://www.dlink.de

E-Mail: support@dlink.de

D-Link®

Building Networks for People

Assistance technique

Vous trouverez la documentation et les logiciels les plus récents sur le site web D-Link.

Vous pouvez contacter le service technique de

D-Link par notre site internet ou par téléphone.

Assistance technique D-Link par téléphone:

0 820 0803 03

0,12 €/min

Hours : Monday - Friday 9h to 13h and 14h to 19h

Saturday 9h to 13h and from 14h to 16h

Assistance technique D-Link sur internet :

Web: http://www.dlink.fr

E-mail: support@dlink.fr

D-Link®

Building Networks for People

Asistencia Técnica

Puede encontrar las últimas versiones de software así como documentación técnica en el sitio web de D-Link.

D-Link ofrece asistencia técnica gratuita para clientes residentes en España durante el periodo de garantía del producto.

Asistencia Técnica de D-Link por teléfono:

+34 902 30 45 45

0,067 €/min

Lunes a Viernes de 9:00 a 14:00 y de 15:00 a 18:00

Web: http://www.dlink.es

E-mail: soporte@dlink.es

D-Link®
Building Networks for People

Supporto tecnico

Gli ultimi aggiornamenti e la documentazione sono disponibili sul sito D-Link.

Supporto Tecnico dal lunedì al venerdì dalle ore 9.00 alle ore 19.00 con orario continuato

Telefono: 199400057

Web: http://www.dlink.it/support

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within Benelux for the duration of the warranty period on this product.

Benelux customers can contact D-Link technical support through our website, or by phone.

Netherlands

0900 501 2007

€0.15ppm anytime

Web: www.dlink.nl

Belgium

070 66 06 40

€0.175ppm peak, €0.0875ppm off peak

Web: www.dlink.be

Luxemburg

+32 70 66 06 40

Web: www.dlink.be

D-Link®

Building Networks for People

Pomoc techniczna

Najnowsze wersje oprogramowania i dokumentacji użytkownika można znaleźć w serwisie internetowym firmy D-Link.

D-Link zapewnia bezpłatną pomoc techniczną klientom w Polsce w okresie gwarancyjnym produktu.

Klienci z Polski mogą się kontaktować z działem pomocy technicznej firmy D-Link za pośrednictwem Internetu lub telefonicznie.

Telefoniczna pomoc techniczna firmy D-Link:

0 801 022 021

Pomoc techniczna firmy D-Link świadczona przez Internet:

Web: http://www.dlink.pl

E-mail: dlink@fixit.pl

D-Link®
Building Networks for People

Technická podpora

Aktualizované verze software a uživatelských příruček najdete na webové stránce firmy D-Link.

D-Link poskytuje svým zákazníkům bezplatnou technickou podporu

Zákazníci mohou kontaktovat oddělení technické podpory přes webové stránky, mailem nebo telefonicky

Telefon: 225 281 553

Land Line 1,78 CZK/min - Mobile 5.40 CZK/min

Telefonická podpora je v provozu: PO- PÁ od 09.00 do 17.00

Web: http://www.dlink.cz/suppport/

E-mail: support@dlink.cz

D-Link®

Building Networks for People

Technikai Támogatás

Meghajtó programokat és frissítéseket a D-Link Magyarország weblapjáról tölthet le.

Tel: 06 1 461-3001

Fax: 06 1 461-3004

Land Line 14,99 HUG/min - Mobile 49.99,HUF/min

Web: http://www.dlink.hu

E-mail: support@dlink.hu

D-Link®

Building Networks for People

Teknisk Support

Du kan finne programvare oppdateringer og bruker dokumentasjon på D-Links web sider.
D-Link tilbyr sine kunder gratis teknisk support under produktets garantitid.
Kunder kan kontakte D-Links teknisk support via våre hjemmesider, eller på tlf.

D-Link Teknisk telefon Support:
800 10 610
(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett:
Web: http://www.dlink.no

D-Link®
Building Networks for People

Teknisk Support

Du finder software opdateringer og bruger-dokumentation på D-Link's hjemmeside.

D-Link tilbyder gratis teknisk support til kunder i Danmark i hele produktets garantiperiode.

Danske kunder kan kontakte D-Link's tekniske support via vores hjemmeside eller telefonisk.

D-Link teknisk support over telefonen:
Tlf. 7026 9040
Åbningstider: kl. 08:00 – 20:00

D-Link teknisk support på Internettet:
Web: http://www.dlink.dk

D-Link®
Building Networks for People

Teknistä tukea asiakkaille Suomessa

D-Link tarjoaa teknistä tukea asiakkailleen.

Tuotteen takuun voimassaoloajan.

Tekninen tuki palvelee seuraavasti:

numerosta : 0800-114 677

Arkisin klo. 9 - 21

Internetin kautta:

Web: http://www.dlink.fi

D-Link®

Building Networks for People

Teknisk Support

På vår hemsida kan du hitta mer information om mjukvaru uppdateringar och annan användarinformation.

D-Link tillhandahåller teknisk support till kunder i Sverige under hela garantitiden för denna produkt.

D-Link Teknisk Support via telefon:

0770-33 00 35

Vardagar 08.00-20.00

D-Link Teknisk Support via Internet:

Web: http://www.dlink.se

D-Link®
Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de utilizador no site de D-Link Portugal http://www.dlink.pt.

A D-Link fornece suporte técnico gratuito para clientes no Portugal durante o período de vigência de garantia deste produto.

Assistência Técnica da D-Link na Internet:

Web: http://www.dlink.pt

E-mail: soporte@dlink.es

D-Link®
Building Networks for People

Τεχνική Υποστήριξη

Μπορείτε να βρείτε software updates και πληροφορίες για τη χρήση των προϊόντων στις ιστοσελίδες της D-Link

Η D-Link προσφέρει στους πελάτες της δωρεάν υποστήριξη

στον Ελλαδικό χώρο

Μπορείτε να επικοινωνείτε με το τμήμα τεχνικής υποστήριξης μέσω της ιστοσελίδας ή μέσω τηλεφώνου

D-Link Hellas Support Center

Κεφαλληνίας 64, 11251 Αθήνα,

Τηλ: 210 86 11 114 (Δευτέρα- Παρασκευή 09:00-17:00)

Φαξ: 210 8611114

Web: http://www.dlink.gr/support

D-Link®

Building Networks for People

Tehnička podrška

Hvala vam na odabiru D-Link proizvoda. Za dodatne informacije, podršku i upute za korištenje uređaja, molimo vas da posjetite D-Link internetsku stranicu na www.dlink.eu

Web: www.dlink.biz/hr

D-Link®
Building Networks for People

Tehnična podpora

Zahvaljujemo se vam, ker ste izbrali D-Link proizvod. Za vse nadaljnje informacije, podporo ter navodila za uporabo prosimo obiščite D-Link - ovo spletno stran www.dlink.eu

Web: www.dlink.biz/sl

D-Link®
Building Networks for People

Suport tehnica

Vă mulțumim pentru alegerea produselor D-Link. Pentru mai multe informații, suport şi manuale ale produselor vă rugăm să vizitați site-ul D-Link www.dlink.eu

Web: www.dlink.ro

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Australia:

Tel: 1300-766-868

Monday to Friday 8:00am to 8:00pm EST

Saturday 9:00am to 1:00pm EST

http://www.dlink.com.au

e-mail: support@dlink.com.au

India:

Tel: 1800-222-002

Monday to Friday 9:30AM to 7:00PM

http://www.dlink.co.in/support/productsupport.aspx

Indonesia, Malaysia, Singapore and Thailand:

Tel: +62-21-5731610 (Indonesia)

Tel: 1800-882-880 (Malaysia)

Tel: +65 66229355 (Singapore)

Tel: +66-2-719-8978/9 (Thailand)

Monday to Friday 9:00am to 6:00pm

http://www.dlink.com.sg/support/

e-mail: support@dlink.com.sg

Korea:

Tel: +82-2-890-5496

Monday to Friday 9:00am to 6:00pm

http://www.d-link.co.kr

e-mail: lee@d-link.co.kr

New Zealand:

Tel: 0800-900-900

Monday to Friday 8:30am to 8:30pm

Saturday 9:00am to 5:00pm

http://www.dlink.co.nz

e-mail: support@dlink.co.nz

D-Link®

Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Egypt:

Tel: +202-2919035 or +202-2919047

Sunday to Thursday 9:00am to 5:00pm

http://support.dlink-me.com

e-mail: amostafa@dlink-me.com

Iran:

Tel: +98-21-88822613

Sunday to Thursday 9:00am to 6:00pm

http://support.dlink-me.com

e-mail: support.ir@dlink-me.com

Israel:

Tel: +972-9-9715701

Sunday to Thursday 9:00am to 5:00pm

http://www.dlink.co.il/support/

e-mail: support@dlink.co.il

Pakistan:

Tel: +92-21-4548158 or +92-21-4548310

Sunday to Thursday 9:00am to 6:00pm

http://support.dlink-me.com

e-mail: support.pk@dlink-me.com

South Africa and Sub Sahara Region:

Tel: +27-12-665-2165

08600 DLINK (for South Africa only)

Monday to Friday 8:30am to 9:00pm South Africa Time

http://www.d-link.co.za

Turkey:

Tel: +90-212-2895659

Monday to Friday 9:00am to 6:00pm

http://www.dlink.com.tr

e-mail: turkiye@dlink-me.com

e-mail: support@d-link.co.za

U.A.E and North Africa:

Tel: +971-4-391-6480 (U.A.E)

Sunday to Wednesday 9:00am to 6:00pm GMT+4

Thursday 9:00am to 1:00pm GMT+4

http://support.dlink-me.com

e-mail: support@dlink-me.com

D-Link®

Building Networks for People

Техническая поддержка

Обновления программного обеспечения и документация доступны на Интернет-сайте D-Link.

D-Link предоставляет бесплатную поддержку для клиентов в течение гарантийного срока.

Клиенты могут обратиться в группу технической поддержки D-Link по телефону или через Интернет.

Техническая поддержка D-Link:

+495-744-00-99

Техническая поддержка через Интернет

http://www.dlink.ru

e-mail: support@dlink.ru

D-Link®

Building Networks for People

Asistencia Técnica

D-Link Latin América pone a disposición de sus clientes, especificaciones, documentación y software mas reciente a través de nuestro Sitio Web

www.dlinkla.com

El servicio de soporte técnico tiene presencia en numerosos países de la Región Latino América, y presta asistencia gratuita a todos los clientes de D-Link, en forma telefónica e internet, a través de la casilla

soporte@dlinkla.com

Soporte Técnico Help Desk Argentina:

TTeléfono: 0800-12235465 Lunes a Viernes 09:00 am a 22:00 pm

Soporte Técnico Help Desk Chile:

Teléfono: 800 8 35465 Lunes a Viernes 08:00 am a 21:00 pm

Soporte Técnico Help Desk Colombia:

Teléfono: 01800-9525465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Ecuador:

Teléfono: 1800-035465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk El Salvador:

Teléfono: 800-6335 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Guatemala:

Teléfono: 1800-8350255 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Panamá:

Teléfono: 00800 0525465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Costa Rica:

Teléfono: 0800 0521478 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Perú:

Teléfono: 0800-00968 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk México:

Teléfono: 001 800 123-3201 Lunes a Viernes 06:00 am a 19:00

Soporte Técnico Help Desk Venezuela:

Teléfono: 0800-1005767 Lunes a Viernes 08:00 am a 21:00 pm

D-Link®
Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de usuário no site da D-Link Brasil www.dlinkbrasil.com.br.

A D-Link fornece suporte técnico gratuito para clientes no Brasil durante o período de vigência da garantia deste produto.

Suporte Técnico para clientes no Brasil:

Telefone

São Paulo +11-2185-9301

Segunda à sexta

Das 8h30 às 18h30

Demais Regiões do Brasil 0800 70 24 104

E-mail:

e-mail: suporte@dlinkbrasil.com.br

D-Link®
Building Networks for People

D-Link 友訊科技 台灣分公司
技術支援資訊

如果您還有任何本使用手冊無法協助您解決的**產**品相關問題，台灣地區用戶可以透過我們的網站、電子郵件或電話等方式與 D-Link台灣地區技術支援工程師聯絡。

D-Link 免付費技術諮詢專線
0800-002-615
服務時間：週一至週五，早上8:30 到 **晚**上9:00
(不含周六、日及國定假日)

網 站：http://www.dlink.com.tw
電子郵件：dssqa_service@dlink.com.tw

如果您是台灣地區以外的用戶，請參考D-Link網站 全球各地分公司的聯絡資訊以取得相關支援服務。

產品保固期限、台灣區維修據點**查**詢，請參考以下網頁說明：
http://www.dlink.com.tw

產品維修：

使用者可直接送至全省聯強直營維修站或請洽您的原購買經銷商。

D-Link®
Building Networks for People

Dukungan Teknis

Update perangkat lunak dan dokumentasi pengguna dapat diperoleh pada situs web D-Link.

Dukungan Teknis untuk pelanggan:

Dukungan Teknis D-Link melalui telepon:

Tel: +62-21-5731610

Dukungan Teknis D-Link melalui Internet:

Email : support@dlink.co.id

Website : http://support.dlink.co.id

D-Link®
Building Networks for People

技术支持

您可以在 D-Link 的官方網站找到產品的軟件升級和使用手冊

办公地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座 26F 02-05 室 邮编: 100013

技术支持中心电话：8008296688/ (028)66052968

技术支持中心传真：(028)85176948

维修中心地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座 26F 02-05 室 邮编: 100013

维修中心电话：(010) 58257789

维修中心传真：(010) 58257790

网址：http://www.dlink.com.cn

办公时间：周一到周五，早09:00到晚18:00

D-Link®
Building Networks for People

International Offices

U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA 92708
TEL: 1-800-326-1688
URL: www.dlink.com

Canada
2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)
D-Link (Europe) Ltd
D-Link House, Abbey Road
Park Royal, London NW10 7BX
United Kingdom
TEL: +44 (0)20 8955 9000
FAX: +44 (0)20 8955 9001
URL: www.dlink.co.uk

Austria
Building A, Level 3, 11 Talavera Rd
North Ryde, NSW, 2113
Tel: (+61 2) 8899 1800
Fax: (+61 2) 8899 1868
URL: www.dlink.at

Belgium
Rue des Colonies 11
B-1000 Brussels,
Belgium
TEL: +32 (0)2 517 7111
FAX: +32 (0)2 517 6500
URL: www.dlink.be

Bulgaria
60A Bulgaria Blvd., Office 1,
Sofia 1680,
Bulgaria
TEL: +359 2 958 22 42
FAX: +359 2 958 65 57
URL: www.dlink.eu

Czech Republic
Vaclavske namesti 36
110 00 Praha 1
Czech Republic
TEL: +420 224 247 500
FAX: +420 224 234 967
Hot line CZ: +420 225 281 553
Hot line SK: +421 263 813 628
URL: www.dlink.cz
URL: www.dlink.sk

Denmark
Naverland 2,
DK-2600 Glostrup, Copenhagen,
Denmark
TEL: +45 43 96 9 040
FAX: +45 43 42 43 47
URL: www.dlink.dk

Finland
Latokartanontie 7A
FIN-00700 Helsinki,
Finland
TEL : +358 10 309 8840
FAX: + 358 10 309 8841
URL: www.dlink.fi

France
41 boulevard Vauban
78280 Guyancourt
France
TEL: +33 (0)1 30 23 86 88
FAX: +33 (0)1 30 23 86 89
URL: www.dlink.fr

Germany
Schwalbacher Strasse 74
D-65760 Eschborn,
Germany
TEL: +49 (0)6196 77 99 0
FAX: +49 (0)6196 77 99 300
URL: www.dlink.de

Greece
101, Panagoulis Str. 163-43
Heliopolis, Athens,
Greece
TEL: +30 210 9914512
FAX:+30 210 9916902
URL: www.dlink.gr

Hungary
Rákóczi út 70-72
HU-1074 Budapest,
Hungary
TEL: +36 (0) 1 461 30 00
FAX: +36 (0) 1 461 30 04
URL: www.dlink.hu

Italy
Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: +39 02 2900 0676
FAX: +39 02 2900 1723
URL: www.dlink.it

Luxembourg
Rue des Colonies 11
B-1000 Brussels,
Belgium
Tel: +32 (0)2 517 7111
FAX: +32 (0)2 517 6500
URL: www.dlink.be

Netherlands
Weena 290
3012NJ Rotterdam,
Netherlands
TEL: +31 (0)10 282 1445
FAX: +31 (0)10 282 1331
URL: www.dlink.nl

Norway
Karihaugveien 89
N-1086 Oslo,
Norway
TEL: +47 99 300 100
FAX: +47 22 30 90 85
URL: www.dlink.no

Poland
Budynek Aurum
ul. Waliców 11
00-851 Warszawa,
Poland
TEL: +48 (0) 22 583 92 75
FAX: +48 (0) 22 583 92 76
URL: www.dlink.pl

Portugal
Rua Fernando Palha, 50 Edificio Simol
1900 Lisbon,
Portugal
TEL: +351 21 8688493
FAX: +351 21 8622492
URL: www.dlink.es

Romania
B-dul Unirii nr. 55, bl. E4A, sc.2, et. 4, ap. 39,
sector 3, Bucuresti,
Romania
Tel: +40(0)21 320 23 05
Fax: +40(0)21 320 23 07
URL: www.dlink.eu

Spain
Avenida Diagonal, 593-95, 9th floor
08014 Barcelona,
Spain
TEL: +34 93 409 07 70
FAX: +34 93 491 07 95
URL: www.dlink.es

Sweden
Gustavslundsvägen 151B
S-167 51 Bromma
Sweden
TEL: +46 (0)8 564 619 00
FAX: +46 (0)8 564 619 01
URL: www.dlink.se

Switzerland
Glatt Tower, 2.OG
Postfach
CH-8301 Glattzentrum
Switzerland
TEL: +41 (0)1 832 11 00
FAX: +41 (0)1 832 11 01
URL: www.dlink.ch

Singapore
1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia
1 Giffnock Avenue
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India
D-Link House, Plot No.5,
Kurla-Bandra Complex Road, Off. CST Road,
Santacruz (E), Mumbai - 400 098
India
TEL: 91-22-26526696/ 30616666
FAX: 91-22-26528914/ 8476
URL: www.dlink.co.in

Middle East (Dubai)
P.O.Box: 500376
Office: 103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel: +971-4-3916480
Fax: +971-4-3908881
URL: www.dlink-me.com

Turkey
Cayazaya Maslak Yolu
S/A Kat: 5,
Istanbul, Turkey
TEL: 0212-289-5659
FAX:0212-289-7606
URL: www.dlink.com.tr

Iran
Unit 6, No. 39, 6th Alley,
Sanaei St, Karimkhan Ave
Tehran-IRAN
Tel: 9821 8882 2613
Fax: 9821 8883 5492

Pakistan
Office#311, Business Avenue
Main Shahrah-e-Faisal
Karachi-Pakistan
Tel: 92-21-4548158, 4548310
Fax: 92-21-4535103

Egypt
47,El Merghany street,Heliopolis
Cairo-Egypt
TEL: +202-2919035, +202-2919047
FAX: +202-2919051
URL: www.dlink-me.com

Israel
11 Hamanofim Street
Ackerstein Towers, Regus Business Center
P.O.B 2148, Hertzelia-Pituach
46120
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

LatinAmerica
Av. Vitacura # 2939, floor 6th
Las Condes, Santiago.
RM Chile
TEL: 56-2-5838-950
FAX: 56-2-5838-952
URL: www.dlinkla.com

Brazil
Av das Nacoes Unidas
11857 – 14- andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000 (Zip Code)
TEL: (55 11) 21859300
FAX: (55 11) 21859322
URL: www.dlinkbrasil.com.br

South Africa
Einstein Park II
Block B
102-106 Witch-Hazel Avenue
First Floor Block B
Einstein Park II
Highveld Techno Park
Centurion
Gauteng
Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www.d-link.co.za

Russia
Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-495-744-0099
FAX: 7-495-744-0099 #350
URL: www.dlink.ru

Japan K.K.
Level 6 Konan YK Building, Konan 2-4-12
Minato-Ku Tokyo 108-0075, Japan
URL: www.dlink-jp.com

China
Room02-05，Floor26，Building B,
Global trade center,36 north third ring road east , Dongcheng District, Beijing 100013 , China.
TEL: (8610) 5825 7789
FAX: (8610) 5825 7792
URL: www.dlink.com.cn

Taiwan
No. 289 , Sinhu 3rd Rd., Neihu District ,
Taipei City 114 ,Taiwan
TEL: 886-2-6600-0123
FAX: 886-2-6600-1188
URL: www.dlink.com.tw

Registration Card

(All Countries and Regions excluding USA)

Print, type or use block letters.

Your name: Mr./Ms_____

Organization: _____Dept. _____

Your title at organization:_____

Telephone:_____ Fax:_____

Organization's full address:_____

_____

Country:_____

Date of purchase (Month/Day/Year):_____

Product Model	**Product Serial No.**	*** Product installed in type of computer**	*** Product installed in computer serial No.**

(* Applies to adapters only)

Product was purchased from:

Reseller's name:_____

Telephone:_____ Fax:_____

Reseller's full address:_____

_____

_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use?

☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use?

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open

☐Banyan Vines ☐Windows NT ☐Windows ME ☐Windows 2000 ☐Windows XP ☐ Windows Vista

☐Others_____

5. What network management program does your organization use?

☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS

☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP

☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM

☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing

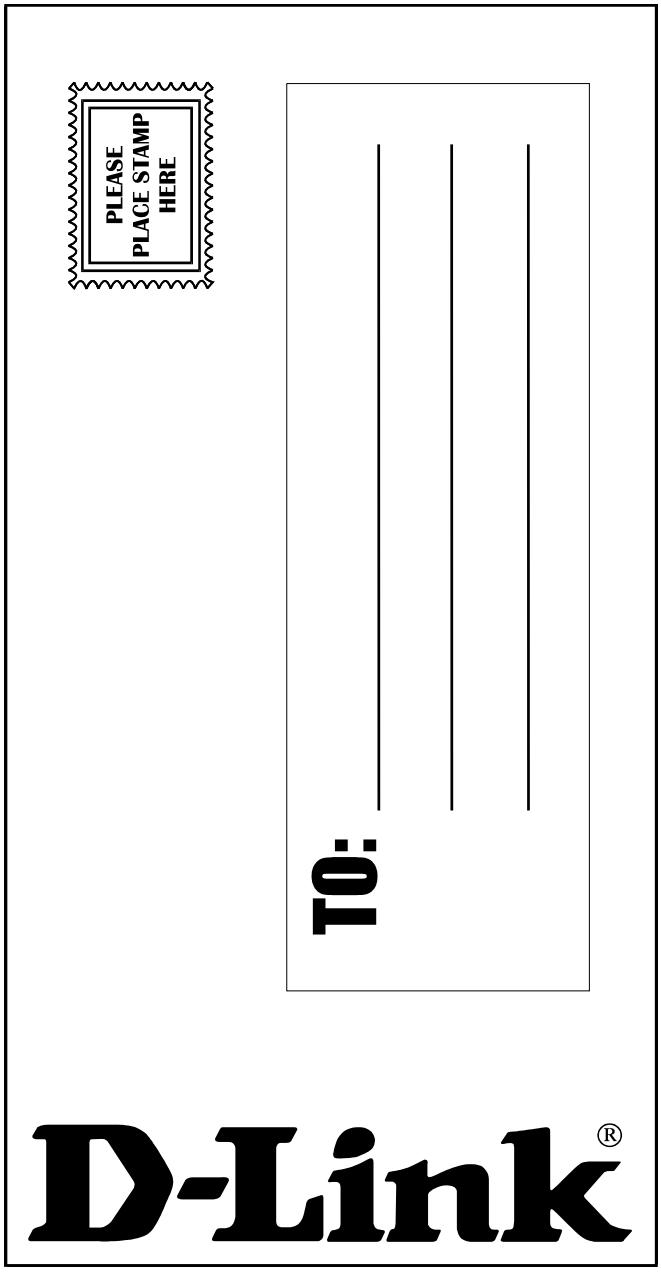
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR

☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10. Your comments on this product?_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®