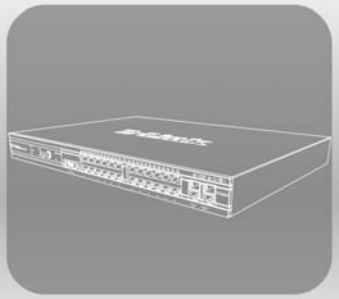
D-Link
Building Networks for People



XSTACK

User Manual

Product Model: xStack™ DES-3800 Series

Layer 3 Stackable Fast Ethernet Managed Switch

Release 4.51

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
xStack DES-3800 Series 1
Gigabit Ethernet Technology 1
Switch Description 1
Features 2
Ports 3
Front-Panel Components 2
Rear Panel Description 6
Side Panel Description 7
Gigabit Ports 7
Installation 8
Package Contents 8
Before You Connect to the Network 8
Installing the Switch without the Rack 9
Installing the Switch in a Rack 9
Mounting the Switch in a Standard 19" Rack 10
Connecting DC Power to the DES-3828DC 11
RPS Installation 12
Connecting the Switch 16
Switch to End Node 16
Switch to Hub or Switch 17
Connecting To Network Backbone or Server 18
Introduction to Switch Management 19
Management Options 19
Web-based Management Interface 19
SNMP-Based Management 19
Connecting the Console Port (RS-232 DCE) 19
First Time Connecting to the Switch 21
Password Protection 22
SNMP Settings 23
IP Address Assignment 24
Web-based Switch Configuration 26

Introduction 26
Login to Web Manager 26
Web-based User Interface 27
Web Pages 28
Administration 29
Device Information 30
IP Address 32
Port Configuration 35
Port Settings 35
Port Description 37
PoE Configuration 38
User Accounts 39
Port Mirroring 41
System Log Settings 42
System Severity Settings 44
SNTP Settings 45
Time Settings 45
Time Zone and DST 46
MAC Notification Settings 48
TFTP Services 49
Multiple Image Services 50
Firmware Information 50
Dual Configuration Services 51
Ping Test 52
SNMP Manager 53
SNMP Settings 53
SNMP User Table 54
SNMP View Table 56
SNMP Group Table 57
SNMP Community Table Configuration 58
SNMP Host Table 59
SNMP Engine ID 61
SNMP Trap Settings 61
D-Link Single IP Management 62
Single IP Management (SIM) Overview 62
SIM Using the Web Interface 63
Topology 65
Tool Tips 67
Right Click 68
Menu Bar 70
Packet to CPU Settings 71
Layer 2 Features 72
VLANs 72

Understanding IEEE 802.1p Priority....72
VLAN Description....72
IEEE 802.1Q VLANs....73
Double VLANs....78
Static VLAN Entry....79
GVRP Setting....83
Double VLAN....84
Trunking....86
Link Aggregation....87
LACP Port Settings....89
IGMP....90
IGMP Snooping....90
Static Router Port Settings....92
IGMP Multicast VLAN....93
MLD Snooping....94
MLD Snooping Settings....95
MLD Snooping Static Router Port Settings....96
Spanning Tree....97
STP Bridge Global Settings....100
MST Configuration Identification....102
MSTP Port Information....104
STP Instance Settings....105
STP Port Settings....106
STP Ports Information of Instance....108
Forwarding....109
Unicast Forwarding....109
Multicast Forwarding....109
Multicast Port Filtering Mode....111
Loopback Detection....113
Protocol VLAN....115
Layer 3 Features....118
IP Multinetting....119
IP Interface Settings....119
Loopback IP Interface....123
MD5 Key Settings....124
Route Redistribution Settings....125
Static/Default Route Settings....126
Route Preference Settings....127
Static ARP Table....130
RIP....131
RIP Global Settings....132
RIP Interface Settings....133
OSPF....135
OSPF Global Settings....151

OSPF Area Settings....151
OSPF Interface Settings....153
OSPF Virtual Link Settings....155
OSPF Area Aggregation Settings....157
OSPF Host Route Settings....158
OSPF Default Information Originate Settings....159
DHCP Server....160
DHCP Server Global Settings....160
DHCP Server Pool Settings....161
DHCP Server Manual Binding Settings....162
DHCP Server Excluded Address Settings....163
DHCP Server Conflict IP Table....163
DHCP Server Binding Table....164
DHCP/BOOTP Relay....165
DHCP / BOOTP Relay Global Settings....165
DHCP/BOOTP Relay Interface Settings....168
DNS Relay....169
DNS Relay Global Settings....169
DNS Relay Static Settings....170
VRRP....171
VRRP Global Settings....171
VRRP Virtual Router Settings....171
VRRP Authentication Settings....175
IP Multicast Routing Protocol....176
IGMP Interface Settings....178
DVMRP Interface Configuration....180
DVMRP Global Settings....180
DVMRP Interface Settings....180
PIM Protocol....182
PIM-SM....182
PIM-DM Interface Configuration....183
PIM Global Settings....183
PIM Interface Settings....183
PIM Candidate BSR Settings....185
PIM Parameter Settings....186
PIM Candidate RP Global Settings....187
PIM Candidate RP Settings....187
PIM Register Checksum Settings....188
PIM Static RP Settings....189
QoS....190
Advantages of QoS....190
Understanding QoS....191
Bandwidth Control....192
QoS Scheduling Mechanism....194

QoS Output Scheduling 195
802.1p Default Priority 196
802.1p User Priority 198
WRED Settings 198
ACL 200
Access Profile Table 201
Flow Metering Table 219
CPU Interface Filtering 220
CPU Interface Filtering Profile Table 220
Security 232
Traffic Control 233
Port Security 235
Port Lock Entries 236
Port Access Entity (802.1X) 237
802.1x Port-Based and MAC-Based Access Control 237
Understanding 802.1x Port-based and MAC-based Network Access Control 240
Port-Based Network Access Control 240
MAC-Based Network Access Control 241
Configure 802.1x Authenticator Parameter 242
Initializing Ports for Port Based 802.1x 244
Initializing Ports for MAC Based 802.1x 245
Reauthenticate Port(s) for Port Based 802.1x 246
Reauthenticate Port(s) for MAC-based 802.1x 246
Authentication RADIUS Server 247
RADIUS Attributes Assignment 248
Guest VLANs 249
Guest VLAN Configuration 249
Trusted Host 250
Access Authentication Control 251
Authentication Policy and Parameter Settings 252
Application Authentication Settings 252
Authentication Server Group 253
Authentication Server Host 254
Login Method Lists 255
Enable Method Lists 257
Configure Local Enable Password 259
Enable Admin 259
Three Level User Accounts 260
Accounting 261
Traffic Segmentation 262
Broadcast Segmentation 263
Secure Socket Layer (SSL) 265
Download Certificate 265

Ciphersuite 265
SSH 268
SSH Server Configuration 268
SSH Authentication Mode and Algorithm Settings 269
SSH User Authentication 270
IP-MAC Binding 272
ACL Mode 272
IP-MAC Binding Port 274
IP-MAC Binding Table 276
IP-MAC Binding Blocked 277
IP-MAC Binding DHCP Snooping Table 277
Limited IP Multicast Range 278
Limited IP Multicast Range Port Settings 278
Limited IP Multicast Max Group Settings 280
Web-based Access Control 281
Conditions and Limitations 281
MAC-Based Access Control 285
Notes About MAC-Based Access Control 285
MAC-Based Access Control Global Settings 286
MAC-Based Access Control Port Settings 287
MAC-Based Access Control Local Database Settings 288
Safeguard Engine 289
Filter 291
CPU Filtering Settings 291
Monitoring 293
Device Status 293
CPU Utilization 294
Safeguard Engine Status 295
Port Utilization 296
Packets 297
Received (RX) 297
UMB Cast (RX) 299
Transmitted (TX) 301
Errors 303
Received (RX) 303
Transmitted (TX) 305
Packet Size 307
Browse Router Port 309
Port Access Control 310
RADIUS Authentication 310
RADIUS Accounting 311
Authenticator State 312
MAC Address Table 314
IP Address Table 315

Browse ARP Table 315
Browse IP Multicast Forwarding Table 316
IGMP Snooping Group 316
IGMP Snooping Forwarding 317
Browse IGMP Group Table 318
DVMRP Monitoring 319
Browse DVMRP Routing Table 319
Browse DVMRP Neighbor Table 319
Browse DVMRP Routing Next Hop Table 319
PIM Monitoring 320
Browse PIM Neighbor Table 320
PIM IP MRoute Table 320
Browse PIM RP Set Table 321
Browse PIM Active RP Table 321
OSPF Monitor 322
Browse OSPF LSDB Table 322
Browse OSPF Neighbor Table 323
Browse OSPF Virtual Neighbor Table 323
Browse WRED Settings 324
Switch Log 325
Switch Maintenance 326
Reset 326
Reboot System 327
Save Changes 328
Logout 328
Technical Specifications 329
System Log Entries 331
Cables and Connectors 341
Console Cable Pin Assignment 342
Cable Lengths 343
ARP Packet Content ACL 344
Glossary 352

Preface

The *xStack DES-3800 Series User 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-3828DC.

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, Administration- A detailed discussion about configuring the basic functions of the Switch, including Device Information, IP Address, Port Configuration, User Accounts, Port Mirroring, System Log Settings, System Severity Settings, SNTP Settings, MAC Notification Settings, TFTP Services, Multiple Image Services, Ping Test, SNMP Manager, and Single IP Management Settings.

Section 7, Layer 2 Features- A discussion of Layer 2 features of the Switch, including VLAN, Trunking, IGMP Snooping, Spanning Tree and Forwarding.

Section 8, Layer 3 Features- A discussion of Layer 3 features of the Switch, including IP Interface Settings, MD5 Key Settings, Route Redistribution Settings, Static/Dynamic Route Settings, Route Preference Settings, Static ARP Settings, RIP, OSPF, DCHP/BOOTP Relay, DNS Relay, VRRP and IP Multicast Routing Protocol.

Section 9, QoS - Features information on QoS, including Bandwidth Control, QoS Scheduling Mechanism, QoS Output, Scheduling, 802.1P Default Priority, 802.1P User Priority and WRED Settings.

Section 10, ACL- Discussion on the ACL function of the Switch, including Access Profile Table and CPU Interface Filtering.

Section 11, Security – A discussion on the Security functions on the Switch, including Traffic Control, Port Security, Port Lock Entries, 802.1X, Trusted Host, Access Authentication Control, Traffic Segmentation, SSL, SSH, IP MAC Binding, Limited IP Multicast Range, Web-based Access Control, MAC-based Access Control and Safeguard Engine.

Section 12, Monitoring – Features information on Monitoring including Device Status, CPU Utilization, Safeguard Engine Status, Port Utilization, Packets, Errors, Packet Size, Browse Router Port, Port Access Control, MAC Address Table, IP Address Table, Browse Routing Table, Browse ARP Table, Browse IP Multicast Forwarding Table, IGMP Snooping Group, IGMP Snooping Forwarding, Browse IGMP Group Table, DVMRP Monitor, PIM Monitor, OSPF Monitor, Browse WRED Status, Browse PoE Status and Switch Log.

Appendix A, Technical Specifications - Technical specifications for the DES-3828, DES-3828P, DES-3828DC and the DES-3852.

Appendix B, System Log Entries – A list of possible system log entries with a brief description.

Appendix C, Cables and Connectors - Describes the RJ-45 receptacle/connector, straight through and crossover cables and standard pin assignments.

Appendix D, Console Cable Pin Assignment – A description of the pin assignment for the console cable.

Appendix E, Cable Lengths - Information on cable types and maximum distances.

Glossary - Lists definitions for terms and acronyms used in this document.

Intended Readers

The *xStack DES-3800 Series User Manual* contains information for setup and management of the Switch. The term, "the Switch" will be used when referring to all three switches. 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
  - –48 VDC for DC power supply unit on DES-3828DC only
- 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.

CAUTION: Do not replace the battery with an incorrect type. The risk of explosion exists if the replacement battery is not the correct lithium battery type. Dispose of used batteries according to the instructions.

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

xStack DES-3800 Series

Gigabit Ethernet Technology

Switch Description

Features

Ports

Front-Panel Components

Side Panel Description

Rear Panel Description

Gigabit Combo Ports

xStack DES-3800 Series

The DES-3800 switch series is a member of the D-Link xStack switch family. xStack is a complete family of stackable devices that ranges from edge 10/100Mbps switches to core Gigabit switches. xStack provides unsurpassed performance, fault tolerance, scalable flexibility, robust security, standard-based interoperability and an impressive support for 10 Gigabit technology to future-proof departmental and enterprise network deployments with an easy migration path.

The following manual describes the installation, maintenance and configurations concerning members of the D-Link DES-3800 switch series, including the DES-3828, DES-3828P, DES-3828DC and the DES-3852. These four switches are identical in configurations (except for PoE Functions on the DES-3828P) and very similar in basic hardware and consequentially, most of the information in this manual will be universal to the total group of Switches. Corresponding screen pictures of the web manager may be taken from any one of these switches but the configuration will be identical, except for varying port counts. For the remainder of this document, we will refer to the DES-3800 as the switch in question for examples, configurations and explanations.

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 Switch is equipped with unshielded twisted-pair (UTP) cable ports providing dedicated 10 or 100 Mbps bandwidth. The Switch has twenty-four 10/100BASE-TX ports for the DES-3828, DES-3828P and DES-3828DC, and forty-eight 10/100BASE-TX ports for the DES-3852, all of which are 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 two combo 1000 Base-T/SFP ports on the front panel and two 1000 Base-T ports on the back. These gigabit combo ports are ideal for connecting to a server or network backbone. See the “Ports” section below for differences between the front and rear Gigabit combo ports.

This 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.

Features

- 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
- 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 32M bytes
- 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
- WRED support
- Web-based Access Control
- MAC-Based Access Control
- MIB support for:
    - RFC1213 MIB II
    - RFC1493 Bridge
    - RFC2819 RMON
    - RFC2665 Ether-like MIB
    - RFC2863 Interface MIB
    - Private MIB
    - RFC4363 for P,Q BRIDGE
    - IEEE 802.1x MIB
    - RFC1724 RIPv2
    - RFC1850 OSPF
    - RFC1907 SNMPv2
    - RFC2021 RMON2
    - RFC2906 IP-FORWARD
    - RFC2571 SNMP-FRAMEWORK
    - RFC2572 SNMP-MPD
    - RFC2573 SNMP-TARGET
    - RFC2574 SNMP-USER-BASED-SM
    - RFC2575 SNMP-VIEW-BASED-ACM

  - RFC2576 SNMP-COMMUNITY
  - RFC2618 RADIUS-AUTH-CLIENT
  - RFC2620 RADIUS-ACC- CLIENT
  - RFC2787 VRRP
  - RFC2863 IF
  - RFC2932 IPMROUTE-STD
  - RFC-2933 IGMP-STD
  - RFC-2934 PIM
  -
- IEEE 802.3x flow control in full duplex mode
- IEEE 802.1p Priority Queues
- IEEE 802.3u 100BASE-TX compliant
- RS-232 DCE console port for Switch management
- Provides parallel LED display for port status such as link/act, speed, etc.
- IEEE 802.3 10BASE-T compliant
- High performance switching engine performs forwarding and filtering at 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.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed

Ports

The Switch provides twenty-four 10/100BASE-TX ports for the DES-3828, DES-3828P and DES-3828DC, and forty-eight 10/100BASE-TX ports for the DES-3852. All 10/100BASE-TX ports comply with the following standards:

- IEEE 802.3
- IEEE 802.3u
- Support Half/Full-Duplex operations
- All ports support Auto MDI-X/MDI-II cross over
- Support back pressure for Half-duplex mode
- IEEE 802.3x Flow Control support for Full-Duplex mode.

NOTE: On the DES-3828P, all twenty-four 10/100BASE-TX ports also comply with the IEEE 802.3af Power over Ethernet standard.

The Switch provides two 1000 BASE-T/SFP combo ports on the front panel for all models. Both 1000BASE-T ports comply with the following standards:

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- Support Full-Duplex operations
- IEEE 802.3x Flow Control support for Full-Duplex mode
- IEEE 802.3z

Both SFP ports support the following transceivers:

- DEM-310GT (1000BASE-LX)
- DEM-311GT (1000BASE-SX)
- DEM-314GT (1000BASE-LH)
- DEM-315GT (1000BASE-ZX)

The Switch provides two 1000 BASE-T ports on the rear panel. Both 1000BASE-T ports comply with the following standards:

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- Support Full-Duplex operations
- IEEE 802.3x Flow Control support for Full-Duplex mode

NOTE: The SFP combo ports on the Switch cannot be used simultaneously with the corresponding 1000BASE-T ports. If both ports are in use at the same time (ex. port 25 of the SFP and port 25 of the 1000BASE-T), the SFP ports will take priority over the combo ports and render the 1000BASE-T ports inoperable.

Front-Panel Components

The front panel of the Switch provides twenty-four 10/100BASE-TX ports for the DES-3828, DES-3828P and DES-3828DC, and forty-eight 10/100BASE-TX ports for the DES-3852, two 1000 Base-T/SFP combo ports, and an RS-232 console port (for the DES-3828, DES-3828P and DES-3828DC only). The DES-3828P also includes a Mode Select button for changing the mode from Link/Act/State to PoE.

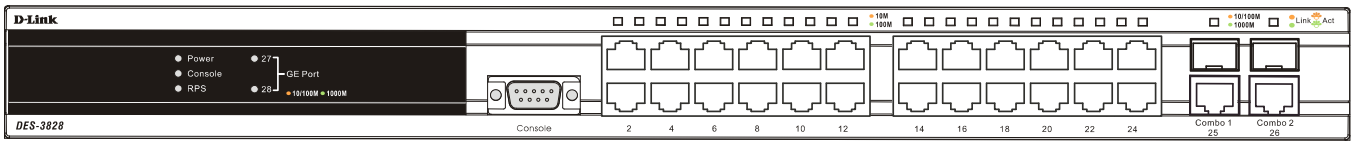


Figure 1- 1. Front Panel of the DES-3828

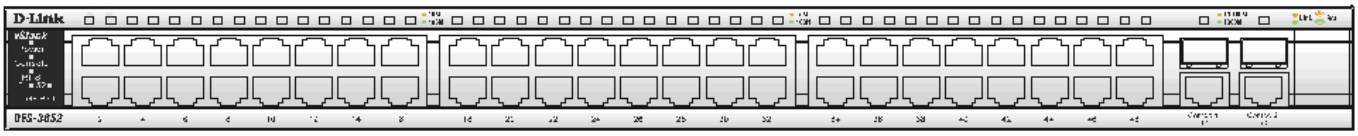


Figure 1- 2. Front Panel of the DES-3852

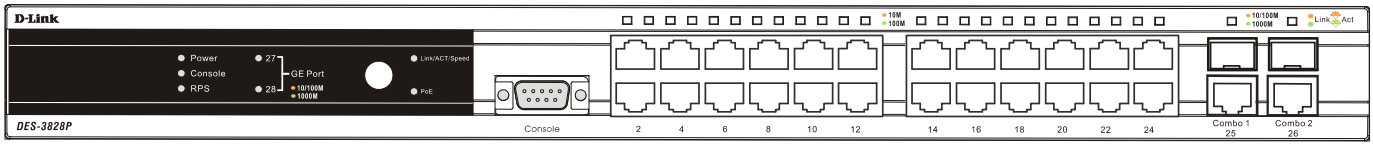


Figure 1- 3. Front Panel of the DES-3828P

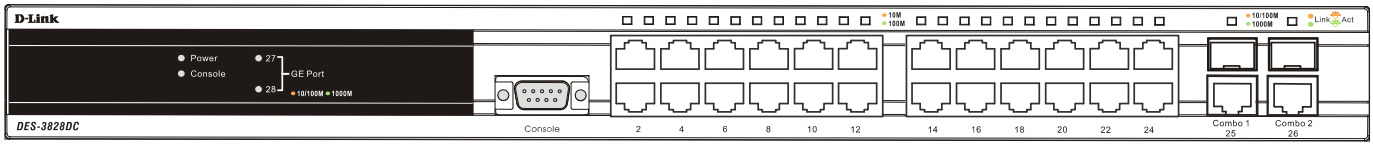


Figure 1- 4. Front Panel of the DES-3828DC

DES-3828P LEDs

LED indicators display the status of the Switch and the network. The front panel of DES-3828P has LED indicators for power, console, RPS, 27GE (rear port), 28 GE (rear port), Link/Act/Speed, PoE, for each of the twenty-four 10/100 Mbps Ethernet ports, and for the two 1000BASE-T/SFP ports.

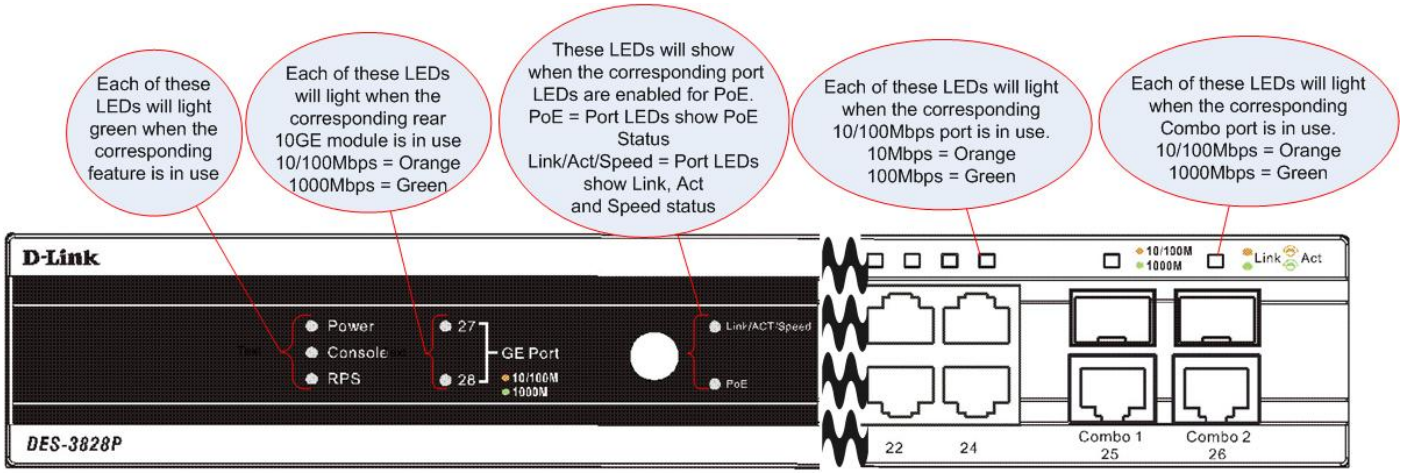


Figure 1- 5. Front Panel View of the DES-3828P

DES-3828/DES-3828DC LEDs

The front panel of DES-3828/DES-3828DC has LED indicators for power, console, RPS (DES-3828 only), 27GE (rear port), 28 GE (rear port), for each of the twenty-four 10/100 Mbps Ethernet ports, and for the two 1000BASE-T/SFP ports.

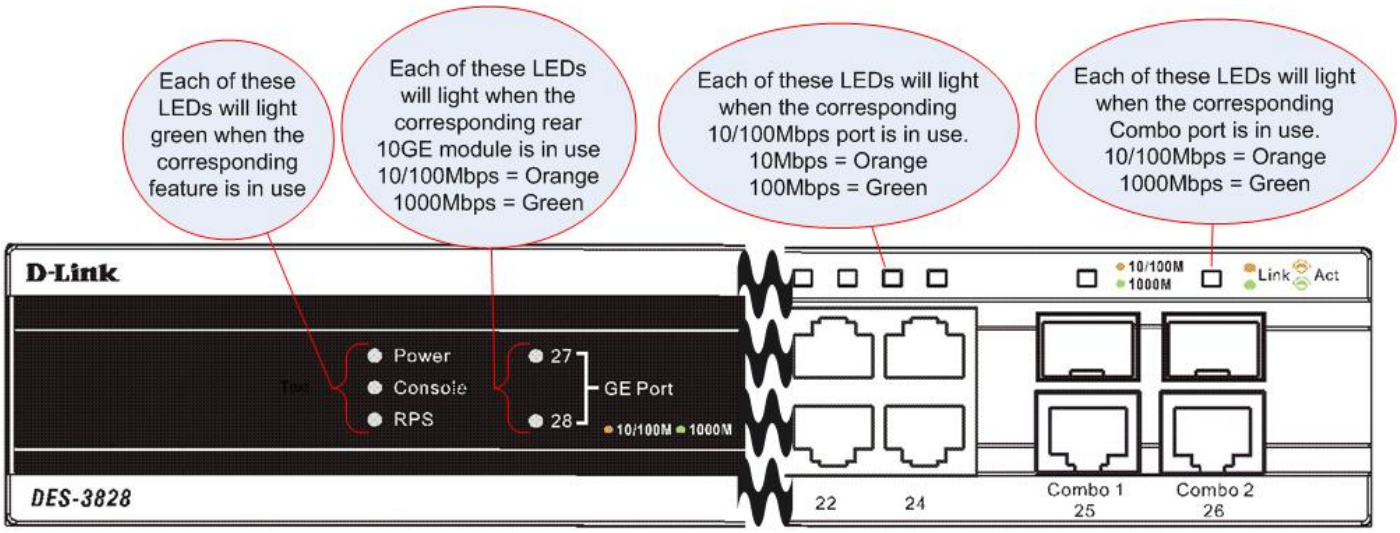


Figure 1- 6. Front Panel View of the DES-3828DC

DES-3852 LEDs

The front panel of DES-3852 has LED indicators for power, console, RPS, port 49 GE, port 50 GE, port 51 GE (rear port), port 52 GE (rear port), for each of the forty-eight 10/100 Mbps Ethernet ports, and for the two 1000BASE-T/SFP ports.

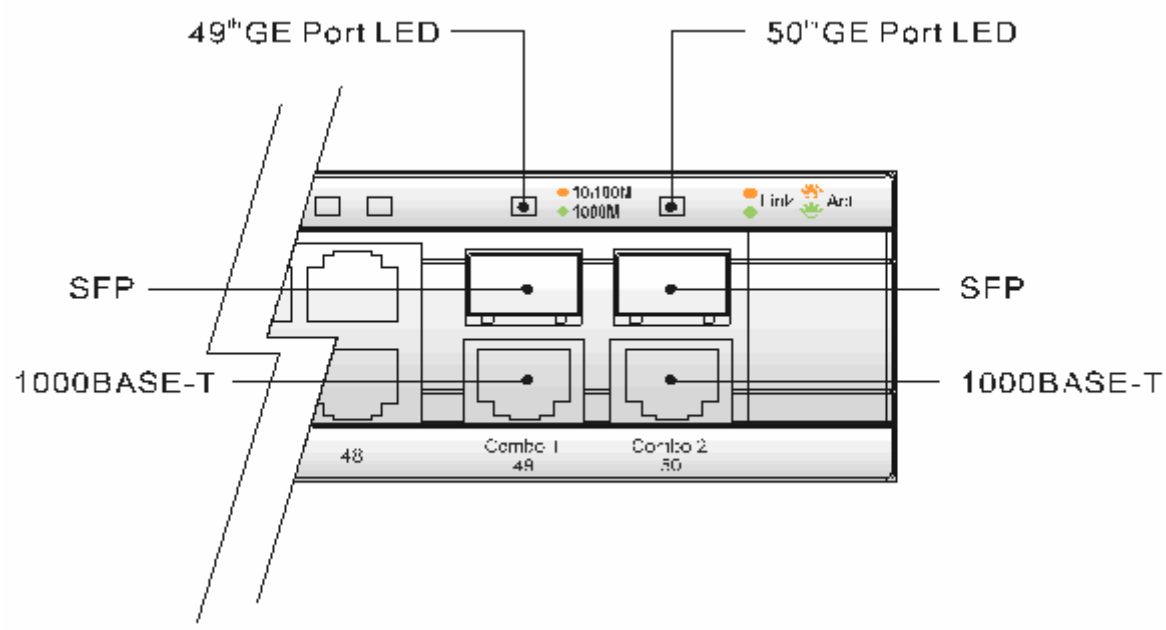


Figure 1- 7. LED Indicators for the DES-3852

The following table describes the LEDs for DES-3828/DES-3828P/DES-3828DC/DES-3852:

LED	Description
Power	Off – Power Off Solid Green – Power On
Console	Solid Green – Switch is being logged in to via the out-of-band/local console management through the RS-232 console port Blinking Green – POST is in progress

RPS (excluding DES-3828DC)	Off – RPS off Solid green – RPS in use
Ports 27, 28 GE (DES-3828/DES-3828P/DES-3828DC) **Ports 51, 52 GE (DES-3852)**	Ports 27 and 28 (51 and 52) represent the 1000BASE-T ports located on the rear panel of the Switch. These port LEDs will light two different colors for 100Mbps and 1000Mbps: • Solid Green – Link for 1000Mbps • Blinking Green – Activity for 1000Mbps • Solid Amber – Link for 100Mbps • Blinking Amber – Activity for 100Mbps • Off – Link down
Link/Act/Speed and PoE (DES-3828P only)	To change the LED mode from Link/Act/Speed to PoE and vice versa, press the LED Mode Select Button. The Link/Act/Speed LED will light solid green when selected and will shut off when PoE is selected. Likewise, when Link/Act/Speed is selected, the PoE LED shuts off and the Link/Act/Speed LED lights solid green. When this LED is in PoE mode, the corresponding port LED denote different meanings: • Solid Green – Power is being used by a device connected to that port. • Blinking Amber – There is a power error occurring on this port. • Off – Power is not currently being fed through this port.
Ports 1-24 (1-48)	One row of LEDs for each port is located above the ports on the front panel. The first LED is for the top port and the second one is for the bottom ports. These port LEDs display the following information: For Link/Act/Speed Mode: • Solid Green – Link for 100Mbps • Blinking Green – Activity for 100Mbps • Solid Amber – Link for 10Mbps • Blinking Amber – Activity for 10Mbps • Off – Link down For PoE Mode: (DES-3828P only) • Solid Green – Power feeding (802.3af-compliant PD was detected, legacy PD detected) • Blinking Amber – A blinking amber LED may signify any of the following: PoE port ERROR (non-standard PD connected, Under load state according to 802.3af (current is below I min), Overload state according to 802.3af (current is above I cut), hardware problems preventing port operation, power budget exceeded, short condition was detected at a port delivering power, temperature overload at the port, succession of Underload and Overload states caused port shutdown (may be caused by a PD's DC/DC fault)...etc.) • Off – No power feeding (no PD detected, or no connection)
Ports 25, 26 combo GE (DES-3828/DES-3828P/DES-3828DC) **Ports 49, 50 combo GE (DES-3852)**	Ports 25 and 26 (49, 50) represent the 1000BASE-T/SFP ports located on the front panel of the Switch. These port LEDs will display the following information: • Solid Green – Link for 1000Mbps • Blinking Green – Activity for 1000Mbps • Solid Amber – Link for 100Mbps • Blinking Amber – Activity for 100Mbps • Off – Link down

Rear Panel Description

The rear panels of DES-3828, DES-3828DC, DES-3828P and DES-3852 are described separately below.

DES-3828

The rear panel of DES-3828 contains ports 27 and 28, (1000BASE-TX), an AC power connector, and an outlet for an optional external RPS.

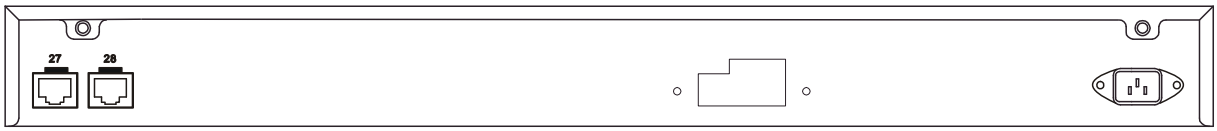


Figure 1- 8. Rear panel view of the DES-3828

For details on ports 27 and 28, see the "Ports" description above. The rear panel includes an outlet for an optional external redundant power supply. When power fails, the optional external RPS will take over all the power immediately and automatically. 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.

DES-3828P

The rear panel of DES-3828P contains ports 27 and 28, (1000BASE-TX), a heat vent, an AC power connector, and an outlet for an optional external RPS.

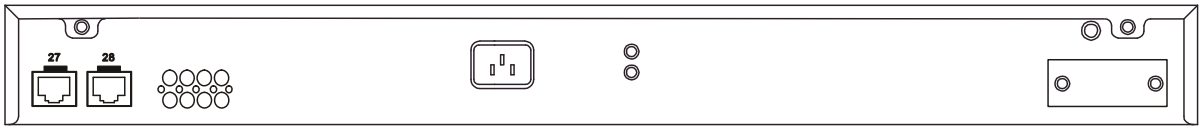


Figure 1- 9. Rear Panel view of DES-3828P

For details on ports 27 and 28, see the "Ports" description above. The rear panel includes a heat vent for the system fan. The system fan is used to dissipate heat. Do not block this opening, and leave at least 6 inches of space at the rear 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. The rear panel also includes an outlet for an optional external redundant power supply. When power fails, the optional external RPS will take over all the power immediately and automatically. 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 maximum output capacity for PoE is 370W. The default power feed for PoE is set at 15.4W per port, but can be set from 1-16.8W per port. See the PoE Configuration in Section 6 for instructions on how to change this setting.

DES-3828DC

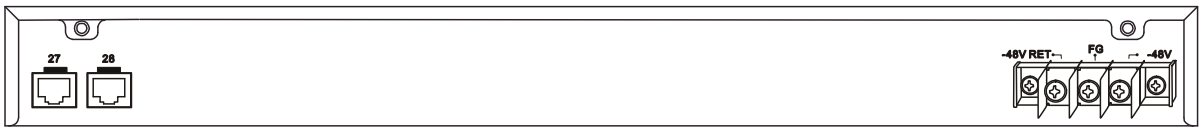


Figure 1- 10. Rear panel view of DES-3828DC

The rear panel of the DC power version of the Switch includes ports 27 and 28, (1000BASE-TX), and an opening designed to accommodate the DC power wiring assembly. See the installation instructions in Section 2 for details.

DES-3852

The rear panel of the DES-3852 contains ports 51 and 52, (1000BASE-TX), an AC power connector, an RS-232 console port and an outlet for an optional external RPS.

Figure 1- 11. Rear Panel of the DES-3852

Side Panel Description

The right-hand side panel of the Switch contains a system fan and ventilation along the entire right side. The left hand panel includes a system fan and a heat vent. The system fans are used to dissipate heat. Do not block these openings on either side of the Switch. 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.

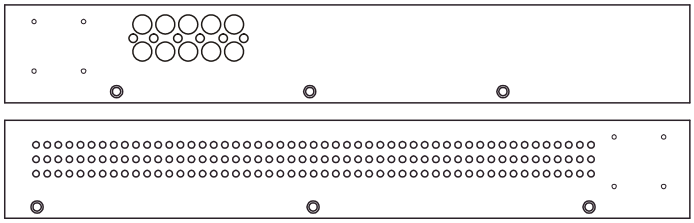


Figure 1- 12. Side Panels

Gigabit Ports

In addition to the twenty-four (forty-eight for DES-3852) 10/100 Mbps ports, the Switch features two 1000BASE-T/SFP Gigabit Ethernet Combo ports on the front panel, and two 1000BASE-T copper ports on the rear panel. The diagrams below show Gigabit ports 25 and 26 (49 and 50) on the far right of the front panel. Gigabit ports 27 and 28 (51 and 52) are on the far left of the rear panel. Please note that PoE is not supported for any Gigabit Ethernet ports.

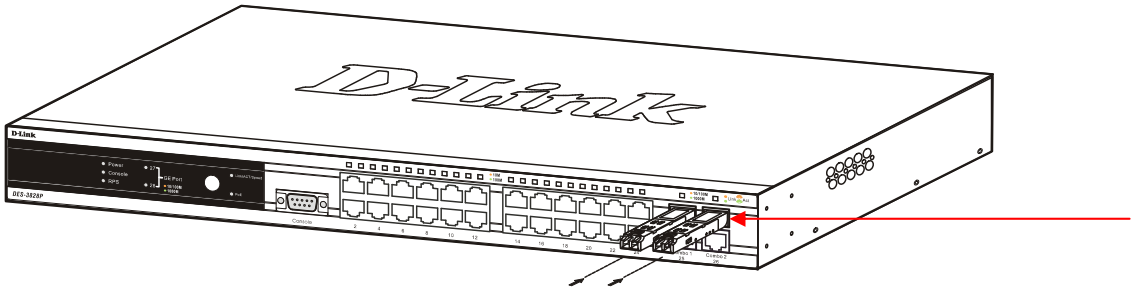


Figure 1- 13. Front Panel Mini-GBIC ports

SECTION 2

Installation

Package Contents

Before You Connect to the Network

Installing the Switch without the Rack

Rack Installation

Power On

Connecting DC Power to DES-3828DC

RPS Installation

Package Contents

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

- One Stand-alone Switch
- One AC power cord (excluding DES-3828DC)
- This Manual on CD
- Mounting kit (two brackets and screws)
- Four rubber feet with adhesive backing
- RS-232 console cable

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

Before You Connect to the Network

The site where users 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 4.24kg (9.35lbs) of weight for DES-3828/DES-3828DC/DES-3852, or 6.02kg (13.27lbs) for DES-3828P. 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/DC 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.

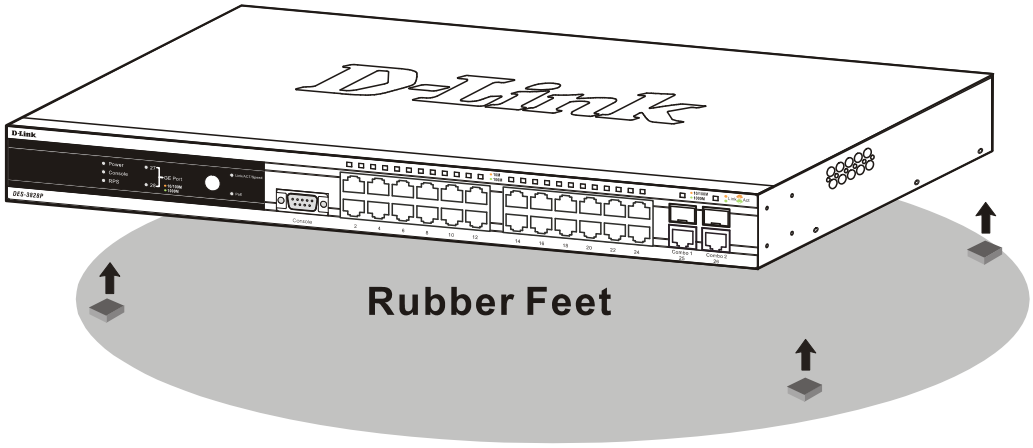


Figure 2 - 1. Prepare Switch for installation on a desktop or shelf

Installing the Switch in a Rack

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

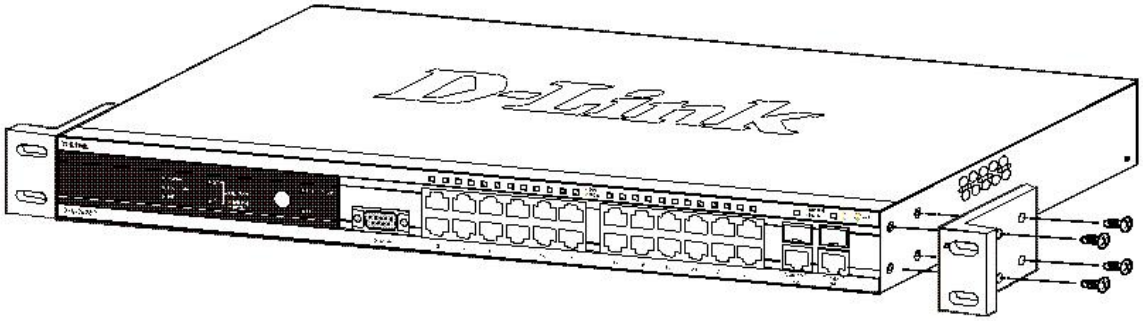


Figure 2 - 2. Fasten mounting brackets to Switch

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, users 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.

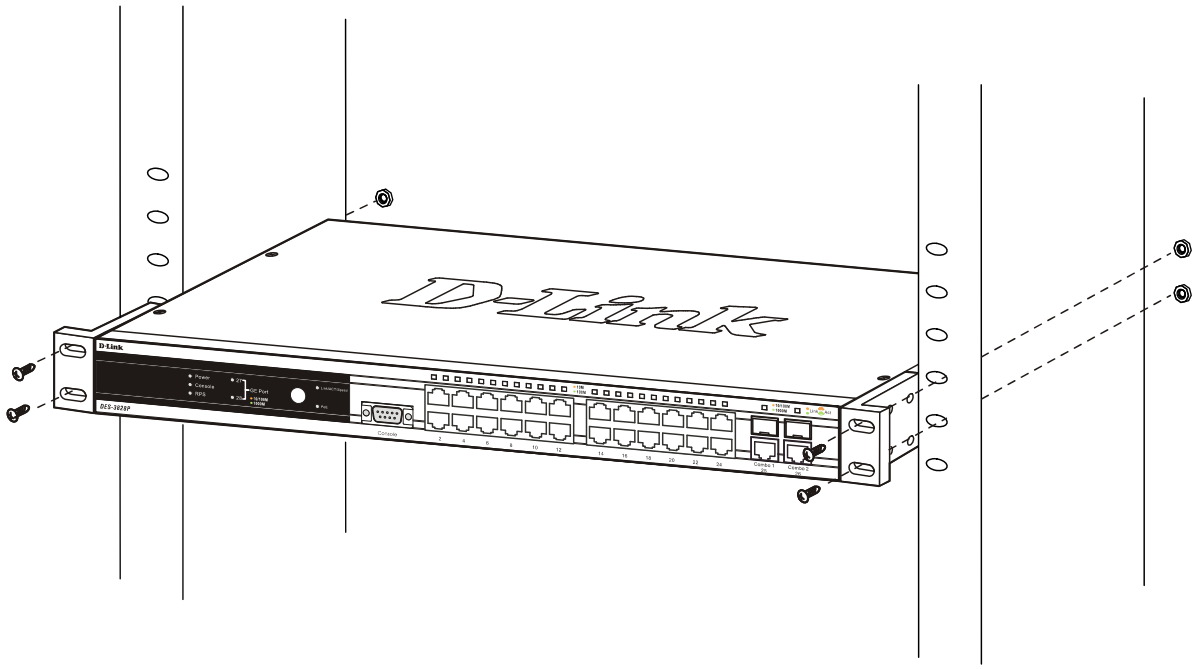


Figure 2 - 3. Installing Switch in a rack

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

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

Connecting DC Power to the DES-3828DC

Follow the instructions below to connect the DC power supply of the DES-3828DC to the DC power source.

Figure 2 - 4. Power connections attached to contacts after assembly

1. Firmly attach the DC power to the negative and positive contacts on the wiring assembly.
    - The negative pole (-) connects to the **-48V** contact.
    - The positive pole (+) connects to the **-48V Return** contact.
    - If available, an earth ground may be connected to the center contact post.
2. Tighten the contact screws to secure the connection.

RPS Installation

Follow the instructions below to connect an RPS power supply to the Switch (DPS-200 to DES-3828/DES-3852 or DPS-600 to DES-3828P). The DPS-200 is a redundant power-supply unit designed to conform to the voltage requirements of the switches being supported. DPS-200 can be installed into DPS-900, or DPS-800.

CAUTION: The AC power cord for the Switch should be disconnected before proceeding with installation of the DPS-200.

DPS-900

The DPS-900 is a standard-size rack mount (5 standard units in height) designed to hold up to eight DPS-200 redundant power supplies.

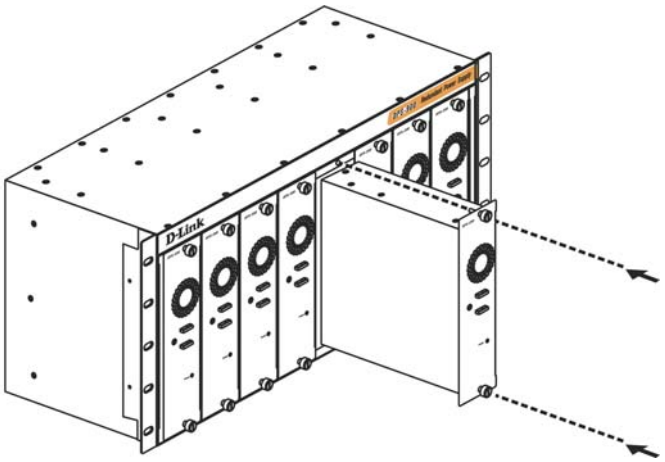


Figure 2 - 5. Installing the DPS-200 into the DPS-900

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

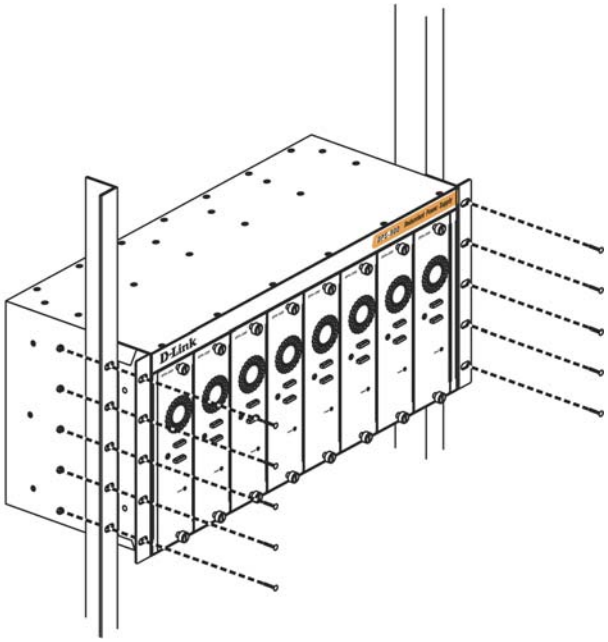


Figure 2 - 6. Installing the DPS-900 into the equipment rack

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.

DPS-800

The DPS-800 is a standard-size rack mount (1 standard unit in height) designed to hold up to two DPS-200 redundant power supplies.

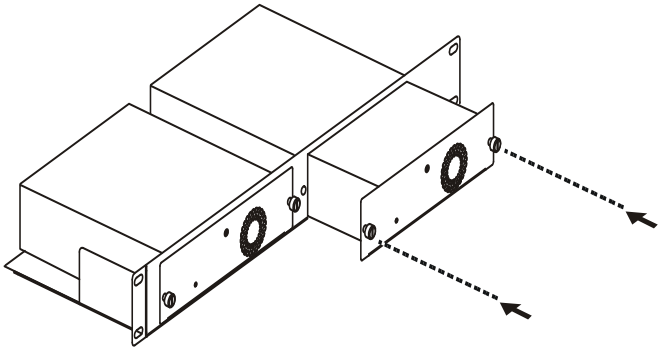


Figure 2 - 7. Install DPS-200 in DPS-800

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

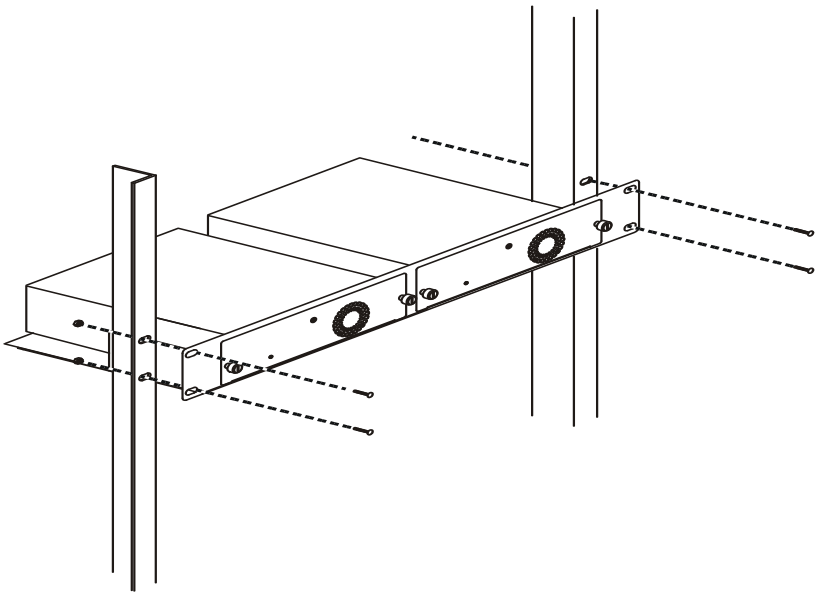


Figure 2 - 8. Install DPS-800 in an Equipment Rack

Connect to RPS

The DPS-200 is connected to the Master Switch using a 14-pin DC power cable. A standard, three-pronged AC power cable connects the redundant power supply to the main power source.

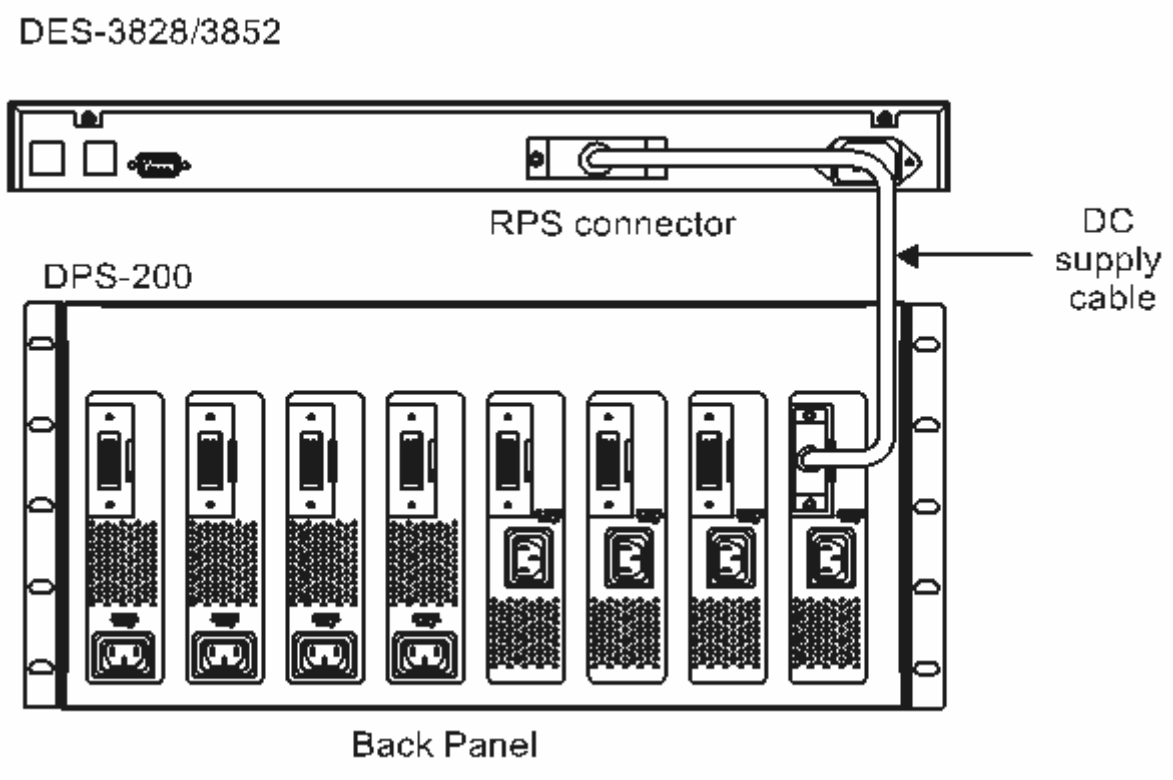


Figure 2 - 9. The DES-3828 with the DPS-200 chassis RPS

1. Insert one end of the 14-pin DC power cable into the receptacle on the Switch and the other end into the redundant power supply.
2. Using a standard AC power cable, connect the redundant power supply to the main AC power source. A green LED on the front of the DPS-200 will glow to indicate a successful connection.
3. Re-connect the switch to the AC power source. On certain switches, such as the DES-3828, an LED indicator will show that a redundant power supply is now in operation.
4. No change in switch configuration is necessary for this installation.

NOTE: See the DPS-200 documentation for more information.

CAUTION: Do not use the Switch with any redundant power system other than the DPS-200 or DPS-600.

DPS-600

DES-3828P also supports the DPS-600 external redundant power supply.

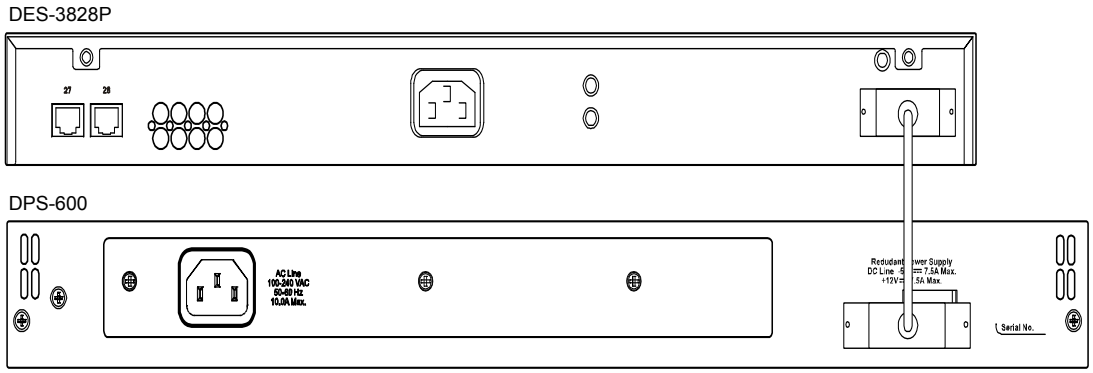


Figure 2 - 10. DES-3828P with the DPS-600 External Redundant Rower Supply

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.

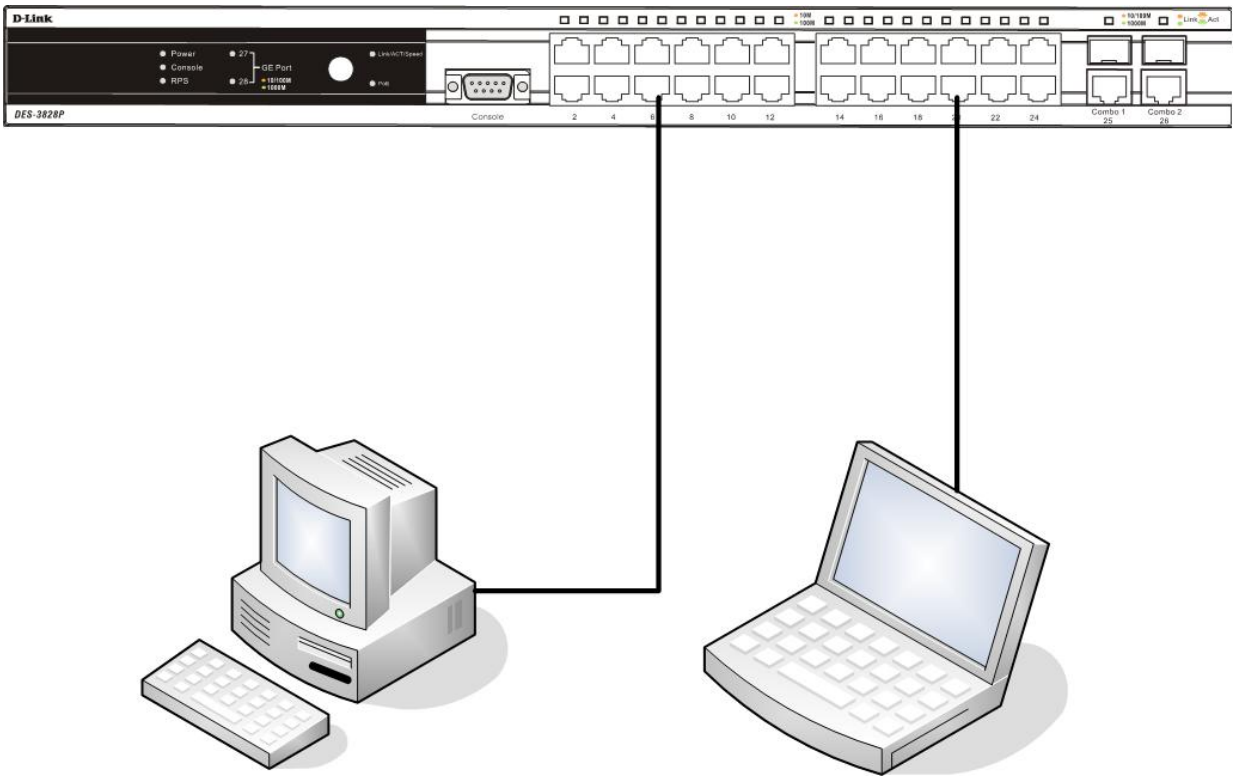


Figure 3- 1. Switch connected to an end node

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.
- A 1000BASE-T switch can be connected to the Switch via a twisted pair Category 5e UTP/STP cable.
- A switch supporting a fiber-optic uplink can be connected to the Switch's SFP ports via fiber-optic cabling.
- The Switch can be changed to PoE mode using the Mode Select button. When in PoE Mode, the DES-3828P will work with all D-Link 802.3af capable devices. The Switch also works in PoE mode with all non-802.3af capable D-Link AP, IP Cam and IP phone equipment via DWL-P50.

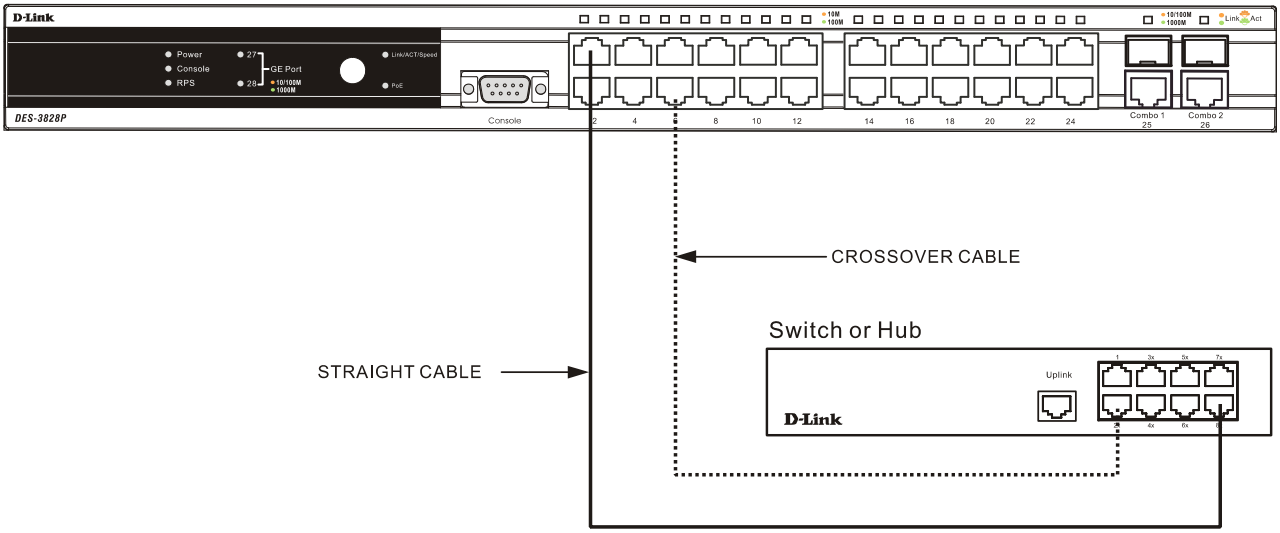


Figure 3- 2. Switch connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

NOTICE: When the SFP transceiver acquires a link, the associated integrated 10/100/1000BASE-T port is disabled.

Connecting To Network Backbone or Server

The two Mini-GBIC combo ports are ideal for unlinking to a network backbone or server. The copper ports operate at a speed of 1000, 100 or 10Mbps in full duplex mode. The fiber optic ports can operate at 1000Mbps in full duplex mode. Connections to the Gigabit Ethernet ports are made using fiber optic cable or Category 5 copper cable, depending on the type of port. A valid connection is indicated when the Link LED is lit.

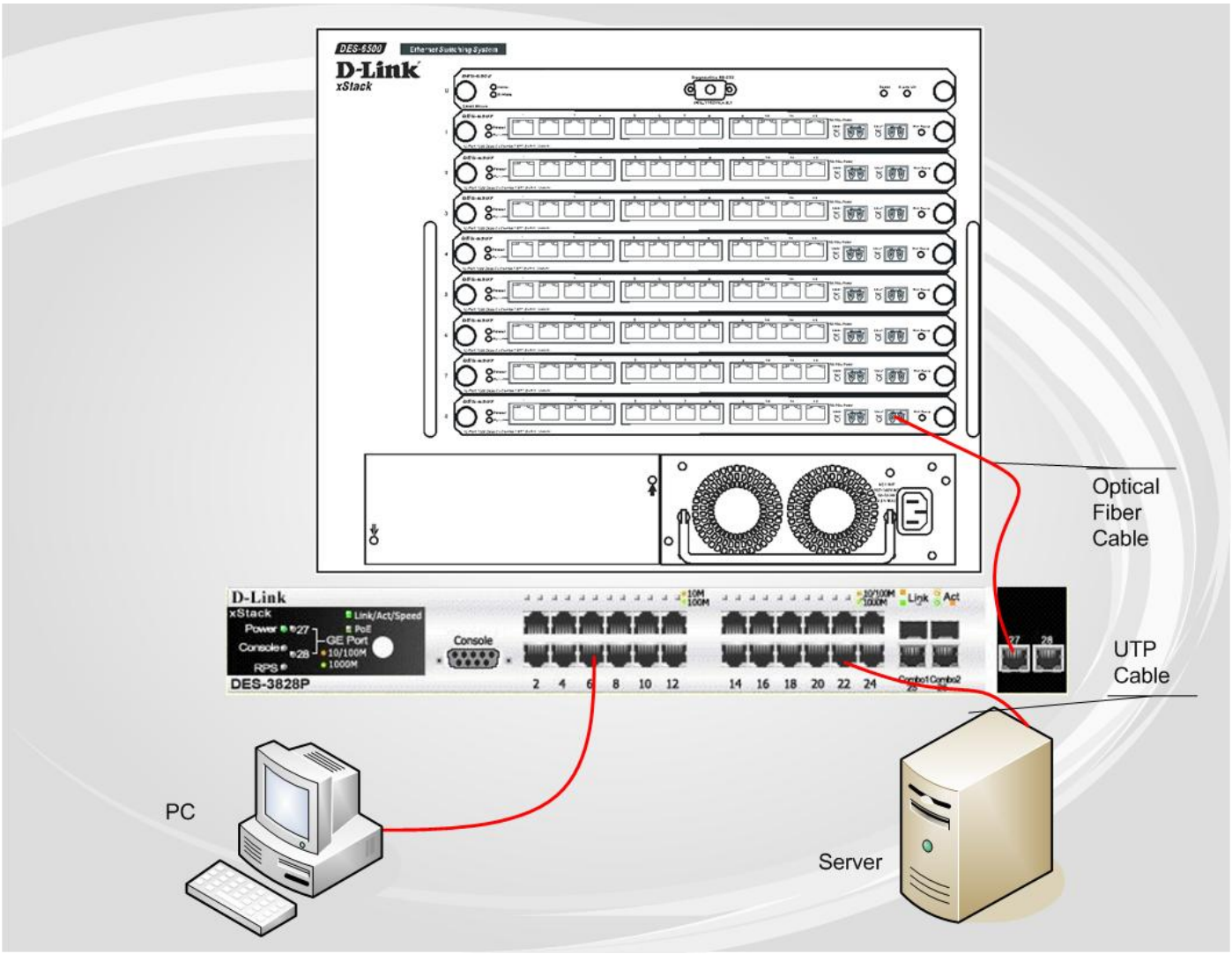


Figure 3- 3. Uplink Connection to a server, PC or switch stack.

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 and higher) or Microsoft® Internet Explorer (version 5.0).

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 Communication 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 straight-through RS-232 cable with a female DB-9 connector for the console port on the Switch.

To connect a terminal to the console port:

1. Connect the female 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 9600 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 user accounts have been previously set, 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 ***xStack DES-3800 Series CLI Manual*** on the documentation CD for a list of all commands and additional information on using the CLI.
13. When all tasks have been completed, 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 users have problems making this connection on a PC, make sure the emulation is set to VT-100. 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 users still do not see anything, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear. 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-3828 Fast Ethernet Switch Command Line Interface

                        Firmware: Build 4.50.B10

     Copyright(c) 2008 D-Link Corporation. All rights reserved.

UserName:
```

Figure 4- 1. Initial screen after first connection

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.

First Time Connecting to the Switch

The Switch supports user-based security that can allow prevention of 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."

Upon initial connection to the Switch, users 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-3828:admin#** shown below:

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

```
        DES-3828 Fast Ethernet Switch Command Line Interface

                      Firmware: Build 4.50.B10

    Copyright(c) 2008 D-Link Corporation. All rights reserved.

UserName:

Password:

DES-3828:admin#
```

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. If logging in using a predefined administrator-level user name, users will have privileged access to the Switch's management software.

After the 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.
- Users will be asked to provide a password. Type the <*password*> used for the administrator account being created and press the Enter key.
- Users will then 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-3828:admin#create account admin newmanager
Command: create account admin newmanager

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

Success.

DES-3828:admin#
```

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

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.

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-3800 Series 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, users 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-3828:admin#show switch
Command:show switch

Device Type : DES-3828 Fast-Ethernet Switch
Combo Port Tpye : 1000Base-T + 1000Base-T
MAC Address : 00-01-02-03-04-00
IP Address : 10.53.13.83 (Manual)
VLAN Name : default
Subnet Mask : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 0.00.010
Firmware Version  : Build 4.50-B10
Hardware Version  : 1A2G
Serial Number     : N/A
Power Status      : Main - Normal, Redundant - Not Present
System Name       : D-Link
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
TELNET            : Enabled (TCP 23)
SSH               : Disabled
WEB               : Enabled (TCP 80)
RMON              : Disabled
RIP               : Disabled
DCMRP             : Disabled
PIN               : Disabled
OSPF              : Disabled
SNMP              : Disabled

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

Figure 4- 3. 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, users 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-3828:admin#config ipif System ipaddress 10.53.13.83/255.0.0.0
Command: config ipif System ipaddress 10.53.13.83/8

Note: All configurations on this interface will return to default
setting.

Success.


DES-3828:admin#
```

Figure 4- 4. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.83 with a subnet mask of 255.0.0.0. The user may also use the CIDR form to set the address (10.53.13.83/8). 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 installed on your computer and point it to the IP address 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.

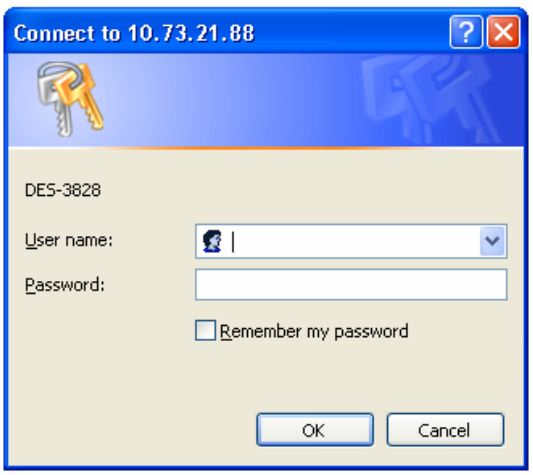


Figure 5- 1. Enter Network Password window

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

Web-based User Interface

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

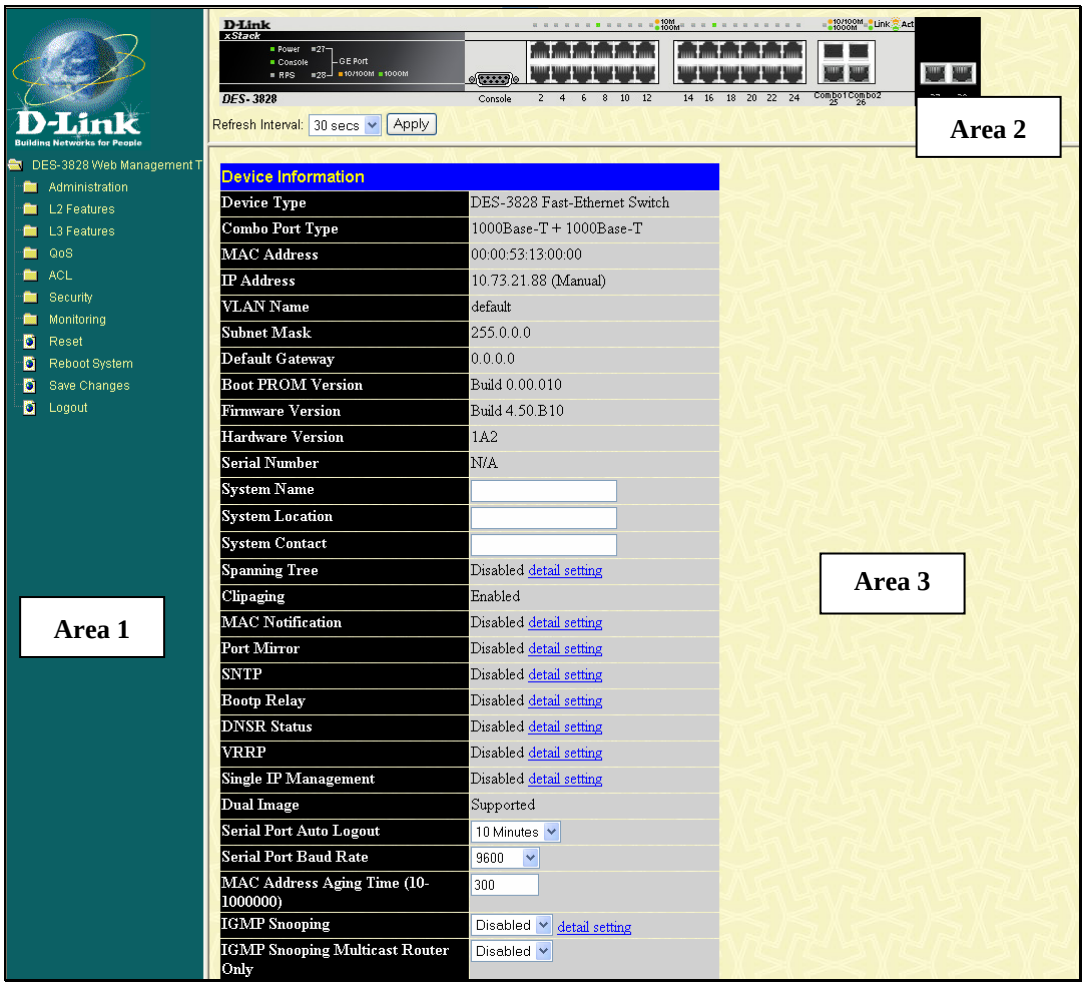


Figure 5- 2. Main Web-Manager page

Area	Function
Area 1	Select the menu or window to be displayed. The folder icons can be opened to display the hyper-linked menu 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 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 users 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:

Administration – Contains windows concerning Device Information, IP Address, Port Configuration, PoE Configuration (for the DES-3828P), User Accounts, Port Mirroring, System Log Settings, System Severity Settings, SNTP Settings, MAC Notification Settings, TFTP Services, Multiple Image Services, Dual Configurations Services, Ping Test, SNMP Manager, and Single IP Management Settings.

Layer 2 Features – Contains windows concerning VLAN, Trunking, IGMP Snooping, Spanning Tree and Forwarding.

Layer 3 Features – Contains windows concerning IP Interfaces Settings, MD5 Key Settings, Route Redistribution Settings, Static/Default Route Settings, Route Preference Settings, Static ARP Settings, RIP, OSPF, DHCP/BOOTP Relay, DNS Relay, VRRP, and IP Multicast Routing Settings.

QoS – Contains windows concerning Bandwidth Control, QoS Scheduling Mechanism, QoS Output Scheduling, 802.1P Default Priority, 802.1P User Priority and WRED Settings.

ACL – Contains the window for the Access Profile Table and CPU Interface Filtering.

Security – Contains windows for Traffic Control, Port Security, Port Lock Entries, 802.1x, Trusted Host, Access Authentication Control, Traffic Segmentation, SSL, SSH, IP-MAC Binding, Limited IP Multicast Range, Web-based Access Control, MAC-based Access Control and Safeguard Engine.

Monitoring – Contains windows for Device Status, CPU Utilization, Safeguard Engine Status, Port Utilization, Packets, Errors, Packet Size, Browse Router Port, Port Access Control, MAC Address Table, IP Address Table, Browse Routing Table, Browse ARP Table, Browse IP Multicast Forwarding Table, IGMP Snooping Group, IGMP Snooping Forwarding, Browse IGMP Group Table, DVMRP Monitor, PIM Monitor, OSPF Monitor, Browse PoE Status, Browse WRED Settings and Switch Log.

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

Section 6

Administration

Device Information

IP Address

Port Configuration

PoE Configuration

User Accounts

Port Mirroring

System Log Settings

System Severity Settings

SNTP Settings

MAC Notification Settings

TFTP Services

Multiple Image Services

Dual Configurations Services

Ping Test

SNMP Manager

Single IP Management Setting

Packet to CPU Settings

Device Information

The **Device Information** window contains the main settings for all major functions for the Switch and appears automatically when you log on. To return to the **Device Information** window, click the **DES-3800 Web Management Tool** folder. The Device Information window shows the Switch's **MAC Address** (assigned by the factory and unchangeable), the **Boot PROM**, **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. The user may also enter a **System Name**, **System Location** and **System Contact** to aid in defining the Switch, to the user's preference. In addition, this screen 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.

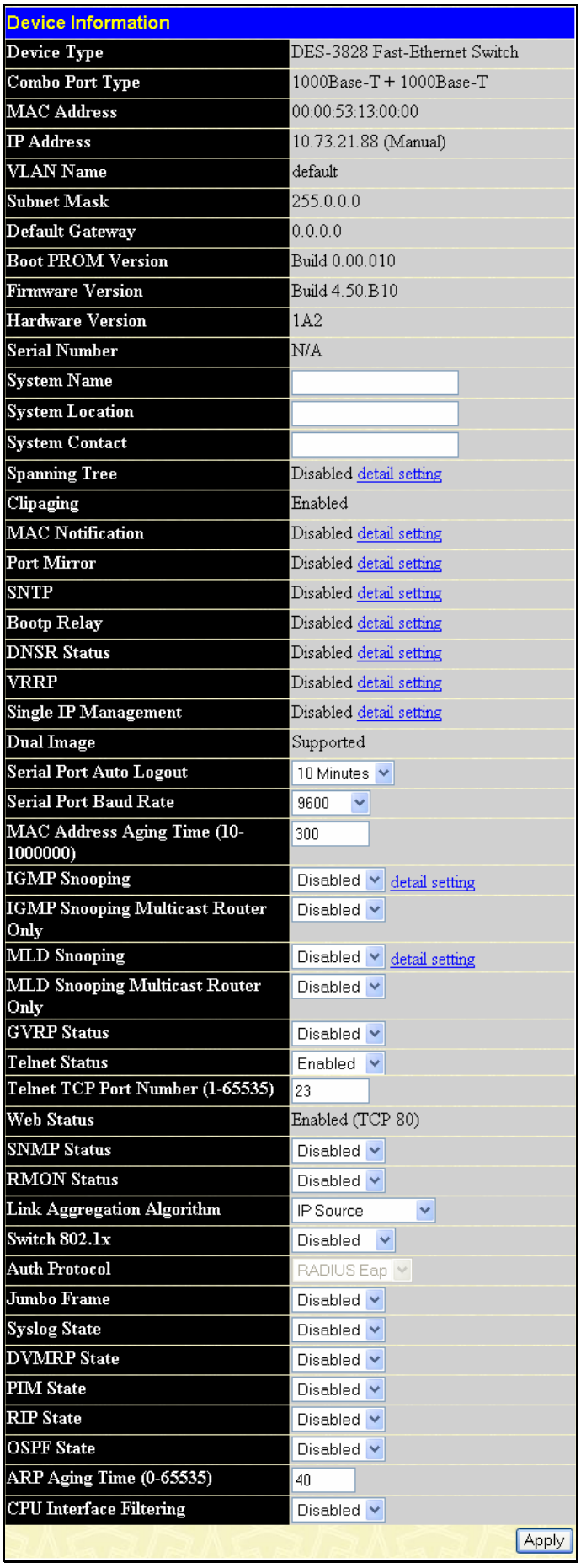


Figure 6- 1. Device Information window

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 the Switch on 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.
Dual Image	Displays the Dual Image support for the Switch, or the ability to store more than one firmware code on the Switch without implementation.
Serial Port Auto Logout Time	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*.
Serial 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 *9600*, which is the default setting.
MAC Address Aging Time	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this, type in a different value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1,000,000* seconds. The default setting is *300* seconds.
IGMP Snooping	To enable system-wide IGMP Snooping capability select *Enabled*. IGMP snooping is *Disabled* by default. Enabling IGMP snooping allows you to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the **IGMP Snooping** located in the **IGMP Snooping** folder contained in the **L2 Features** folder.
Multicast Router Only	This field specifies that the Switch should only forward all multicast traffic to a multicast-enabled router, if enabled. Otherwise, the Switch will forward all multicast traffic to any IP router. The default is *Disabled*.
GVRP Status	Use this pull-down menu to enable or disable GVRP on the Switch.
Telnet Status	Telnet configuration is *Enabled* by default. If you do not want to allow configuration of the system through Telnet choose *Disabled*.
Telnet TCP Port Number (1-65535)	The TCP port number. TCP ports are numbered between *1* and *65535*. The "well-known" TCP port for the Telnet protocol is *23*.
Web Status	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.
SNMP Status	Simple Network Monitoring Protocol (SNMP) of the Switch is *Enabled* or *Disabled* here. The Default is *Disabled*.
RMON Status	Remote monitoring (RMON) of the Switch is *Enabled* or *Disabled* here.
Link Aggregation 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 Src & Dest*, *IP Source, IP Destination* or *IP Src & Dest* (See the Link Aggregation section of this manual).
Switch 802.1x	MAC Address may enable by port or the Switch's 802.1x function; the default is *Disabled*. This field must be enabled to view and configure certain windows for 802.1x. More information regarding 802.1x, its functions and implementation can be found later in this section, under the **Port Access Entity** folder. Port-Based 802.1x specifies that ports configured for 802.1x are initialized based on the port number only and are subject to any authorization parameters configured. MAC-based Authorization specifies that ports configured for 802.1x are initialized based on

	the port number and the MAC address of the computer being authorized and are then subject to any authorization parameters configured.
Auth Protocol	The 802.1x authentication protocol on the Switch is set to RADIUS Eap and cannot be altered.
Jumbo Frame	This field will enable or disable the Jumbo Frame function on the Switch. The default is Disabled. When enabled, jumbo frames (frames larger than the standard Ethernet frame size of 1518 bytes) of up to 9K (and 9220 bytes tagged) can be transmitted by the Switch.
Syslog State	Enables or disables Syslog State; default is *Disabled*.
DVMRP State	The user may globally enable or disable the Distance Vector Multicast Routing Protocol (DVMRP) function by using the pull down menu.
PIM State	The user may globally enable or disable the Protocol Independent Multicast (PIM) function by using the pull down menu.
RIP State	The user may globally enable or disable the Routing Information Protocol (RIP) function by using the pull down menu.
OSPF State	The user may globally enable or disable the Open Shortest Path first (OSPF) function by using the pull down menu.
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.
CPU Interface Filtering	The user may globally enable or disable the CPU Interface Filtering function by using the pull down menu.

Click **Apply** to implement changes made.

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 *xStack DES-3800 Series 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 menu located in the Administration folder.

To configure the Switch's IP address:

The web manager will display the Switch's current IP settings in the IP configuration menu, as seen below. To view this window click, **Administration** > **IP Address**.

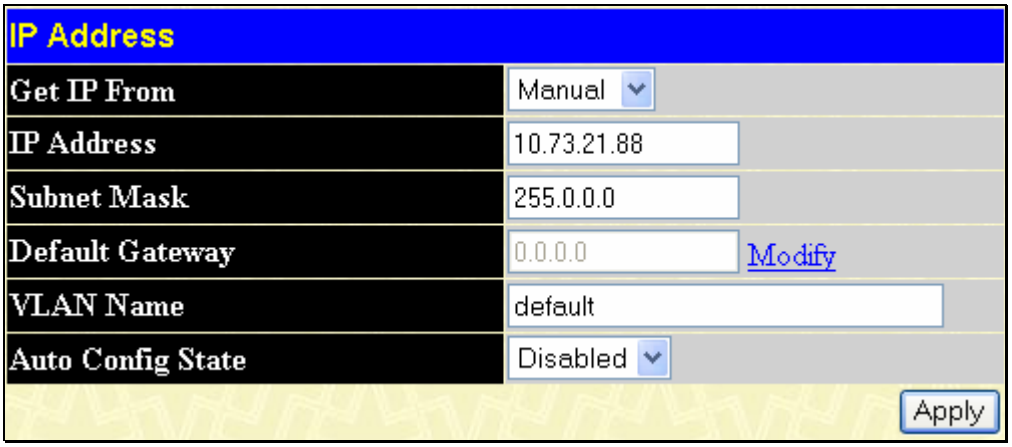


Figure 6- 2. IP Address Settings window

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

1. Select *Manual* from the Get IP From drop-down menu.
2. Enter the appropriate IP Address and Subnet Mask.

3. To access the Switch from a different subnet from the one it is installed on, click the **Modify** link next to *Default Gateway* and enter the IP address of the Default Gateway. To manage the Switch from the subnet on which it is installed, leave the default entry in this field.
4. If no VLANs have been previously configured on the Switch, 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, users will need to enter the *VLAN ID* 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, use the **Get IP From** pull-down menu to choose from *BOOTP* or *DHCP*. This selects how the Switch will be assigned an IP address on the next reboot.

NOTE: If you enable the **AutoConfig**, the **Get IP From** setting will automatically become DHCP.

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.
Manual	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.
Default 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.
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 menu. 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.
Auto Config State	When autoconfig is enabled, the Switch is instructed to get a configuration file via TFTP, and it becomes a DHCP client automatically. The configuration file will be loaded upon booting up. In order to use Auto Config, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be running and have the requested configuration file stored in its base directory when the request is received from the Switch. Consult the DHCP server and/or TFTP server software instructions for information on loading a configuration file for use by a client.

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

Click **Apply** to let changes 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 actuall 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 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 **Administration** > **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.
2. Use the remaining pull-down menus to configure the parameters described below:

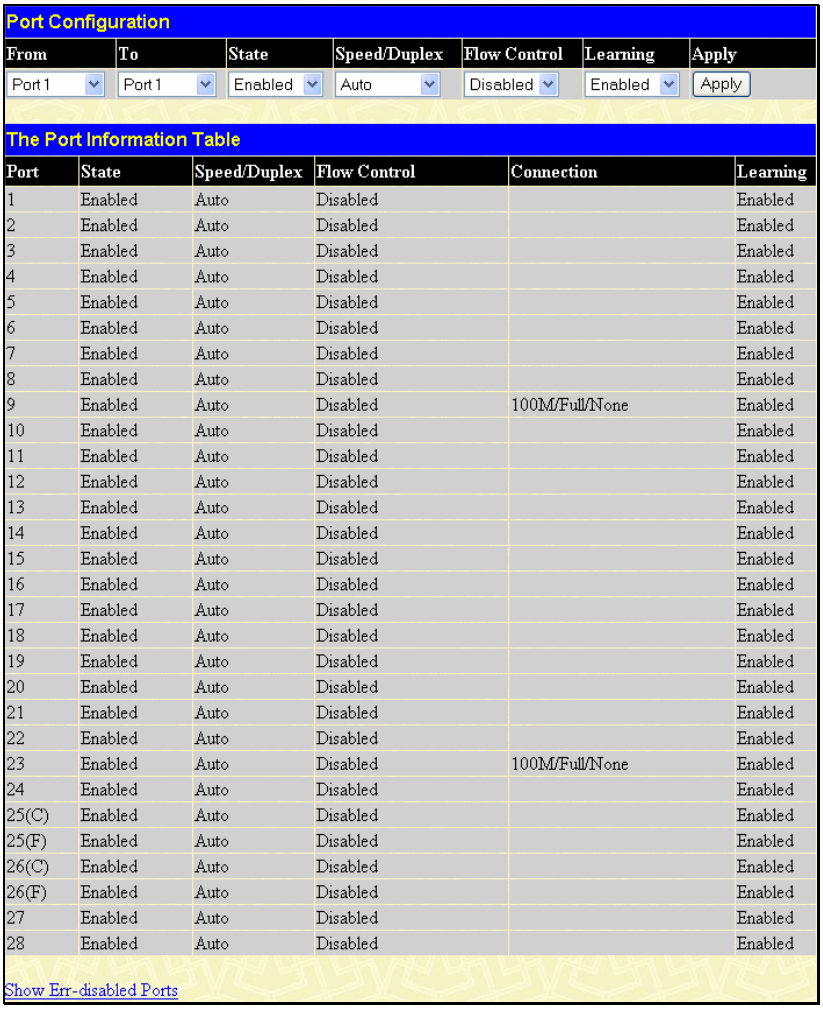


Figure 6- 3. Port Configuration window

The following parameters can be configured:

Parameter	Description
From / To	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*, *100M/Full and 1000M/Full*. There is no automatic adjustment of port settings with any option other than Auto.

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*.
Learning	Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is *Disabled*.

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

At the bottom of the Port Configuration window is a Show Err-disabled ports link to display the information about ports that have had their connection status disabled, for reasons such as loopback detection or link down status. Clicking this link will display the following window:

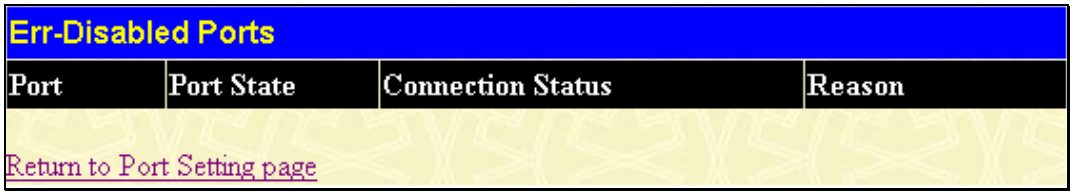


Figure 6- 4. Err-Disabled Ports window

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 **Administration** > **Port Configuration** > **Port Description** to view the following window:

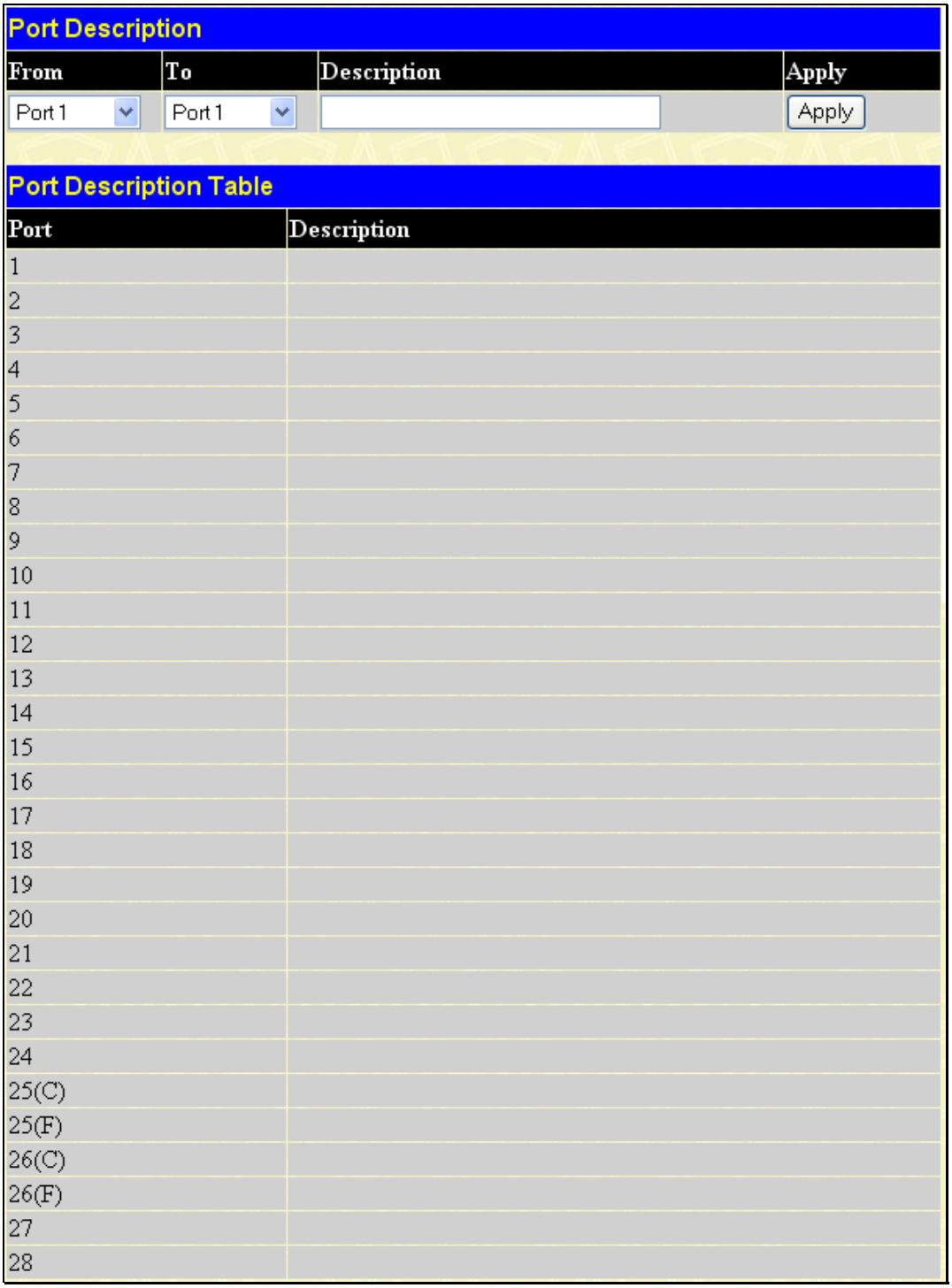


Figure 6- 5. Port Description Setting window

Use the **From** and **To** pull down menus to choose a port or range of ports that need descriptions and then enter a description of the port(s). Click **Apply** to set the descriptions in the **Port Description Table**.

PoE Configuration

The DES-3828P supports Power over Ethernet (PoE) as defined by the IEEE 802.3af specification. Ports 1-24 can supply 48 VDC power to Power Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. DES-3828P follows the standard PSE (Power Source over Ethernet) pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. DES-3828P works with all D-Link 802.3af capable devices.

DES-3828P includes the following PoE features:

- Auto-discovery recognizes the connection of a PD (Power Device) and automatically sends power to it.
- The Auto-disable feature will occur under two conditions: first, if the total power consumption exceeds the system power limit; and second, if the per port power consumption exceeds the per port power limit.
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

PDs receive power according to the following classification:

Class	Max power used by PD
0	0.44 to 12.95W
1	0.44 to 3.84W
2	3.84 to 6.49W
3	6.49 to 12.95W

PSE provides power according to the following classification:

Class	Max power used by PSE
0	15.4W
1	4.0W
2	7.0W
3	15.4W

To configure the PoE features on the DES-3828P, click **Administration** > **PoE Configuration**. The **PoE System** window is used to assign a power limit and power disconnect method for the whole PoE system. To configure the **Power Limit** for the PoE system, enter a value between 37W and 370W in the Power Limit field. The default setting is 370W. When the total consumed power exceeds the power limit, the PoE controller (located in the PSE) disconnects the power to prevent overloading the power supply.

To configure PoE for the Switch, click **Administration > PoE Configuration**, which will reveal the following window for the user to configure:

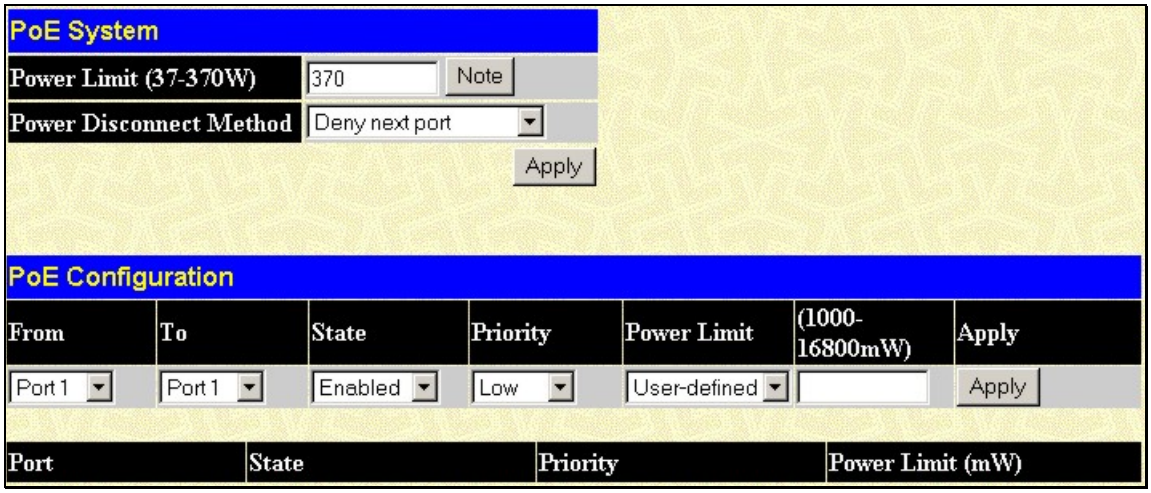


Figure 6- 6. PoE Configuration window

The previous window contains the following fields to configure for PoE:

Parameter	Description
PoE System	
Power Limit	Sets the limit of power to be used from the Switch's power source to PoE ports. The user may configure a Power Limit between 37 and 370w.
Power Disconnect Method	The PoE controller uses either **Deny next port** or **Deny low priority port** to offset the power limit being exceeded and keep the Switch's power at a usable level. Use the drop down menu to select a **Power Disconnect Method**. The default for the Power Disconnect Method is **Deny next port**. Both Power Disconnection Methods are described below: **Deny next port** - After the power limit has been exceeded, the next port attempting to power up is denied, regardless of its priority. **Deny low priority port -** After the power limit has been exceeded, the next port attempting to power up causes the port with the lowest priority to shut down to allow the high-priority and critical priority ports to power up.
PoE Configuration	
From… To…	Select a range of ports from the pull-down menus to be enabled or disabled for PoE.
State	Use the pull-down menu to enable or disable ports for PoE.
Priority	Use the pull-down menu to select the priority of the PoE ports.
Power Limit	Sets the power limit per PoE port. Once this threshold has been reached on the port, the PoE will go into the Power Disconnect Method, as described above. The user may set a limit between 1000 and 16800mW

Click **Apply** to implement changes made to the PoE settings. The port status of all PoE configured ports is displayed in the table in the bottom half of the screen shown above.

User Accounts

Use the **User Account Management** window to control user privileges. To view existing User Accounts, click **Administration** > **User Accounts**.

Figure 6- 7. User Accounts window

To add a new user, click on the **Add** button. To modify or delete an existing user, click on the **Modify** button for that user.

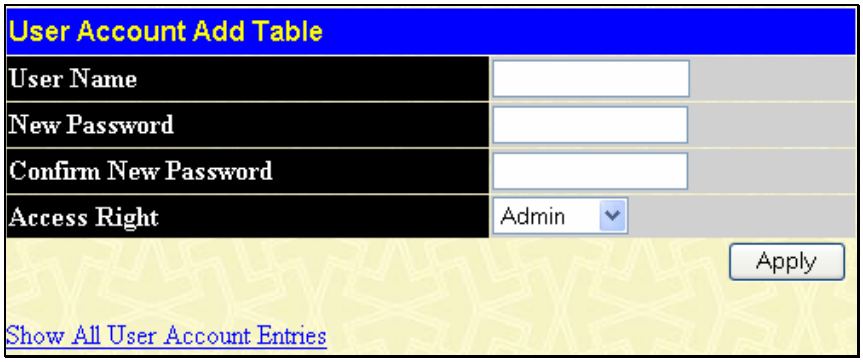


Figure 6- 8. User Accounts Add Table

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

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.

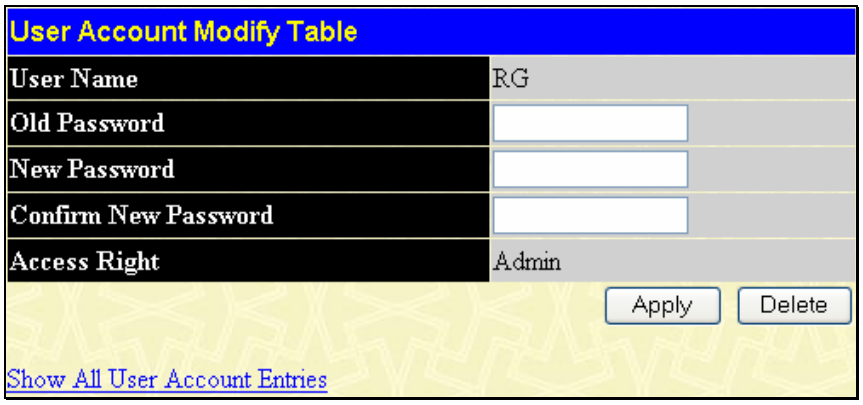


Figure 6- 9. User Accounts Modify Table

Modify or delete an existing user account in the **User Account Modify Table**. To delete the user account, click on the **Delete** button. To change the password, type in the *New Password* and retype it in the *Confirm New Password* entry field. The level of privilege (*Admin, Operator* or *User*) can be viewed in the **Access Right** field.

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

After establishing a User Account with Admin-level privileges, be sure to save the changes by clicking **Maintenance** > **Save Changes** > **Save Configuration** button.

Port Mirroring

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 Mirroring** window, click **Administration > Port Mirroring**.

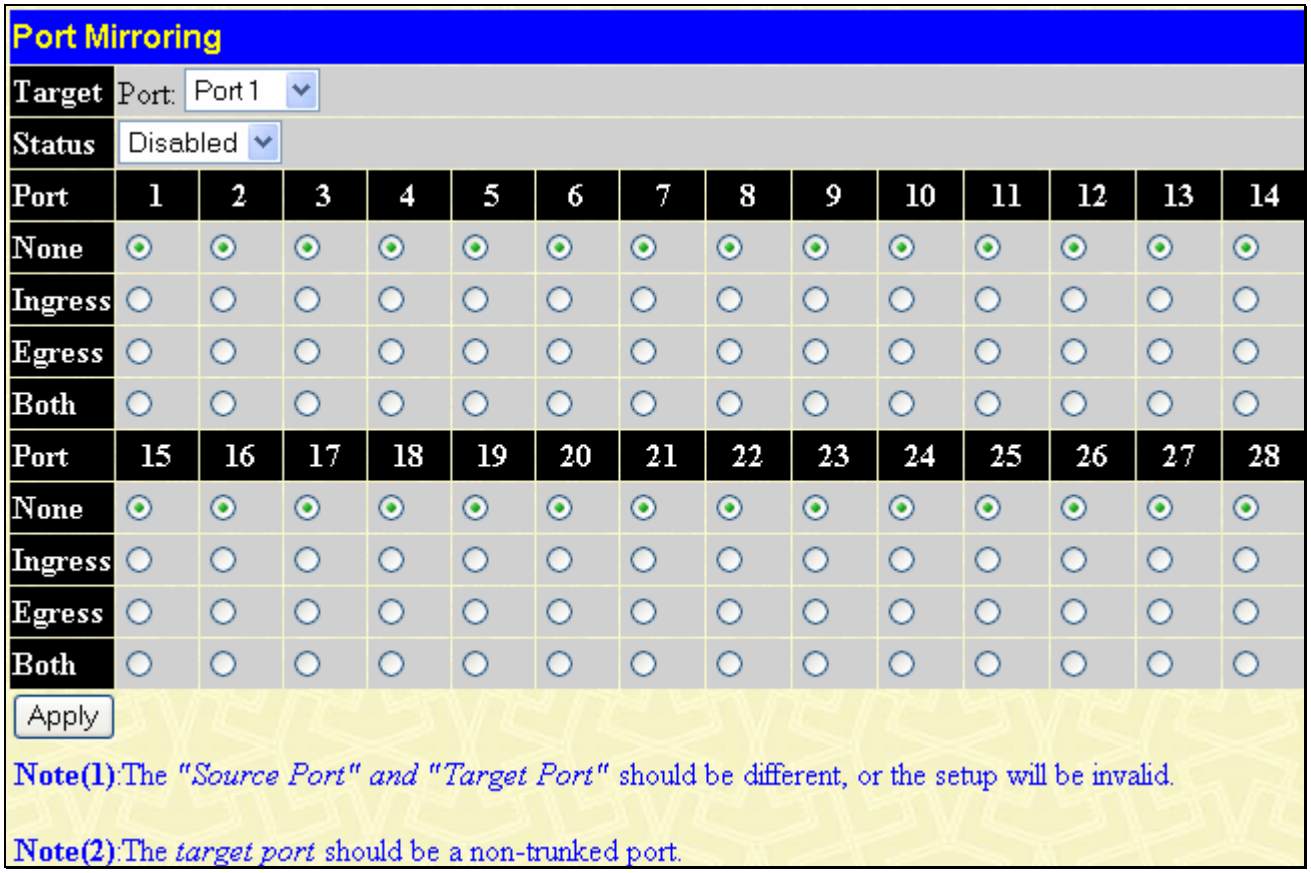


Figure 6- 10. Port Mirroring window

To configure a mirror port:

1. Select the Source Port from where you want to copy frames and the Target Port, which receives the copies from the source port.
2. Select the Source Direction, Ingress, Egress, or Both and change the Status drop-down menu to *Enabled*.
3. Click **Apply** to let the changes take effect.

System Log Settings

The Switch can send Syslog messages to up to four designated servers using the **System Log Server**. Click **Administration** > **System Log Settings** to view the window shown below.

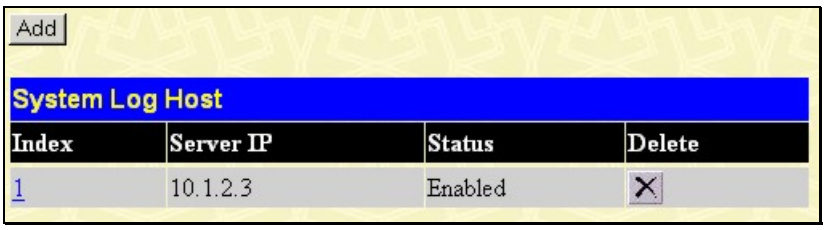


Figure 6- 11. System Log Host window

The parameters configured for adding and editing **System Log Server** settings are the same. See the table below for a description.

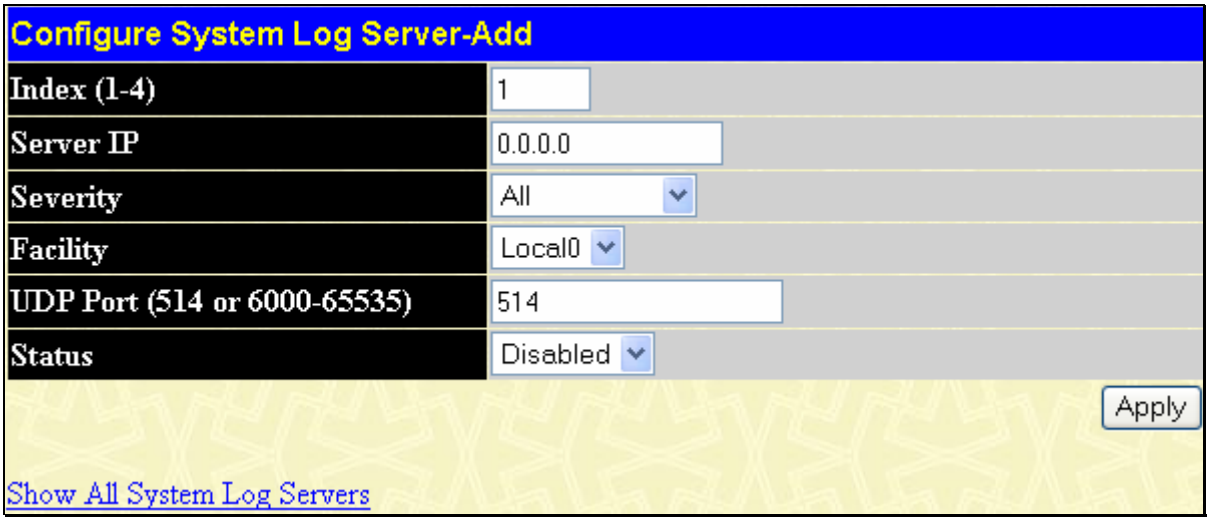


Figure 6- 12. Configure System Log Server – Add

The following parameters can be set:

Parameter	Description
Index	Syslog server settings index (1-4).
Server IP	The IP address of the Syslog server.
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 Code** **Facility**

	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)**
UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is 514.	
Status	Choose *Enabled* or *Disabled* to activate or deactivate.	

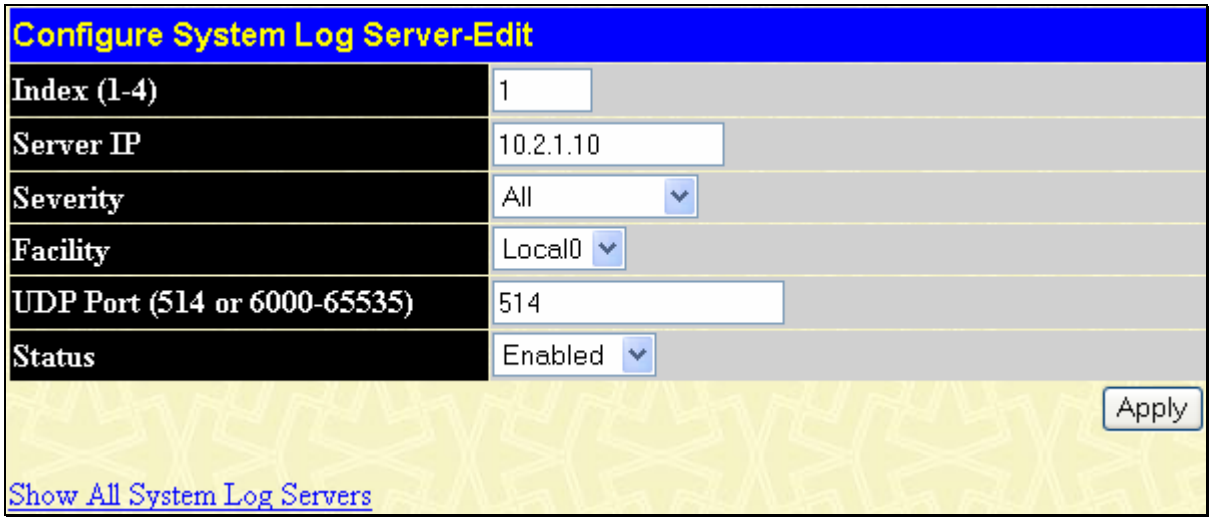


Figure 6- 13. Configure System Log Server– Edit

To set the System Log Server configuration, click **Apply**. To delete an entry from the **System Log Host** window, click the corresponding ✕ under the Delete heading of the entry to delete. To return to the **System Log Host** window, click the Show All System Log Servers link.

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. Click **Administration** > **System Severity Settings**, to view the window shown below.

Figure 6- 14. 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.

SNTP Settings

Time Settings

To configure the time settings for the Switch, click **Administration** > **SNTP Settings** > **Time Settings** link, revealing the following window for the user to configure.

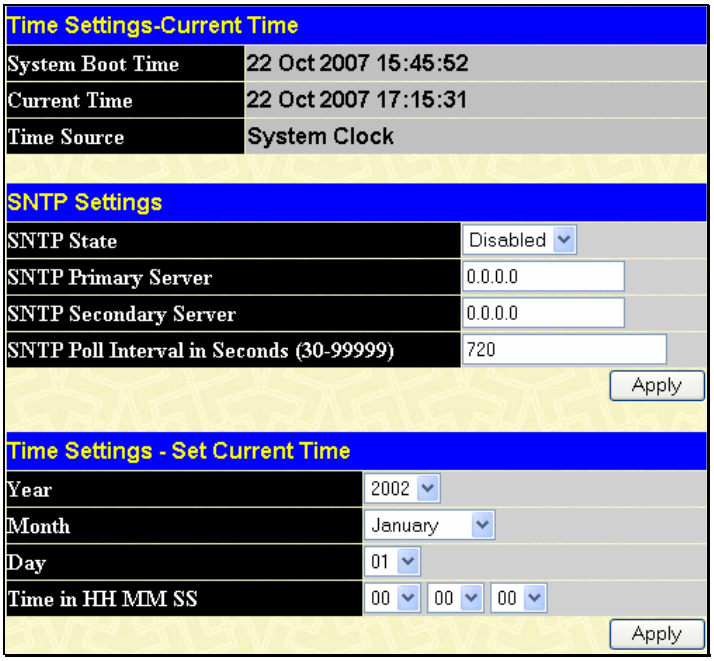


Figure 6- 15. Time Settings window

The following parameters can be set or are displayed:

Parameter	Description
Current Time	
System Boot Time	Displays the time when the Switch was initially started for this session.
Current Time	Displays the Current Time set on the Switch.
Time Source	Displays the time source for the system.
SNTP Settings	
SNTP State	Use this pull-down menu to *Enabled* or *Disabled* SNTP.
SNTP Primary Server	This is the IP address of the primary server the SNTP information will be taken from.
SNTP Secondary 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	
Year	Enter the current year, if you want to update the system clock.
Month	Enter the current month, if you would like to update the system clock.
Day	Enter the current day, if you would like to update the system clock.
Time in HH MM SS	Enter the current time in hours, minutes, and seconds.

Click **Apply** to implement your changes.

Time Zone and DST

The following are windows used to configure time zones and Daylight Savings time settings for SNTP. Click **Administration** > **SNTP Settings** > **Time Zone and DST**, which will reveal the following window.

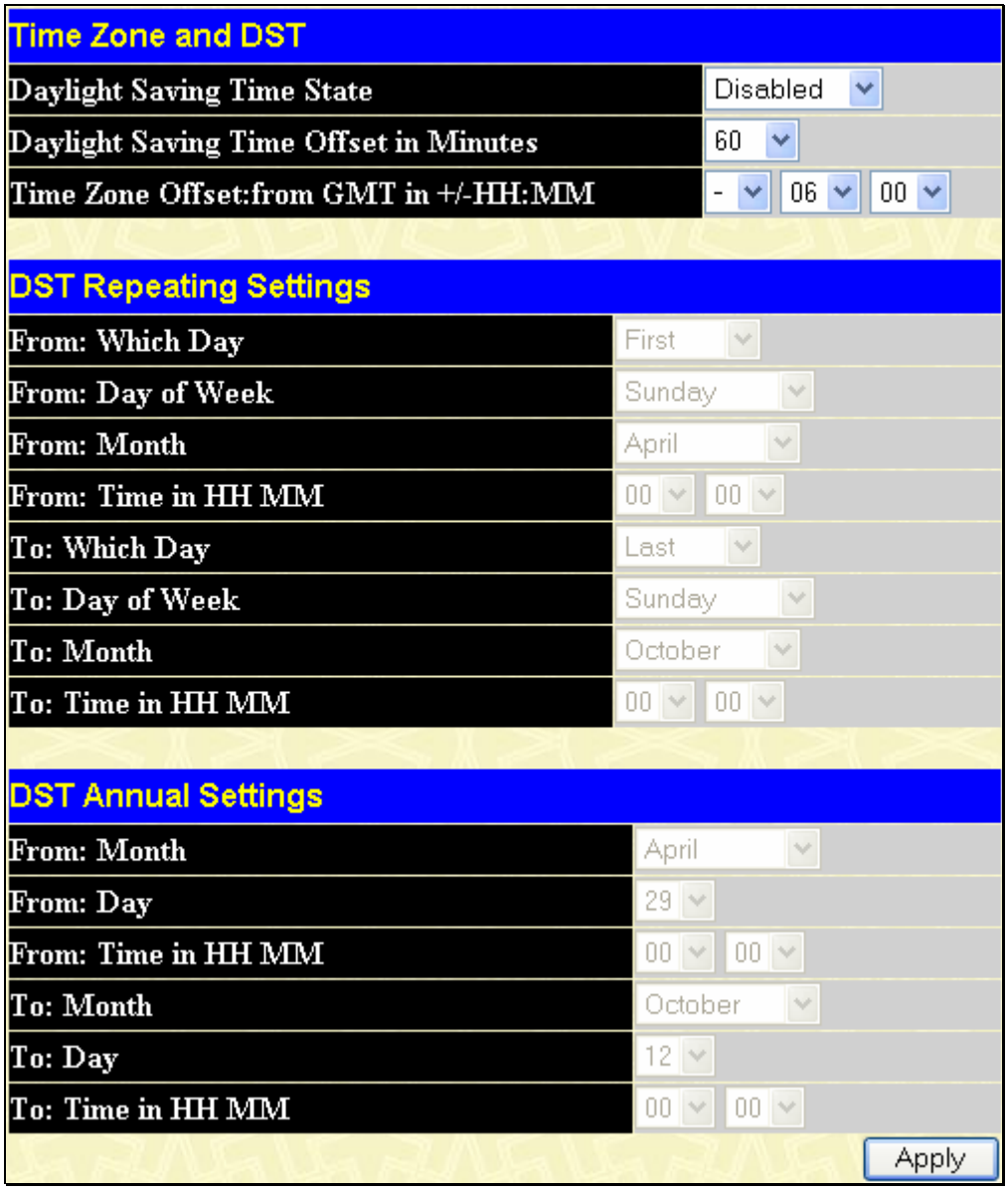


Figure 6- 16. Time Zone and DST Settings window

The following parameters can be set:

Parameter	Description
Time Zone and DST	
Daylight Saving Time State	Use this pull-down menu to select disable or Repeating or Annual 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 Day	Enter the week of the month that DST will start.
From: Day of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: Time in HH:MM	Enter the time of day that DST will start on.
To: Which Day	Enter the week of the month the DST will end.
To: Day of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: Time in HH:MM	Enter the time DST will end.
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 day of the week 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 clicking **Administration** > **MAC Notification Settings**.

Global Settings

The following parameters may be viewed and modified:

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

Port Settings

To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters.

Parameter	Description
From…To	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 made.

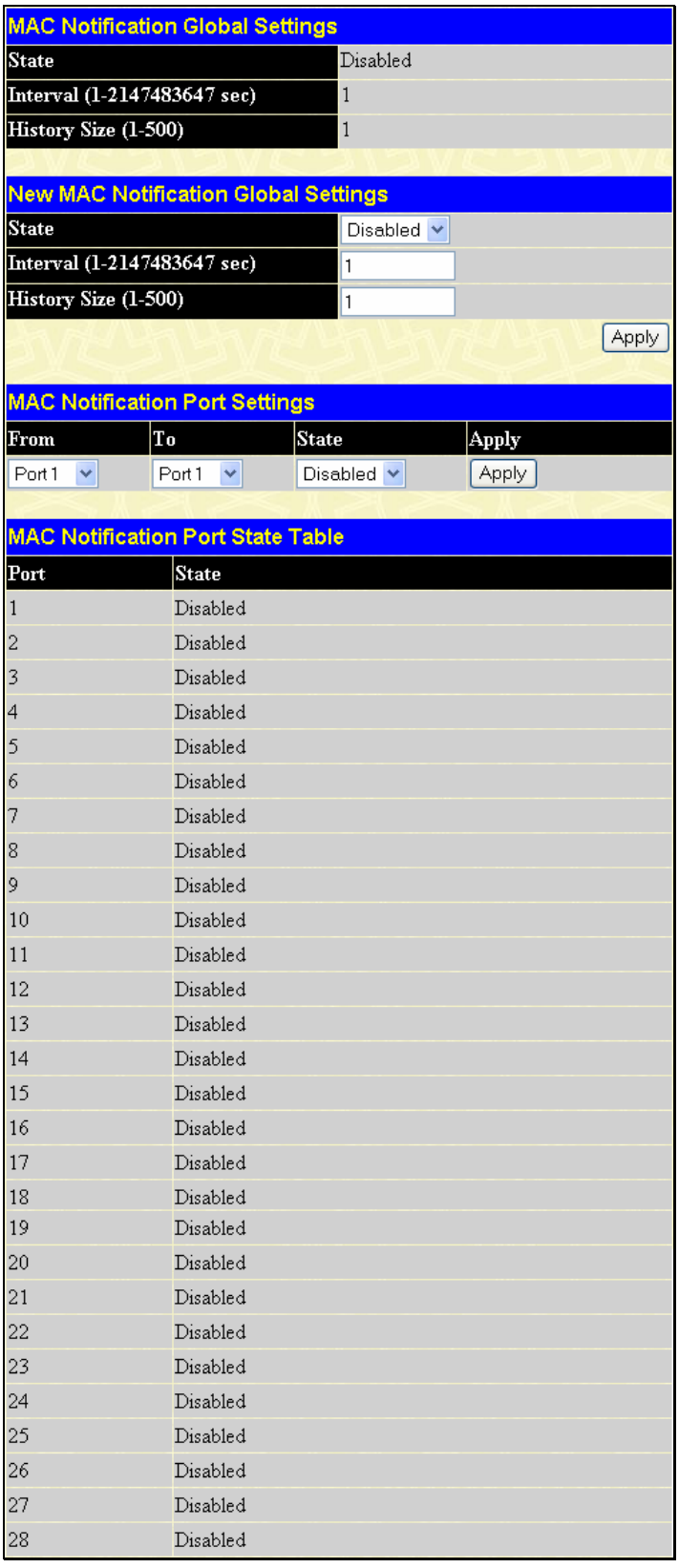


Figure 6- 17. MAC Notification Settings

TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch's firmware to be upgraded by transferring a new firmware file from a TFTP server to the Switch. A configuration file can also be loaded into the Switch from a TFTP server. Switch settings can be saved to the TFTP server, and a history log can be uploaded from the Switch to the TFTP server. The TFTP server must be running TFTP server software to perform the file transfer.

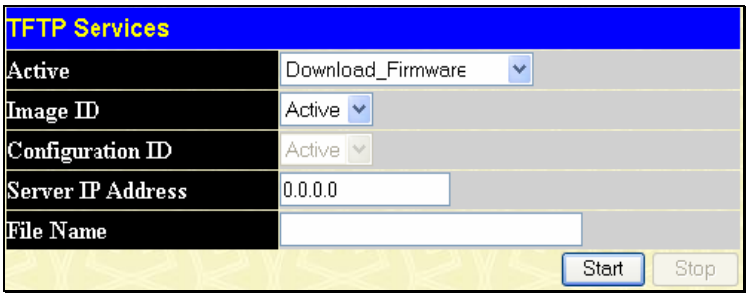


Figure 6- 18. TFTP Services window

TFTP server software is a part of many network management software packages – such as NetSight, or can be obtained as a separate program. To update the Switch's firmware or configuration file, click **Administration** > **TFTP Services**.

The following parameters can be configured:

Parameter	Description
Active	Select a service for the TFTP server to perform from the drop down window: • **Download Firmware** - Enter the IP address of the TFTP server and specify the location of the new firmware on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. • **Download Configuration** - Enter the IP address of the TFTP server, and the path and filename for the Configuration file on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. • **Upload Configuration** - Enter the IP address of the TFTP server and the path and filename for the switch settings on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. • **Upload Log** - Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.
Image ID	Select the **Image ID** of the firmware. The Switch can hold two firmware images in its memory. Image ID 1 will always be the boot up firmware for the Switch unless specified by the user. Choosing **Active** will download the firmware to the Boot Up Image ID, depending on the user's configuration. Information on configuring Image IDs can be found in this section, under the heading **Multiple Image Services**.
Configuration ID	Select the **Configuration ID** for uploading or downloading configuration files from or to the Switch. Like the Image ID, the Switch can hold two configuration files in its memory. Choosing **Active** will download the configuration to the Boot Up Configuration ID, depending on the user's configuration.
Server IP Address	Enter the IP address of the server from which to download firmware or configuration files.
File Name	Enter the path and filename of the firmware or configuration file to upload or download.

Multiple Image Services

The **Multiple Image Services** window allows switch administrators to configure and view information regarding firmware located on the Switch. The Switch allows two firmware images to be stored in its memory and either may be configured to be the boot up firmware for the Switch. For information regarding firmware images located on the Switch, open the **Firmware Information** link. The default setting for the Switch's firmware will have the boot up firmware stored in Image 1, but the user may set either firmware stored to be the boot up firmware by using configuration screens located in the **Dual Configurations Services** folder.

Firmware Information

The following screen allows the user to view information about current firmware images stored on the Switch. To access the following screen, click **Administration > Multiple Image Services**.

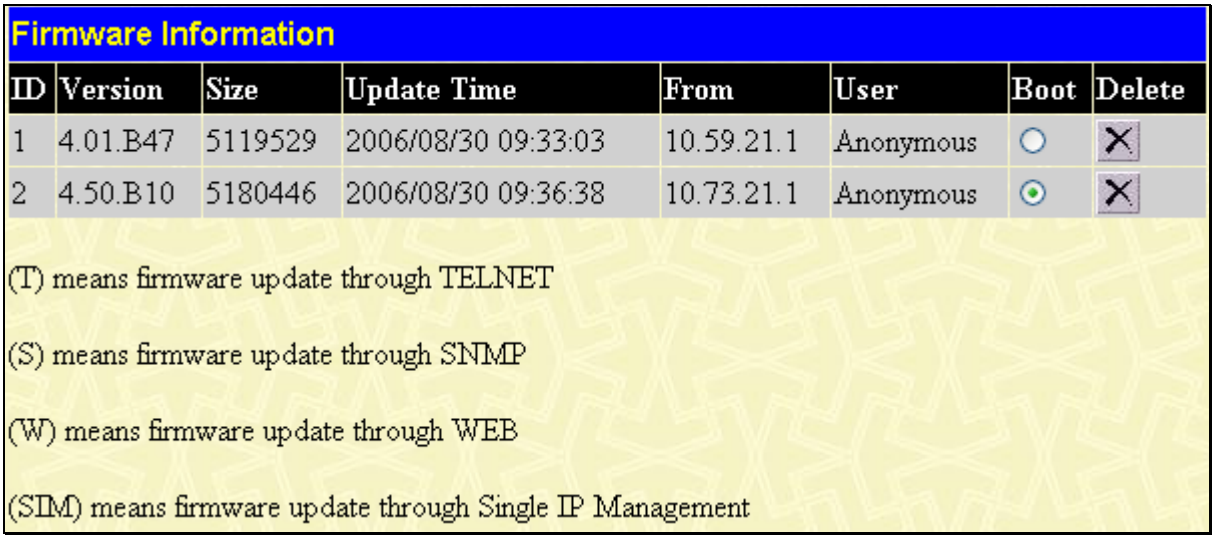


Figure 6- 19. Firmware Information window

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. • **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. • **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 Services

The following window is used to configure firmware information set in the Switch. The xStack DES-3800 series has the capability to store two firmware images in its memory. To view this window, click **Administration** > **Dual Configuration Services**, which will in turn display the following window.

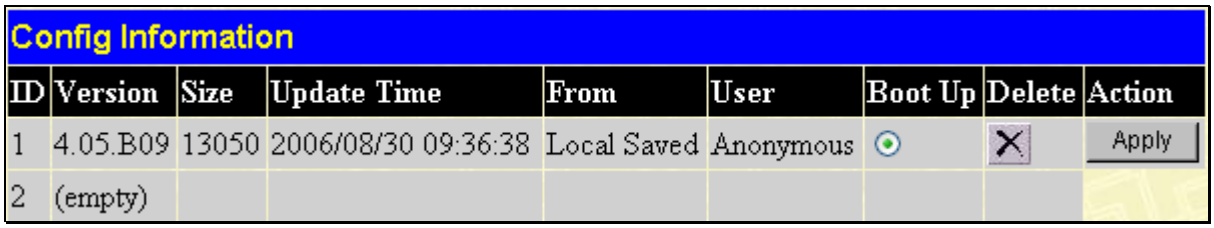


Figure 6- 20. Config Information window

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	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 Up	Click the radio 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.
Delete	Click the corresponding ✕ under this heading to delete this configuration file from the Switch's memory.
Apply	Click **Apply** to implement any changes made to the configuration file settings.

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.

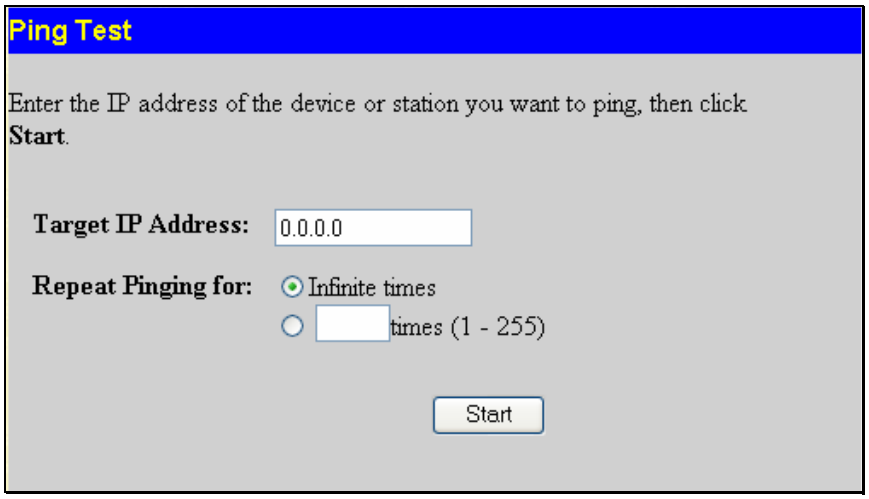


Figure 6- 21. Ping Test window

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 clicking its radio button and entering a number between *1* and *255*. Click **Start** to initiate the Ping program.

SNMP Manager

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-3800 Series supports the SNMP versions 1, 2c, and 3. The default SNMP setting is disabled. You must enable SNMP. Once SNMP is enabled you can choose which version you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

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

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

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

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

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

Traps

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

MIBs

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

The xStack DES-3800 Series incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The xStack DES-3800 Series supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

SNMP User Table

The **SNMP User Table** displays all of the SNMP users currently configured on the Switch.

Click **Administration > SNMP Manager** > **SNMP User Table,** this will open the **SNMP User Table** window, as shown below.

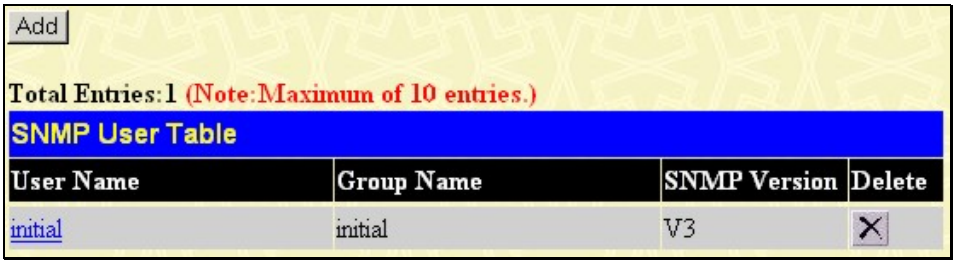


Figure 6- 22. SNMP User Table window

To delete an existing **SNMP User Table** entry, click the ✕ below the Delete heading corresponding to the entry you wish to delete.

To display the detailed entry for a given user, click on the hyperlinked User Name. This will open the **SNMP User Table Display** window, as shown below.

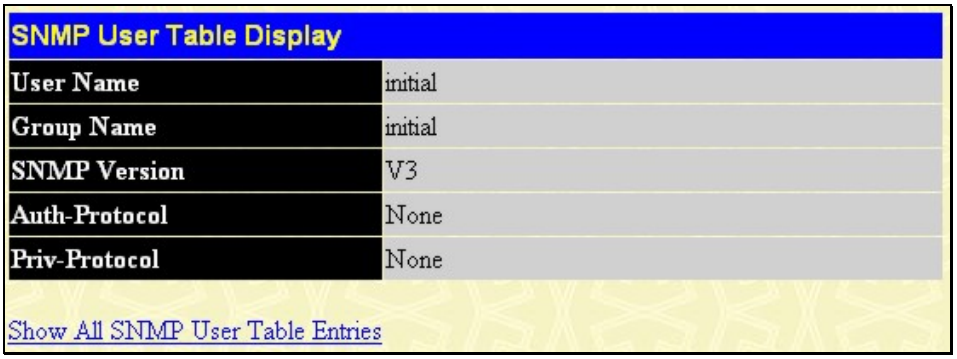


Figure 6- 23. SNMP User Table Display window

The following parameters are displayed:

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.
Auth-Protocol	*None* - Indicates that no authentication protocol is in use. *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	*None* - Indicates that no privacy (encryption) protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

To return to the SNMP User Table, click the Show All SNMP User Table Entries link. To add a new entry to the **SNMP User Table Configuration** window, click on the **Add** button on the **SNMP User Table** window. This will open the **SNMP User Table Configuration** window, as shown below.

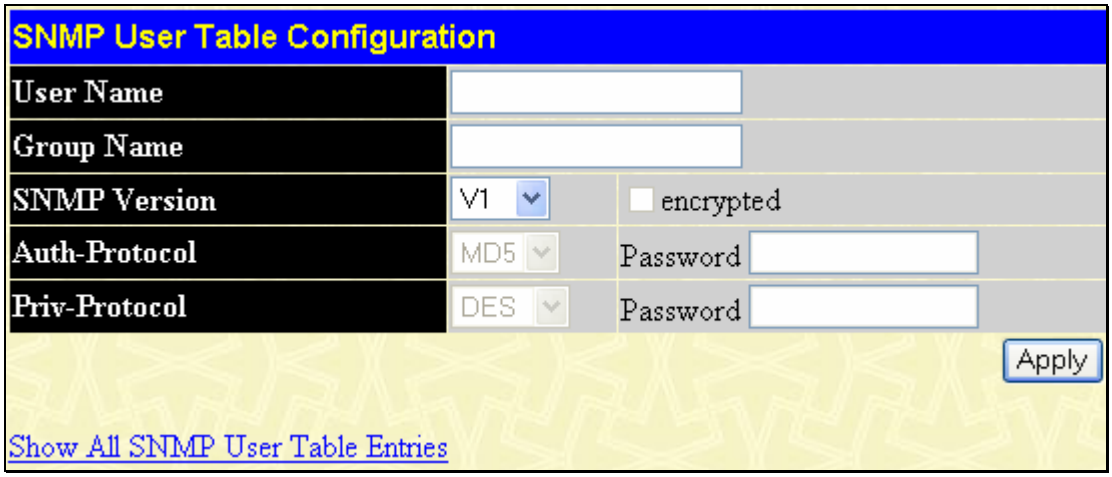


Figure 6- 24. SNMP User Table Configuration window

The following parameters can set:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V1* - Specifies that SNMP version 1 will be used. *V2c* - Specifies that SNMP version 2c will be used. *V3* - Specifies that SNMP version 3 will be used.
Auth-Protocol	*MD5* - Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encrypted field has been checked. This field will require the user to enter a password. *SHA* - Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encrypted field has been checked. This field will require the user to enter a password.
Priv-Protocol	*None* - Specifies that no privacy (encryption) protocol is in use. *DES* - Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when *V3* is selected in the SNMP Version field and the Encrypted field has been checked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.
Encrypted	Checking the corresponding box will enable encryption for SNMP V3 and is only operable in SNMP V3 mode.

To implement changes made, click **Apply**. To return to the SNMP User Table, click the Show All SNMP User Table Entries link.

SNMP View Table

The SNMP View Table is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. To view the **SNMP View Table** window, click **Administration > SNMP Manager** > **SNMP View Table**. The following window should appear:

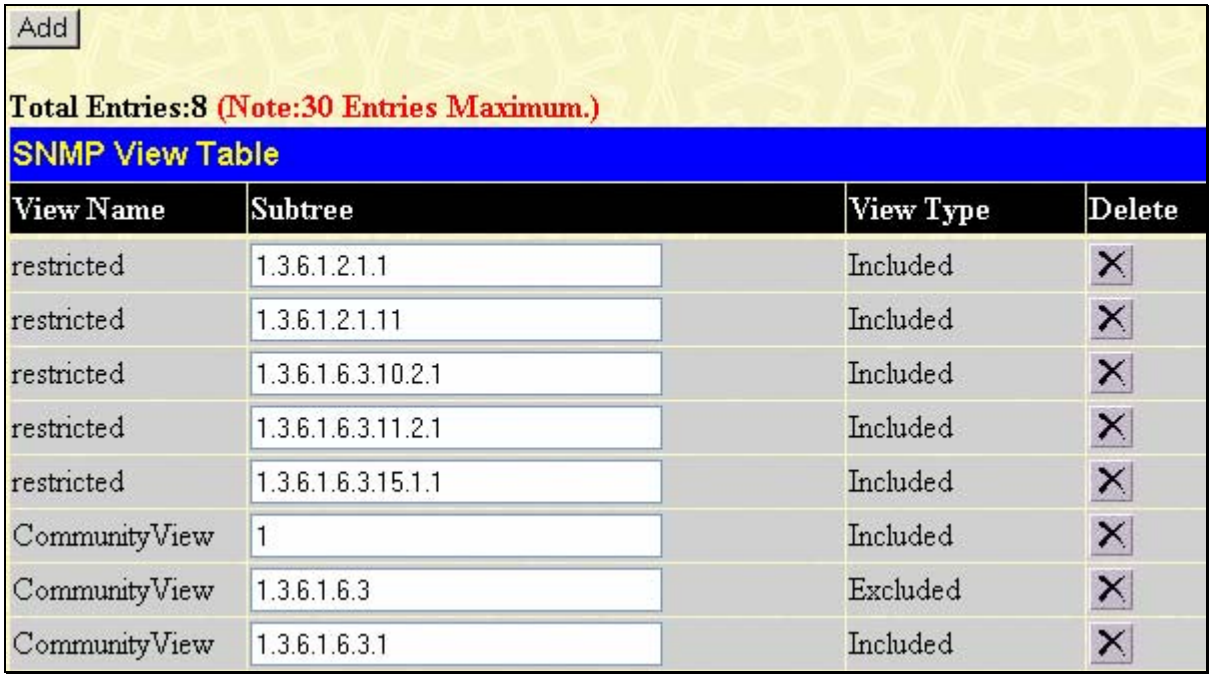


Figure 6- 25. SNMP View Table window

To delete an existing SNMP View Table entry, click the ✕ in the Delete column corresponding to the entry to delete. To create a new entry, click the **Add** button and a separate window will appear.

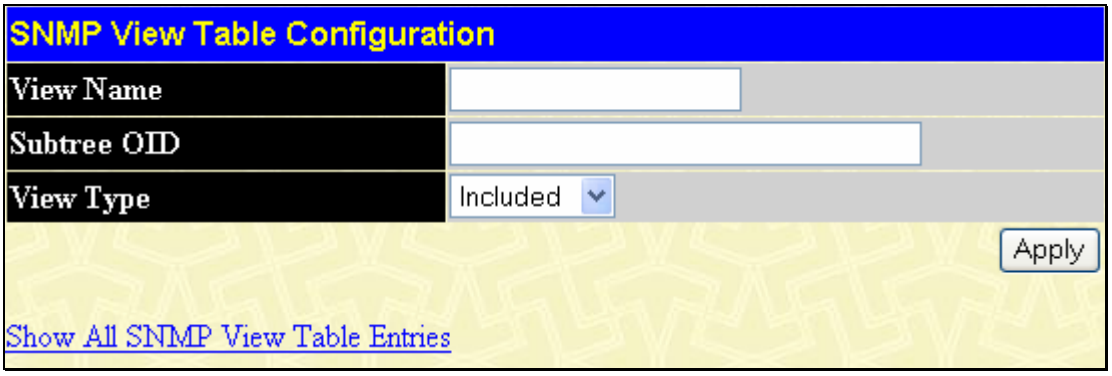


Figure 6- 26. SNMP View Table Configuration window

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

The following parameters can 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 return to the **SNMP View Table**, click the Show All SNMP View Table Entries link.

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 the **SNMP Group Table** window, click **Administration > SNMP Manager > SNMP Group Table**, the following window should appear:

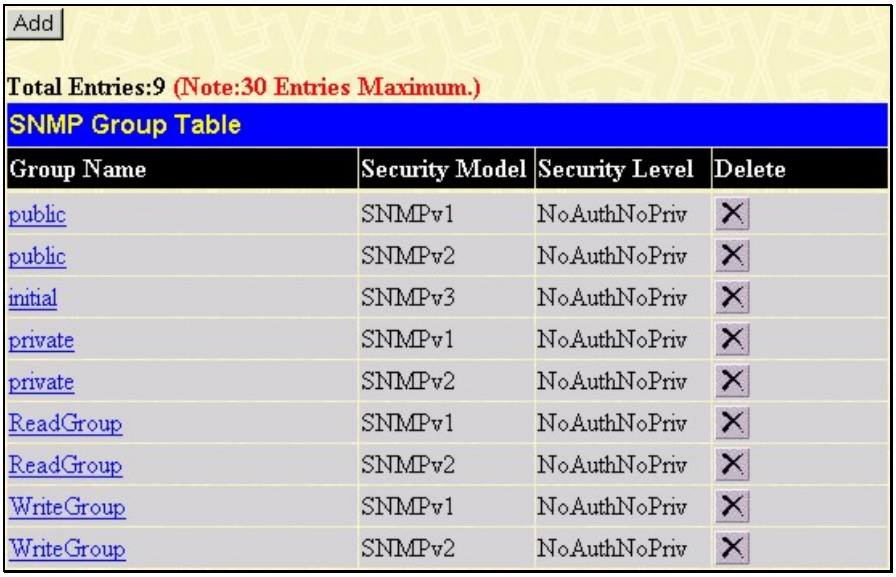


Figure 6- 27. SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding ✕ under the Delete heading.

To display the current settings for an existing **SNMP Group Table** entry, click the hyperlink for the entry under the **Group Name**.

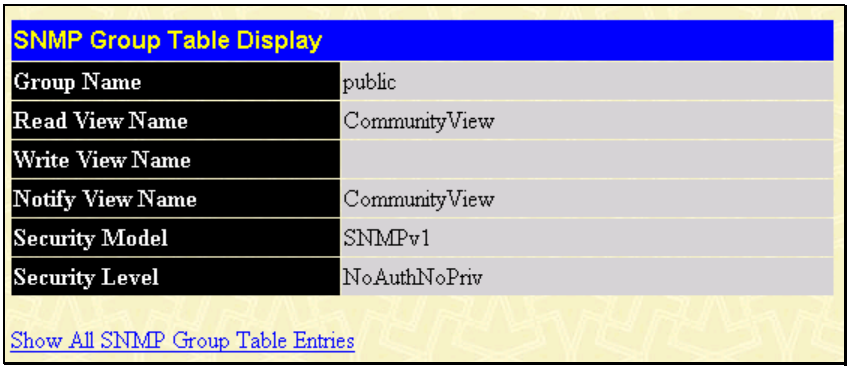


Figure 6- 28. SNMP Group Table Display window

To add a new entry to the Switch's SNMP Group Table, click the **Add** button in the upper left-hand corner of the **SNMP Group Table** window. This will open the **SNMP Group Table Configuration** window, as shown below.

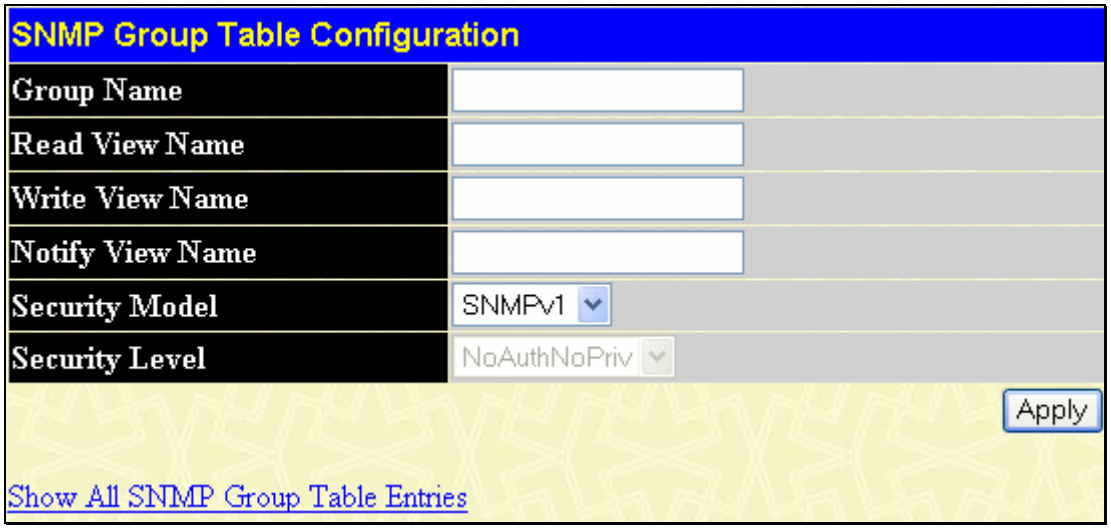


Figure 6- 29. SNMP Group Table Configuration window

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 that 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.
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 authentication and no encryption of packets sent between the Switch and a remote SNMP manager. *AuthNoPriv* - Specifies that authentication will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *AuthPriv* - Specifies that authentication will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

To implement your new settings, click **Apply**. To return to the SNMP Group Table, click the Show All SNMP Group Table Entries link.

SNMP Community Table Configuration

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

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

To configure SNMP Community entries, click **Administration** > **SNMP Manager** > **SNMP Community Table**, which will open the following window:

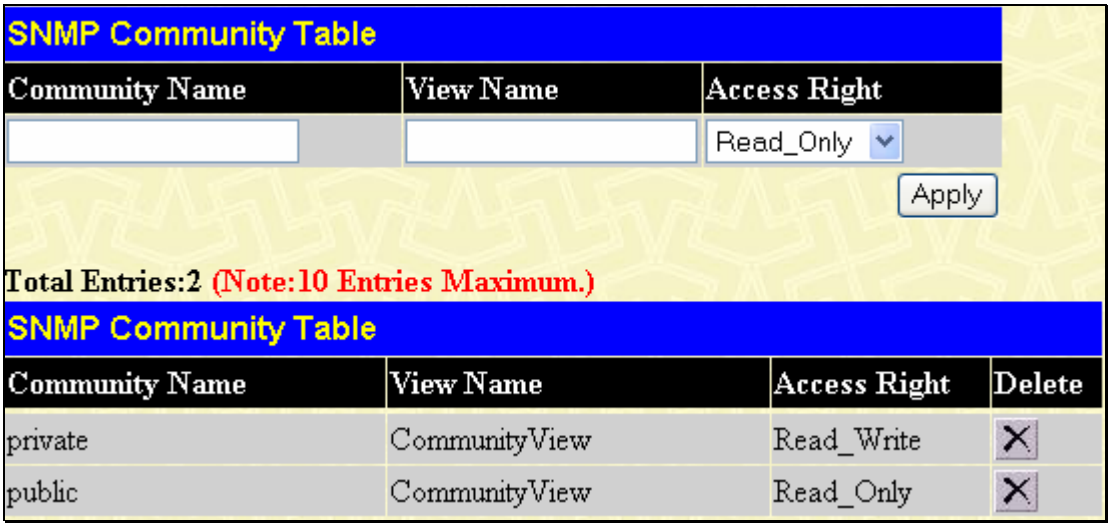


Figure 6- 30. SNMP Community Table Configuration window

The following parameters can be 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 ✕ under the Delete heading, corresponding to the entry to delete.

SNMP Host Table

Use the **SNMP Host Table** window to set up SNMP trap recipients. Click **Administration** > **SNMP Manager** > **SNMP Host Table Configuration**. This will open the **SNMP Host Table** window, as shown to the right. To delete an existing SNMP Host Table entry, click the corresponding ✕ under the Delete heading. To display the current settings for an existing **SNMP Host Table** entry, click the blue link for the entry under the Host IP Address heading.

To add a new entry to the Switch's SNMP Host Table, click the **Add** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown to the right.

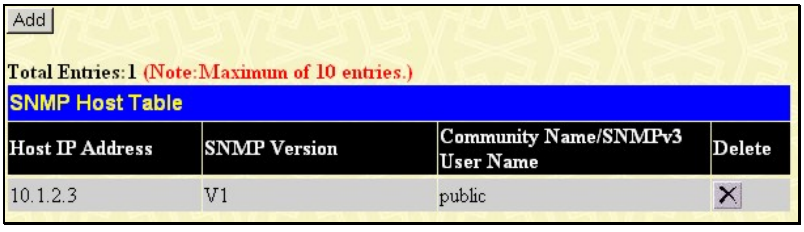


Figure 6- 31. SNMP Host Table window

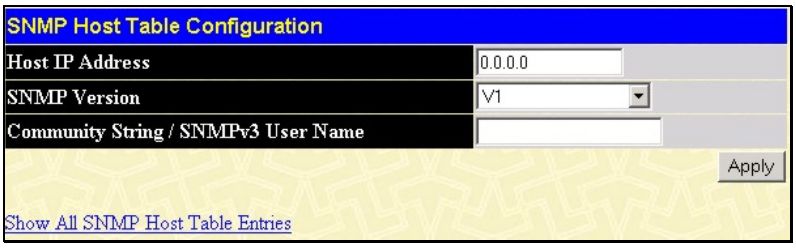


Figure 6- 32. SNMP Host Table Configuration window

The following parameters can set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	*V1* - To specifies that SNMP version 1 will be used. *V2c* - To specify that SNMP version 2c will be used. *V3-NoAuth-NoPriv* - To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level. *V3-Auth-NoPriv* - To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level. *V3-Auth-Priv* - To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String/ SNMP V3 User Name	Type in the community string or the SNMP V3 user name as appropriate.

To implement your new settings, click **Apply.** To return to the **SNMP Host Table**, click the Show All SNMP Host Table Entries link.

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 **Administration > SNMP Manger > SNMP Engine ID**. This will open the **SNMP Engine ID Configuration** window, as shown below.

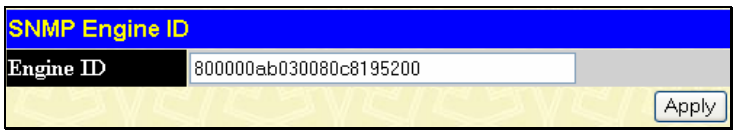


Figure 6- 33. SNMP Engine ID Configuration window

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

SNMP Trap Settings

The following window is used to enable and disable trap settings for the SNMP function on the Switch. To configure the SNMP Trap Settings, click **Administration > SNMP Manager > SNMP Trap**:

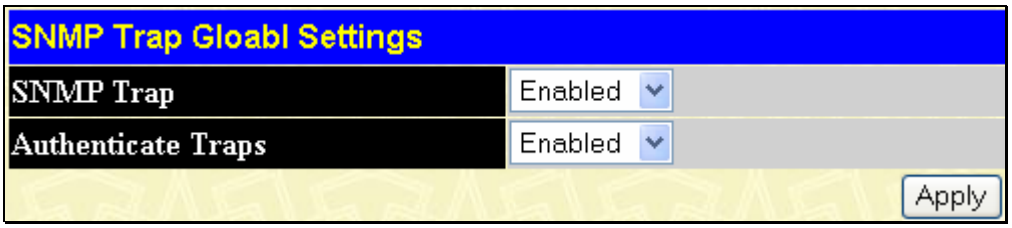


Figure 6-34. SNMP Trap Settings window

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

D-Link Single IP Management

Single IP Management (SIM) Overview

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.

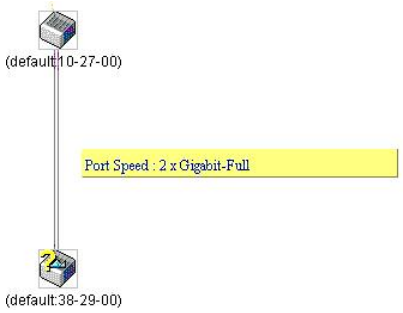
The Upgrade to v1.6

To better improve SIM management, the xStack DES-3800 series switches have 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 Using the Web Interface

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 **Administration > Single IP Management Settings** > **SIM Settings**, to reveal the following window.

Figure 6- 35. SIM Settings window (disabled)

Change the **SIM State** to *Enabled* using the pull down menu and click **Apply**. The screen will then refresh and the **SIM Settings** window will look like this:

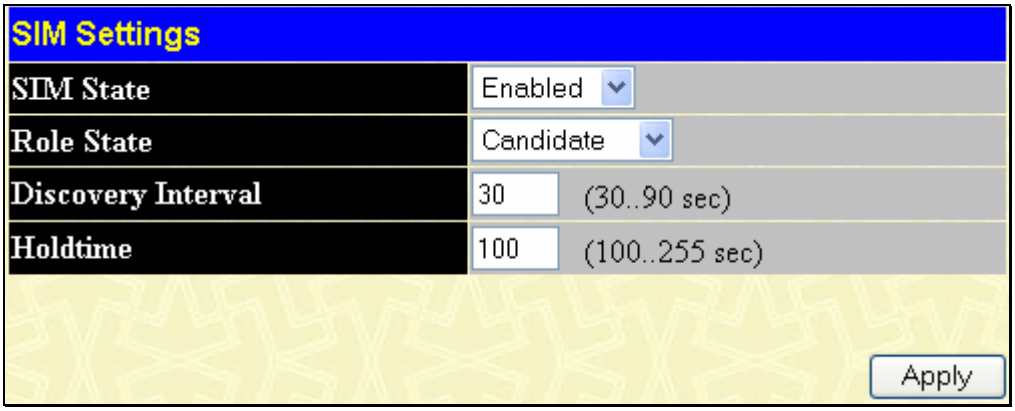


Figure 6- 36. SIM Settings window (enabled)

If the Switch Administrator wishes to configure the Switch as a Commander Switch (CS), select commander from the **Role State** field and click **Apply**. The window will change once again to look like this:

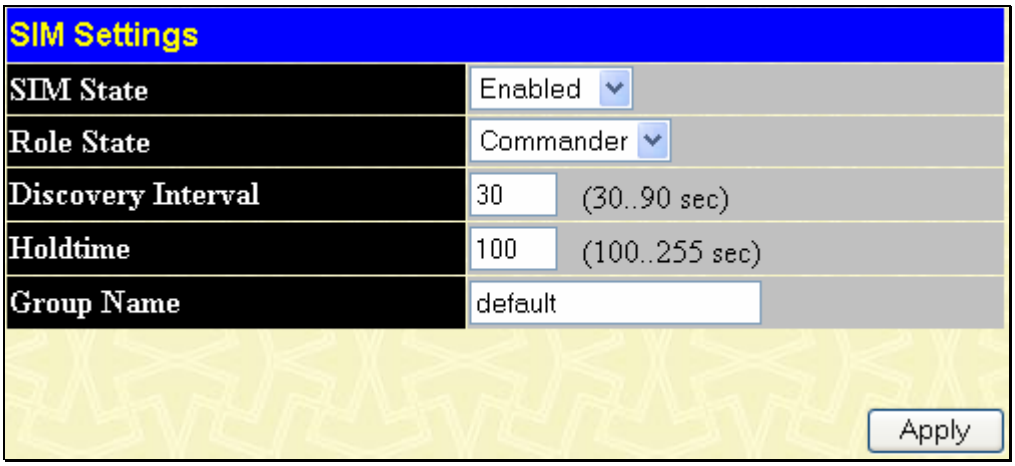


Figure 6- 37. SIM Settings window (Commander enabled)

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	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.
Holdtime	This parameter may be set for the time, in seconds, that the Switch will store information sent to it from other switches, utilizing the **Discovery Interval**. The user may set the hold time from 100 to 255 seconds.
Group Name	The administrator may set the name of the SIM group that the Switch has been nominated Commander for in this field. The default name for the Group is *default*.

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

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.

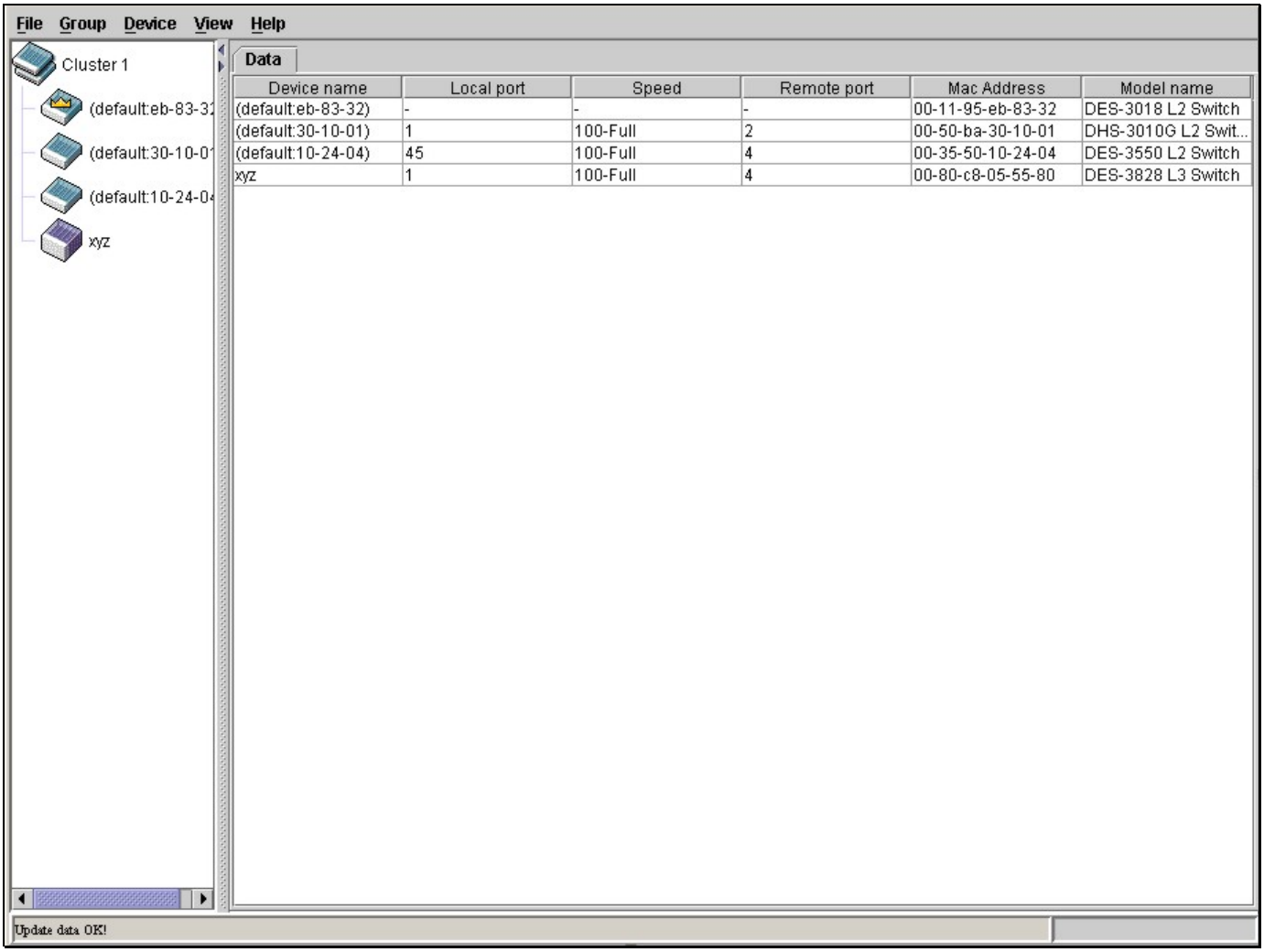


Figure 6- 38. Single IP Management window - Tree View

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 screen. The **Topology View** will refresh itself periodically (20 seconds by default).

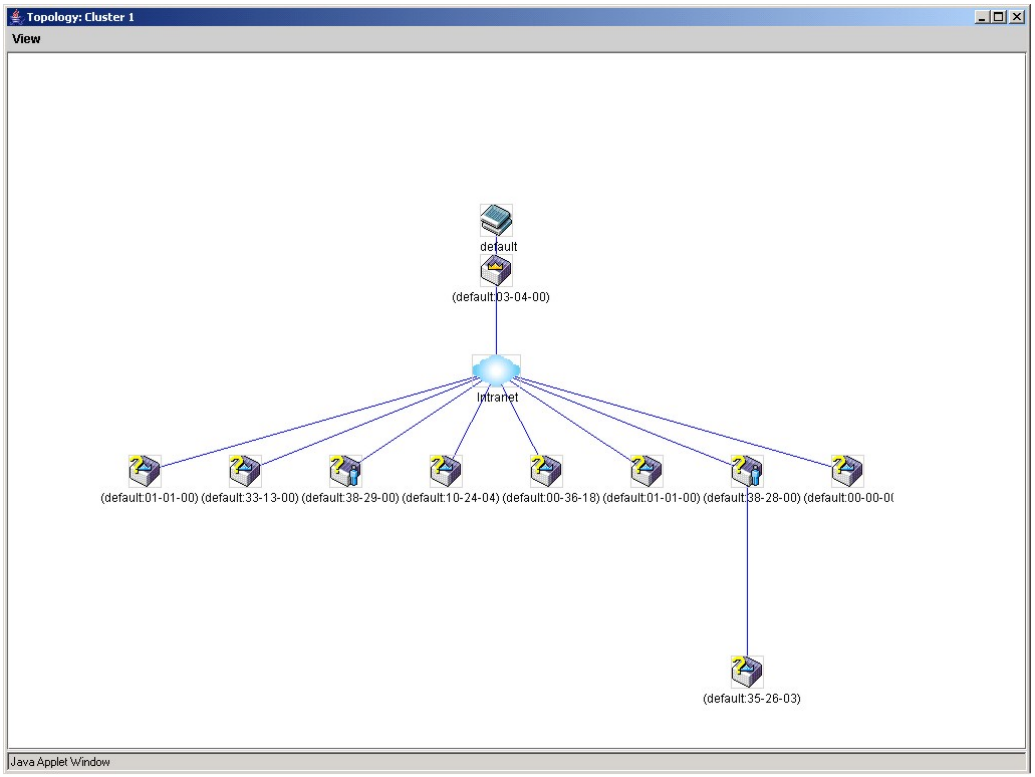


Figure 6- 39. Topology view

This screen 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.

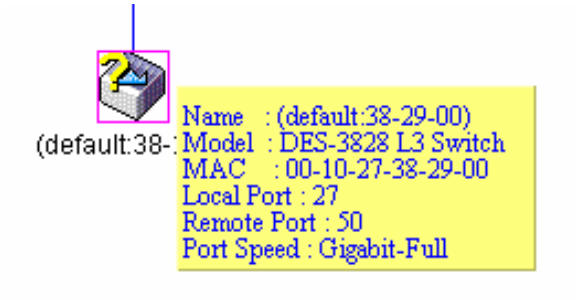


Figure 6- 40. Device Information Utilizing the Tool Tip

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

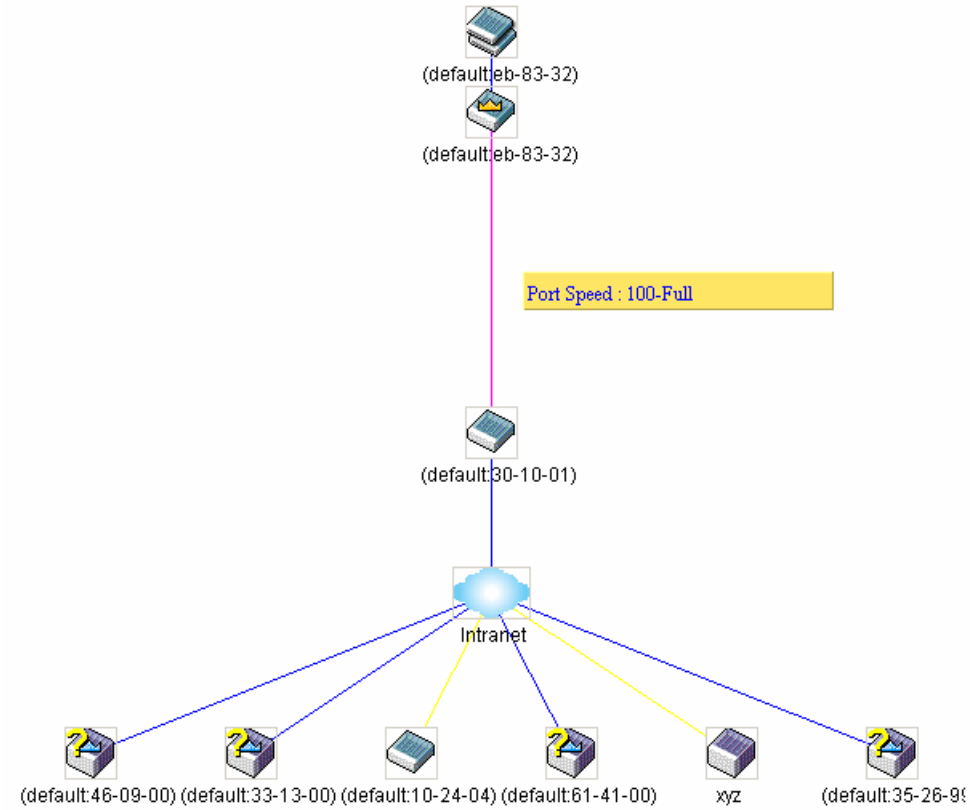


Figure 6- 41. Port Speed Utilizing the Tool Tip

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

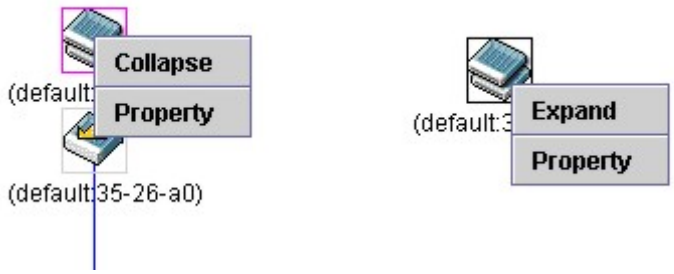


Figure 6- 42. Right Clicking a Group Icon

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.

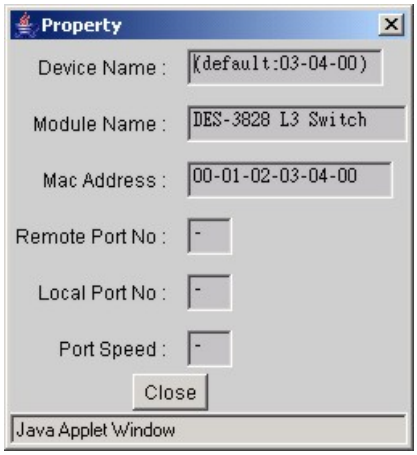


Figure 6- 43. Property window

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

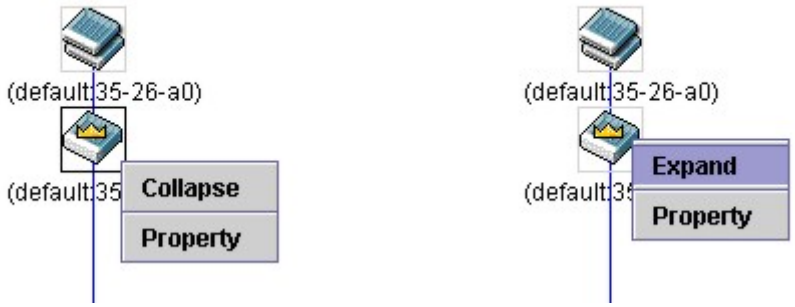


Figure 6- 44. Right Clicking a Commander Icon

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

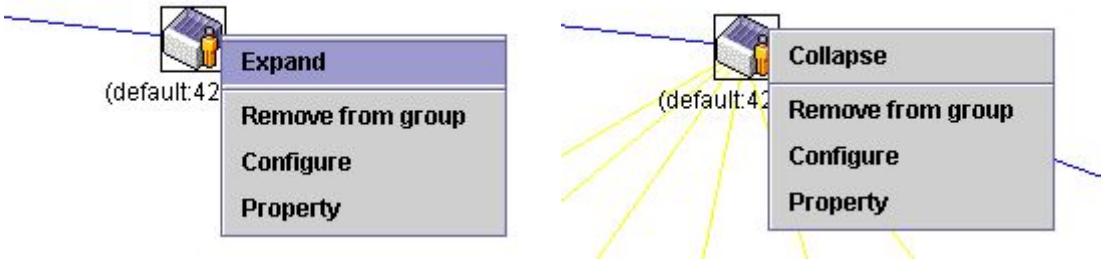


Figure 6- 45. Right Clicking a Member icon

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

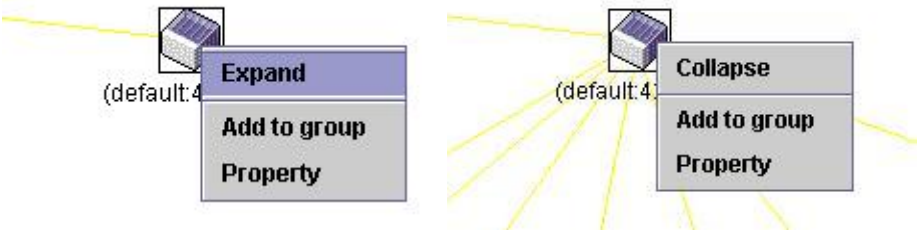


Figure 6- 46. Right Clicking a Candidate icon

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 screen 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.

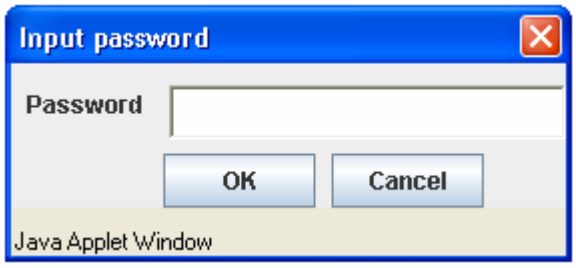


Figure 6- 47. Input password window.

- **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- 48. 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 screen 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.

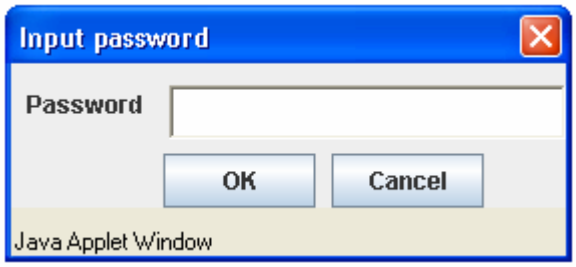


Figure 6- 49. Input password window.

- **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.

NOTE: Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the ***DES-3800 CLI Manual*** for more information on SIM and its configurations.

Packet to CPU Settings

This screen is used to enable or disable the feature that controls whether to capture IP packets with a Zero TTL to the CPU. In the DES-3800 series the default setting for this feature is off. If you disable this feature, the device will not respond to traceroute packets.

To access the following window, click **Administration > Packet to CPU Settings**.

Figure 6- 50. Packet to CPU Settings window

Choose *Enabled/Disabled* from the **Use Zero TTL IP State** drop-down menu to enable or disable the Zero TTL IP State on the Switch. Click the **Apply** button to apply the change.

Section 7

Layer 2 Features

VLAN

Trunking

IGMP Snooping

MLD Snooping

Spanning Tree

Forwarding

Loopback Detection

Protocol VLAN

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for VLAN, Trunking, IGMP Snooping, Spanning Tree, and Forwarding, all discussed in detail in the following section.

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 on the DES-3800 Series

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 DES-3800 Series 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.

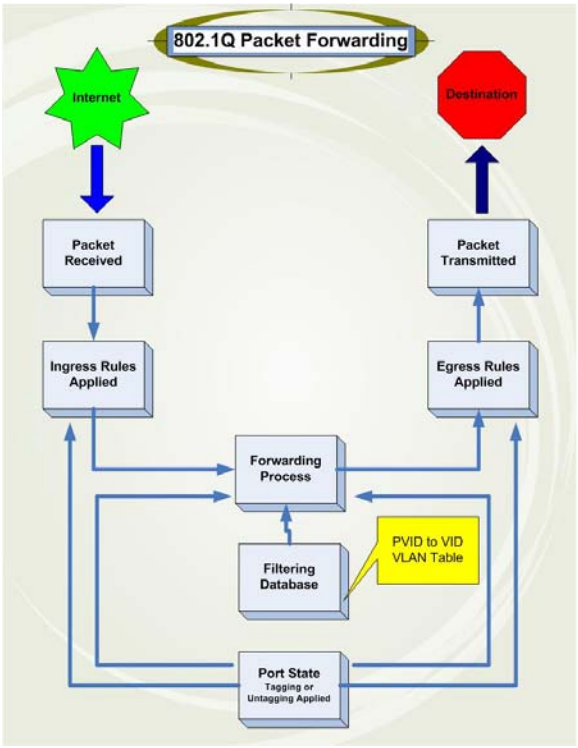


Figure 7- 1. IEEE 802.1Q Packet Forwarding

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.

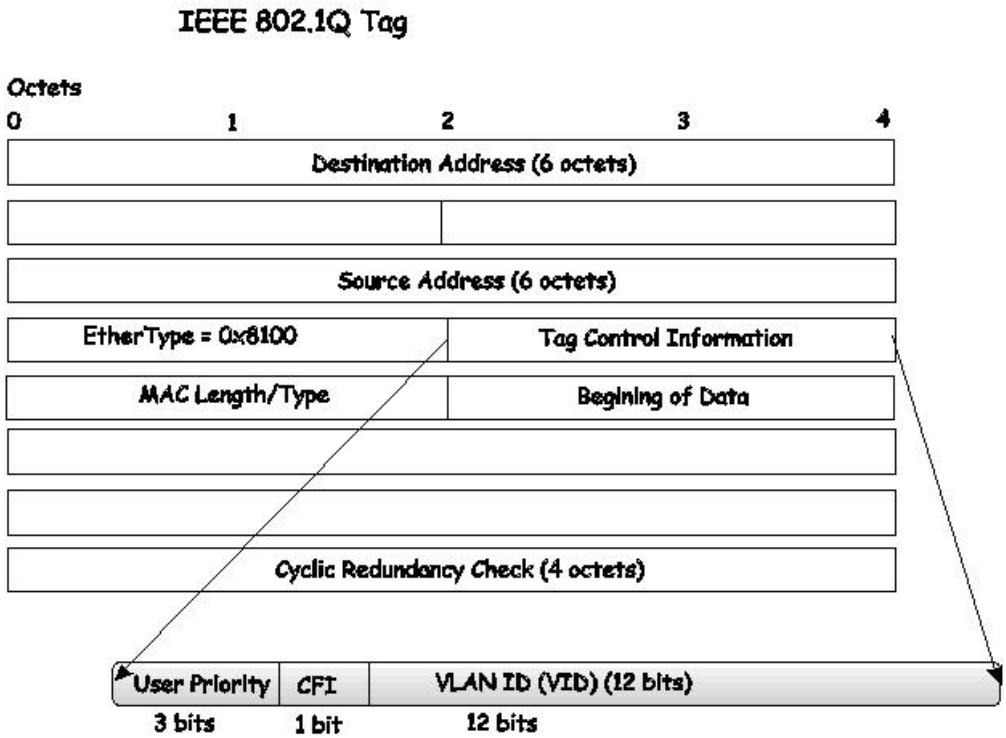


Figure 7- 2. IEEE 802.1Q Tag

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.

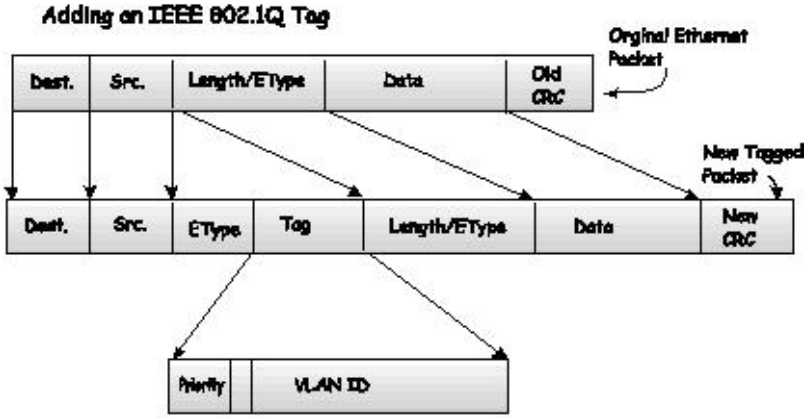


Figure 7- 3. Adding an IEEE 802.1Q Tag

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- 4. 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:

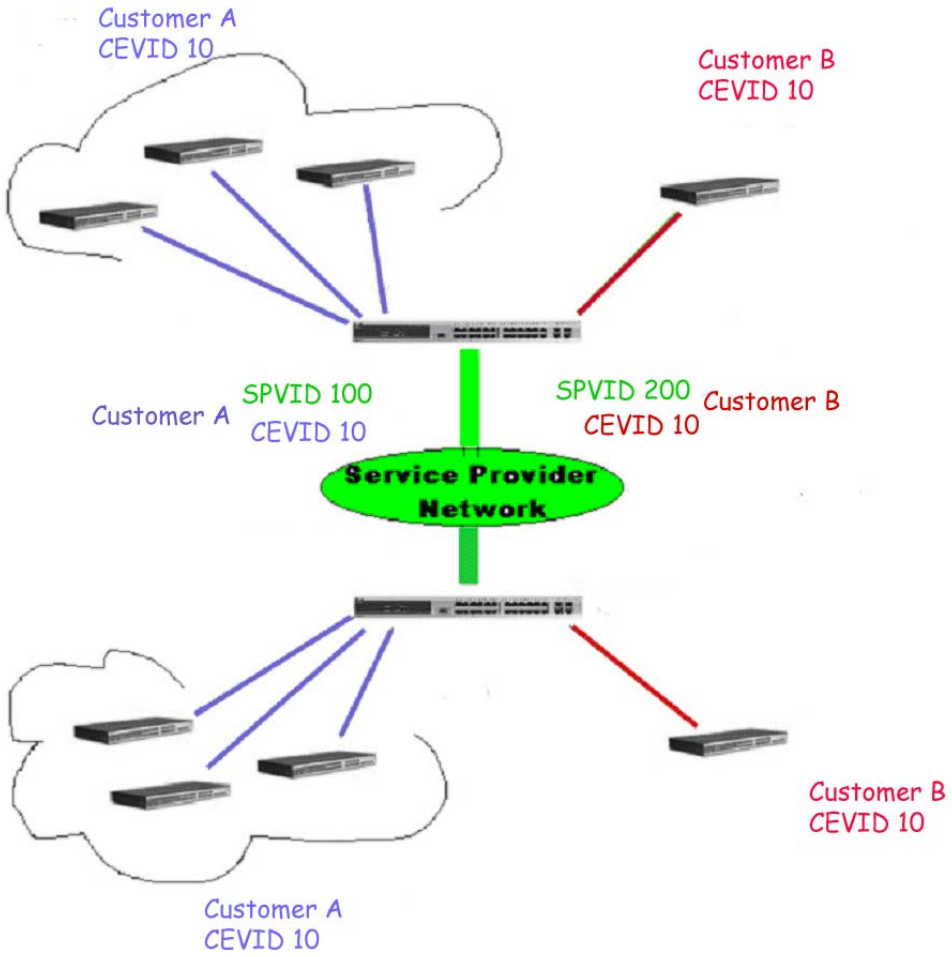


Figure 7- 5. Double VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs with different SPVIDs for specific customers (say Customer A and Customer B). Both CEVLANs (Customer VLANs), 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

Static VLAN Entry

Click **L2 Features** > **VLAN** > **Static VLAN Entry** to open the following window:

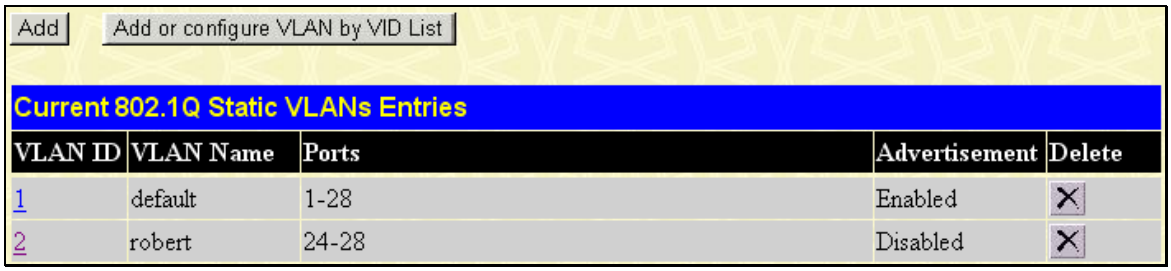


Figure 7- 6. Current 802.1Q Static VLANs Entries window

The **Current 802.1Q Static VLAN Entries** window lists all previously configured VLANs by VLAN ID and VLAN Name. To delete an existing 802.1Q VLAN, click the corresponding ✕ button under the **Delete** heading.

To create a new 802.1Q VLAN, click the **Add** button in the **802.1Q Static VLANs** 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.

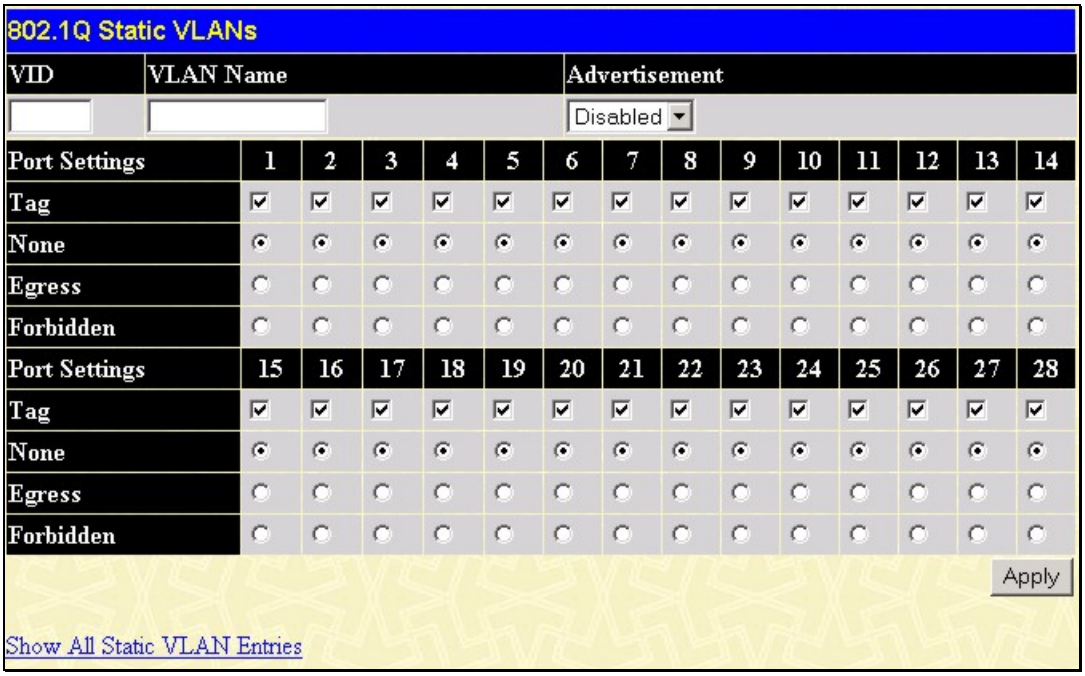


Figure 7- 7. 802.1Q Static VLAN window - Add

To return to the **802.1Q Static VLANs** window, click the Show All Static VLAN Entries link. To change an existing 802.1Q VLAN entry, click the Hyperlinked **VLAN ID** of the corresponding entry to modify. A new menu will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table at the end of the section for a description of the parameters in the new menu.

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

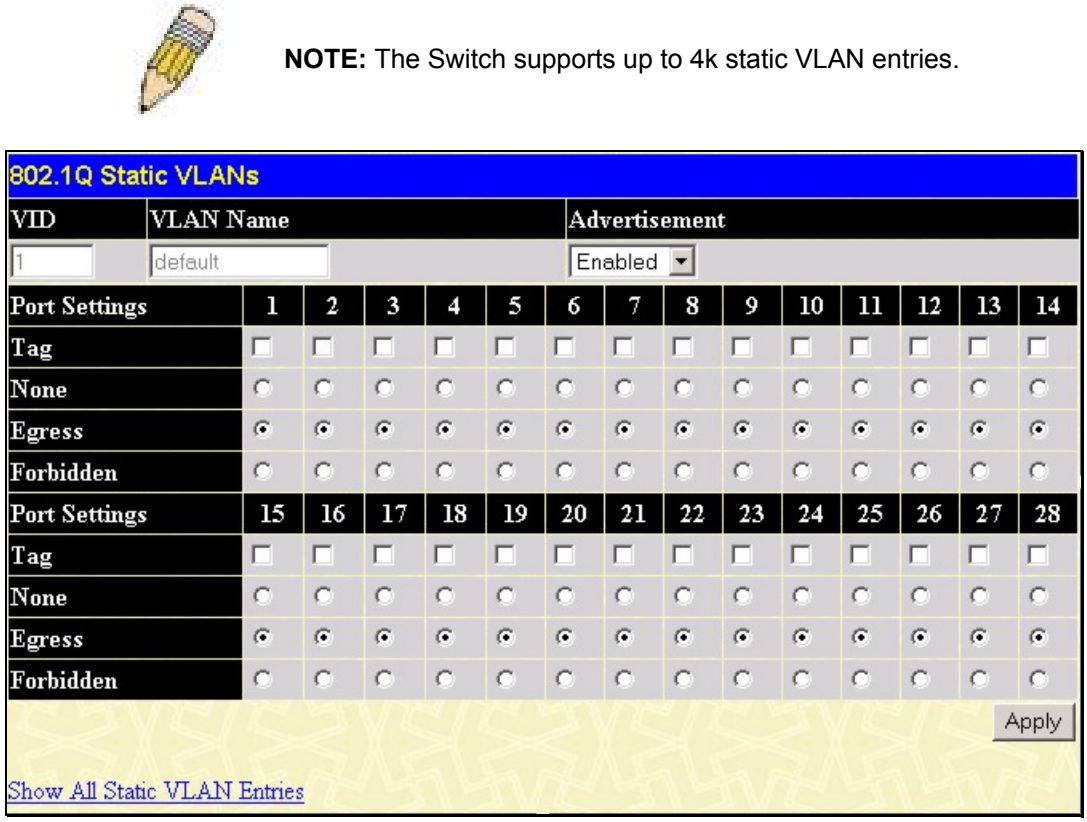


Figure 7- 8. 802.1Q Static VLANs – Modify

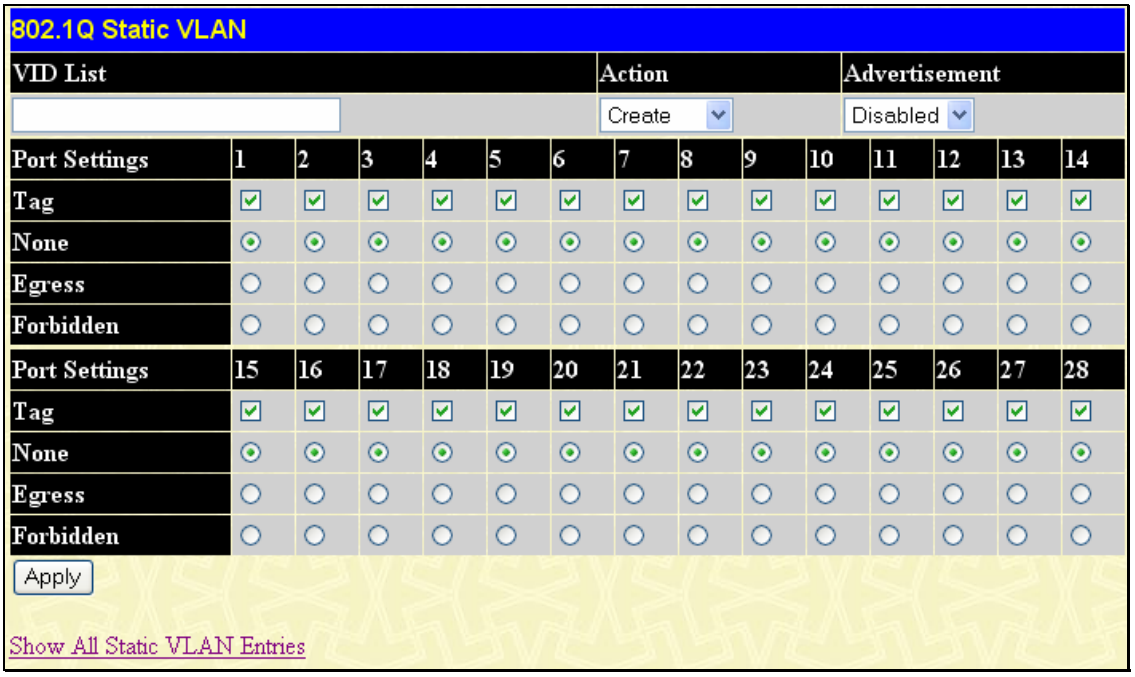
The following fields can then be set in either the **Add** or **Modify** 802.1Q Static VLANs windows:

Parameter	Description
VID (VLAN ID)	Allows the entry of a VLAN ID in the **Add** window, or displays the VLAN ID of an existing VLAN in the **Modify** window. VLANs can be identified by either the VID or the VLAN name.

VLAN Name	Allows the entry of a name for the new VLAN in the **Add** window, or for editing the VLAN name in the **Modify** window.
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.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
None	Allows an individual port to be specified as a non-VLAN member.
Egress	Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or 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.

To add or configure a VLAN by VID List, click the **Add or configure VLAN by VID list** button in the **802.1Q Static VLANs Entries** 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.



The following fields can then be set in the 802.1Q Static VLAN window:

Parameter	Description
VID List	Type in a new VID List number to create a new VID List or type in the VID List number of the VLAN you want to modify or delete. The VID range is from 1 to 4094.
Action	Choose the action required from the drop-down menu: ▪ Choose *Create* to create a new VLAN. ▪ Choose *Configure* to alter the configuration of an existing VLAN ▪ Choose *Delete* to delete the specified VLAN.
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.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
None	Allows an individual port to be specified as a non-VLAN member.
Egress	Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or 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.

GVRP Setting

The **GVRP Settings** window, shown right, allows you 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 does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

Click **L2 Features** > **VLAN** > **GVRP Settings**.

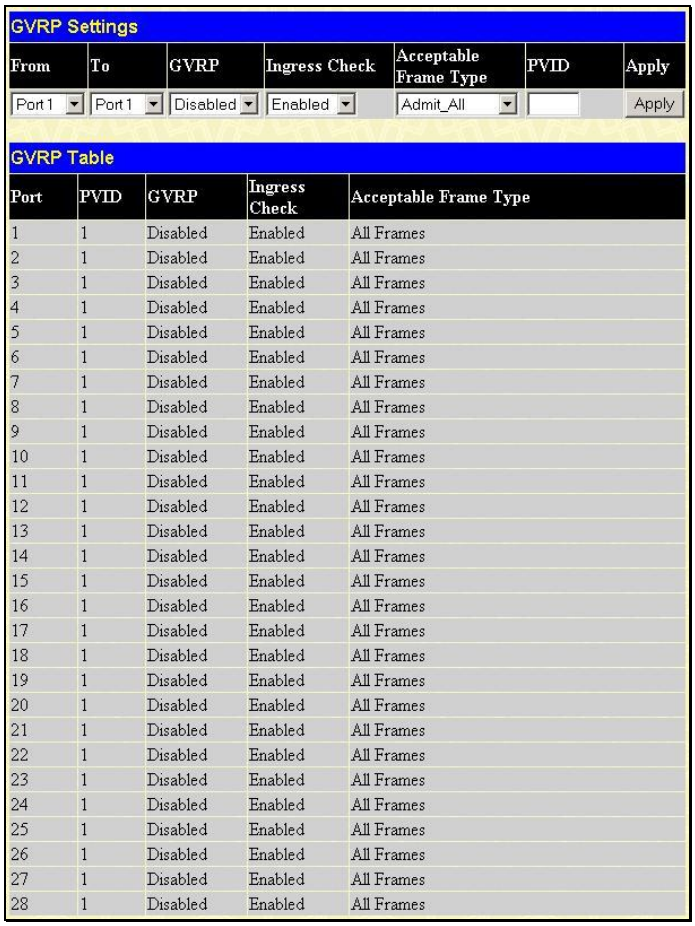


Figure 7- 9. GVRP Settings window

NOTE: The Switch supports up to 4k Dynamic Entries.

The following fields can be set:

Parameter	Description
From/To	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.
Ingress Check	This field can be toggled between *Enabled* and *Disabled* using the drop-down menu. *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.
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.

Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *Admit_All*, which mean both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.

Click **Apply** to implement changes made.

Double VLAN

Click **L2 Features** > **VLAN** > **Double VLAN Settings**, which will display the following window to enable the Double VLAN feature.

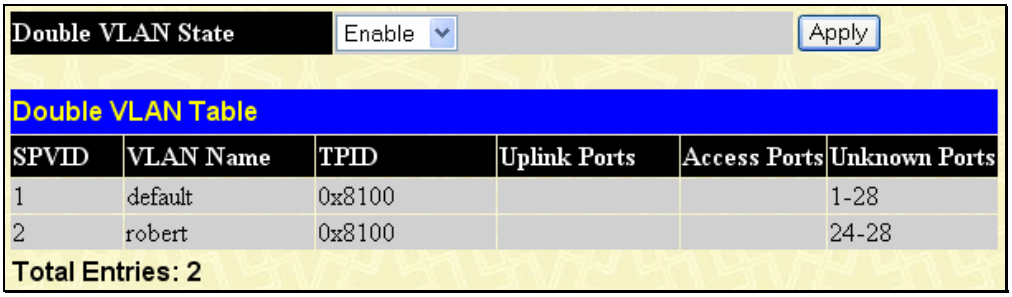
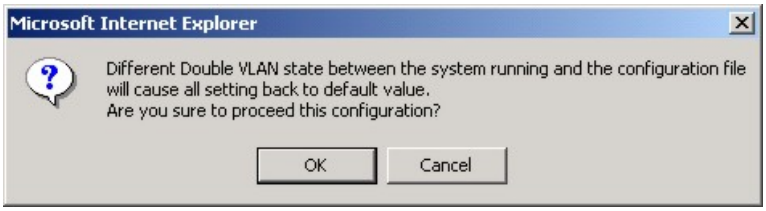


Figure 7- 10. Double VLAN State Settings

Choose *Enable* using the pull-down menu and click **Apply**. The user will be prompted with the following warning window. Click **OK** to continue. When **OK** is clicked, all switch settings except the IP will return to their default values.



After being prompted with a success message, the user will be presented with this window to configure for Double VLANs.

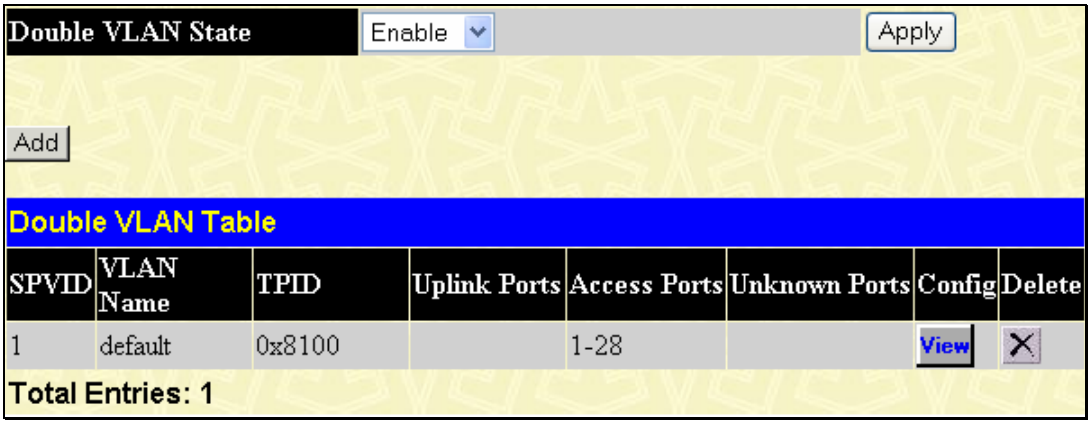


Figure 7- 11. Double VLAN Table

Parameters shown in the previous window are explained below:

Parameter	Description
Double VLAN State	Use the pull-down menu to enable or disable the Double VLAN function on this Switch. Enabling the Double VLAN will return all previous VLAN configurations to the factory default settings and remove Static VLAN configurations from the GUI.
SPVID	The VLAN ID number of this potential Service Provider VLAN.
VLAN Name	The name of the VLAN on the Switch.
TPID	The tagged protocol ID of the corresponding VLAN that will be used in identification of this potential Double VLAN, written in hex form.
Uplink Ports	Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source. Only

	gigabit ports can be configured as uplink ports.
Access Ports	Access ports are for connecting VLANs setup on the Switch to the customer VLANs. Gigabit ports cannot be configured as access ports.
Unknown Ports	This field displays the ports which have an unknown status.

The user may edit configurations for a Double VLAN by clicking its corresponding View button, which will display the following window:

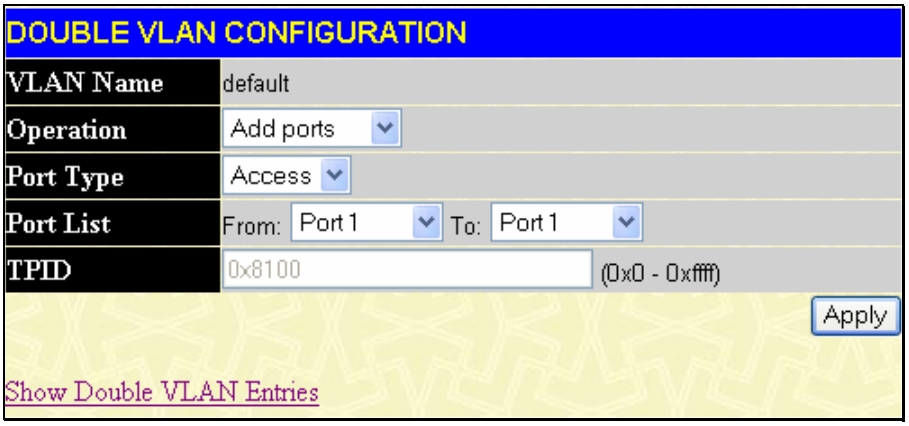


Figure 7- 12. Double VLAN Configuration window

The parameters shown in the window above are explained below:

Parameter	Description
VLAN Name	The name of the VLAN on the Switch.
Operation	Allows you to select Add Ports, Delete Ports or Config TPID.
Port Type	Allows the user to choose the type of port being utilized by the Service Provider VLAN. The user may choose: *Access* - Access ports are for connecting Switch VLANs to customer VLANs. Gigabit ports cannot be configured as access ports. *Uplink* - Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports.
Port List	Use the *From* and *To* fields to set a list of ports to be placed in, or removed from, the Service Provider VLAN.
TPID	The tagged protocol ID of the corresponding VLAN that will be used in identification of this potential Double VLAN, written in hex form.

To create a Double VLAN, click the **Add** button, revealing the following window for the user to configure.

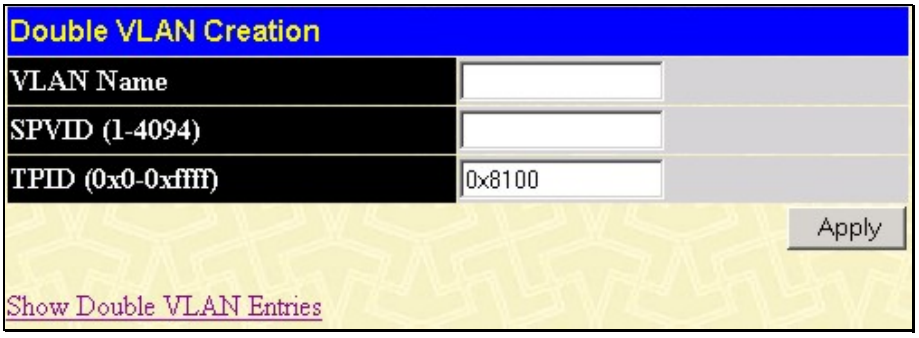


Figure 7- 13. Double VLAN Creation

To create a Double VLAN, enter the following parameters and click **Apply**.

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a Double VLAN.

SPVID	Enter the VID for the Service Provider VLAN with an integer between 1 and 4094.
TPID	Enter the TPID in hex form to aid in packet identification of the Service Provider VLAN.

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-3800 Series supports up to 32 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

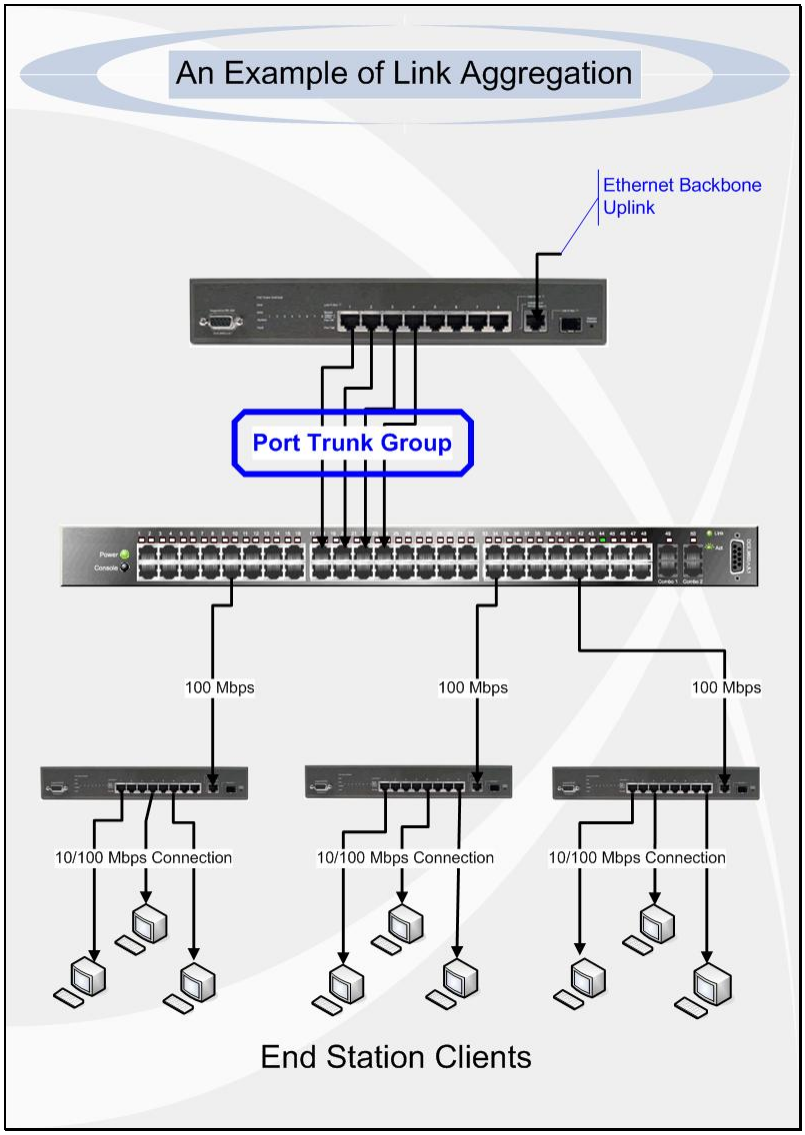


Figure 7- 14. Example of Port Trunk Group

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 32 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.

Link Aggregation

To configure port trunking, click **L2 Features > Trunking > Link Aggregation** to display the following window:

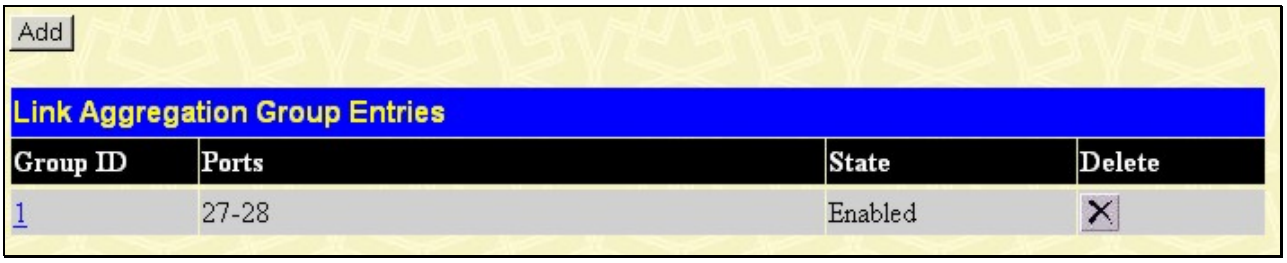


Figure 7- 15. Port Link Aggregation Group window

To configure port trunk groups, click the **Add** button to add a new trunk group and use the **Link Aggregation Group Configuration** window (see example below) to set up trunk groups. To modify a port trunk group, click the Hyperlinked Group ID. To delete a port trunk group, click the corresponding ✕ under the Delete heading in the **Link Aggregation Group Entries** table.

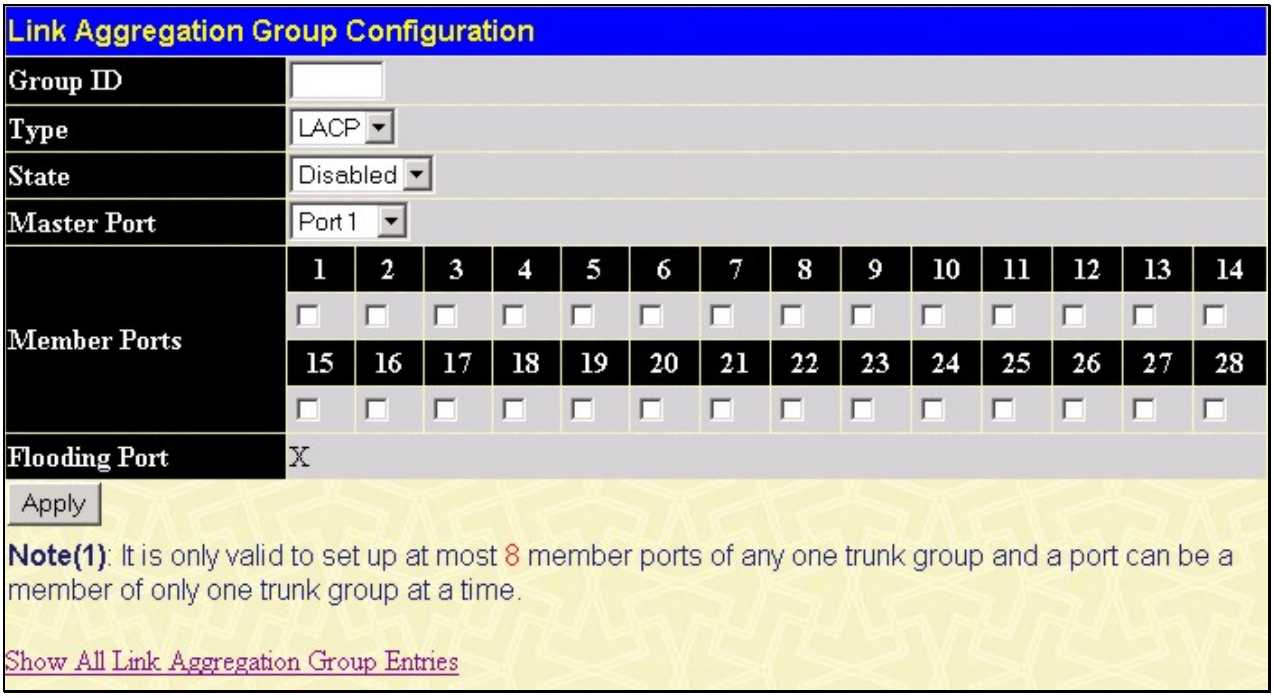


Figure 7- 16. Link Aggregation Group Configuration – Add

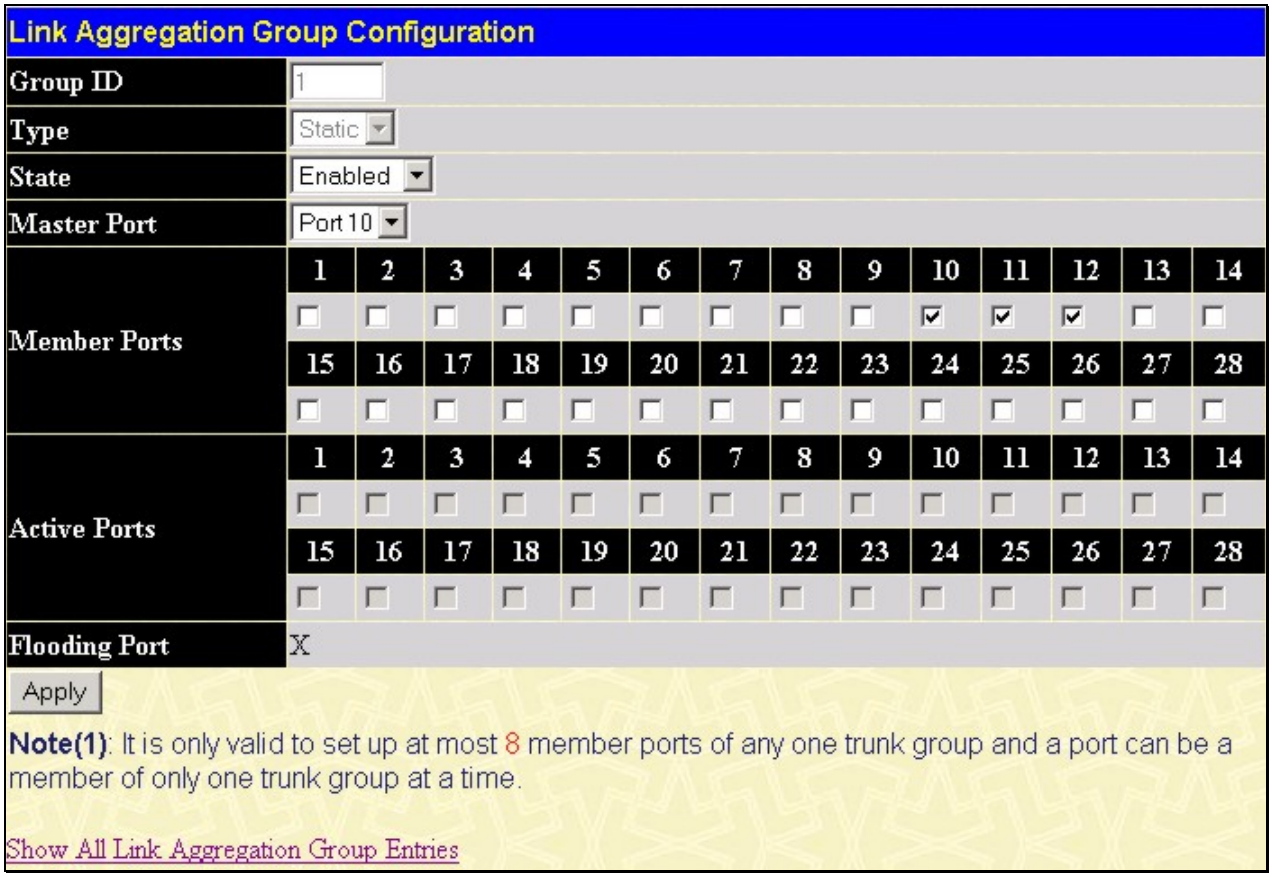


Figure 7- 17. Link Aggregation Group Configuration - Modify

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group, between *1* and *32*.
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.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
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.
Active Port	Shows the port that is currently forwarding packets.
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.

After setting the previous parameters, click **Apply** to allow your changes to be implemented. Successfully created trunk groups will be shown in the **Link Aggregation Group Entries** table as seen in Figure 7-17.

LACP Port Settings

The **LACP Port Settings** window is used in conjunction with the **Link Aggregation** window to create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames. To view this window, click **L2 Features > Trunking > LACP Port Settings**.

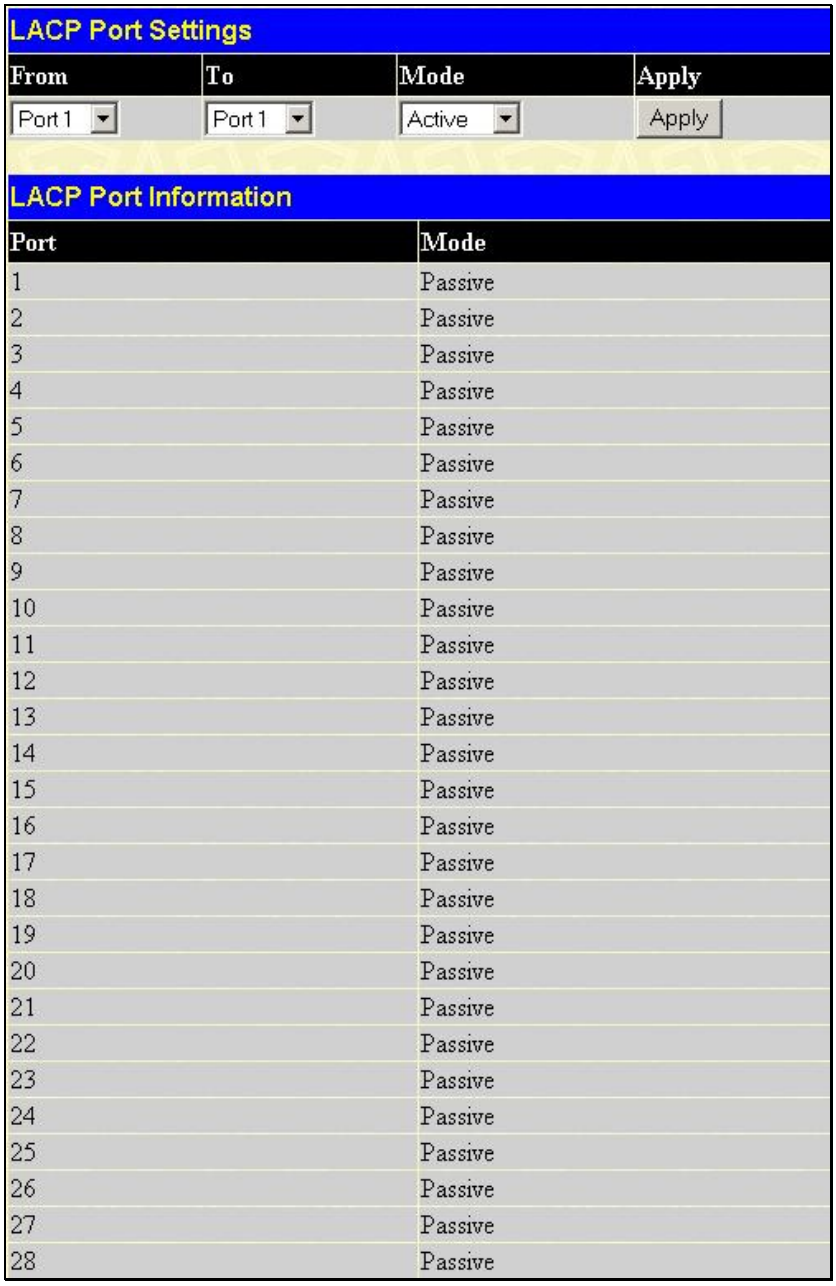


Figure 7- 18. LACP Port Settings window

The user may set the following parameters:

Parameter	Description
From/To	A consecutive group of ports may be configured starting with the selected port.
Mode	*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).

After setting the previous parameters, click **Apply** to allow your changes to be implemented. The **LACP Port Table** shows which ports are active and/or passive.

IGMP

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-3800 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

Use the **L2 Features > IGMP Snooping > IGMP Snooping Settings** to view configurations. To modify the settings, click the **Modify** button of the VLAN ID to change.

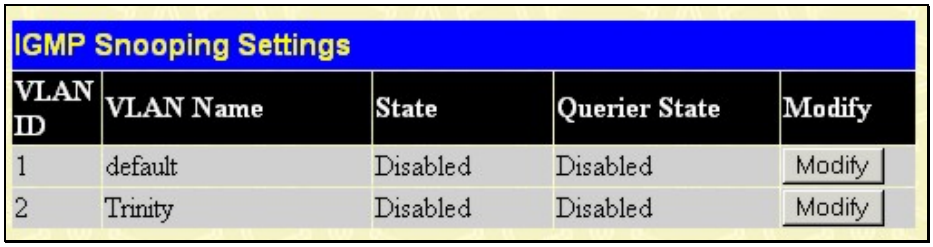


Figure 7- 19. IGMP Snooping Settings window

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

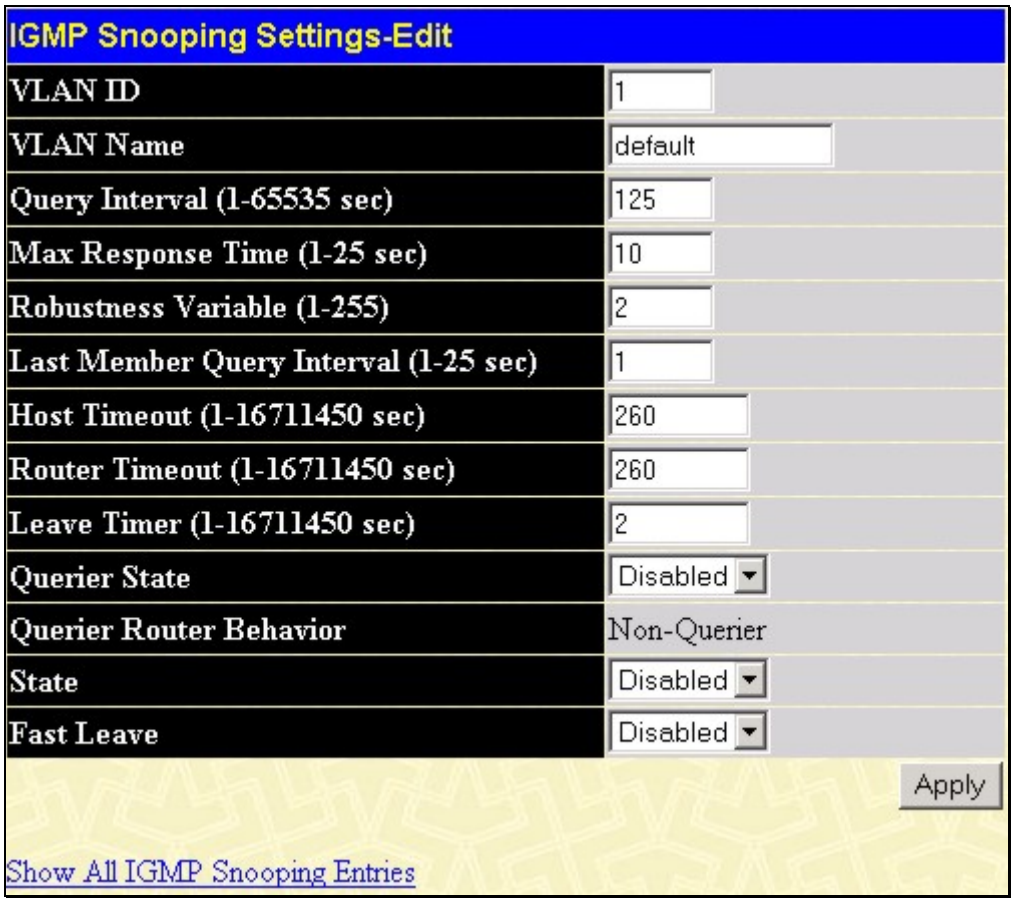


Figure 7- 20. IGMP Snooping Settings-Edit window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the 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	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	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	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	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	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*.
Route Timeout	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	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*.
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.
State	Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default.
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*.

Click **Apply** to implement the new settings. Click the Show All IGMP Group Entries link to return to the **IGMP Snooping Settings** window.

Static Router Port Settings

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router.

A router port has the following behavior:

- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of a Layer 3 switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast or PIM-DM multicast packets are detected flowing into a port.

Open the **L2 Features > IGMP folder** > **Static Router Port Settings** link to open the following page, as shown below.

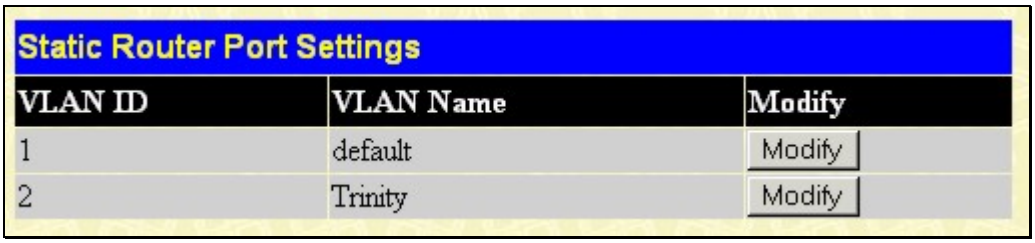


Figure 7- 21. Static Router Ports Settings window

The previous window displays all of the current entries to the Switch's static router port table. To modify an entry, click the **Modify** button. This will open the **Static Router Ports Settings** window, as shown below.

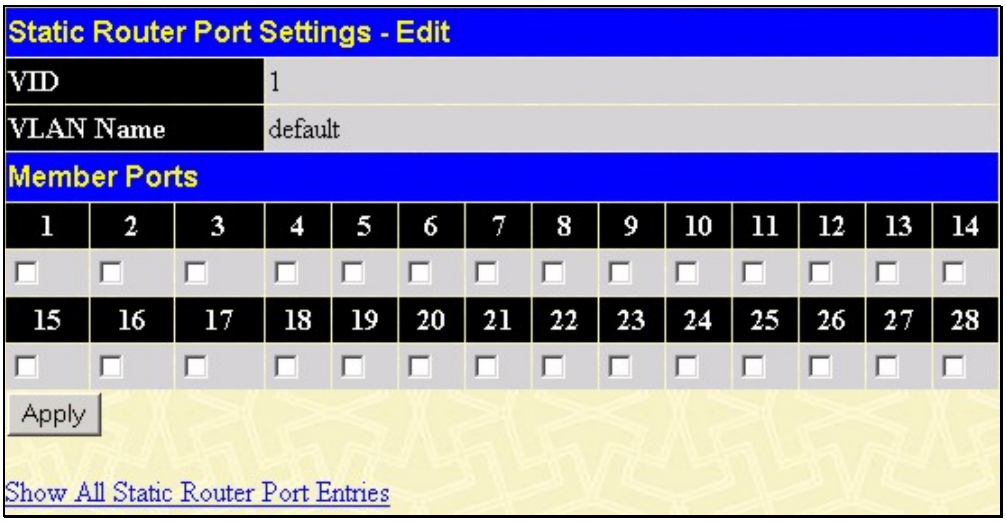


Figure 7- 22. Static Router Ports Settings - Edit window

The following parameters can be set:

Parameter	Description
VID (VLAN ID)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN where the multicast router is attached.
VLAN Name	This is the name of the VLAN where the multicast router is attached.
Member Ports	Ports on the Switch that will have a multicast router attached to them.

Click **Apply** to implement the new settings, Click the Show All Static Router Port Entries link to return to the **Static Router Port Settings** window.

IGMP Multicast VLAN

IGMP Multicast Vlan enables the switch to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

To configure the ISM Vlan Settings window, click **L2 Features > IGMP Snooping > IGMP Multicast VLAN,** which will open the following window:

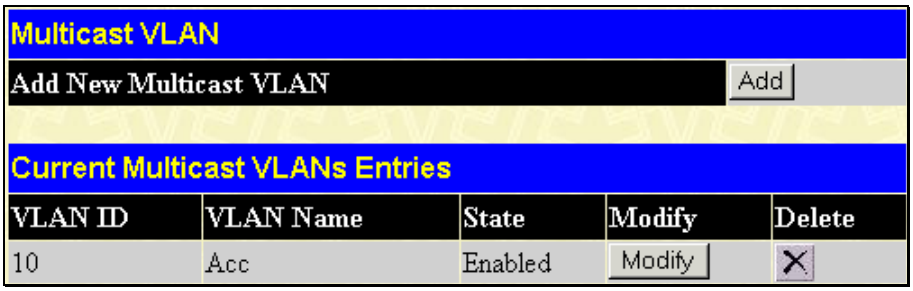


Figure 7- 23. IGMP Multicast VLAN Table window

Clicking the **Add** button will reveal the following window to configure:

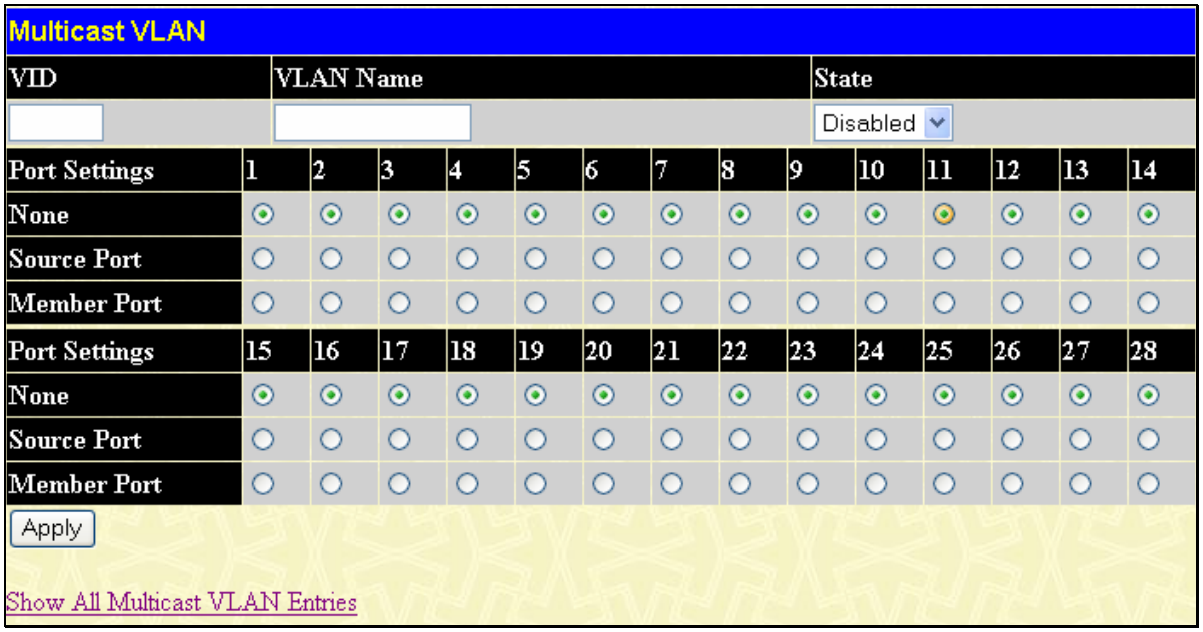


Figure 7- 24. IGMP Multicast VLAN Settings - Add window

Parameter	Description
VID ()	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
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.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*

To view the settings for a particular entry, click on the hyperlinked **Show All Multicast VLAN Entries**, which will reveal the following window.

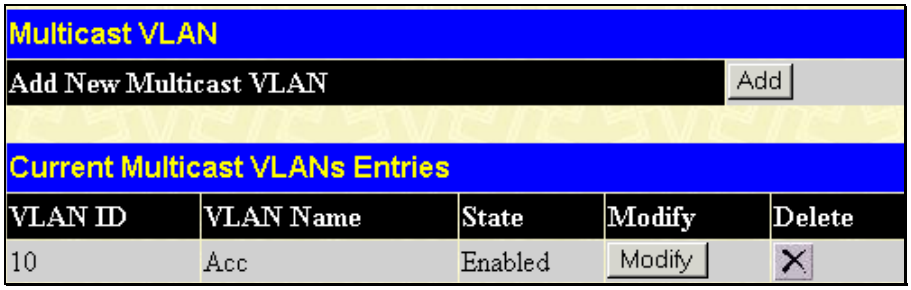


Figure 7- 25. IGMP Multicast VLAN Entries window

To configure the IGMP Snooping Multicast VLAN settings, click its corresponding Modify button, which will produce the following window for the user to configure. To delete an entry, click the corresponding ✕ under the Delete heading.

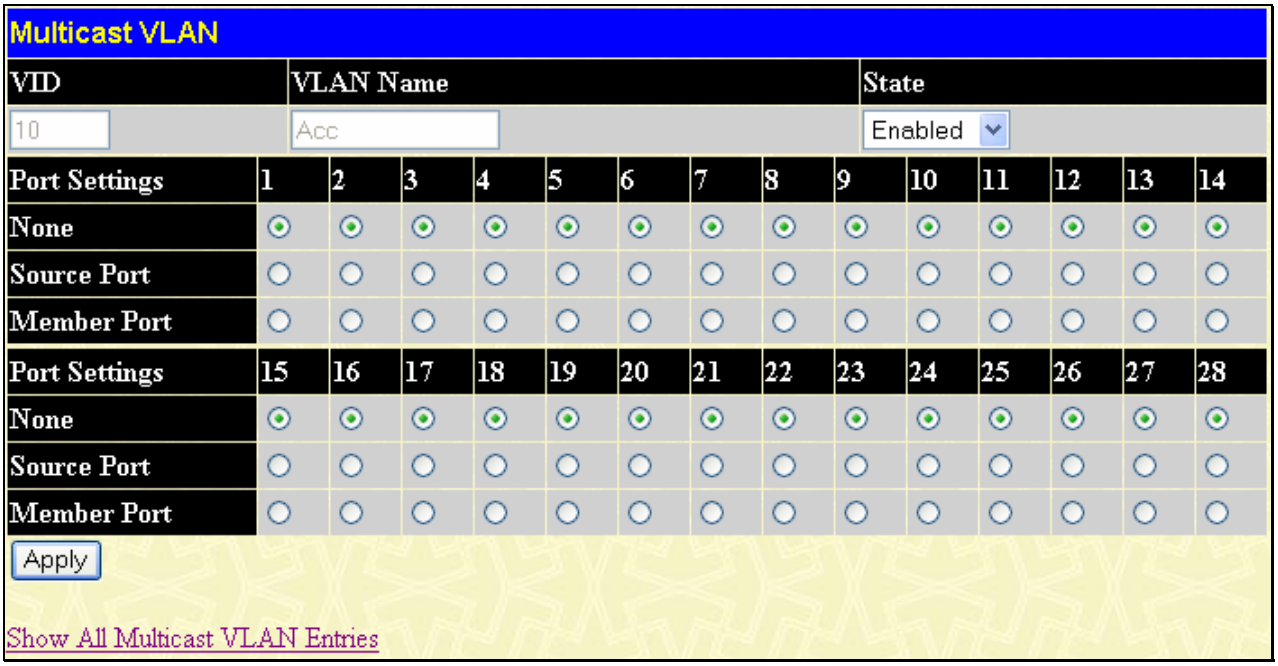


Figure 7- 26. IGMP Multicast VLAN - Modify window

MLD Snooping

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

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

MLD Control Messages

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

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

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

MLD Snooping Settings

To configure the settings for MLD snooping, click **L2 Features > MLD Snooping > MLD Snooping Settings**, which will open the following window.

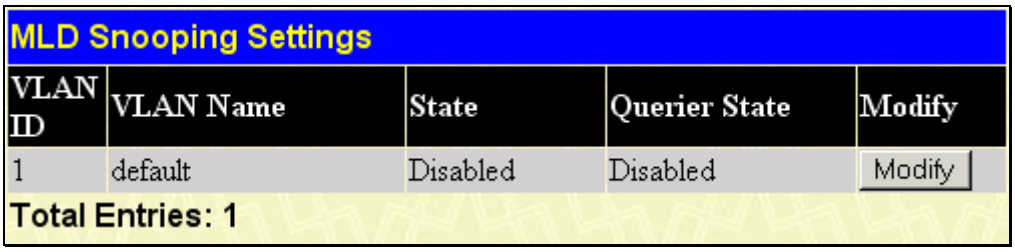


Figure 7- 27. MLD Snooping Settings window

This window displays the current MLD Snooping settings set on the Switch, defined by VLAN. To configure a specific VLAN for MLD snooping, click the VLAN's corresponding Modify button, which will display the following window for the user to configure.

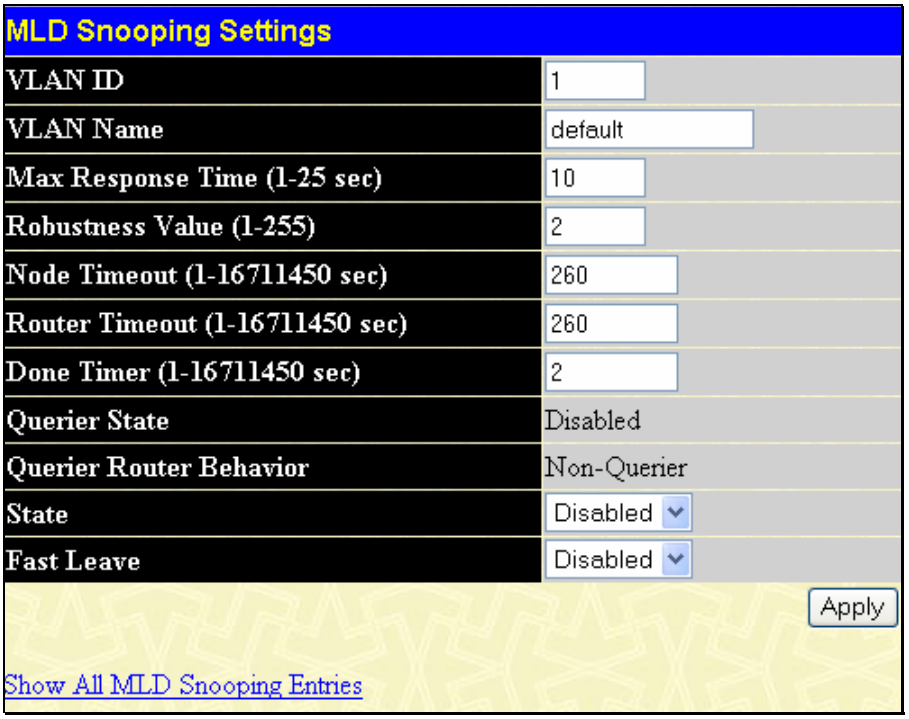


Figure 7- 28. MLD Snooping Settings - Edit window

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.
Max Response Time	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 have a high loss, the user may wish to increase this interval.
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*. The field will always display "Disabled", it will always be in MLD-Snooping non-querier state.
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.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
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.

NOTE: The robustness variable of the MLD snooping querier is used in creating the following MLD message intervals:

Group Listener Interval – The amount of time that must pass before a multicast router decides that there are no more listeners present of a group on a network. Calculated as (robustness variable * query interval) + (1 * query interval).

Querier Present Interval – The amount of time that must pass before a multicast router decides that there are no other querier devices present. Calculated as (robustness variable * query interval) + (0.5 * query response interval).

Last Listener Query Count – The amount of group-specific queries sent before the router assumes there are no local listeners in this group. The default value is the value of the robustness variable.

Click **Apply** to implement changes made. Click the Show All MLD Snooping Entries link to return to the MLD Snooping Settings window.

MLD Snooping Static Router Port Settings

The following window is used to designate a port or range of ports as being connected to multicast enabled routers. When IPv6 routing control packets, such as DVMRP, OSPF or RIP, or MLD Query packets are found in an Ethernet port or specified VLAN, the Switch will set these ports as dynamic router ports. Once set, this will ensure that all packets with a multicast router as its destination will arrive at the multicast-enabled router, regardless of protocol. If the Router's Aging Time expires and no routing control packets or query packets are received by the port, that port will be removed from being a router port.

To configure the settings for MLD Router Ports, click **L2 Features > MLD Snooping > MLD Snooping Static Router Port Settings**, which will open the following window.

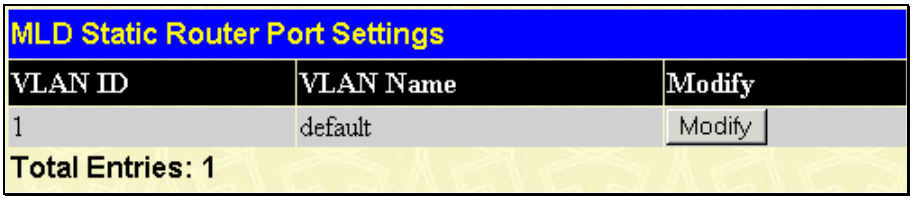


Figure 7- 29. MLD Static Router Port Settings Window

To configure the router ports settings for a specified VLAN, click its corresponding Modify button, which will produce the following window for the user to configure.

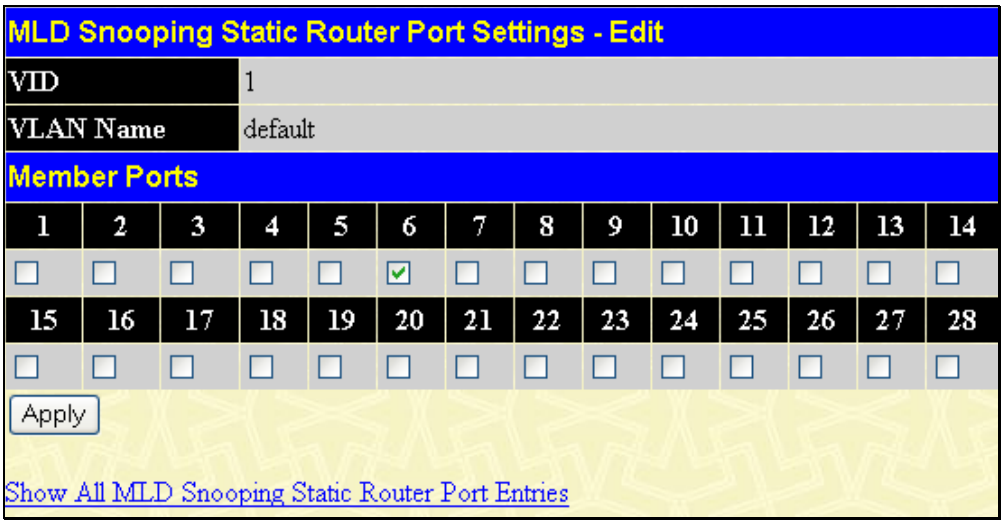


Figure 7- 30. MLD Snooping Static Router Port Settings- Edit window

The following parameters are displayed:

Parameter	Description
VID (VLAN ID)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN where the MLD multicast router is attached.
VLAN Name	This is the name of the VLAN where the MLD multicast router is attached.

Tick the port numbers that are connected to multicast enabled routers and click **Apply** to implement the changes made. Click the Show All Snooping Static Router Port Entries link to return to the MLD Snooping Settings window

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 802.1s MSTP. 802.1d STP will be familiar to most networking professionals. However, since 802.1w RSTP and 802.1s MSTP 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, 802.1w RSTP and 802.1s MSTP.

802.1s MSTP

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

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

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

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4096-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

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

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

802.1w Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1s, 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. MSTP and RSTP combine 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/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-1 below compares how the three protocols differ regarding the port state transition.

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

802.1s MSTP	802.1w RSTP	802.1d STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	Discarding	Blocking	No	No
Discarding	Discarding	Listening	No	No
Learning	Learning	Learning	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

Figure 7- 31. Comparing Port States

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

Edge Port

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

P2P Port

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

802.1d/802.1w/802.1s Compatibility

MSTP or 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 MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

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

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

STP Bridge Global Settings

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

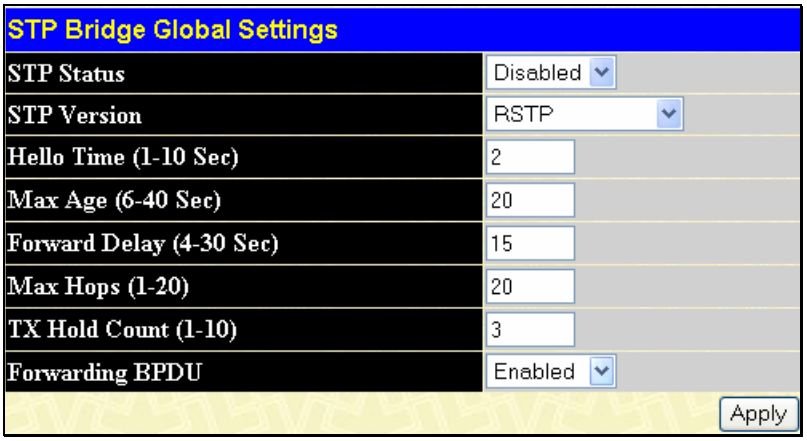


Figure 7- 32. STP Bridge Global Settings window –RSTP (Default)

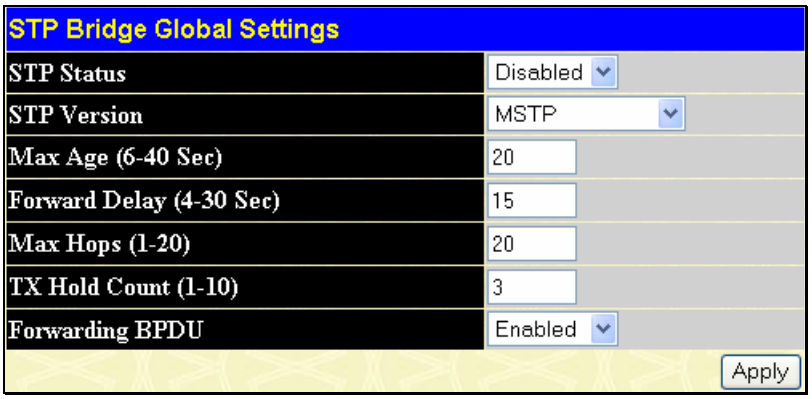


Figure 7- 33. STP Bridge Global Settings window - MSTP

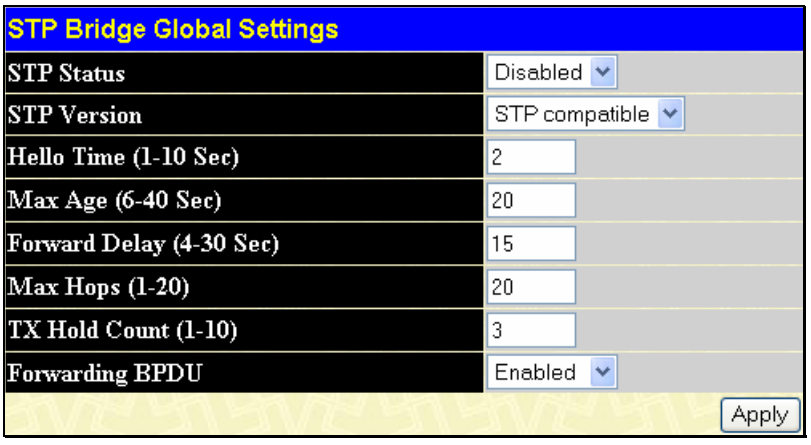


Figure 7- 34. STP Bridge Global Settings – STP Compatible window

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)

The following parameters can be set:

Parameter	Description
STP Status	Use the pull-down menu to enable or disable STP globally on the Switch. The default is *Disabled*.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are two choices: *STP compatable* - 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.
Hello Time (1-10 Sec)	Type in a value between 1 and 10 seconds to specify how often the switch will broadcast its hello messages to other switches.
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.
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.
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 BDPU 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.
TX Hold Count	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is 3.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When set to *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 screens in the **MST Configuration Identification** window 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**:

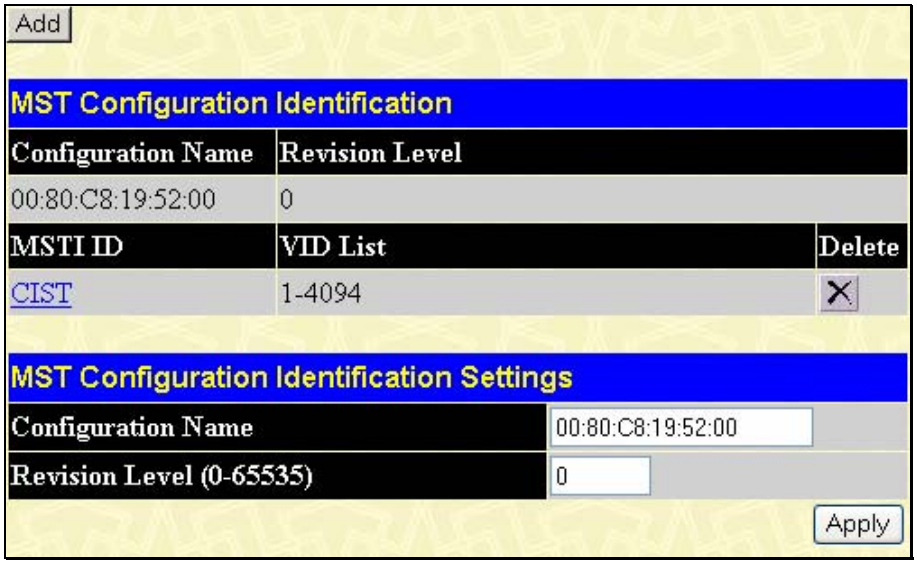


Figure 7- 35. MST Configuration Identification and Settings window

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	This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between 0-65535 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.
VID List	This field displays the VLAN IDs associated with the specific MSTI.

Clicking the **Add** button will reveal the following window to configure:

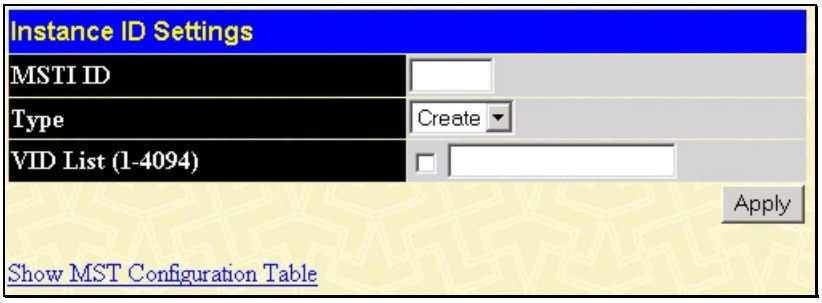


Figure 7- 36. Instance ID Settings window – Add

The user may configure the following parameters to create a MSTI in the Switch.

Parameter	Description
MSTI ID	Enter a number between *1* and *4 to* set a new MSTI on the Switch.
Type	*Create* is selected to create a new MSTI. No other choices are available for this field when creating a new MSTI.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*.

Click **Apply** to implement changes made.

To configure the settings for the CIST, click on its hyperlinked name in the **MST Configuration Identification** window, which will reveal the following window to configure:

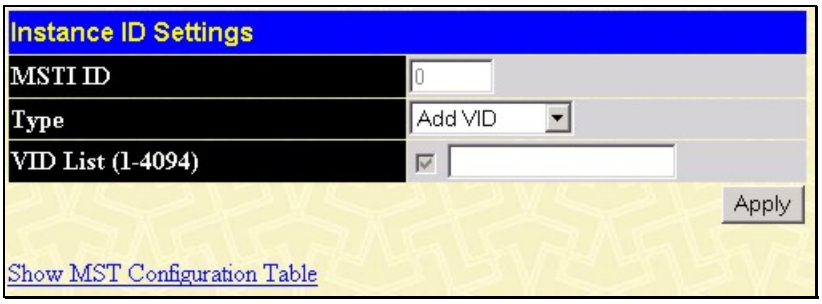


Figure 7- 37. Instance ID Settings window - CIST modify

The user may configure the following parameters to configure the CIST on the Switch.

Parameter	Description
MSTI ID	The MSTI ID of the CIST is *0* and cannot be altered.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has 2 choices. • *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. • *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*. This field is inoperable when configuring the CIST.

Click **Apply** to implement changes made.

To configure the parameters for a previously set MSTI, click on its hyperlinked MSTI ID number, which will reveal the following window for configuration.

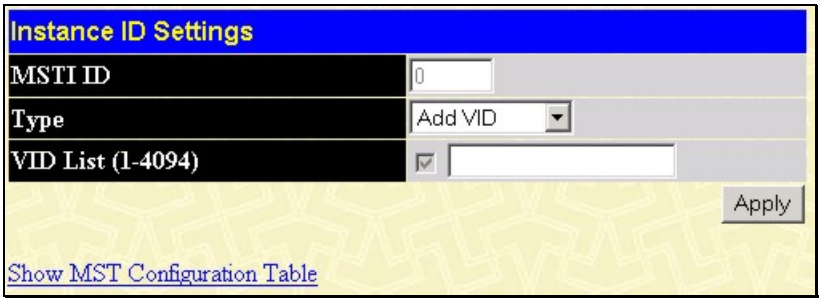


Figure 7- 38. Instance ID Settings window – modify

The user may configure the following parameters for a MSTI on the Switch.

Parameter	Description
MSTI ID	Displays the MSTI ID previously set by the user.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has four choices. • *Add* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. • Remove - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch that the user wishes to add to this MSTI ID. Supported VIDs on the Switch range from ID number *1* to *4094*. This parameter can only be utilized if the Type chosen is *Add* or *Remove*.

Click **Apply** to implement changes made.

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**:

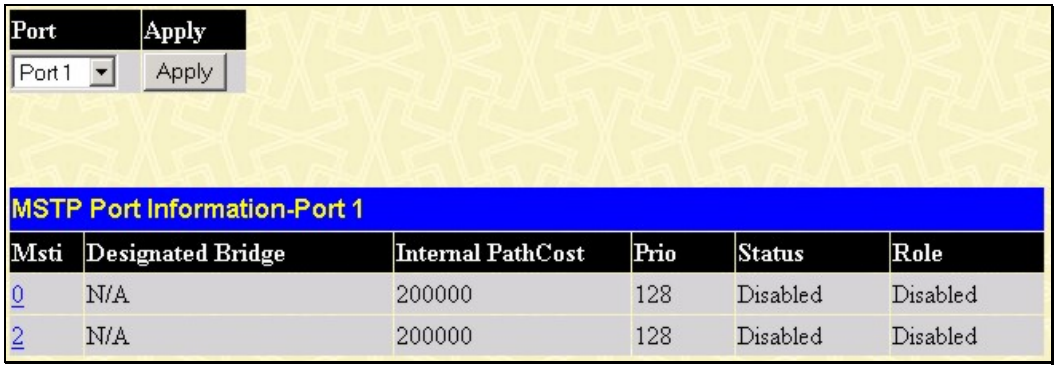


Figure 7- 39. MSTP Port Information window

To view the MSTI settings for a particular port, select the Port number, located in the top left hand corner of the screen and click **Apply**. To modify the settings for a particular MSTI Instance, click on its hyperlinked MSTI ID, which will reveal the following window.

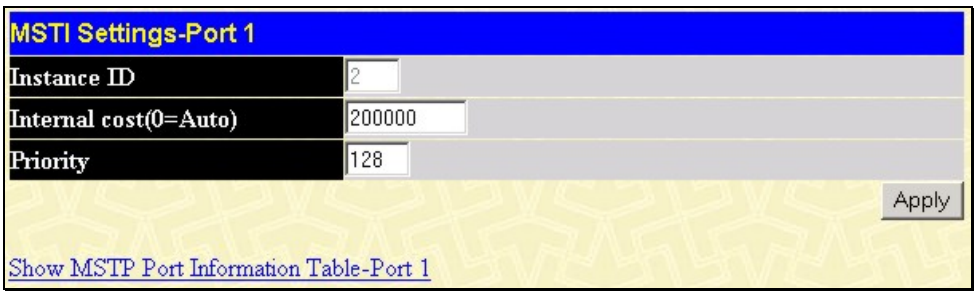


Figure 7- 40. MSTI Settings window

The following parameters can be viewed or set:

Parameter	Description
Instance ID	Displays the MSTI ID of the instance being configured. An entry of 0 in this field denotes the CIST (default MSTI).
Internal cost (0=Auto)	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 1-2000000* - Selecting this parameter with a value in the range of 1-2000000 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.

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**:

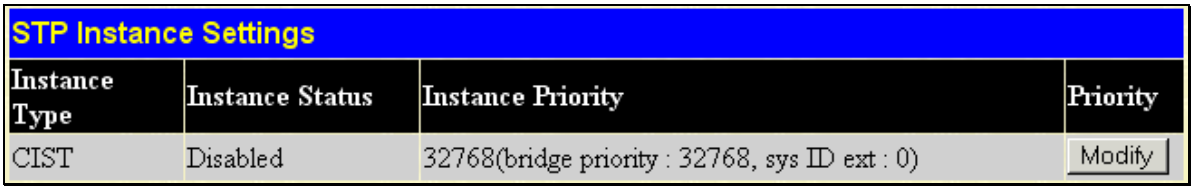


Figure 7- 41. STP Instance Table window

The following information is displayed:

Parameter	Description
Instance Type	Displays the instance type(s) currently configured on the Switch. Each instance type is classified by a MSTI ID. CIST refers to the default MSTI configuration set on the Switch.
Instance Status	Displays the current status of the corresponding MSTI ID
Instance Priority	Displays the priority of the corresponding MSTI ID. The lowest priority will be the root bridge.

Click **Apply** to implement changes made.

Click the **Modify** button to change the priority of the MSTI. This will open the Instance ID Settings window to configure.

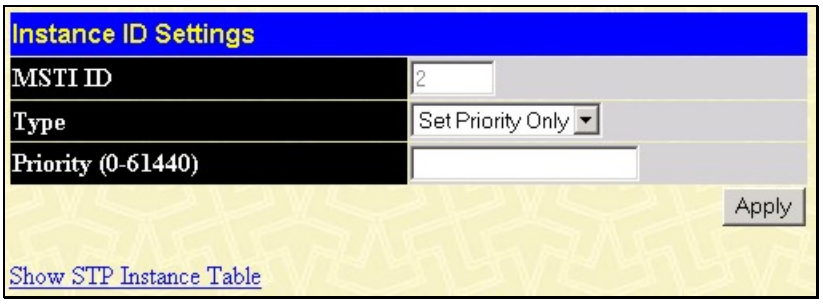


Figure 7- 42. STP Instance Settings - modify priority window

The following parameters can be viewed or 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).
Type	The Type field in this window will be permanently set to *Set Priority Only*.
Priority (0-61440)	Enter the new priority in the Priority field. The user may set a priority value between 0-61440.

Click **Apply** to implement the new priority setting.

STP Port Settings

STP can be set up on a port per port basis. To view the STP Port Settings window click **L2 Features** > **Spanning Tree** > **STP Port Settings**.

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.

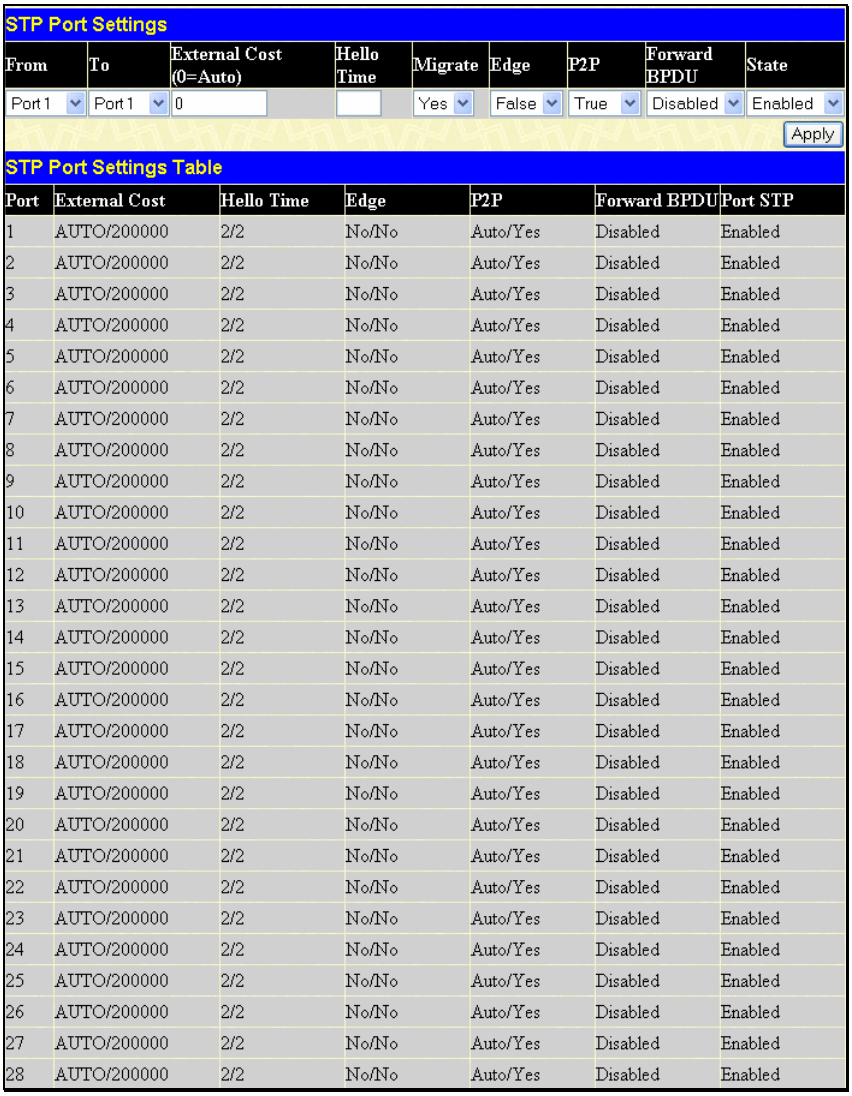


Figure 7- 43. STP Port Settings window

The following STP Port Settings fields can be set:

Parameter	Description
From/To	A consecutive group of ports may be configured starting with the selected port.
External Cost (0=Auto)	This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto). *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.
Hello Time	The time interval between transmissions of configuration messages by the designated port, to other devices on the bridged LAN. The user may choose a time between *1* and *10* seconds. The default is 2 seconds. This field is only operable when the Switch is enabled for MSTP.
Migrate	When operating in RSTP mode, selecting *Yes* forces the port that has been selected to transmit RSTP BPDUs.
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*.
Forward BPDU	Choosing *Enabled* will allow the forwarding of BPDU packets in the specified ports from other network devices. This will go into effect only if STP is globally disabled AND Forwarding BPDU is globally enabled (See **STP Bridge Global Settings** above). The default setting *Disabled*, does not forward BPDU packets when STP is disabled.
State	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is *Enabled*.

Click **Apply** to implement changes made.

NOTE: If you want to enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1. STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. These are the default settings configurable in the **STP Bridge Global Settings** menu discussed previously.

STP Ports Information of Instance

Information about a previously created STP Port instance can be viewed in the STP Port Instance Information window. To view the STP Port Instance Information window click **L2 Features > Spanning Tree > STP Port Information of Instance**. All information in this window is read-only and are described previously in this section. Each port has information regarding the individual port spanning tree settings.

Instance: 0 | Apply

STP Ports Instance Information 0

Port	Designated Bridge	Internal PathCost	External Cost	Pri	Edge	P2P	Hello Time	Status	Role
1	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
2	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
3	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
4	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
5	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
6	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
7	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
8	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
9	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Forwarding	NonStp
10	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
11	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
12	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
13	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
14	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
15	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
16	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
17	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
18	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
19	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
20	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
21	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
22	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
23	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Forwarding	NonStp
24	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
25	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
26	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
27	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled
28	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	2/2	Disabled	Disabled

Figure 7- 44. STP Ports Instance Information window

Forwarding

Unicast Forwarding

The following figure and table describe how to set up **Unicast Forwarding** on the Switch. Click **L2 Features** > **Forwarding** > **Unicast Forwarding** to view the following table.

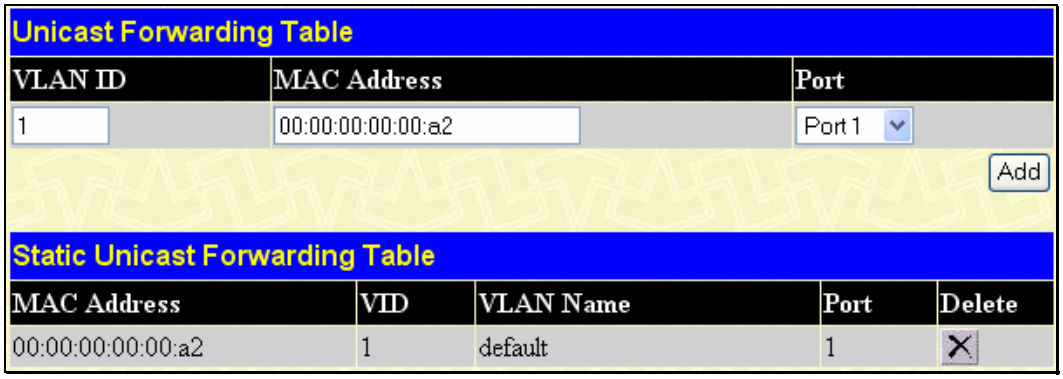


Figure 7- 45. Unicast Forwarding Table window

To add an entry, define the following parameters and then click **Add**:

Parameter	Description
VLAN ID	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	Use the drop-down menu to select the port number, where the MAC address entered above resides on.

To delete an entry in the **Unicast Forwarding Table**, click the corresponding ✕ under the Delete heading.

Multicast Forwarding

The following figure and table describe how to set up **Multicast Forwarding** on the Switch. Click **L2 Features** > **Forwarding** > **Multicast Forwarding**, to view the screen below:

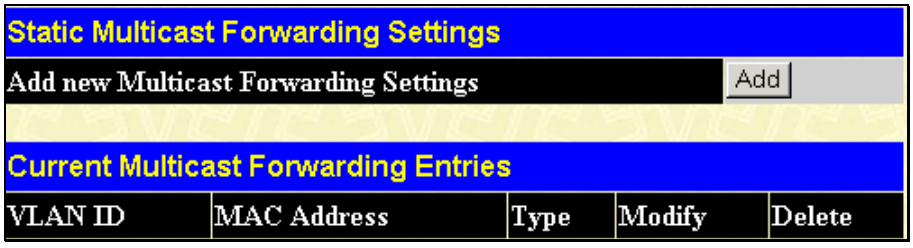


Figure 7- 46. Static Multicast Forwarding Settings window

The **Static Multicast Forwarding Settings** window displays all of the entries made into the Switch's static multicast forwarding table. Click the **Add** button to open the **Setup Static Multicast Forwarding Table** window, as shown below:

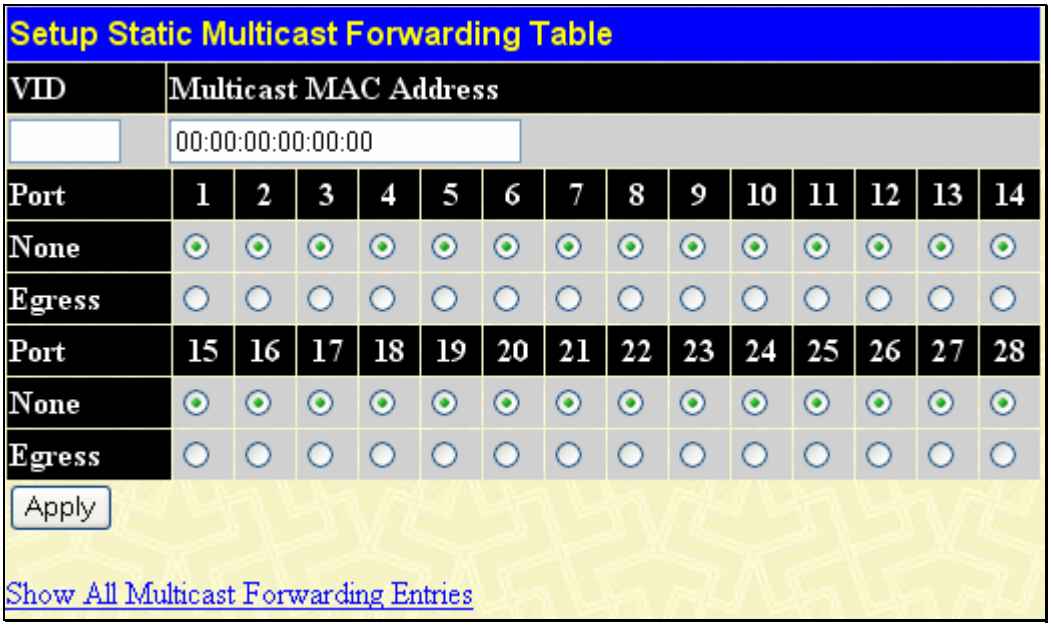


Figure 7- 47. Setup Static Multicast Forwarding Table window

The following parameters can be set:

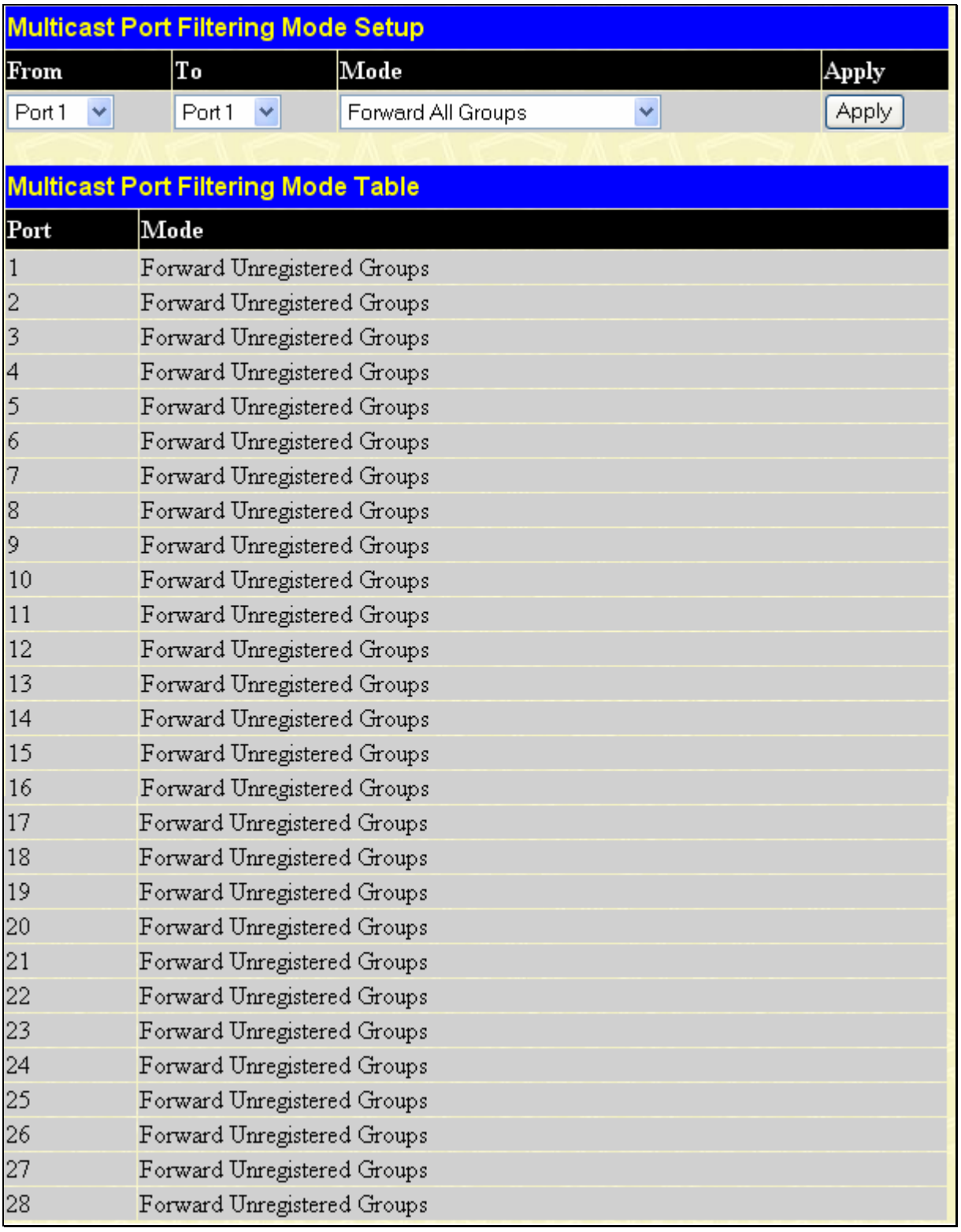
Parameter	Description
VID	The VLAN ID of the VLAN to which the corresponding Multicast MAC address belongs.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When None is chosen, the port will not be a member of the Static Multicast Group. *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 ✕ under the Delete heading. Click the **Show All Multicast Forwarding Entries** link to return to the **Static Multicast Forwarding Settings** window.

NOTE: When IGMP Snooping is enabled, the Static Multicast Forwarding Settings will not take effect.

Multicast Port Filtering Mode

The following figure and table describes how to setup the **Multicast Port Filtering Mode** feature on the Switch. Click **L2 Features > Forwarding** > **Multicast Port Filtering** to view the window below:



Multicast Port Filtering Mode Setup

From	To	Mode	Apply
Port 1	Port 1	Forward All Groups	Apply

Multicast Port Filtering Mode Table

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

Figure 7- 47. The Multicast Port Filtering Mode Settings window

The **Multicast Port Filtering Mode** window is divided into two sections. The top section allows the user to change the multicast port filtering mode of specific ports. The bottom section of the window displays all the ports on the Switch and the Multicast Port Filtering Mode they have been configured with.

The following parameters can be set in the **Multicast Port Filtering Mode Setup** section of the window:

Parameter	Description
From/To	Select the ports that require their Multicast Port Filtering Mode to be changed from the drop-down menus.
Mode	Choose the following Multicast Port Filtering Mode from the drop-down menu: *Forward All Groups*- In this mode all frames destined for group MAC addresses are forwarded according to the VLAN rule. *Forward Unregistered Groups*- In this mode if the Group MAC Address Registration entries exist in the Multicast Table, frames destined for the corresponding Group MAC addresses are forwarded only to ports identified in the member port set. On the other hand, if the Group MAC address does not exist in the Multicast Table the frames are forwarded according to the VLAN rule. *Filter Unregistered Groups*- In this mode frames destined for group MAC addresses are only forwarded only if such forwarding is explicitly permitted by a Group Address entry in the Multicast Table. In other words, if the Group MAC address does not exist in the Multicast table, the packets are dropped.

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

Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port.

To view the **Loopback Detection Settings** window, click **L2 Features** > **Loopback Detection**.

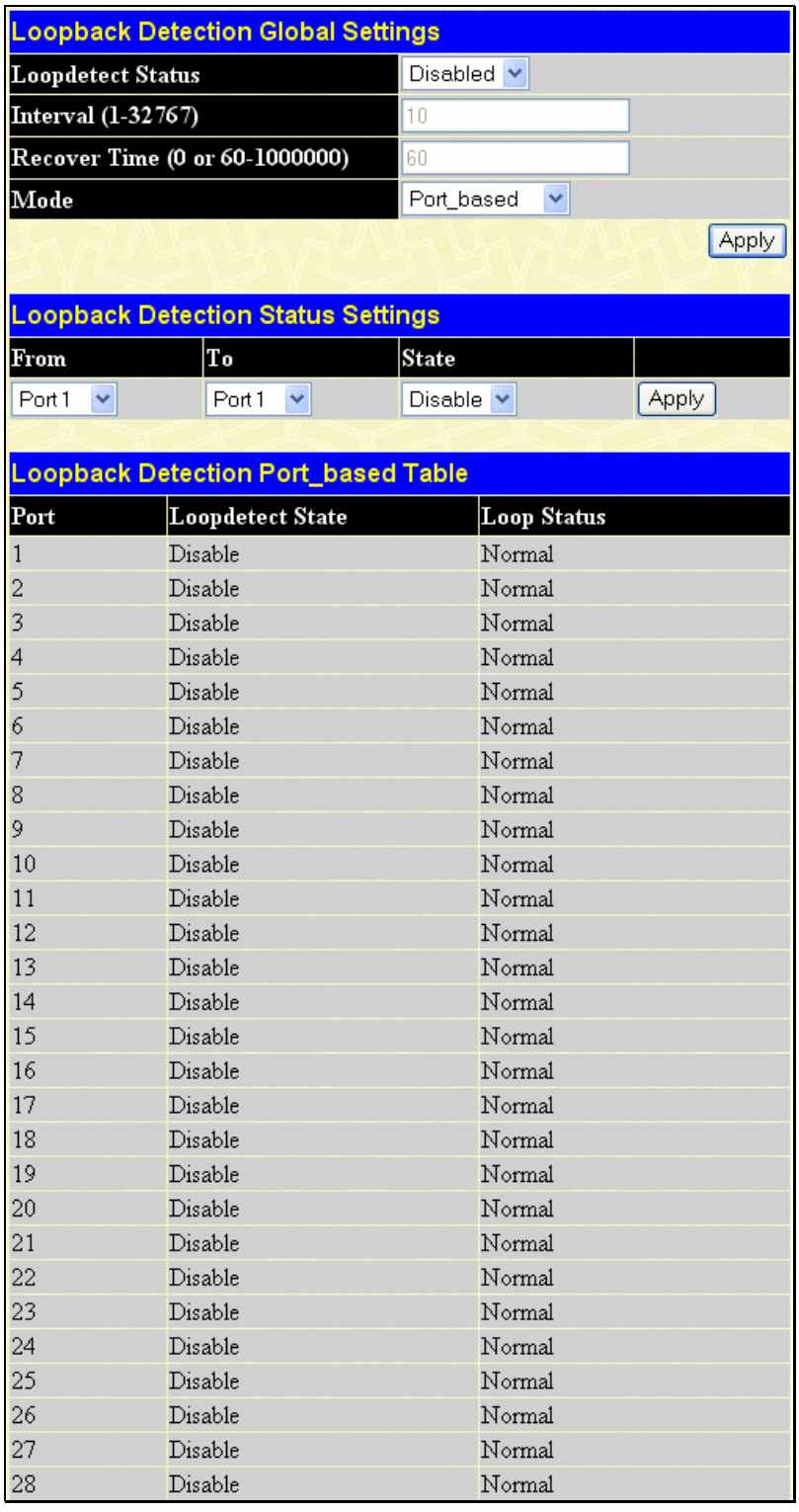


Figure 7- 48. Loopback Detection Global Settings

Parameter	Description
Loopdetect Status	Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*
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.
Mode	Use the drop-down menu to toggle between *Port_ Based* and *VLAN_ Based*.
From	Use the drop-down menu to select a beginning port number.
To	Use the drop-down menu to select an ending port number.
State	Use the drop-down menu to toggle between *Enable* and *Disable.*

Protocol VLAN

The DES -3800 Switch Series incorporates the idea of protocol-based VLANs. This standard, defined by the IEEE 802.1v standard maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. After assessing the protocol, the Switch will forward the packets to all ports within the protocol-assigned VLAN. This feature will benefit the administrator by better balancing load sharing and enhancing traffic classification. The Switch supports fourteen (14) pre-defined protocols for configuration. The user may also choose a protocol that is not one of the fourteen defined protocols by properly configuring the *userDefined* protocol VLAN. The supported protocols for the protocol VLAN function on this switch include IP, IPX, DEC LAT, SNAP, NetBIOS, AppleTalk, XNS, SNA, IPv6, RARP and VINES.

The following is a list of type headers for each protocol listed for VLAN configuration.

Protocol	Type Header in Hexadecimal Form
IP over Ethernet	0x0800
IPX 802.3	0xFFFF
IPX 802.2	0xE0E0
IPX SNAP	0x8137
IPX over Ethernet2	0x8137
DEC LAT	0x6004
SNA 802.2	0x0404
netBios	0xF0F0
XNS	0x0600
VINES	0x0BAD
IPv6	0x86DD
AppleTalk	0x809B
RARP	0x8035
SNA over Ethernet2	0x80D5

Figure 7- 49. Protocol VLAN and the corresponding type header

In configuring the user-defined protocol, the administrator must make sure that the pre-defined user type header does not match any other type header. A match may cause discrepancies within the local network and failure to define the VLAN to which to forward packets.

The following table describes how to setup **Protocol Vlan Group Settings** on the Switch. Click **L2 Features > Protocol Vlan > Protocol VLAN Group Settings** to view the screen below:

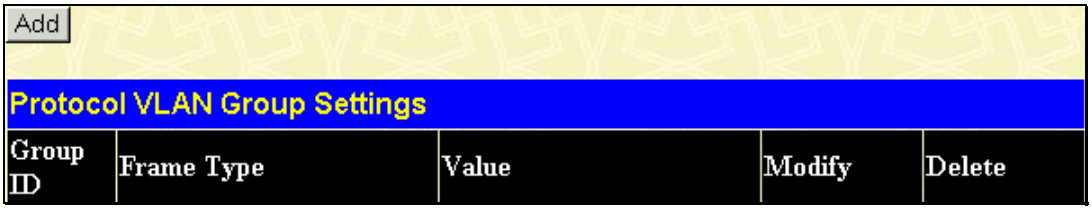


Figure 7- 50. Protocol VLAN Group Settings window

Click the **Add** button to open the **Protocol VLAN Group - ADD** window, as shown below:

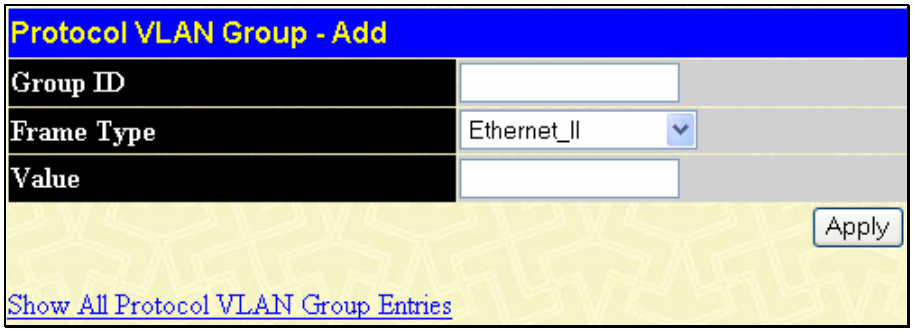


Figure 7- 51. Protocol VLAN Group - Add window

Parameter	Description
Group ID	Select an ID number for the group, between *1* and *2147483647.*
Frame Type	This 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*.
Value	Enter a value for the Group.

To edit an entry, click on its corresponding **Modify** button, which will reveal the following window. Click the corresponding ✕ button under the Delete heading to delete an entry.

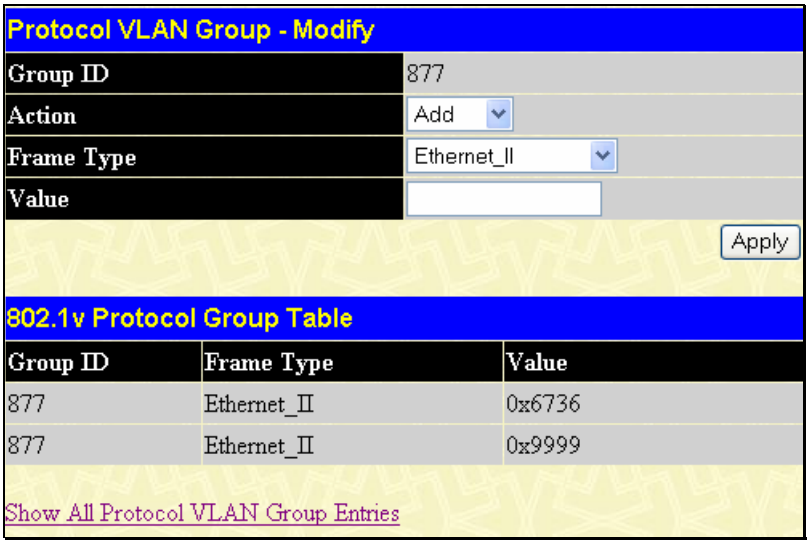


Figure 7- 52. Protocol VLAN Group - Modify window

To view the parameters for a previously set Group, click on its hyperlinked **Show All Protocol VLAN Group Entries**, which will return you to this window.

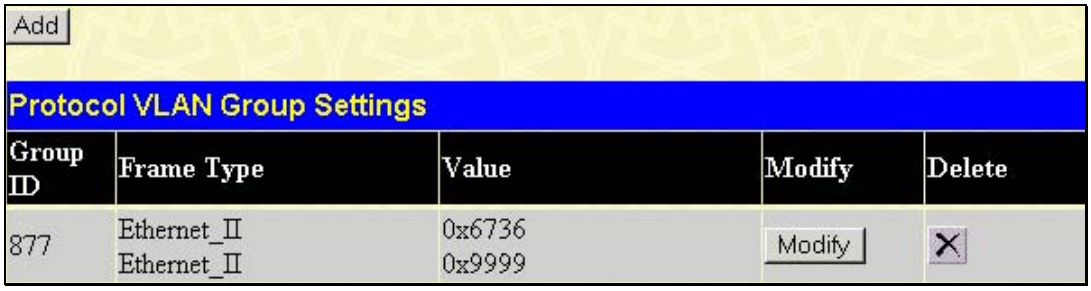


Figure 7- 53. Protocol VLAN Group Settings - window

The following table displays the **Protocol VLAN Port Settings** on the Switch. Click **L2 Features** > **Protocol Vlan** > **Protocol VLAN Port Settings** to view the screen below:

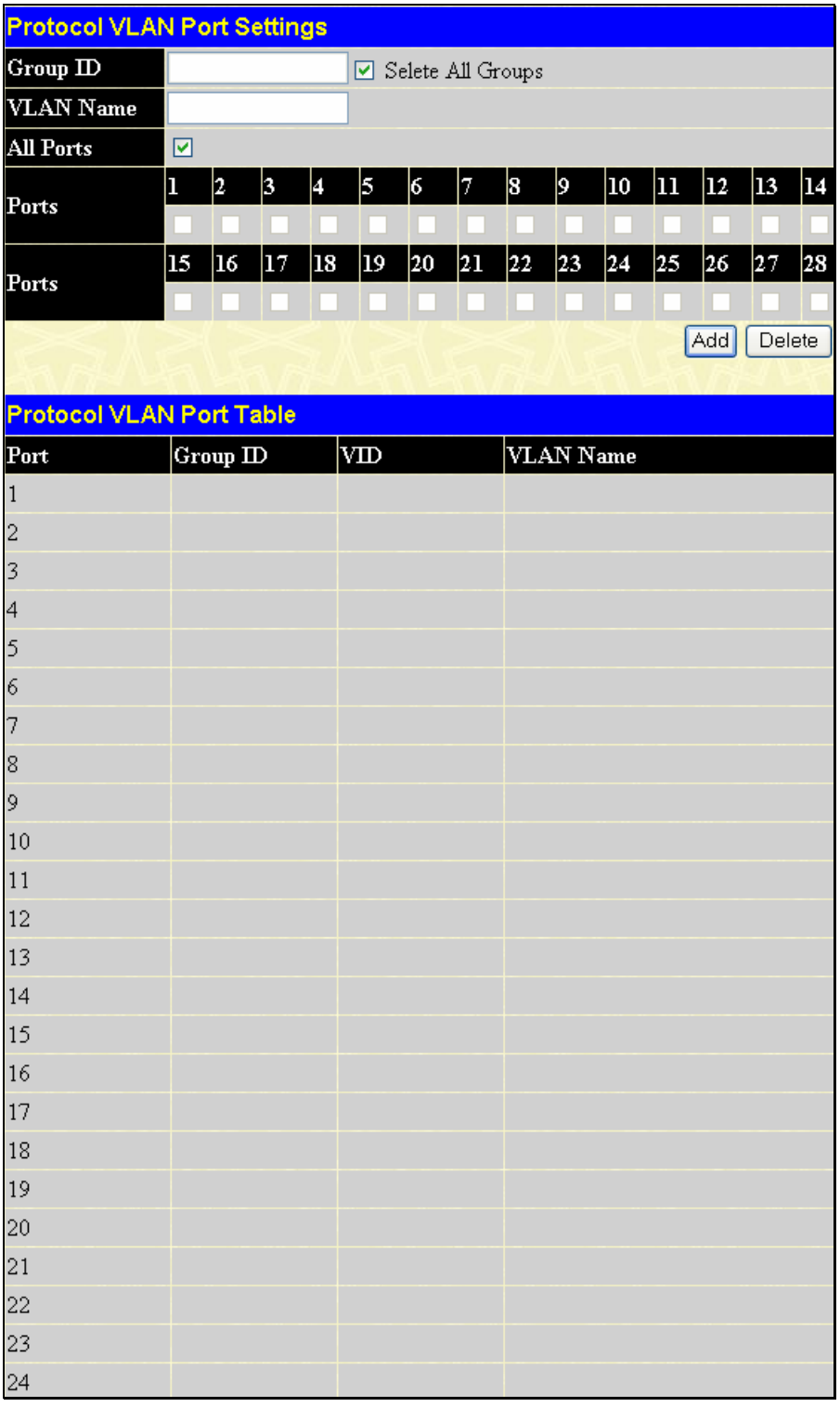


Figure 7- 54. Protocol VLAN Port Settings window

Parameter	Description
Group ID	Allows the entry of a VLAN ID or displays the VLAN ID. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN or editing an existing entry.
All Ports	To select all ports by tick the All Ports checkbox. Untick the checkbox to select individual port to be specified as member of a VLAN.

Click **Add** to implement changes made or **Delete** to remove an entry.

Section 8

Layer 3 Features

IP Interface Settings

Loopback IP Interface Settings

MD5 Key Settings

Route Redistribution Settings

Static/Default Route Settings

Route Preference Settings

Static ARP Settings

RIP

OSPF

DHCP Server

DHCP/BOOTP Relay

DNS Relay

VRRP

IP Multicast Routing Protocol

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for IP Interface Settings, MD5 Key Settings, Route Redistribution Settings, Static/Default Route Settings, Route Preference Settings, Static ARP Settings, RIP, OSPF, DCHP/BOOTP Relay, DNS Relay, VRRP and IP Multicast Routing Protocol all discussed in detail in the following section.

IP Multinetting

IP Multinetting is a function that allows multiple IP interfaces to be assigned to the same VLAN. This is beneficial to the administrator when the number of IPs on the original interface is insufficient and the network administrator wishes not to resize the interface. IP Multinetting is capable of assigning another IP interface on the same VLAN without affecting the original stations or settings of the original interface.

Two types of interfaces are configured for IP multinetting, *primary* and *secondary*, and every IP interface must be classified as one of these. A *primary* interface refers to the first interface created on a VLAN, with no exceptions. All other interfaces created will be regarded as *secondary* only, and can only be created once a *primary* interface has been configured. There may be five interfaces per VLAN (one primary, and up to four secondary) and they are, in most cases, independent of each other. *Primary* interfaces cannot be deleted if the VLAN contains a *secondary* interface. Once the user creates multiple interfaces for a specified VLAN (*primary* and *secondary*), that set IP interface cannot be changed to another VLAN.

Application Limitation: A multicast router cannot be connected to IP interfaces that are utilizing the IP Multinetting function.

NOTE: Only the primary IP interface will support the BOOTP relay agent.

IP Multinetting is a valuable tool for network administrators requiring a multitude of IP addresses, but configuring the Switch for IP multinetting may cause troubleshooting and bandwidth problems, and should not be used as a long term solution. Problems may include:

- The Switch may use extra resources to process packets for multiple IP interfaces.
- The amount of broadcast data, such as RIP update packets and PIM hello packets, will be increased.

IP Interface Settings

Each VLAN must be configured prior to setting up the VLAN's corresponding IP interface.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineer	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 8- 1. VLAN Example - Assigned Ports

In this case, six IP interfaces are required, so a CIDR notation of 10.32.0.0/11 (or a 11-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

Using a 10.xxx.xxx.xxx IP address notation, the above example would give 6 network addresses and 6 subnets. Any IP address from the allowed range of IP addresses for each subnet can be chosen as an IP address for an IP interface on the switch. For this example, we have chosen the next IP address above the network address for the IP interface's IP Address:

VLAN Name	VID	Network Number	IP Address
System (default)	1	10.32.0.0	10.32.0.1
Engineer	2	10.64.0.0	10.64.0.1
Marketing	3	10.96.0.0	10.96.0.1
Finance	4	10.128.0.0	10.128.0.1
Sales	5	10.160.0.0	10.160.0.1
Backbone	6	10.192.0.0	10.192.0.1

Table 8- 2. VLAN Example - Assigned IP Interfaces

The six IP interfaces, each with an IP address (listed in the table above), and a subnet mask of 255.224.0.0 can be entered into the **IP Interface Settings** window.

Proxy ARP

The Proxy ARP (Address Resolution Protocol) feature of the Switch will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP requester. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway.

The host, usually a layer 3 switch, will respond to packets destined for another device. For example, if hosts A and B are on different physical networks, B will not receive ARP broadcast requests from A and therefore cannot respond. Yet, if the physical network of A is connected by a router or layer 3 switch to B, the router or Layer 3 switch will see the ARP request from A.

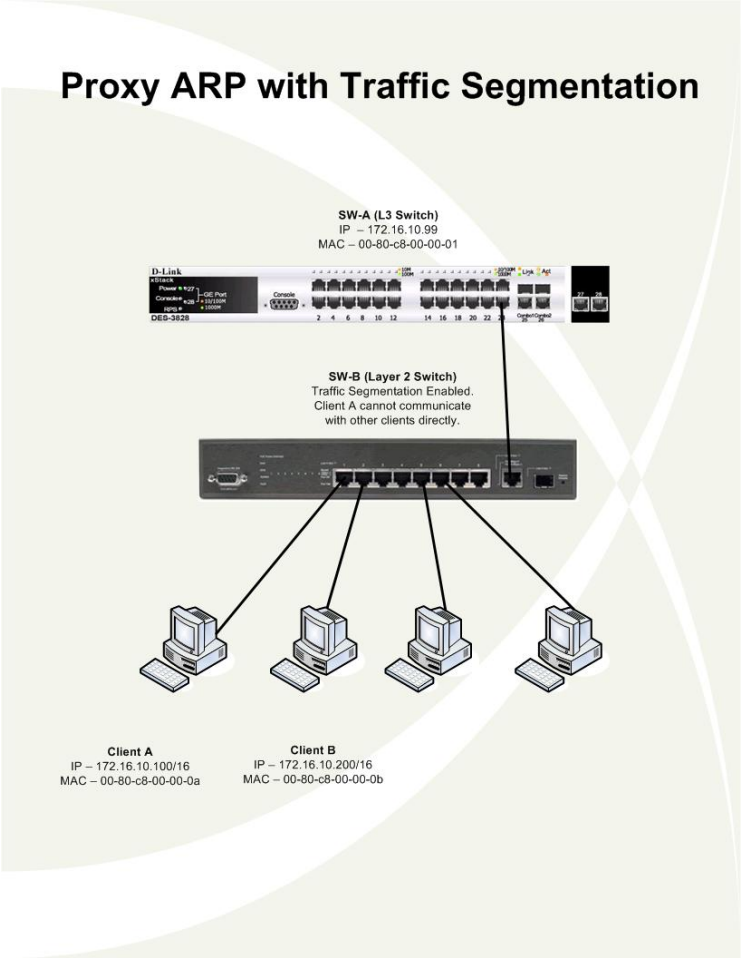


Figure 8- 1. Proxy ARP with Traffic Segmentation

To setup IP Interfaces on the Switch:

To view the IP Interface Settings on the Switch, click **L3 Features > IP Interfaces Settings**:

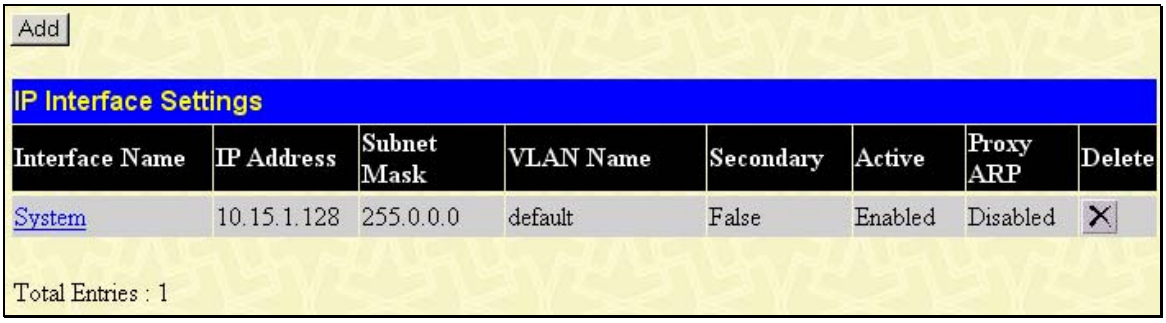


Figure 8- 2. IP Interface Settings window

To setup a new IP interface, click the **Add** button. To edit an existing IP Interface entry, click on an entry under the **Interface Name** heading. Both actions will result in the same screen to configure, as shown below.

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

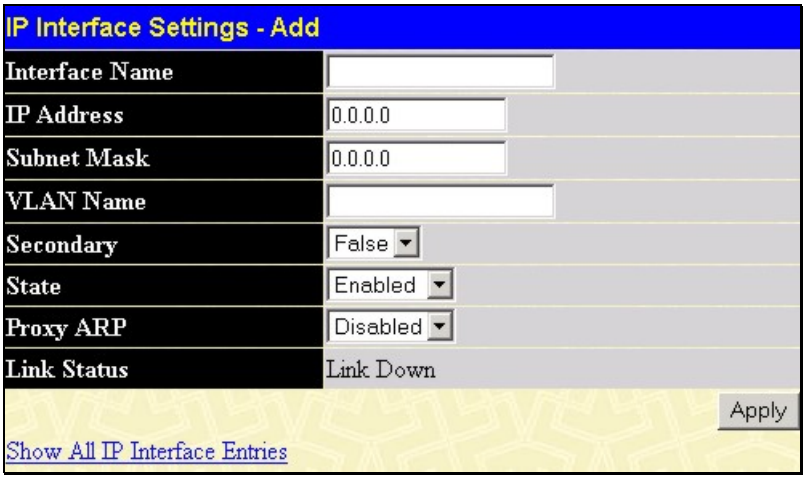


Figure 8- 3. IP Interface Settings – Add

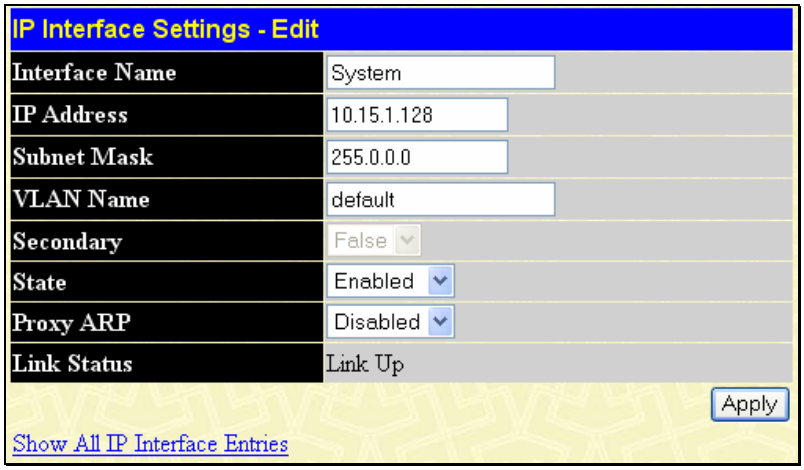


Figure 8- 4. IP Interface Settings - Edit

Enter a name for the new interface to be added in the **Interface Name** field (if you are editing an IP interface, the **Interface Name** will already be in the top field as seen in the window above). Enter the interface's IP address and subnet mask in the corresponding fields. Pull the **State** pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. To view entries in the **IP Interface Table**, click the Show All IP Interface Entries hyperlink. Use the **Save Changes** dialog box to enter the changes into NV-RAM.

The following fields can be set:

Parameter	Description
Interface Name	This field displays the name for the IP interface. The default IP interface is named "System".
IP Address	This field allows the entry of an IP address to be assigned to this IP interface.
Subnet Mask	This field allows the entry of a subnet mask to be applied to this IP interface.
VLAN Name	This field allows the entry of the VLAN Name for the VLAN the IP interface belongs to.
Secondary	Use the pull-down menu to set the IP interface as *True* or *False*. *True* will set the interface as secondary and *False* will denote the interface as the primary interface of the VLAN entered above. *Secondary* interfaces can only be configured if a *primary* interface is first configured.
State	This field may be altered between *Enabled* and *Disabled* using the pull down menu. This entry determines whether the interface will be active or not.
Proxy ARP	Use the pull-down menu to enable or disable the Proxy ARP feature on this interface.
Link Status	This read only field states the current status of the IP Interface on the Switch. *Link Up* denotes that the IP interface is up and running on the Switch. *Link Down* will denote that the IP interface is not currently set and/or enabled on the Switch.

Click **Apply** to implement changes made.

Loopback IP Interface

Loopback IP interfaces are network interfaces that are not associated with a physical interface. Physical interfaces have some form of physical element, for example VLAN, physical ports or even interface MAC address. Unlike a physical interface, the loopback interface exists only in software; there are no physical elements. In DES3800, you identify an individual loopback interface using the interface name and IP address which is an independent subnet.

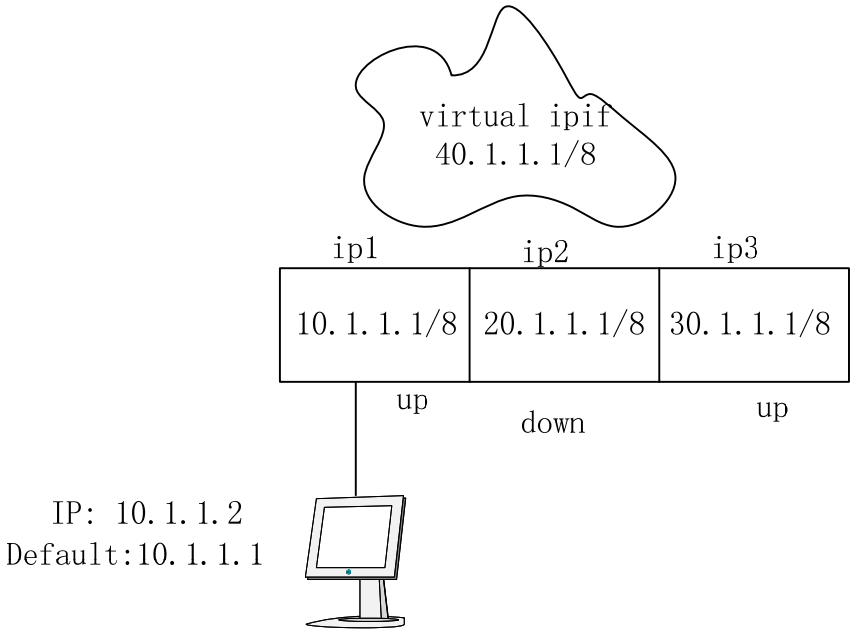
The benefits of loopback interfaces provide:

1. A stable interface on which you can assign a layer-3 address such as an IP address. The address should be a host address instead of network address.
2. A stable source interface to ensure that the IP address assigned to the interface is always reachable as long as the IP routing protocol on the physical interfaces continue to advertise this subnet or host IP assigned to the loopback interface.
3. The loopback interface can be considered stable because once you enable it, it will remain enabled until you shut it down (disable it).
4. It can also be used to establish a Telnet session or Web session.

The loopback interface doesn't participate in routing or application relay. The path to the loopback interface is via a routing mechanism. Otherwise, there is no path to the loopback interface. The following defines more clearly the behavior of the loopback interface:

1. There is no routing protocol running on the loopback interface.
2. It doesn't have both MAC addresses and ARP because of loopback IP interface. When it needs a source MAC address, it takes the outbound physical interface MAC address.
3. It is never link down even if none of the ports are link up.
4. The route to the loopback interface needs to be advertised by routing protocols running on other interfaces or it is only reachable by the static route.
5. For the loopback interface, there is no physical connection through the loopback interface. And, because the loopback interface is software-only, it has no corresponding VLAN.
6. Users can use the loopback interface as the termination address for open shortest path first (OSPF) sessions. In applications where other routers or access servers attempt to reach this loopback interface, users should configure a routing protocol to distribute the subnet assigned to the loopback address.
7. OSPF uses the highest IP address configured on the interfaces as its router ID. If this interface is down or removed, the OSPF process must recalculate a new router ID and resend all its routing information out over its interfaces. If a loopback interface is configured with an IP address, OSPF uses this IP address as its router ID, even if other interfaces have higher IP addresses. Because loopback interfaces never fail, this provides greater stability. OSPF automatically prefers a loopback interface over other interfaces, and it chooses the highest IP address among all loopback interfaces.

In the following example, **ip1** and **ip3** are up, and **ip2** is down. A user (10.1.1.2) wants to access the device through a telnet session. "telnet 20.1.1.1" will fail because **ip2** is down, however, "telnet 40.1.1.1" will succeed, because this **loopback interface** is always up. But if another user (20.1.1.2) wants to access the loopback ipif (40.1.1.1), it will fail because **ip2** is down. This rule is applied to other access methods, for example, **ping**.



To setup Loopback IP Interfaces on the switch, click **Layer 3 Features > Loopback IP Interface Settings** to open the following window:

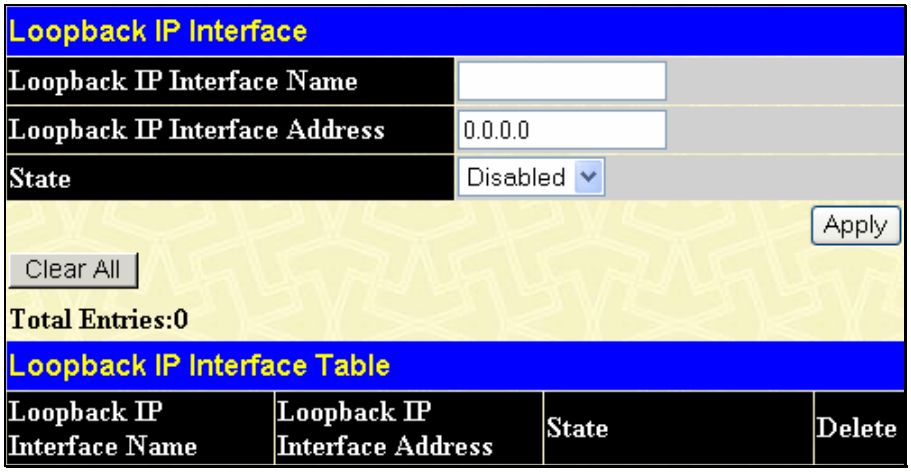


Figure 8- 5. Loopback Detection Global Settings

Parameter	Description
Loopback IP Interface Name	The name for the Loopback IP Interface.
Loopback IP Interface Address	The IP Address of the new Loopback IP Interface.
State	Use the drop-down menu to enable or disable the Loopback IP Interface state.

MD5 Key Settings

The **MD5 Key Settings** menu allows the entry of a 16-character Message Digest – version 5 (MD5) key which can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain. MD5 Keys created here can be used in the **OSPF** menu below.

To configure an **MD5 Key**, click **Layer 3 Features > MD5 Key Settings** to open the following window:

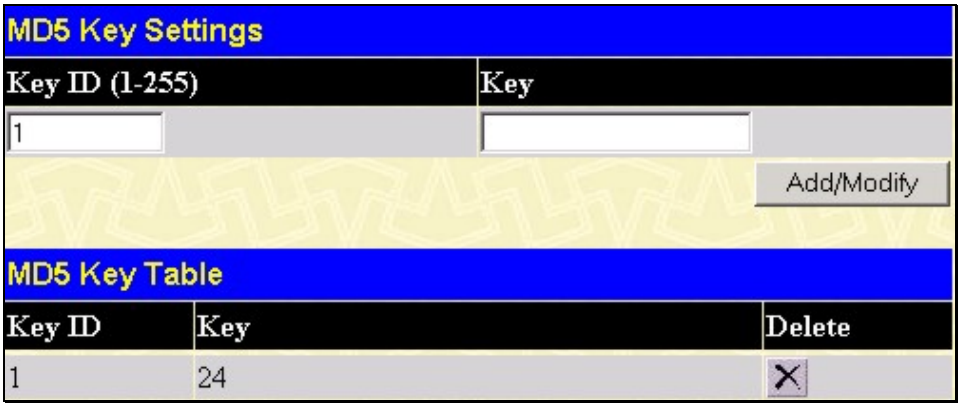


Figure 8- 6. MD5 Key Settings and Table window

The following fields can be set:

Parameter	Description
Key ID (1-255)	A number from 1 to 255 used to identify the MD5 Key.
Key	An alphanumeric string of between 1 and 16 case-sensitive characters used to generate the Message Digest which is in turn, used to authenticate OSPF packets within the OSPF routing domain.

Route Redistribution Settings

Route redistribution allows routers on the network, which are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various routers' routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual router's current routing protocol. The Switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the **Static Routing Table** on the local switch is also redistributed.

The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed to RIP and OSPF protocol respectively.

Route Destination: RIP

Route Source	Metric	Type
OSPF	0 to 16	All Internal External ExtType1 ExtType2 Inter-E1 Inter-E2
Static	0 to 16	not applicable
Local	0 to 16	not applicable

Route Destination: OSPF

Route Source	Metric	Metric Type
RIP	0 to 16777214	Type-1 Type-2
Static	0 to 16777214	Type-1 Type-2
Local	0 to 16777214	Type-1 Type-2

Table 8- 3. Route Redistribution Source tables

This window will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. To access the **Route Redistribution Settings** window, go to **> L3 Features > Route Redistribution Settings**:

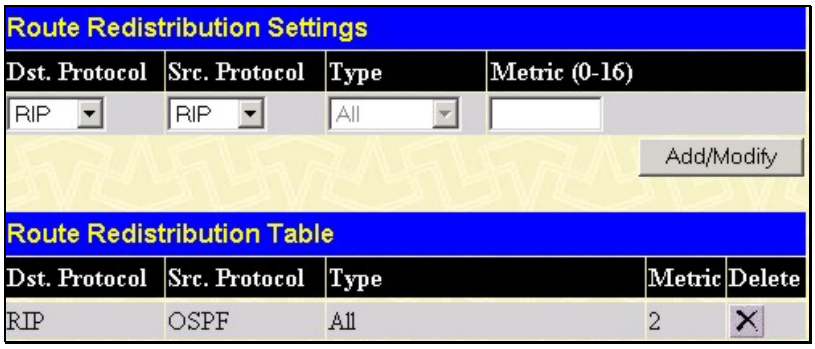


Figure 8- 7. Route Redistribution Settings and Table window

The following parameters may be set or viewed:

Parameter	Description
Dst. Protocol	Allows for the selection of the protocol for the destination device. Choose between *RIP* and *OSPF.*
Src. Protocol	Allows for the selection of the protocol for the source device. Choose between *RIP*, *OSPF, Static* and *Local*.
Type	Allows for the selection of one of six methods of calculating the metric value. The user may choose between *All*, *Internal*, *External*, *ExtType1*, *ExtType2*, *Inter-E1*, *Inter* 頁 : 126 , *Type-1, Type-2* *All* means all OSPF routing information which includes *Internal* and *External* will be redistributed to RIP. *Internal* means OSPF AS internal routing information will be redistributed to RIP. *External* means OSPF AS external routing information which includes *ExtType1* and *ExtType2* will be redistributed to RIP. *ExtType1* means OSPF AS external routing information of Type 1 external metrics will be redistributed to RIP. *ExtType2* means OSPF AS external routing information of Type 2 external metrics will be redistributed to RIP. *Inter-E1* means OSPF routing information which includes *Internal* and *ExtType1* will be redistributed to RIP. *Inter-E2* means OSPF routing information which includes *Internal* and *ExtType2* will be redistributed to RIP. *Type-1* means routing information will be redistributed to OSPF as AS external Type 1 routing. *Type-2* means routing information of RIP, Static and Local will be redistributed to OSPF as AS external Type 2 routing. See 頁 : 126 Table 8-3 above for available metric and type value for each source protocol.
Metric	頁 : 126 Allows the entry of an OSPF or RIP interface cost. For RIP as destination protocol this is analogous to a Hop Count in the RIP routing protocol. The user may specify a cost between 0 and 16. For OSPF as destination protocol : this is OSPF interface cost in AS external Type 1 routing and is the major cost between AS'es in AS external Type 2 routing. The user may specify a cost between 0 and 16777214.

Click **Add/Modify** to implement changes made.

NOTE: The source protocol (**Src. Protocol**) entry and the destination protocol (**Dst. Protocol**) entry cannot be the same.

Static/Default Route Settings

Entries into the Switch's forwarding table can be made using both MAC addresses and IP addresses. Static IP forwarding is accomplished by the entry of an IP address into the Switch's **Static IP Routing Table**. To view the following window, click **L3 Features > Static/Default Route Settings**.

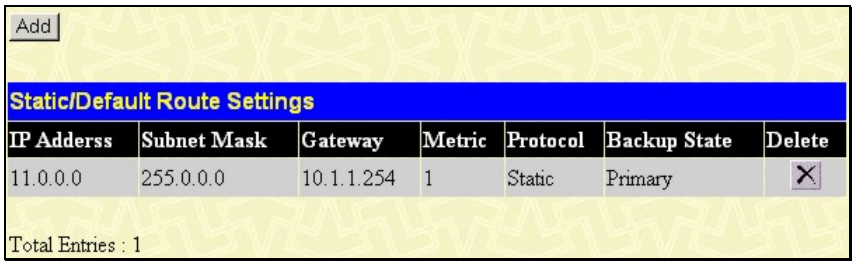


Figure 8- 8. Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IP Address	The IP address of the Static/Default Route.
Subnet Mask	The corresponding Subnet Mask of the IP address entered into the table.
Gateway	The corresponding Gateway of the IP address entered into the table.
Metric	Represents the metric value of the IP interface entered into the table. This field may read a number between 1-65535 for an OSPF setting, and 1-16 for a RIP setting.
Protocol	Represents the protocol used for the Routing Table entry of the IP interface. This field may read OSPF, RIP, Static or Local.
Backup State	Represents the Backup state that this IP interface is configured for. This field may read Primary or Backup.
Delete	Click the ✕ to delete this entry from the Static/Default Route Settings table.

To enter an IP Interface into the Switch's **Static/Default Route Settings** window, click the **Add** button, revealing the following window to configure.

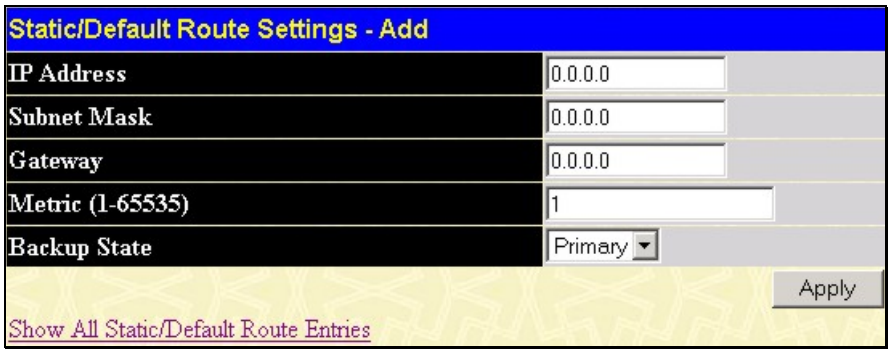


Figure 8- 9. Static/Default Route Settings – Add window

The following fields can be set:

Parameter	Description
IP Address	Allows the entry of an IP address that will be a static entry into the Switch's Routing Table.
Subnet Mask	Allows the entry of a subnet mask corresponding to the IP address above.
Gateway IP	Allows the entry of an IP address of a gateway for the IP address above.
Metric (1-65535)	Allows the entry of a routing protocol metric representing the number of routers between the Switch and the IP address above.
Backup State	The user may choose between *Primary* and *Backup.* If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.

Click **Apply** to implement changes made.

Route Preference Settings

Route Preference is a way for routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. The majority of routing protocols are not compatible when used in conjunction with each other. This Switch supports and may be configured for many routing protocols, as a stand-alone switch or more importantly, in utilizing the stacking function and Single IP Management of the Switch. Therefore, the ability to exchange route information and select the best path is essential to optimal use of the Switch and its capabilities.

The first decision the Switch will make in selecting the best path is to consult the Route Preference Settings table of the switch. This table can be viewed by clicking **Configuration** > **L3 IP Networking** > **Route Preference Settings**, and it holds the list of possible routing protocols currently implemented on the Switch, along with a **Preference** value which determines which routing protocol will be the most dependable to route packets. Below is a list of the default route preferences set on the Switch.

Route Type	Validity Range	Default Value
Local	0 - Permanently set on the Switch and not configurable.	0
Static	1 - 999	60
OSPF Intra	1 - 999	80
OSPF Inter	1 - 999	90
RIP	1 - 999	100
OSPF ExtT1	1 - 999	110
OSPF ExtT2	1 - 999	115

As shown above, *Local* will always be the first choice for routing purposes and the next most reliable path is *Static* due to the fact that its has the next lowest value. To set a higher reliability for a route, change its value to a number less than the value of a route preference that has a greater reliability value using the **New Route Preference Settings** window command. For example, if the user wishes to make RIP the most reliable route, the user can change its value to one that is less than the lowest value (Static - 60) or the user could change the other route values to more than 100.

The user should be aware of three points before configuring the route preference:

1. No two route preference values can be the same. Entering the same route preference may cause the Switch to crash due to indecision by the Switch.

2. If the user is not fully aware of all the features and functions of the routing protocols on the Switch, a change in the default route preference value may cause routing loops or black holes.

3. After changing the route preference value for a specific routing protocol, that protocol needs to be restarted because the previously learned routes have been dropped from the switch. The Switch must learn the routes again before the new settings can take affect.

To view the **Route Preference Settings** window, click **L3 Features > Route Preference Settings:**

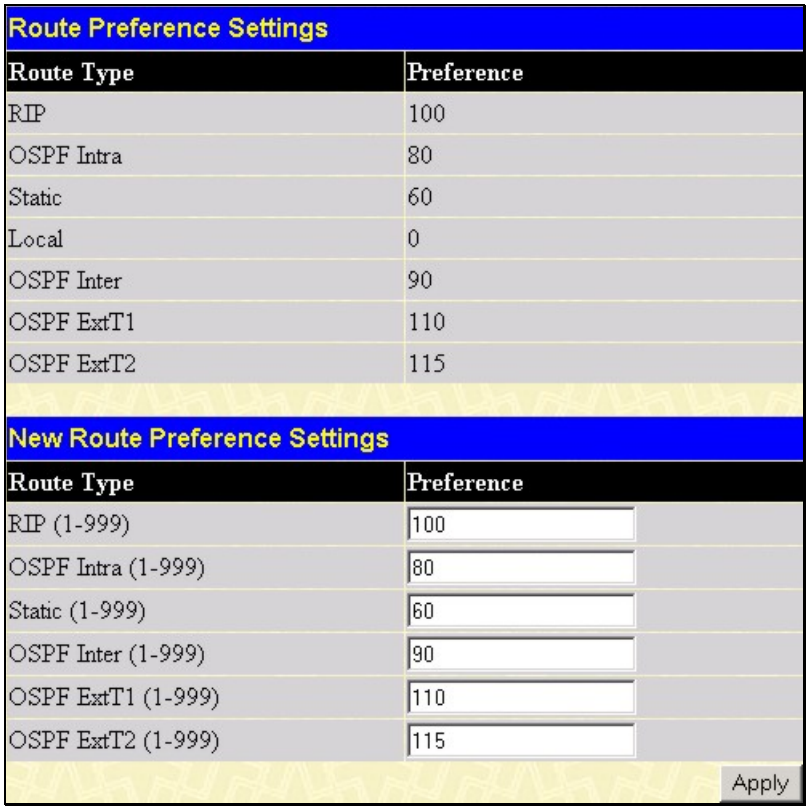


Figure 8- 10. Route Preference Settings window

The following fields can be viewed or set:

Parameter	Description
RIP (1-999)	Enter a value between 1 and 999 to set the route preference for *RIP*. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 100.
OSPF Intra (1-999)	Enter a value between 1 and 999 to set the route preference for *OSPF Intra*. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 80.
STATIC (1-999)	Enter a value between 1 and 999 to set the route preference for *Static*. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 60.
OSPF Inter (1-999)	Enter a value between 1 and 999 to set the route preference for *OSPF Inter*. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 90.
OSPF ExtT1 (1-999)	Enter a value between 1 and 999 to set the route preference for *OSPF ExtT1*. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 110.
OSPF ExtT2 (1-999)	Enter a value between 1 and 999 to set the route preference for *OSPF ExtT2*. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 115.

Click **Apply** to implement changes made.

Static ARP Table

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 open the **Static ARP Table** click, **L3 Features** > **Static ARP Settings**.

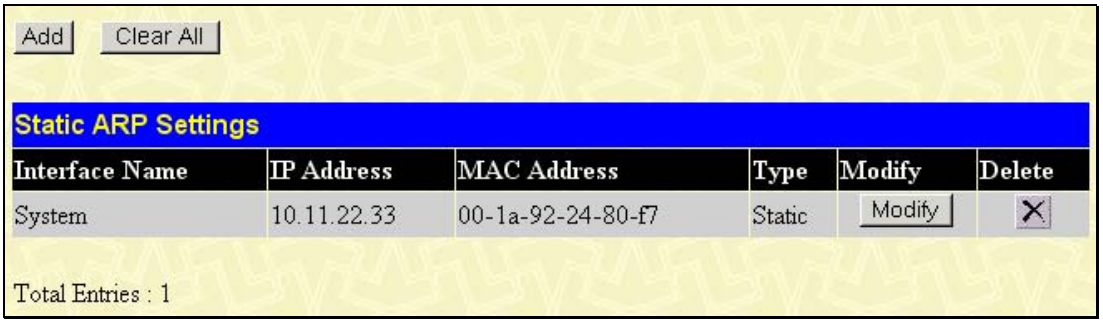


Figure 8- 11. Static ARP Settings window

To add a new entry, click the **Add** button, revealing the following window to configure:

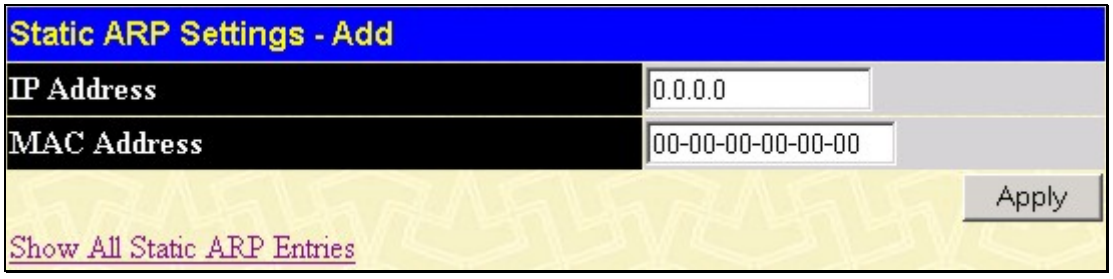


Figure 8- 12. Static ARP Table – Add window

The following fields can be set:

Parameter	Description
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 **Clear All** button.

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

RIP

The Routing Information Protocol is a distance-vector routing protocol. There are two types of network devices running RIP - active and passive. Active devices advertise their routes to others through RIP messages, while passive devices listen to these messages. Both active and passive routers update their routing tables based upon RIP messages that active routers exchange. Only routers can run RIP in the active mode.

Every 30 seconds, a router running RIP broadcasts a routing update containing a set of pairs of network addresses and a distance (represented by the number of hops or routers between the advertising router and the remote network). So, the vector is the network address and the distance is measured by the number of routers between the local router and the remote network.

RIP measures distance by an integer count of the number of hops from one network to another. A router is one hop from a directly connected network, two hops from a network that can be reached through a router, etc. The more routers between a source and a destination, the greater the RIP distance (or hop count).

There are a few rules to the routing table update process that help to improve performance and stability. A router will not replace a route with a newly learned one if the new route has the same hop count (sometimes referred to as 'cost'). So learned routes are retained until a new route with a lower hop count is learned.

When learned routes are entered into the routing table, a timer is started. This timer is restarted every time this route is advertised. If the route is not advertised for a period of time (usually 180 seconds), the route is removed from the routing table.

RIP does not have an explicit method to detect routing loops. Many RIP implementations include an authorization mechanism (a password) to prevent a router from learning erroneous routes from unauthorized routers.

To maximize stability, the hop count RIP uses to measure distance must have a low maximum value. Infinity (that is, the network is unreachable) is defined as 16 hops. In other words, if a network is more than 16 routers from the source, the local router will consider the network unreachable.

RIP can also be slow to converge (to remove inconsistent, unreachable or looped routes from the routing table) because RIP messages propagate relatively slowly through a network.

Slow convergence can be solved by using split horizon update, where a router does not propagate information about a route back to the interface on which it was received. This reduces the probability of forming transient routing loops.

Hold down can be used to force a router to ignore new route updates for a period of time (usually 60 seconds) after a new route update has been received. This allows all routers on the network to receive the message.

A router can 'poison reverse' a route by adding an infinite (16) hop count to a route's advertisement. This is usually used in conjunction with triggered updates, which force a router to send an immediate broadcast when an update of an unreachable network is received.

RIP Version 1 Message Format

There are two types of RIP messages: routing information messages and information requests. Both types use the same format.

The Command field specifies an operation according the following table:

Command	Meaning
1	Request for partial or full routing information
2	Response containing network-distance pairs from sender's routing table
3	Turn on trace mode (obsolete)
4	Turn off trace mode (obsolete)
5	Reserved for Sun Microsystem's internal use
9	Update Request
10	Update Response
11	Update Acknowledgement

RIP Command Codes

The field VERSION contains the protocol version number (1 in this case), and is used by the receiver to verify which version of RIP the packet was sent.

RIP 1 Message

RIP is not limited to TCP/IP. Its address format can support up to 14 octets (when using IP, the remaining 10 octets must be zeros). Other network protocol suites can be specified in the Family of Source Network field (IP has a value of 2). This will determine how the address field is interpreted.

RIP specifies that the IP address, 0.0.0.0, denotes a default route.

The distances, measured in router hops are entered in the Distance to Source Network, and Distance to Destination Network fields.

RIP 1 Route Interpretation

RIP was designed to be used with classed address schemes, and does not include an explicit subnet mask. An extension to version 1 does allow routers to exchange subnetted addresses, but only if the subnet mask used by the network is the same as the subnet mask used by the address. This means the RIP version 1 cannot be used to propagate classless addresses.

Routers running RIP version 1 must send different update messages for each IP interface to which it is connected. Interfaces that use the same subnet mask as the router's network can contain subnetted routes, other interfaces cannot. The router will then advertise only a single route to the network.

RIP Version 2 Extensions

RIP version 2 includes an explicit subnet mask entry, so RIP version 2 can be used to propagate variable length subnet addresses or CIDR classless addresses. RIP version 2 also adds an explicit next hop entry, which speeds convergence and helps prevent the formation of routing loops.

RIP2 Message Format

The message format used with RIP2 is an extension of the RIP1 format:

RIP version 2 also adds a 16-bit route tag that is retained and sent with router updates. It can be used to identify the origin of the route.

Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

RIP Global Settings

To setup RIP for the IP interfaces configured on the Switch, the user must first globally enable RIP and then configure RIP settings for the individual IP interfaces. To globally enable RIP on the Switch, click **L3 Features** > **RIP** > **RIP Global Settings** which will reveal the following screen:

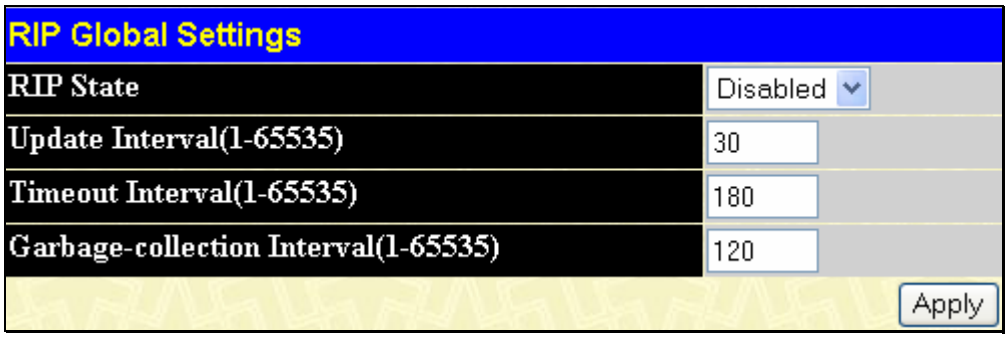


Figure 8- 13. RIP Global Settings window

The following fields can be set.

Parameter	Description
RIP State	To enable RIP Global Settings, simply use the pull-down menu, and select **Enabled.**
Update Interval (1-65535)	The update timer clocks the interval between periodic routing updates. Its default setting is 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors.

Timeout Interval (1-65535)	Each route entry has a timeout timer associated with it. When the timeout timer expires, the route is marked invalid but is retained until the garbage-collection timer expires. The interval of the timeout timer is set to a default of 180 seconds.
Garbage-collection Interval (1-65535)	When the timeout timer for a route entry expires, this route entry has a garbage-collection timer associated with it. When the garbage-collection timer expires, this route is deleted. The interval of the garbage-collection timer is set to a default of 120 seconds.

RIP Interface Settings

RIP settings are configured for each IP interface on the Switch. The menu appears in table form listing settings for IP interfaces currently on the Switch. To configure RIP settings for an individual interface, click on the hyperlinked **Interface Name**. To view this window, click **L3 Features** > **RIP** > **RIP Interface Settings**.

RIP Interface Settings

Interface Name	IP Address	TX Mode	RX Mode	Auth.	State
System	10.15.1.128	V2 Only	V1 and V2	Disabled	Disabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled

Figure 8- 14. RIP Interface Settings window

Click the hyperlinked name of the interface you want to set up for RIP, which will give access to the following menu:

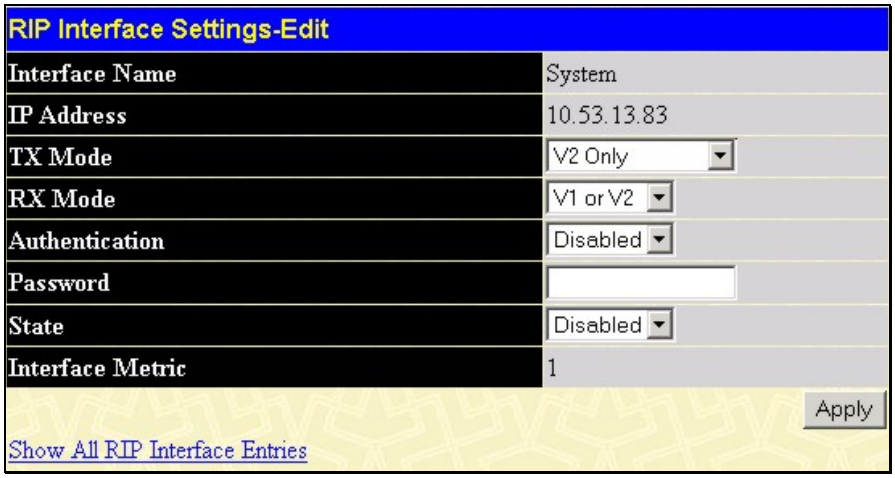


Figure 8- 15. RIP Interface Settings - Edit window

Refer to the table below for a description of the available parameters for RIP interface settings.

The following RIP settings can be applied to each IP interface:

Parameter	Description
Interface Name	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.
IP Address	The IP address corresponding to the Interface Name showing in the field above.
TX Mode	Toggle among *Disabled*, *V1 Only*, *V1 Compatible*, and *V2 Only*. This entry specifies which version of the RIP protocol will be used to transmit RIP packets. *Disabled* prevents the transmission of RIP packets.
RX Mode	Toggle among *Disabled*, *V1 Only*, *V2 Only*, and *V1 or V2*. This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. *Disabled* prevents the reception of RIP packets.
Authentication	Toggle between *Disabled* and *Enabled* to specify that routers on the network should us the Password above to authenticate router table exchanges.
Password	A password to be used to authenticate communication between routers on the network.
State	Toggle between *Disabled* and *Enabled* to disable or enable this RIP interface on the switch.
Interface Metric	A read only field that denotes the Metric value of the current IP Interface setting.

Click **Apply** to implement changes made.

OSPF

The Open Shortest Path First (OSPF) routing protocol uses a *link-state* algorithm to determine routes to network destinations. A "link" is an interface on a router and the "state" is a description of that interface and its relationship to neighboring routers. The state contains information such as the IP address, subnet mask, type of network the interface is attached to, other routers attached to the network, etc. The collection of link-states is then collected in a link-state database that is maintained by routers running OSPF.

OSPF specifies how routers will communicate to maintain their link-state database and defines several concepts about the topology of networks that use OSPF.

To limit the extent of link-state update traffic between routers, OSPF defines the concept of *Area.* All routers within an area share the exact same link-state database, and a change to this database on one router triggers an update to the link-state database of all other routers in that area. Routers that have interfaces connected to more than one area are called *Border Routers* and take the responsibility of distributing routing information between areas.

One area is defined as *Area 0* or the *Backbone.* This area is central to the rest of the network in that all other areas have a connection (through a router) to the backbone. Only routers have connections to the backbone and OSPF is structured such that routing information changes in other areas will be introduced into the backbone, and then propagated to the rest of the network.

When constructing a network to use OSPF, it is generally advisable to begin with the backbone (area 0) and work outward

Link-State Algorithm

An OSPF router uses a link-state algorithm to build a shortest path tree to all destinations known to the router. The following is a simplified description of the algorithm's steps:

- When OSPF is started, or when a change in the routing information changes, the router generates a link-state advertisement. This advertisement is a specially formatted packet that contains information about all the link-states on the router.
- This link-state advertisement is flooded to all router in the area. Each router that receives the link-state advertisement will store the advertisement and then forward a copy to other routers.
- When the link-state database of each router is updated, the individual routers will calculate a Shortest Path Tree to all destinations – with the individual router as the root. The IP routing table will then be made up of the destination address, associated cost, and the address of the next hop to reach each destination. Unlike RIP, OSPF protocol maintains multiple equal-cost routes to all destinations. DES-3800 series can support up to 8 equal-cost routes for the same destination network in hardware chip.
- Once the link-state databases are updated, Shortest Path Trees calculated, and the IP routing tables written – if there are no subsequent changes in the OSPF network (such as a network link going down) there is very little OSPF traffic.

Shortest Path Algorithm

The Shortest Path to a destination is calculated using the Dijkstra algorithm. Each router is places at the root of a tree and then calculates the shortest path to each destination based on the cumulative cost to reach that destination over multiple possible routes. Each router will then have its own Shortest Path Tree (from the perspective of its location in the network area) even though every router in the area will have and use the exact same link-state database.

The following sections describe the information used to build the Shortest Path Tree.

OSPF Cost

Each OSPF interface has an associated cost (also called "metric") that is representative of the overhead required to send packets over that interface. This cost is inversely proportional to the bandwidth of the interface (i.e. a higher bandwidth interface has a lower cost). There is then a higher cost (and longer time delays) in sending packets over a 56 Kbps dial-up connection than over a 10 Mbps Ethernet connection. The formula used to calculate the OSPF cost is as follows:

Cost = 100,000,000 / bandwidth in bps

As an example, the cost of a 10 Mbps Ethernet line will be 10 and the cost to cross a 1.544 Mbps T1 line will be 64.

Shortest Path Tree

To build Router A's shortest path tree for the network diagramed below, Router A is put at the root of the tree and the smallest cost link to each destination network is calculated.

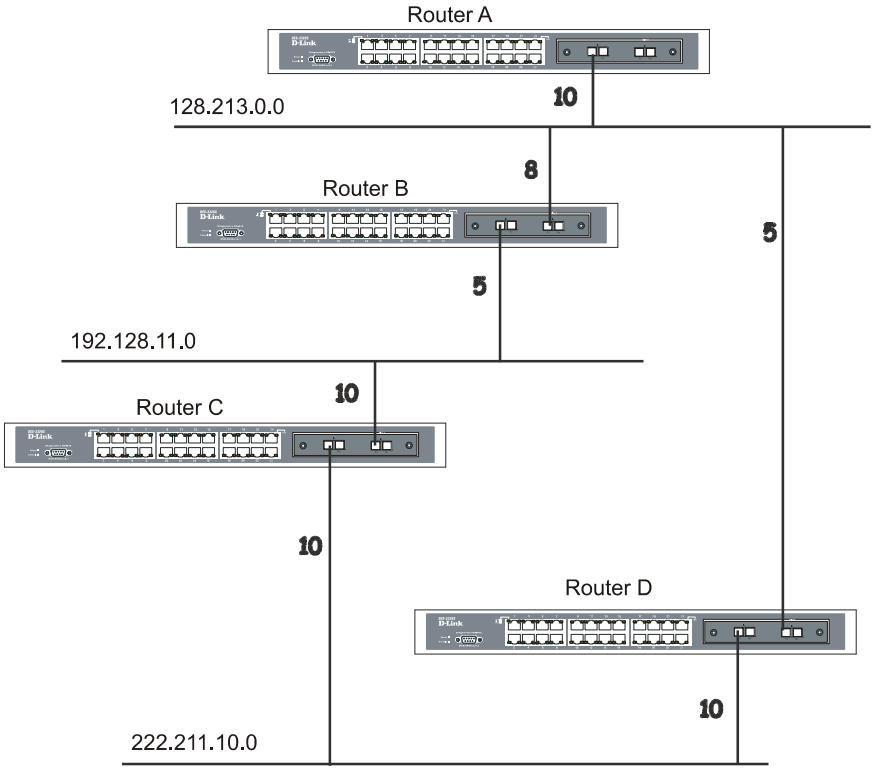


Figure 8- 16. Constructing a Shortest Path Tree

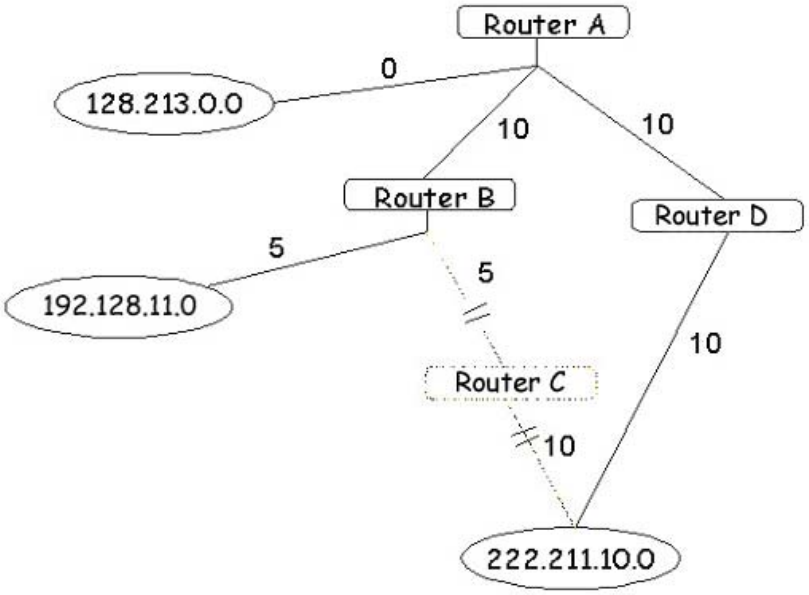


Figure 8- 17. Constructing a Shortest Path Tree

The diagram above shows the network from the viewpoint of Router A. Router A can reach 192.128.11.0 through Router B with a cost of 10 + 5 = 15. Router A can reach 222.211.10.0 through Router D with a cost of 10 + 10 = 20. Router A can also reach 222.211.10.0 through Router B and Router C with a cost of 10 + 5 + 10 = 25, but the cost is higher than the route through Router D. This higher-cost route will not be included in the Router A's shortest path tree. The resulting tree will look like this:

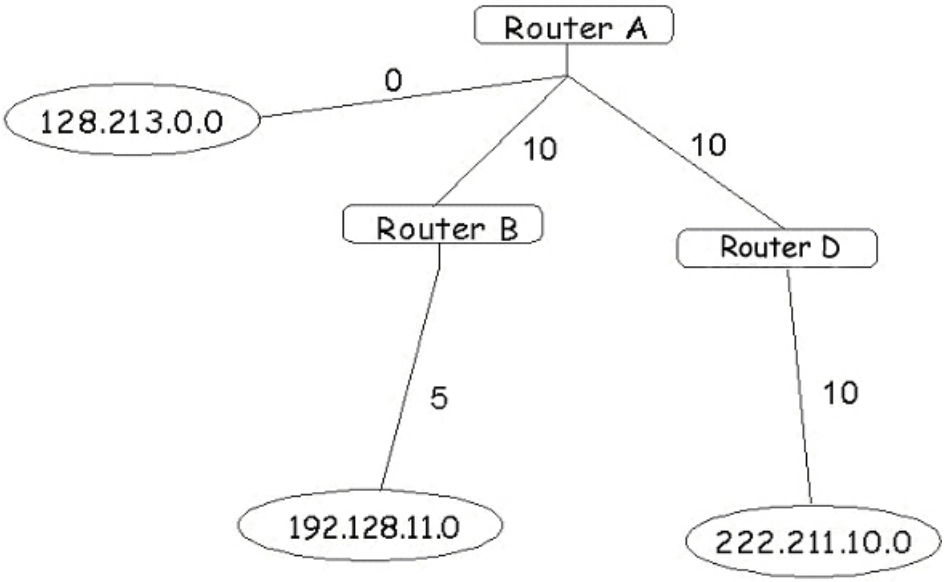


Figure 8- 18. Constructing a Shortest Path Tree - Completed

Note that this shortest path tree is only from the viewpoint of Router A. The cost of the link from Router B to Router A, for instance is not important to constructing Router A's shortest path tree, but is very important when Router B is constructing its shortest path tree.

Note also that directly connected networks are reached at a cost of zero, while other networks are reached at the cost calculated in the shortest path tree.

Router A can now build its routing table using the network addresses and costs calculated in building the above shortest path tree.

Areas and Border Routers

OSPF link-state updates are forwarded to other routers by flooding to all routers on the network. OSPF uses the concept of areas to define where on the network routers that need to receive particular link-state updates are located. This helps ensure that routing updates are not flooded throughout the entire network and to reduce the amount of bandwidth consumed by updating the various router's routing tables.

Areas establish boundaries beyond which link-state updates do not need to be flooded. So the exchange of link-state updates and the calculation of the shortest path tree are limited to the area that the router is connected to.

Routers that have connections to more than one area are called Border Routers (BR). The Border Routers have the responsibility of distributing necessary routing information and changes between areas.

Areas are specific to the router interface. A router that has all of its interfaces in the same area is called an Internal Router. A router that has interfaces in multiple areas is called a Border Router. Routers that act as gateways to other networks (possibly using other routing protocols) are called Autonomous System Border Routers (ASBRs).

Link-State Packets

There are a number of different types of link-state packets, four of which are illustrated below:

- Router Link-State Updates – These describe a router's links to destinations within an area.
- Summary Link-State Updates – Issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).
- Network Link-State Updates – Issued by multi-access areas that have more than one attached router. One router is elected as the Designated Router (DR) and this router issues the network link-state updates describing every router on the segment.
- External Link-State Updates – Issued by an Autonomous System Border Router and describes routes to destinations outside the AS or a default route to the outside AS.

The format of these link-state updates is described in more detail below.

Router link-state updates are flooded to all routers in the current area. These updates describe the destinations reachable through all of the router's interfaces.

Summary link-state updates are generated by Border Routers to distribute routing information about other networks within the AS. Normally, all Summary link-state updates are forwarded to the backbone (area 0) and are then forwarded to all other areas in the network. Border Routers also have the responsibility of distributing routing information from the Autonomous System Border Router in order for routers in the network to get and maintain routes to other Autonomous Systems.

Network link-state updates are generated by a router elected as the Designated Router on a multi-access segment (with more than one attached router). These updates describe all of the routers on the segment and their network connections.

External link-state updates carry routing information to networks outside the Autonomous System. The Autonomous System Border Router is responsible for generating and distributing these updates.

OSPF Authentication

OSPF packets can be authenticated as coming from trusted routers by the use of predefined passwords. The default for routers is to use not authentication.

There are two other authentication methods – simple password authentication (key) and Message Digest authentication (MD-5).

Message Digest Authentication (MD-5)

MD-5 authentication is a cryptographic method. A key and a key-ID are configured on each router. The router then uses an algorithm to generate a mathematical "message digest" that is derived from the OSPF packet, the key and the key-ID. This message digest (a number) is then appended to the packet. The key is not exchanged over the wire and a non-decreasing sequence number is included to prevent replay attacks.

Simple Password Authentication

A password (or key) can be configured on a per-area basis. Routers in the same area that participate in the routing domain must be configured with the same key. This method is possibly vulnerable to passive attacks where a link analyzer is used to obtain the password.

Backbone and Area 0

OSPF limits the number of link-state updates required between routers by defining areas within which a given router operates. When more than one area is configured, one area is designated as area 0 – also called the backbone.

The backbone is at the center of all other areas – all areas of the network have a physical (or virtual) connection to the backbone through a router. OSPF allows routing information to be distributed by forwarding it into area 0, from which the information can be forwarded to all other areas (and all other routers) on the network.

In situations where an area is required, but is not possible to provide a physical connection to the backbone, a virtual link can be configured.

Virtual Links

Virtual links accomplish two purposes:

- Linking an area that does not have a physical connection to the backbone.
- Patching the backbone in case there is a discontinuity in area 0.

Areas Not Physically Connected to Area 0

All areas of an OSPF network should have a physical connection to the backbone, but in some cases it is not possible to physically connect a remote area to the backbone. In these cases, a virtual link is configured to connect the remote area to the backbone. A virtual path is a logical path between two border routers that have a common area, with one border router connected to the backbone.

Partitioning the Backbone

OSPF also allows virtual links to be configured to connect the parts of the backbone that are discontinuous. This is equivalent to linking different area 0s together using a logical path between each area 0. Virtual links can also be added for redundancy to protect against a router failure. A virtual link is configured between two border routers that both have a connection to their respective area 0s.

Neighbors

Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers.

Any two routers must meet the following conditions before the become neighbors:

- **Area ID** – Two routers having a common segment – their interfaces have to belong to the same area on that segment. Of course, the interfaces should belong to the same subnet and have the same subnet mask.
- **Authentication** – OSPF allows for the configuration of a password for a specific area. Two routers on the same segment and belonging to the same area must also have the same OSPF password before they can become neighbors.
- **Hello and Dead Intervals** – The Hello interval specifies the length of time, in seconds, between the hello packets that a router sends on an OSPF interface. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the OSPF router down. OSPF routers exchange Hello packets on each segment in order to acknowledge each other's existence on a segment and to elect a Designated Router on multi-access segments. OSPF requires these intervals to be exactly the same between any two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
- **Stub Area Flag** – Any two routers also have to have the same stub area flag in their Hello packets in order to become neighbors.

Adjacencies

Adjacent routers go beyond the simple Hello exchange and participate in the link-state database exchange process. OSPF elects one router as the Designated Router (DR) and a second router as the Backup Designated Router (BDR) on each multi-access segment (the BDR is a backup in case of a DR failure). All other routers on the segment will then contact the DR for link-state database updates and exchanges. This limits the bandwidth required for link-state database updates.

Designated Router Election

The election of the DR and BDR is accomplished using the Hello protocol. The router with the highest OSPF priority on a given multi-access segment will become the DR for that segment. In case of a tie, the router with the highest Router ID wins. The default OSPF priority is 1. A priority of zero indicates a router that cannot be elected as the DR.

Building Adjacency

Two routers undergo a multi-step process in building the adjacency relationship. The following is a simplified description of the steps required:

- **Down** – No information has been received from any router on the segment.
- **Attempt** – On non-broadcast multi-access networks (such as Frame Relay or X.25), this state indicates that no recent information has been received from the neighbor. An effort should be made to contact the neighbor by sending Hello packets at the reduced rate set by the Poll Interval.
- **Init** – The interface has detected a Hello packet coming from a neighbor but bi-directional communication has not yet been established.
- **Two-way** – Bi-directional communication with a neighbor has been established. The router has seen its address in the Hello packets coming from a neighbor. At the end of this stage the DR and BDR election would have been done. At the end of the Two-way stage, routers will decide whether to proceed in building an adjacency or not. The decision is based on whether one of the routers is a DR or a BDR or the link is a point-to-point or virtual link.
- **Exstart** – (Exchange Start) Routers establish the initial sequence number that is going to be used in the information exchange packets. The sequence number insures that routers always get the most recent information. One router will become the primary and the other will become secondary. The primary router will poll the secondary for information.
- **Exchange** – Routers will describe their entire link-state database by sending database description packets.
- **Loading** – The routers are finalizing the information exchange. Routers have link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated will be put on the request list. Any update that is sent will be put on the retransmission list until it gets acknowledged.
- **Full** – The adjacency is now complete. The neighboring routers are fully adjacent. Adjacent routers will have the same link-state database.

Adjacencies on Point-to-Point Interfaces

OSPF Routers that are linked using point-to-point interfaces (such as serial links) will always form adjacencies. The concepts of DR and BDR are unnecessary.

OSPF Packet Formats

All OSPF packet types begin with a standard 24-byte header and there are five packet types. The header is described first, and each packet type is described in a subsequent section.

All OSPF packets (except for Hello packets) forward link-state advertisements. Link-State Update packets, for example, flood advertisements throughout the OSPF routing domain.

- OSPF packet header
- Hello packet
- Database Description packet
- Link-State Request packet
- Link-State Update packet
- Link-State Acknowledgment packet

OSPF Packet Header

Every OSPF packet is preceded by a common 24-byte header. This header contains the information necessary for a receiving router to determine if the packet should be accepted for further processing.

The format of the OSPP packet header is shown below:

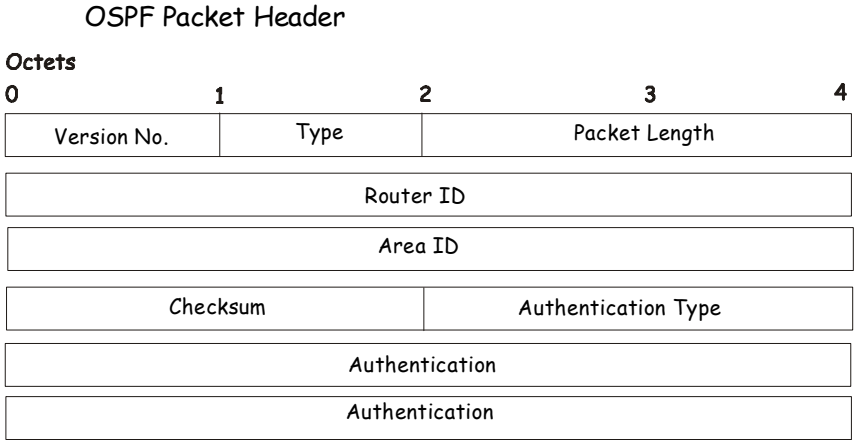


Figure 8- 19. OSPF Packet Header Format

Field	Description
Version No.	The OSPF version number
Type	The OSPF packet type. The OSPF packet types are as follows: 1 means Hello packet, 2 means Database Description packet, 3 means Link State Request packet, 4 means Link State Update packet, 5 means Link State Acknowledgement packet.
Packet Length	The length of the packet in bytes. This length includes the 24-byte header.
Router ID	The Router ID of the packet's source.
Area ID	A 32-bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Packets traversing a virtual link are assigned the backbone Area ID of 0.0.0.0
Checksum	A standard IP checksum that includes all of the packet's contents except for the 64-bit authentication field.
Authentication Type	The type of authentication to be used for the packet.
Authentication	A 64-bit field used by the authentication scheme.

Hello Packet

Hello packets are OSPF packet type 1. They are sent periodically on all interfaces, including virtual links, in order to establish and maintain neighbor relationships. In addition, Hello Packets are multicast on those physical networks having a multicast or broadcast capability, enabling dynamic discovery of neighboring routers.

All routers connected to a common network must agree on certain parameters such as the Network Mask, the Hello Interval, and the Router Dead Interval. These parameters are included in the hello packets, so that differences can inhibit the forming of neighbor relationships. A detailed explanation of the receive process for Hello packets is necessary so that differences can inhibit the forming of neighbor relationships.

The format of the Hello packet is shown below:

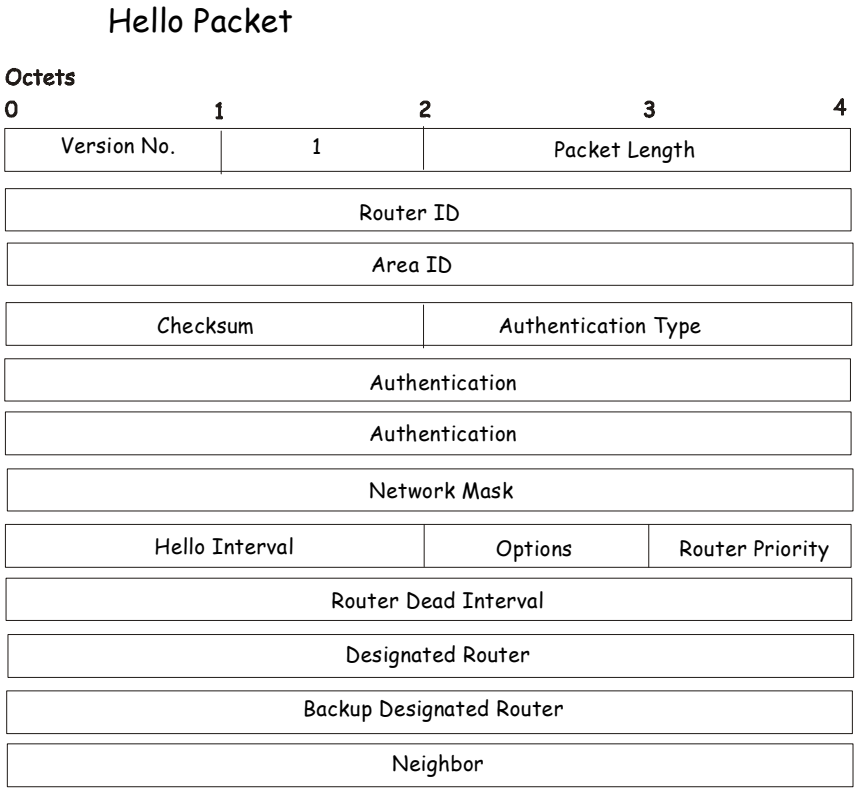


Figure 8- 20. Hello Packet

Field	Description
Network Mask	The network mask associated with this interface.
Options	The optional capabilities supported by the router.
Hello Interval	The number of seconds between this router's Hello packets.
Router Priority	This router's Router Priority. The Router Priority is used in the election of the DR and BDR. If this field is set to 0, the router is ineligible become the DR or the BDR.
Router Dead Interval	The number of seconds that must pass before declaring a silent router as down.
Designated Router	The identity of the DR for this network, in the view of the advertising router. The DR is identified here by its IP interface address on the network.
Backup Designated Router	The identity of the Backup Designated Router (BDR) for this network. The BDR is identified here by its IP interface address on the network. This field is set to 0.0.0.0 if there is no BDR.
Neighbor	The Router IDs of each router from whom valid Hello packets have been seen within the Router Dead Interval on the network.

Database Description Packet

Database Description packets are OSPF packet type 2. These packets are exchanged when an adjacency is being initialized. They describe the contents of the topological database. Multiple packets may be used to describe the database. For this purpose, a poll-response procedure is used. One of the routers is designated to be master, the other a slave. The master sends Database Description packets (polls) that are acknowledged by Database Description packets sent by the slave (responses). The responses are linked to the polls via the packets' DD sequence numbers.

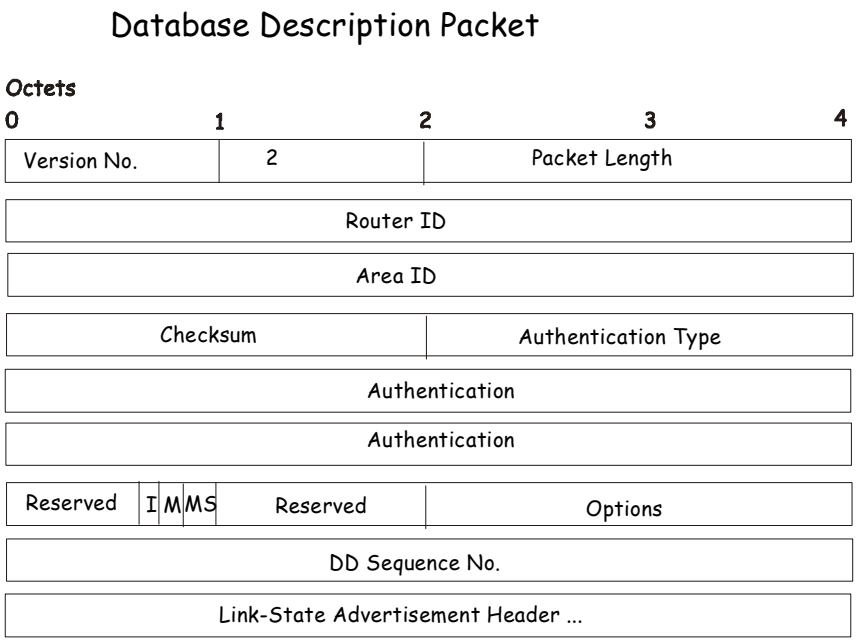


Figure 8- 21. Database Description Packet

Field	Description
Options	The optional capabilities supported by the router.
I - bit	The Initial bit. When set to 1, this packet is the first in the sequence of Database Description packets.
M - bit	The More bit. When set to 1, this indicates that more Database Description packets will follow.
MS - bit	The Master Slave bit. When set to 1, this indicates that the router is the master during the Database Exchange process. A zero indicates the opposite.
DD Sequence Number	User to sequence the collection of Database Description Packets. The initial value (indicated by the Initial bit being set) should be unique. The DD sequence number then increments until the complete database description has been sent.

The rest of the packet consists of a list of the topological database's pieces. Each link state advertisement in the database is described by its link state advertisement header.

Link-State Request Packet

Link-State Request packets are OSPF packet type 3. After exchanging Database Description packets with a neighboring router, a router may find that parts of its topological database are out of date. The Link-State Request packet is used to request the pieces of the neighbor's database that are more up to date. Multiple Link-State Request packets may need to be used. The sending of Link-State Request packets is the last step in bringing up an adjacency.

A router that sends a Link-State Request packet has in mind the precise instance of the database pieces it is requesting, defined by LS sequence number, LS checksum, and LS age, although these fields are not specified in the Link-State Request packet itself. The router may receive even more recent instances in response.

The format of the Link-State Request packet is shown below:

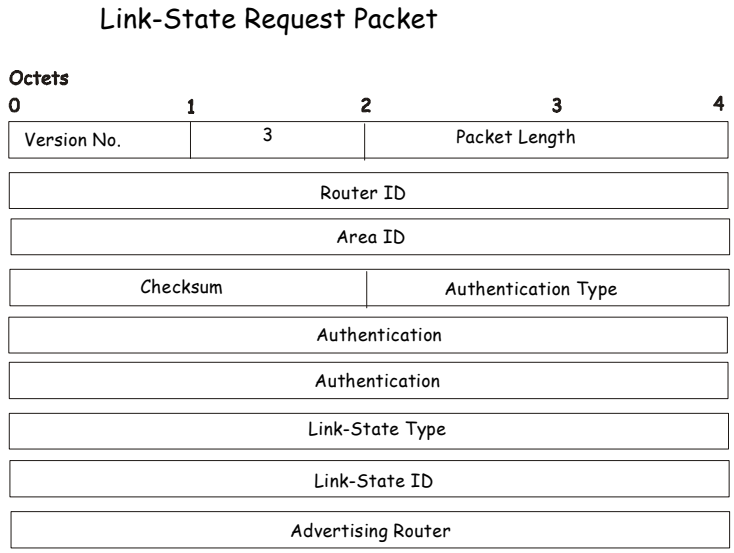


Figure 8- 22. Link-State Request Packet

Each advertisement requested is specified by its Link-State Type, Link-State ID, and Advertising Router. This uniquely identifies the advertisement, but not its instance. Link-State Request packets are understood to be requests for the most recent instance.

Link-State Update Packet

Link-State Update packets are OSPF packet type 4. These packets implement the flooding of link-state advertisements. Each Link-State Update packet carries a collection of link-state advertisements one hop further from its origin. Several link-state advertisements may be included in a single packet.

Link-State Update packets are multicast on those physical networks that support multicast/broadcast. In order to make the flooding procedure reliable, flooded advertisements are acknowledged in Link-State Acknowledgment packets. If retransmission of certain advertisements is necessary, the retransmitted advertisements are always carried by unicast Link-State Update packets.

The format of the Link-State Update packet is shown below:

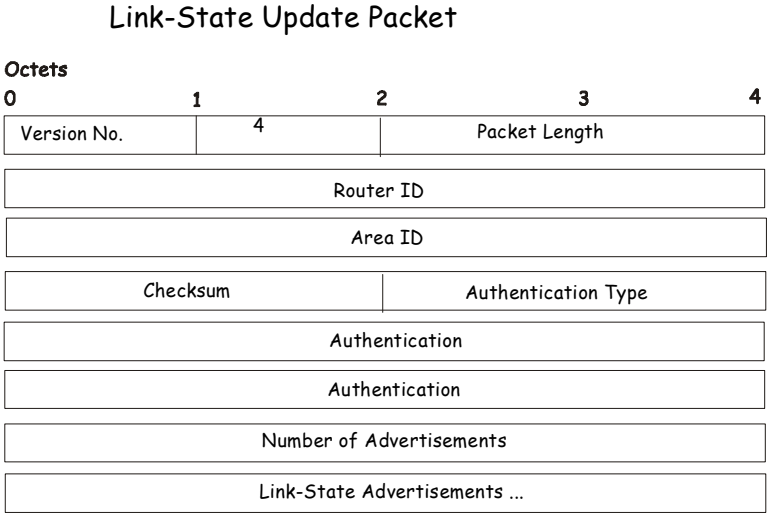


Figure 8- 23. Link-State Update Packet

The body of the Link-State Update packet consists of a list of link-state advertisements. Each advertisement begins with a common 20-byte header, the link-state advertisement header. Otherwise, the format of each of the five types of link-state advertisements is different.

Link-State Acknowledgment Packet

Link-State Acknowledgment packets are OSPF packet type 5. To make the folding of link-state advertisements reliable, flooded advertisements are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link-State Acknowledgment packets. Multiple link-state advertisements can be acknowledged in a single Link-State Acknowledgment packet.

Depending on the state of the sending interface and the source of the advertisements being acknowledged, a Link-State Acknowledgment packet is sent either to the multicast address AllSPFRouters, to the multicast address AllDRouters, or as a unicast packet.

The format of this packet is similar to that of the Data Description packet. The body of both packets is simply a list of link-state advertisement headers.

The format of the Link-State Acknowledgment packet is shown below:

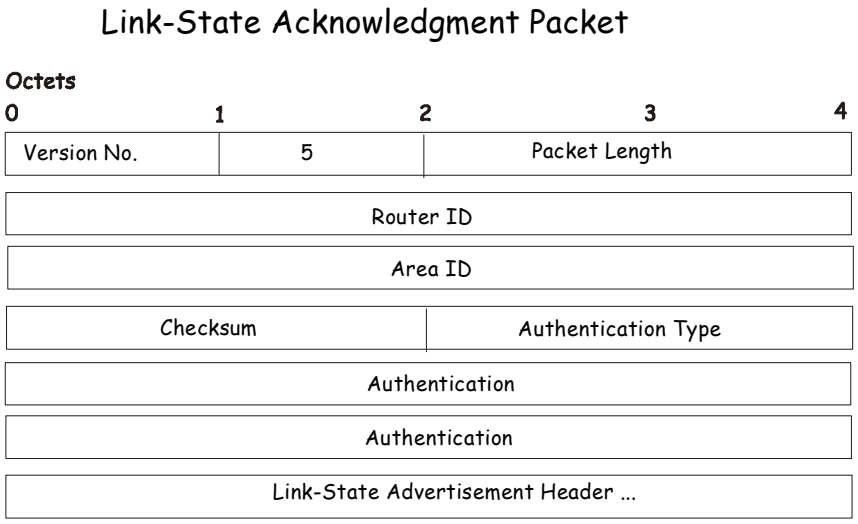


Figure 8- 24. Link State Acknowledge Packet

Each acknowledged link-state advertisement is described by its link-state advertisement header. It contains all the information required to uniquely identify both the advertisement and the advertisement's current instance.

Link-State Advertisement Formats

There are five distinct types of link-state advertisements. Each link-state advertisement begins with a standard 20-byte link-state advertisement header. Succeeding sections then diagram the separate link-state advertisement types.

Each link-state advertisement describes a piece of the OSPF routing domain. Every router originates a router links advertisement. In addition, whenever the router is elected as the Designated Router, it originates a network links advertisement. Other types of link-state advertisements may also be originated. The flooding algorithm is reliable, ensuring that all routers have the same collection of link-state advertisements. The collection of advertisements is called the link-state (or topological) database.

From the link-state database, each router constructs a shortest path tree with itself as root. This yields a routing table.

There are four types of link state advertisements, each using a common link state header. These are:

- Router Links Advertisements
- Network Links Advertisements
- Summary Link Advertisements
- Autonomous System Link Advertisements

Link State Advertisement Header

All link state advertisements begin with a common 20-byte header. This header contains enough information to uniquely identify the advertisements (Link State Type, Link State ID, and Advertising Router). Multiple instances of the link state advertisement may exist in the routing domain at the same time. It is then necessary to determine which instance is more recent. This is accomplished by examining the link state age, link state sequence number and link state checksum fields that are also contained in the link state advertisement header.

The format of the Link State Advertisement Header is shown below:

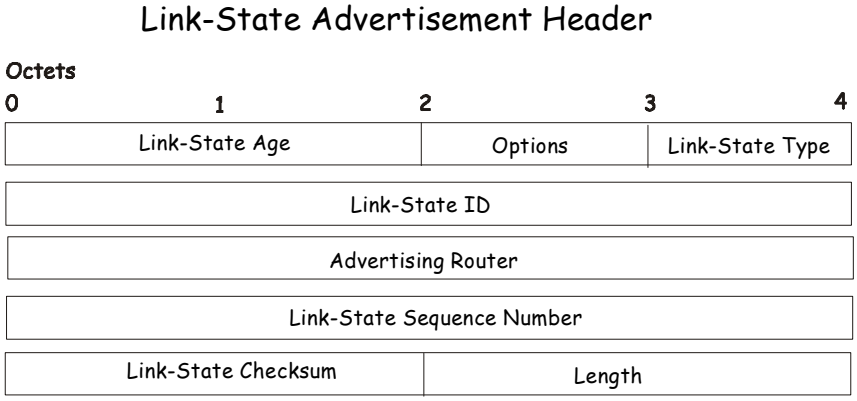


Figure 8- 25. Link State Advertisement Header

Field	Description
Link State Age	The time is seconds since the link state advertisement was originated.
Options	The optional capabilities supported by the described portion of the routing domain.
Link State Type	The type of the link state advertisement. Each link state type has a separate advertisement format. The link state type are as follows: Router Links, Network Links, Summary Link (IP Network), Summary Link (ASBR), AS External Link.
Link State ID	This field identifies the portion of the internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's Link State Type.
Advertising Router	The Router ID of the router that originated the Link State Advertisement. For example, in network links advertisements this field is set to the Router ID of the network's Designated Router.
Link State Sequence Number	Detects old or duplicate link state advertisements. Successive instances of a link state advertisement are given successive Link State Sequence numbers.
Link State Checksum	The Fletcher checksum of the complete contents of the link state advertisement, including the link state advertisement header by accepting the Link State Age field.
Length	The length in bytes of the link state advertisement. This includes the 20-byte link state advertisement header.

Router Links Advertisements

Router links advertisements are type 1 link state advertisements. Each router in an area originates a routers links advertisement. The advertisement describes the state and cost of the router's links to the area. All of the router's links to the area must be described in a single router links advertisement.

The format of the Router Links Advertisement is shown below:

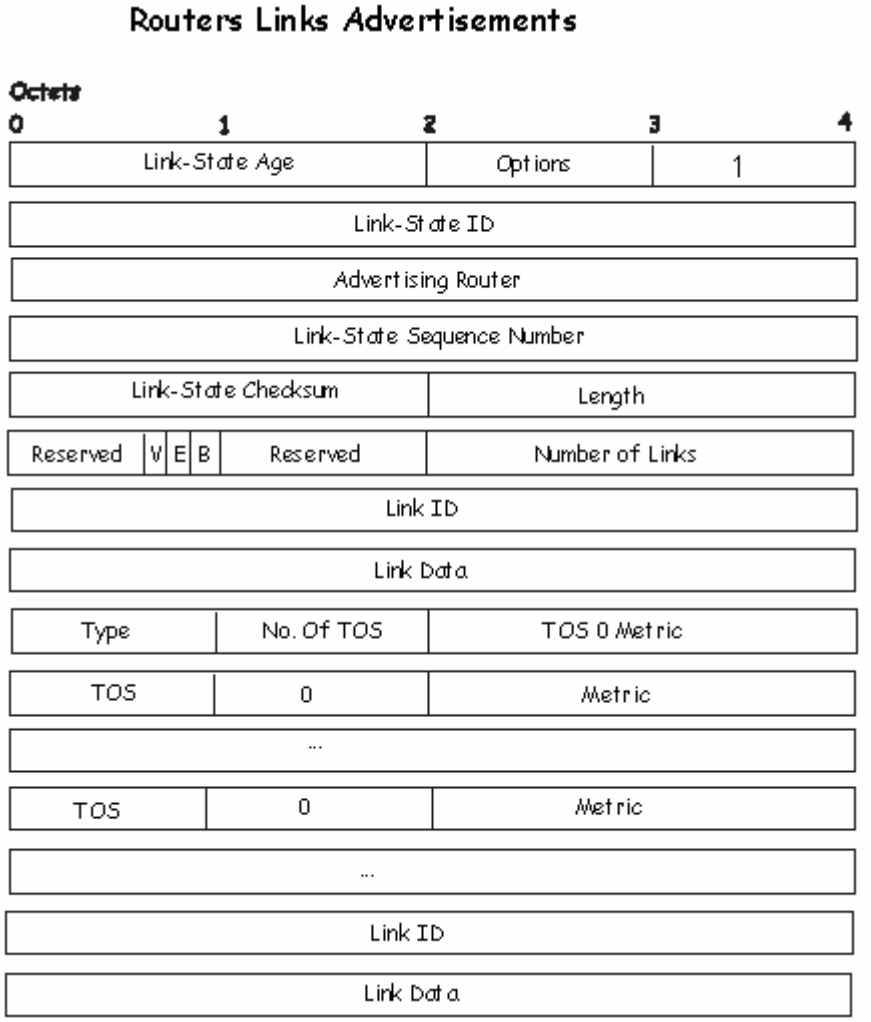


Figure 8- 26. Routers Links Advertisements

In router links advertisements, the Link State ID field is set to the router's OSPF Router ID. The T - bit is set in the advertisement's Option field if and only if the router is able to calculate a separate set of routes for each IP Type of Service (TOS). Router links advertisements are flooded throughout a single area only.

Field	Description
V - bit	When set, the router is an endpoint of an active virtual link that is using the described area as a Transit area (V is for Virtual link endpoint).
E - bit	When set, the router is an Autonomous System (AS) boundary router (E is for External).
B - bit	When set, the router is an area border router (B is for Border).
Number of Links	The number of router links described by this advertisement. This must be the total collection of router links to the area.

The following fields are used to describe each router link. Each router link is typed. The Type field indicates the kind of link being described. It may be a link to a transit network, to another router or to a stub network. The values of all the other fields describing

a router link depend on the link's Type. For example, each link has an associated 32-bit data field. For links to stub networks, this field specifies the network's IP address mask. For other link types, the Link Data specifies the router's associated IP interface address.

Field	Description
Link ID	Identifies the object that this router link connects to. Value depends on the link's Type. When connecting to an object that also originates a link state advertisement (i.e. another router or a transit network) the Link ID is equal to the neighboring advertisement's Link State ID. This provides the key for looking up an advertisement in the link state database. Type Link ID Neighboring router's Router ID. IP address of Designated Router. IP network/subnet number. Neighboring router's Router ID
Link Data	Contents again depend on the link's Type field. For connections to stub networks, it specifies the network's IP address mask. For unnumbered point-to-point connection, it specifies the interface's MIB-II ifIndex value. For other link types it specifies the router's associated IP interface address. This latter piece of information is needed during the routing table build process, when calculating the IP address of the next hop.
No. of TOS	The number of different Type of Service (TOS) metrics given for this link, not counting the required metric for TOS 0. If no additional TOS metrics are given, this field should be set to 0.
TOS 0 Metric	The cost of using this router link for TOS 0.

For each link, separate metrics may be specified for each Type of Service (TOS). The metric for TOS 0 must always be included, and was discussed above. Metrics for non-zero TOS are described below. Note that the cost for non-zero TOS values that are not specified defaults to the TOS 0 cost. Metrics must be listed in order of increasing TOS encoding. For example, the metric for TOS 16 must always follow the metric for TOS 8 when both are specified.

Field	Description
TOS	IP Type of Service that this metric refers to.
Metric	The cost of using this outbound router link, for traffic of the specified TOS.

Network Links Advertisements

Network links advertisements are Type 2 link state advertisements. A network links advertisement is originated for each transit network in the area. A transit network is a multi-access network that has more than one attached router. The network links advertisement is originated by the network's designated router. The advertisement describes all routers attached to the network, including the Designated Router itself. The advertisement's Link State ID field lists the IP interface address of the Designated Router.

The distance form the network to all attached routers is zero, for all TOS. This is why the TOS and metric fields need not be specified in the network links advertisement.

The format of the Network Links Advertisement is shown below:

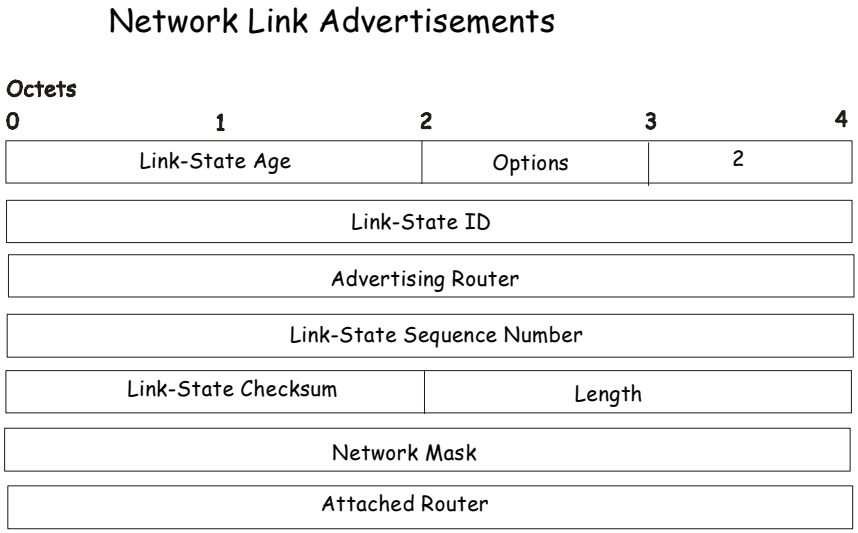


Figure 8- 27. Network Link Advertisements

Field	Description
Network Mask	The IP address mask for the network.
Attached Router	The Router Ids of each of the routers attached to the network. Only those routers that are fully adjacent to the Designated Router (DR) are listed. The DR includes itself in this list.

Summary Link Advertisements

Summary link advertisements are Type 3 and 4 link state advertisements. These advertisements are originated by Area Border routers. A separate summary link advertisement is made for each destination known to the router, that belongs to the Autonomous System (AS), yet is outside the area.

Type 3 link state advertisements are used when the destination is an IP network. In this case, the advertisement's Link State ID field is an IP network number. When the destination is an AS boundary router, a Type 4 advertisement is used, and the Link State ID field is the AS boundary router's OSPF Router ID. Other than the difference in the Link State ID field, the format of Type 3 and 4 link state advertisements is identical.

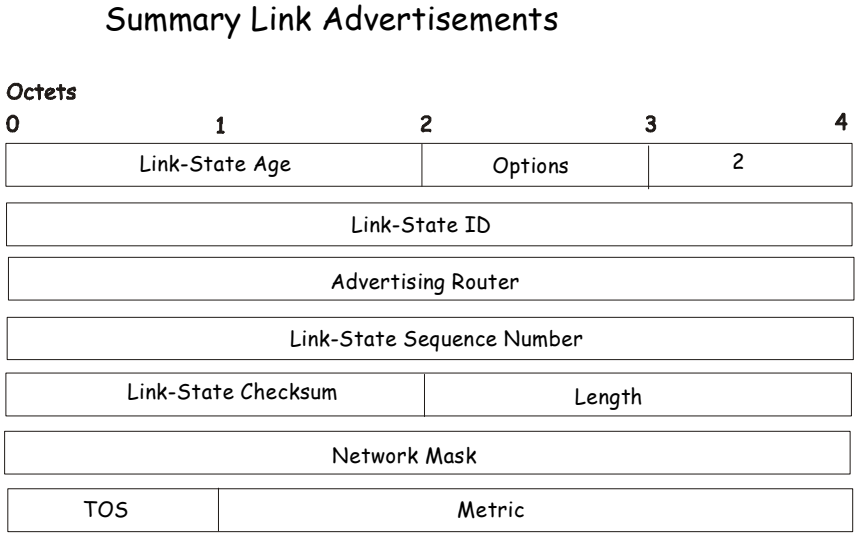


Figure 8- 28. Summary Link Advertisements

For stub area, Type 3 summary link advertisements can also be used to describe a default route on a per-area basis. Default summary routes are used in stub area instead of flooding a complete set of external routes. When describing a default summary route, the advertisement's Link State ID is always set to the Default Destination – 0.0.0.0, and the Network Mask is set to 0.0.0.0.

Separate costs may be advertised for each IP Type of Service. Note that the cost for TOS 0 must be included, and is always listed first. If the T-bit is reset in the advertisement's Option field, only a route for TOS 0 is described by the advertisement. Otherwise, routes for the other TOS values are also described. If a cost for a certain TOS is not included, its cost defaults to that specified for TOS 0.

Field	Description
Network Mask	For Type 3 link state advertisements, this indicates the destination network's IP address mask. For example, when advertising the location of a class A network the value 0xff000000
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. Expressed in the same units as the interface costs in the router links advertisements.

Autonomous Systems External Link Advertisements

Autonomous Systems (AS) link advertisements are Type 5 link state advertisements. These advertisements are originated by AS boundary routers. A separate advertisement is made for each destination known to the router that is external to the AS.

AS external link advertisements usually describe a particular external destination. For these advertisements the Link State ID field specifies an IP network number. AS external link advertisements are also used to describe a default route. Default routes are used when no specific route exists to the destination. When describing a default route, the Link Stat ID is always set the Default Destination address (0.0.0.0) and the Network Mask is set to 0.0.0.0.

The format of the AS External Link Advertisement is shown below:

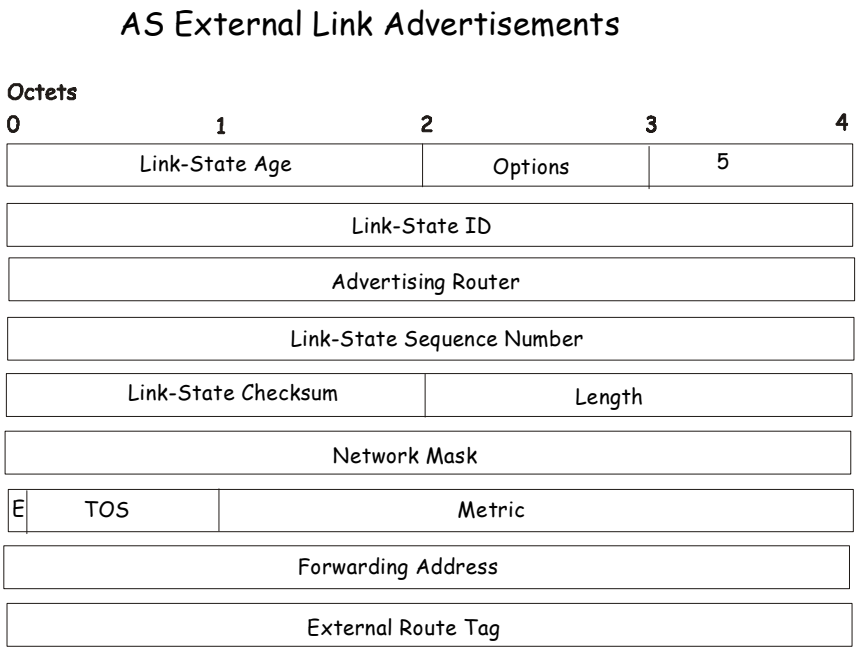


Figure 8- 29. AS External Link Advertisements

Field	Description
Network Mask	The IP address mask for the advertised destination.
E - bit	The type of external metric. If the E - bit is set, the metric specified is a Type 2 external metric. This means the metric is considered larger than any link state path. If the E - bit is zero, the specified metric is a Type 1 external metric. This means that is comparable directly to the link state metric.
Forwarding Address	Data traffic for the advertised destination will be forwarded to this address. If the Forwarding Address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. The interpretation of this metric depends on the external type indication (the E - bit above).
External Route Tag	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

OSPF Global Settings

The **OSPF Global Settings** menu allows OSPF to be enabled or disabled on the Switch – without changing the Switch's OSPF configuration. To view the following window, click **L3 Features > OSPF > OSPF Global Settings**. To enable OSPF, first supply an **OSPF Route ID** (see below), select *Enabled* from the **State** drop-down menu and click the **Apply** button.

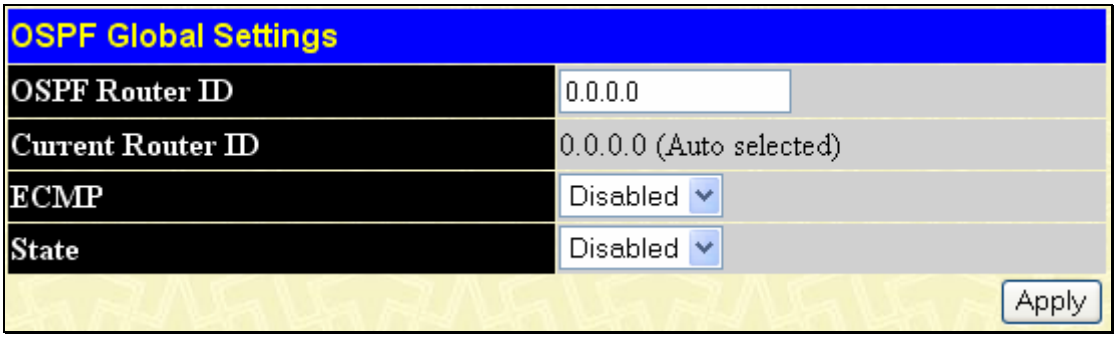


Figure 8- 30. OSPF Global Settings window

The following parameters are used for general OSPF configuration:

Parameter	Description
OSPF Route ID	A 32-bit number (in the same format as an IP address – xxx.xxx.xxx.xxx) that uniquely identifies the Switch in the OSPF domain. It is common to assign the highest IP address assigned to the Switch (router). In this case, it would be 10.53.13.189, but any unique 32-bit number will do. If 0.0.0.0 is entered, the highest IP address assigned to the Switch will become the OSPF Route ID.
Current Route ID	Displays the OSPF Route ID currently in use by the Switch. This Route ID is displayed as a convenience to the user when changing the Switch's OSPF Route ID.
ECMP	Use the drop-down menu to enable or disable the Equal Cost Multipath Protocol.
State	Allows OSPF to be enabled or disabled globally on the Switch without changing the OSPF configuration.

OSPF Area Settings

This menu allows the configuration of OSPF Area IDs and to designate these areas as either **Normal**, **Stub** or **NSSA**. Normal OSPF areas allow Link-State Database (LSDB) advertisements of routes to advertise to networks that are external to the area. Stub areas do not allow LSDB advertisements of external routes. Stub areas use a default summary external route (0.0.0.0 or Area 0) to reach external destinations. Not-So- Stubby-Area (NSSA) areas are similar to Stub areas, however they only allow a limited exchange of external information across an NSSA area border, therefore reducing the amount of Link State Advertisements.

To set up an OSPF area configuration click **Layer 3 Features > OSPF > OSPF Area Settings** link to open the following dialog box:

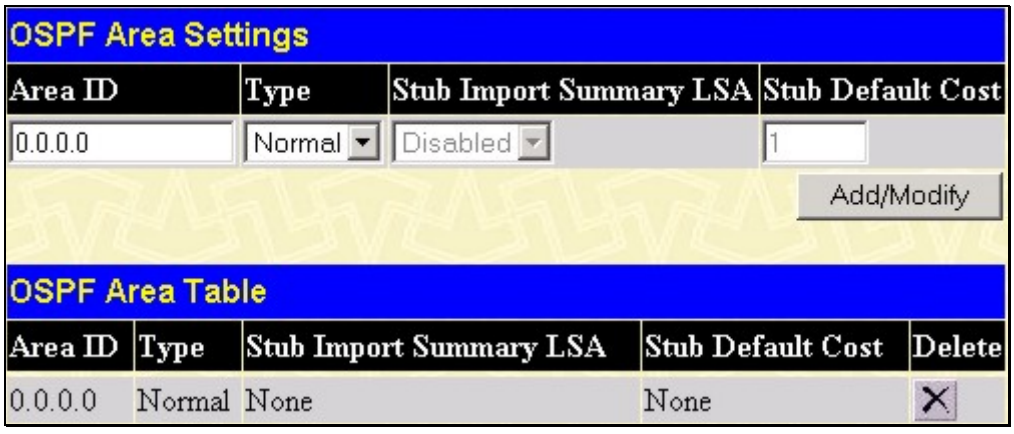


Figure 8- 31. OSPF Area Settings and Table window

To add an OSPF Area to the table, type a unique **Area ID** (see below) select the **Type** from the drop-down menu. For a Stub type, choose *Enabled* or *Disabled* from the **Stub Import Summary LSA** drop-down menu and determine the **Stub Default Cost**. Click the **Add/Modify** button to add the area ID set to the table.

To remove an Area ID configuration set, simply click ✕ in the **Delete** column for the configuration.

To change an existing set in the list, type the **Area ID** of the set you want to change, make the changes and click the **Add/Modify** button. The modified OSPF area ID will appear in the table.

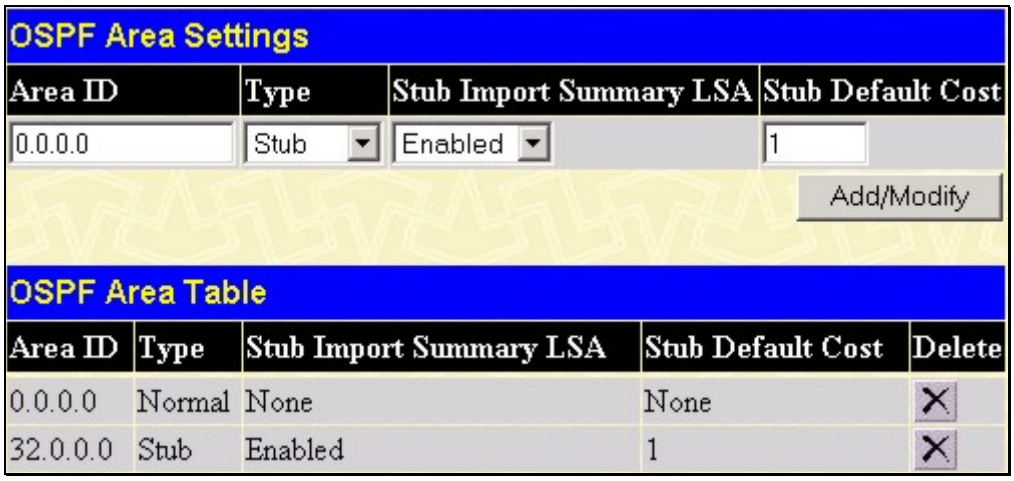


Figure 8- 32. OSPF Area Settings example window

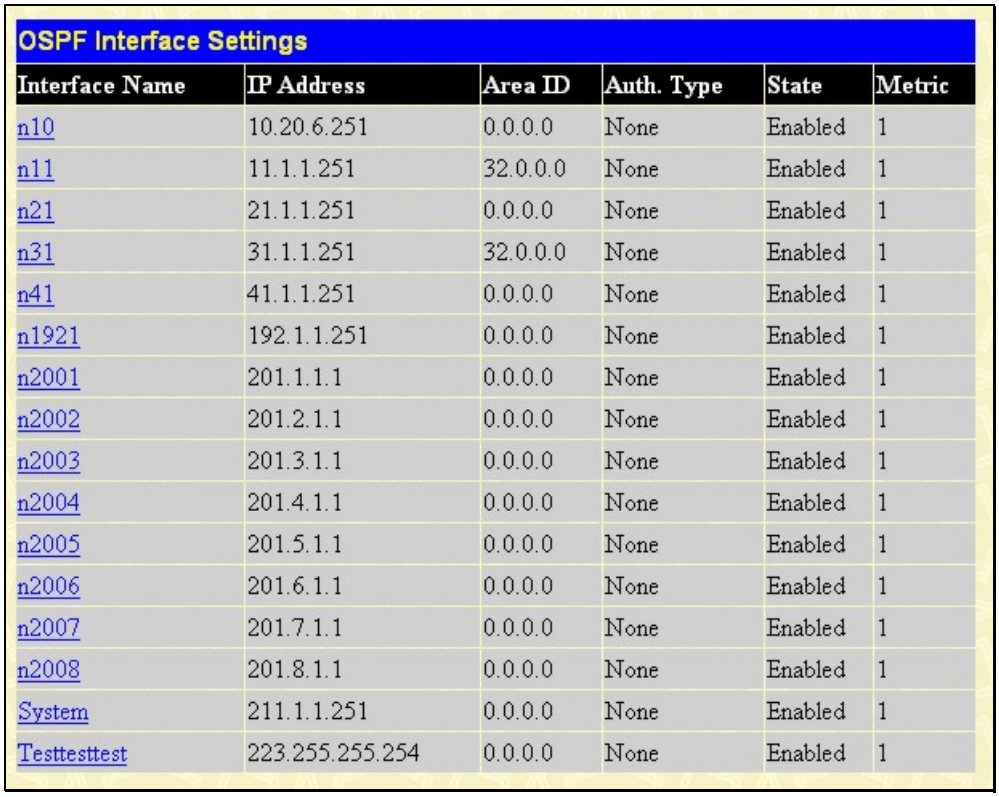
See the parameter descriptions below for information on the **OSPF Area ID Settings**.

The **Area ID** settings are as follows:

Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	Use the drop-down menu to choose from *Normal, Stub* and NSSA. When it is toggled to *Stub* or NSSA two additional fields are available – **Stub Import Summary LSA** and **Stub Default Cost**.
Stub Import Summary LSA	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Stub Default Cost	Displays the default cost for the route to the stub of between 0 and 65,535. The default is 1.

OSPF Interface Settings

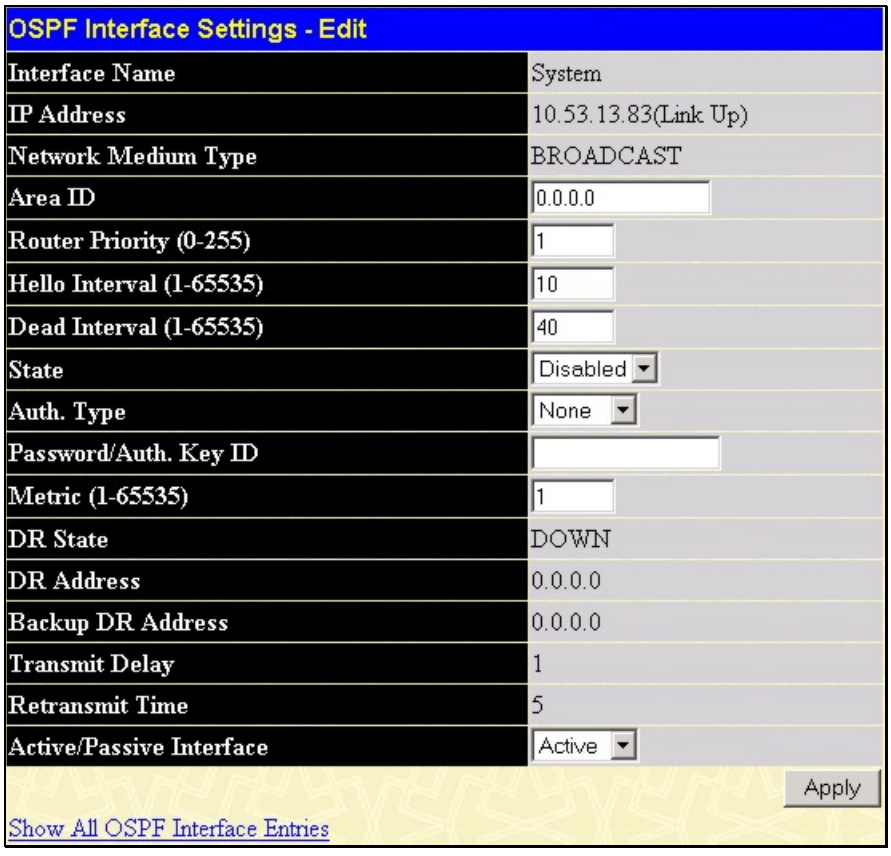
To set up OSPF interfaces, click **L3 Features > OSPF > OSPF Interface Settings** to view OSPF settings for existing IP interfaces. If there are no IP interfaces configured (besides the default System interface), only the System interface settings will appear listed. To change settings for an IP interface, click on the hyperlinked name of the interface to see the configuration menu for that interface.



OSPF Interface Settings

Interface Name	IP Address	Area ID	Auth. Type	State	Metric
n10	10.20.6.251	0.0.0.0	None	Enabled	1
n11	11.1.1.251	32.0.0.0	None	Enabled	1
n21	21.1.1.251	0.0.0.0	None	Enabled	1
n31	31.1.1.251	32.0.0.0	None	Enabled	1
n41	41.1.1.251	0.0.0.0	None	Enabled	1
n1921	192.1.1.251	0.0.0.0	None	Enabled	1
n2001	201.1.1.1	0.0.0.0	None	Enabled	1
n2002	201.2.1.1	0.0.0.0	None	Enabled	1
n2003	201.3.1.1	0.0.0.0	None	Enabled	1
n2004	201.4.1.1	0.0.0.0	None	Enabled	1
n2005	201.5.1.1	0.0.0.0	None	Enabled	1
n2006	201.6.1.1	0.0.0.0	None	Enabled	1
n2007	201.7.1.1	0.0.0.0	None	Enabled	1
n2008	201.8.1.1	0.0.0.0	None	Enabled	1
System	211.1.1.251	0.0.0.0	None	Enabled	1
Testtesttest	223.255.255.254	0.0.0.0	None	Enabled	1

Figure 8- 33. OSPF Interface Settings window



OSPF Interface Settings - Edit

Interface Name	System
IP Address	10.53.13.83(Link Up)
Network Medium Type	BROADCAST
Area ID	0.0.0.0
Router Priority (0-255)	1
Hello Interval (1-65535)	10
Dead Interval (1-65535)	40
State	Disabled
Auth. Type	None
Password/Auth. Key ID	
Metric (1-65535)	1
DR State	DOWN
DR Address	0.0.0.0
Backup DR Address	0.0.0.0
Transmit Delay	1
Retransmit Time	5
Active/Passive Interface	Active

Apply

Show All OSPF Interface Entries

Figure 8- 34. OSPF Interface Settings - Edit window

Configure each IP interface individually using the **OSPF Interface Settings - Edit** menu. Click the **Apply** button when you have entered the settings. The new configuration appears listed in the **OSPF Interface Settings** table. To return to the **OSPF Interface Settings** table, click the Show All OSPF Interface Entries link.

OSPF interface settings are described below. Some OSPF interface settings require previously configured OSPF settings. Read the descriptions below for details.

Parameter	Description
Interface Name	Displays the name of an IP interface previously configured on the Switch.
Area ID	Allows the entry of an OSPF Area ID configured above.
Router Priority (0-255)	Allows the entry of a number between 0 and 255 representing the OSPF priority of the selected area. If a Router Priority of 0 is selected, the Switch cannot be elected as the Designated Router for the network.
Hello Interval (1-65535)	Allows the specification of the interval between the transmissions of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The **Hello Interval, Dead Interval, Authorization Type**, and **Authorization Key** should be the same for all routers on the same network.
Dead Interval (1-65535)	Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The **Dead Interval** must be evenly divisible by the **Hello Interval**.
State	Allows the OSPF interface to be disabled for the selected area without changing the configuration for that area.
Auth Type	This field can be toggled between **None**, **Simple**, and **MD5** using the space bar. This allows a choice of authorization schemes for OSPF packets that may be exchanged over the OSPF routing domain. • **None** specifies no authorization. • **Simple** uses a simple password to determine if the packets are from an authorized OSPF router. When Simple is selected, the Auth Key field allows the entry of an 8-character password that must be the same as a password configured on a neighbor OSPF router. • **MD5** uses a cryptographic key entered in the MD5 Key Table Configuration menu. When MD5 is selected, the Auth Key ID field allows the specification of the Key ID as defined in the MD5 configuration above. This must be the same MD5 Key as used by the neighboring router.
Password/Auth. Key ID	Enter a Key ID of up to 5 characters to set the Auth. Key ID for either the Simple Auth Type or the MD5 Auth Type, as specified in the previous parameter.
Metric (1-65535)	This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1.
DR State	A read only field describing the Designated Router state of the IP interface. This field may be read **DR** if the interface is the designated router, or **Backup DR** if the interface is the Backup Designated Router. The highest IP address will be the Designated Router and is determined by the OSPF Hello Protocol of the Switch.
DR Address	The IP address of the aforementioned Designated Router.
Backup DR Address	The IP address of the aforementioned Backup Designated Router.
Transmit Delay	A read only field that denotes the estimated time to transmit a Link State Update Packet over this interface, in seconds.

Retransmit Time	A read only field that denotes the time between LSA retransmissions over this interface, in seconds.
Active or Passive Interface	The user may select Active or Passive for this OSPF interface. Active interfaces actively advertise OSPF to routers on other Intranets that are not part of this specific OSPF group. Passive interface will not advertise to any other routers than those within its OSPF intranet.

OSPF Virtual Link Settings

Click the **OSPF Virtual Interface Setting**s link to view the current **OSPF Virtual Interface Settings**. There are not virtual interface settings configured by default, so the first time this table is viewed there will be not interfaces listed. To add a new OSPF virtual interface configuration set to the table, click the **Add** button. A new menu appears (see below). To change an existing configuration, click on the hyperlinked **Transit Area ID** for the set you want to change. The menu to modify an existing set is the same as the menu used to add a new one. To eliminate an existing configuration, click the ✕ in the **Delete** column.

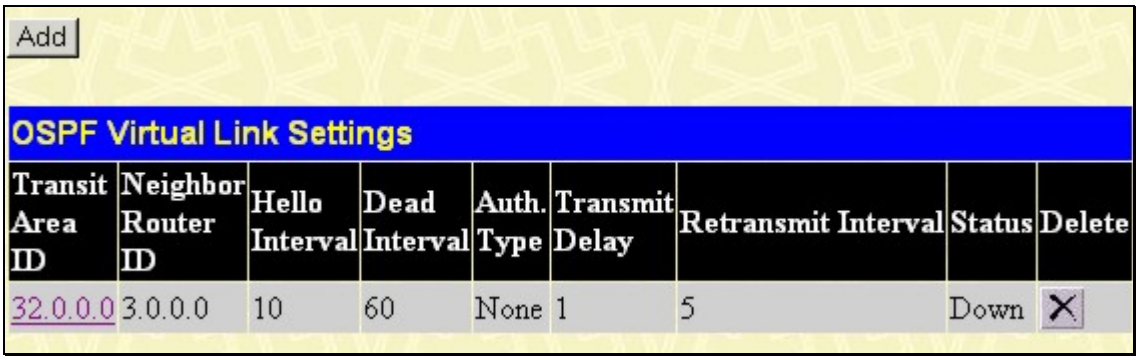


Figure 8- 35. OSPF Virtual Interface Settings

The status of the virtual interface appears (Up or Down) in the **Status** column.

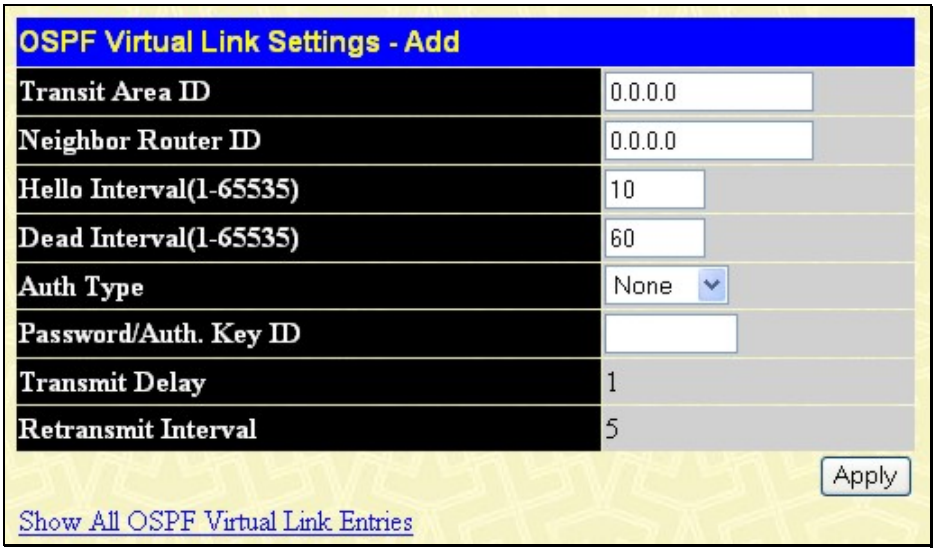


Figure 8- 36. OSPF Virtual Link Settings – Add

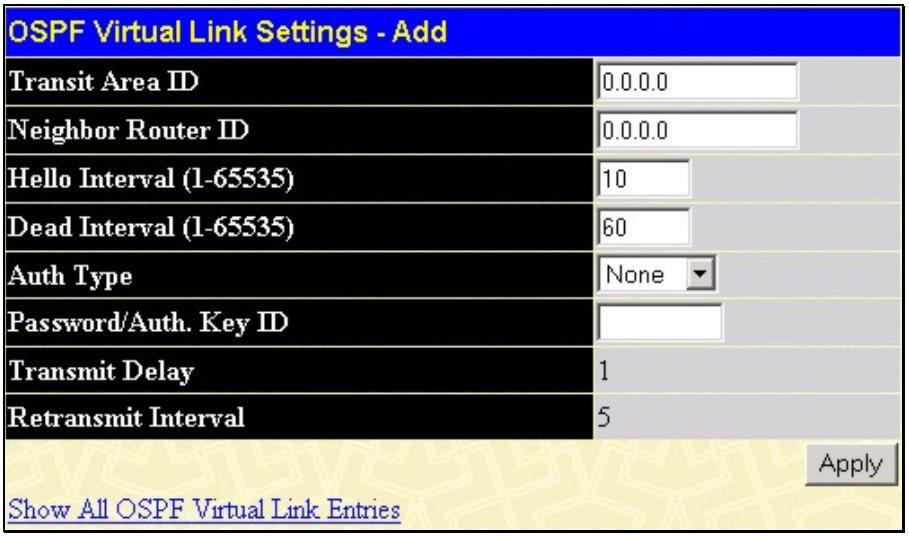


Figure 8- 37. OSPF Virtual Link Settings - Edit

Configure the following parameters if you are adding or changing an **OSPF Virtual Interface**:

Parameter	Description
Transit Area ID	Allows the entry of an OSPF Area ID – previously defined on the Switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
Neighbor Router	The OSPF router ID for the remote router. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
Hello Interval (1-65535)	Specify the interval between the transmission of OSPF Hello packets, in seconds. Enter a value between 1 and 65535 seconds. The **Hello Interval**, **Dead Interval**, **Authorization Type**, and **Authorization Key** should have identical settings for all routers on the same network.
Dead Interval (1-65535)	Specify the length of time between (receiving) Hello packets from a neighbor router before the selected area declares that router down. Again, all routers on the network should use the same setting.
Auth Type	If using authorization for OSPF routers, select the type being used. MD5 key authorization must be set up in the MD5 Key Settings menu.
Password/Auth. Key ID	Enter a case-sensitive password for simple authorization or enter the MD5 key you set in the MD5 Key settings menu.
Transmit Delay	The number of seconds required to transmit a link state update over this virtual link. Transit delay takes into account transmission and propagation delays. This field is fixed at 1 second.
RetransInterval	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. This field is fixed at 5 seconds.

Click **Apply** to implement changes made.

NOTE: For OSPF to function properly some settings should be identical on all participating OSPF devices. These settings include the Hello Interval and Dead Interval. For networks using authorization for OSPF devices, the Authorization Type and Password or Key used must likewise be identical.

OSPF Area Aggregation Settings

Area Aggregation allows all of the routing information that may be contained within an area to be aggregated into a summary LSDB advertisement of just the network address and subnet mask. This allows for a reduction in the volume of LSDB advertisement traffic as well as a reduction in the memory overhead in the Switch used to maintain routing tables. Click **Layer 3 Features > OSPF > OSPF Area Aggregation Settings** link to view the current settings. There are no aggregation settings configured by default, so there will not be any listed the first accessing the menu. To add a new **OSPF Area Aggregation** setting, click the **Add** button. A new menu (pictured below) appears. To change an existing configuration, click on the hyperlinked Area ID for the set you want to change. The menu to modify an existing configuration is the same as the menu used to add a new one. To eliminate an existing configuration, click the ✕ in the **Delete** column for the configuration being removed.

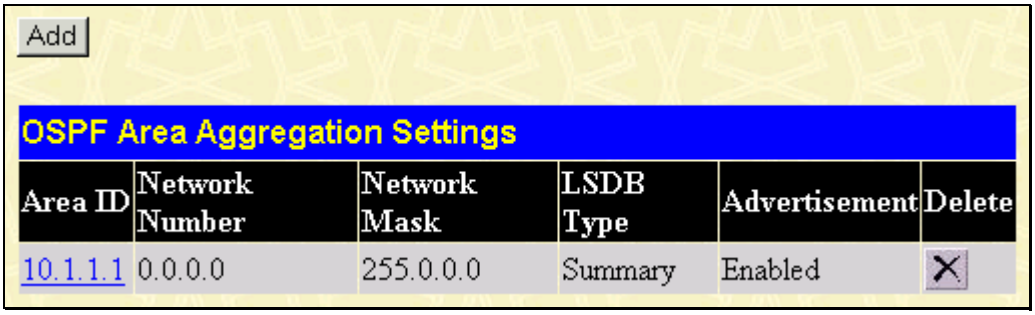


Figure 8- 38. OSPF Area Aggregation Settings

Use the menu below to add a new or edit an **OSPF Area Aggregation** setting.

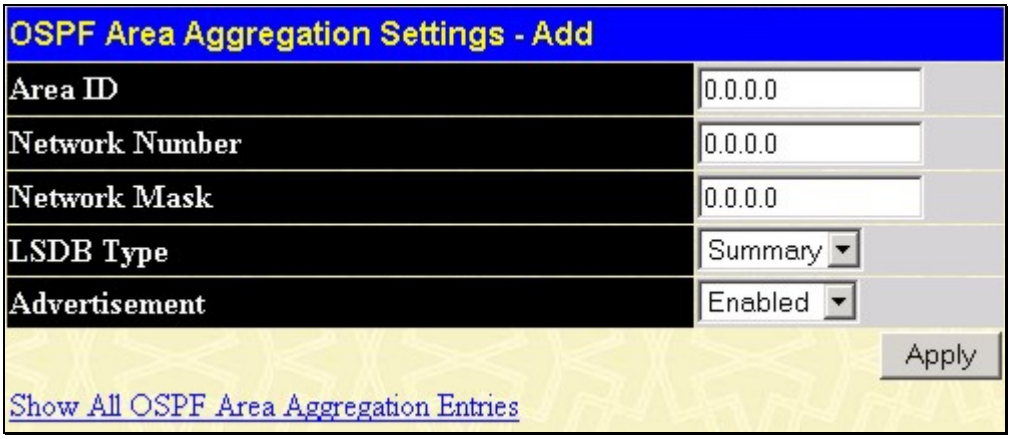


Figure 8- 39. OSPF Area Aggregation Settings - Add

Specify the OSPF aggregation settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Area Aggregation Settings** table. To view the table, click the Show All OSPF Aggregation Entries link to return to the previous window.

Use the following parameters to configure the following settings for **OSPF Area Aggregation Settings**:

Parameter	Description
Area ID	Allows the entry the OSPF Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the Switch.
Network Number	Sometimes called the Network Address. The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area above.
Network Mask	The corresponding network mask for the Network Number specified above.
LSDB Type	Use the drop-down menu to set the type of address aggregation. Choose *Summary* to specify that a summary Link State Database will be used. Choose *NSSA* to specify that a Not So Stubby Area Database will be used.

Advertisement	Select *Enabled* or *Disabled* to determine whether the selected OSPF Area will advertise it's summary LSDB (Network-Number and Network-Mask).

Click **Apply** to implement changes made.

OSPF Host Route Settings

OSPF host routes work in a way analogous to RIP, only this is used to share OSPF information with other OSPF routers. This is used to work around problems that might prevent OSPF information sharing between routers. To configure OSPF host routes, click the **OSPF Host Route Settings** link. To add a new OSPF Route, click the **Add** button. Configure the setting in the menu that appears. The **Add** and **Modify** menus for OSPF host route setting are nearly identical. The difference being that if you are changing an existing configuration you will be unable to change the **Host Address**. To change an existing configuration, click on the hyperlinked **Host Address** in the list for the configuration to change and proceed to change the metric or area ID. To eliminate an existing configuration, click the ✕ in the **Delete** column for the configuration being removed.

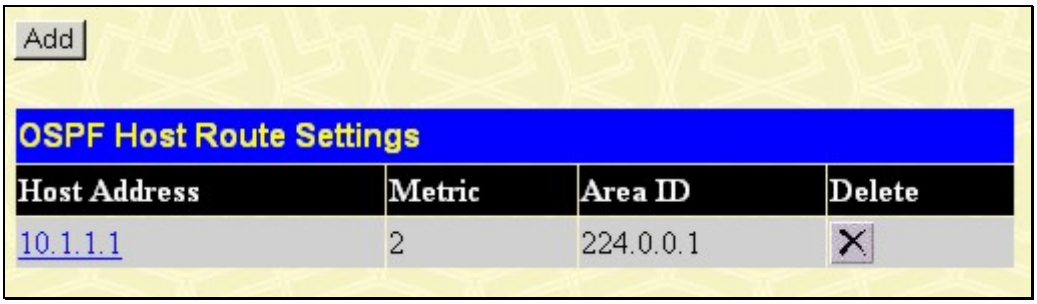


Figure 8- 40. OSPF Host Route Settings table

Use the menus below to add or edit OSPF host routes.

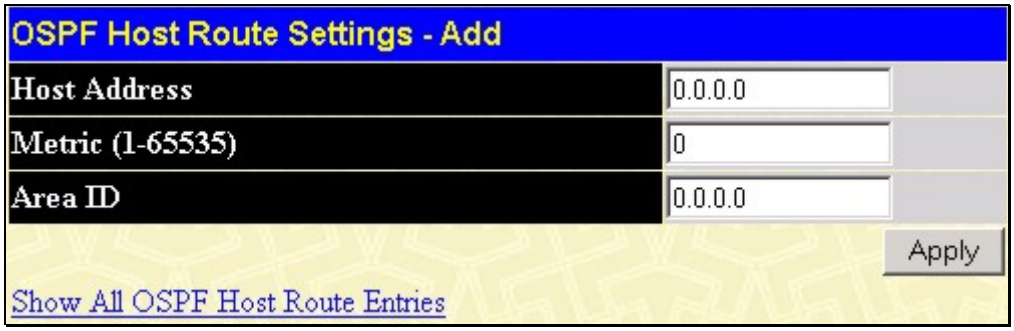


Figure 8- 41. OSPF Host Route Settings - Add

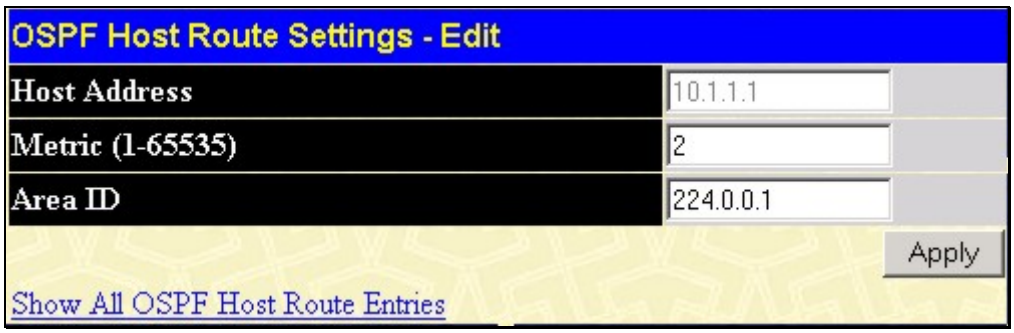


Figure 8- 42. OSPF Host Route Settings - Edit

Specify the host route settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Host Route Settings** list. To view the previous window, click the Show All OSPF Host Route Entries link to return to the previous window.

The following fields are configured for OSPF host route:

Parameter	Description
Host Address	The IP address of the OSPF host.

Metric	A value between 1 and 65535 that will be advertised for the route.
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

OSPF Default Information Originate Settings

To access the OSPF Default Information Originate Settings, click **L3 features** > **OSPF** > **OSPF Default Information Originate Settings**.

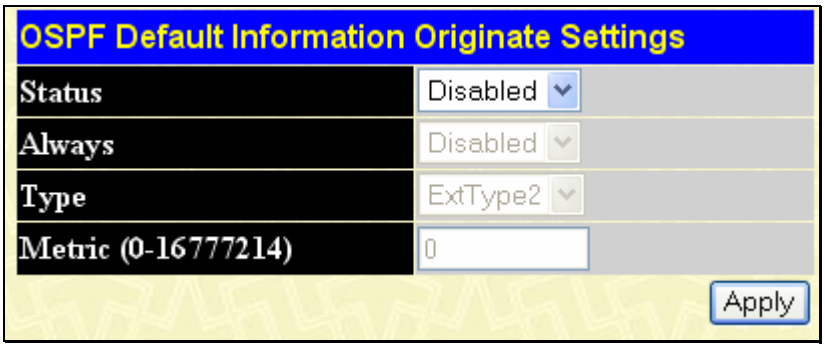


Figure 8- 43. OSPF Default Information Originate Settings window

The following parameters may be configured.

Parameter	Description
Status	Select *Enabled* from the drop-down menu to allow the generation and advertisement of the default route into OSPF. Select *Disabled* to disable.
Always	Choose *Enabled* from the drop-down menu to specify that the advertising router should advertise its default route into OSPF, if it has one set in its configuration. If the advertising router doesn't have a default-route it should generate a default route and advertise it into OSPF. If *Disabled* is chosen from the drop-down menu, the default route will only be advertised when the default route exists in the redistributed routes.
Type	This parameter specifies the type of AS external route. OSPF supports two types of external metrics. Choose the OSPF Default Information Originate type from the drop-down menu: *ExtType1* *ExtType2*
Metric (0-16777214)	Specifies the cost of default route to be advertised into OSPF. The range is 0 to 16777214. The metric value 0 will be set in OSPF as the metric value 20.

Click **Apply** to implement changes made.

DHCP Server

For this release of the xStack DES-3800, the Switch now has the capability to act as a DHCP server to devices which are located in its locally attached networks or relayed by DHCP relay agent. DHCP, or Dynamic Host Configuration Protocol, allows the switch to delegate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it returns a response to the client, containing the previously mentioned IP information that the DHCP client then utilizes and sets on its local configurations.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allotted IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the pool as not to make identical entries on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address.

To begin configuring the DHS-3828 as a DHCP Server, open the **L3 Features** folder, then the **DHCP Server** folder which will display 5 links to aid the user in configuring the DHCP server.

DHCP Server Global Settings

The following window will allow users to globally enable the switch as a DHCP server and set the DHCP Ping Settings to test connectivity between the DHCP Server and Client. To view this window, click **L3 features** > **DHCP Server** > **DHCP Server Global Settings**.

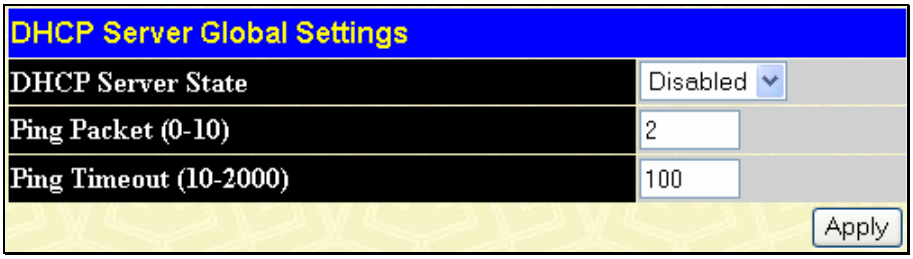


Figure 8- 44. DHCP Server Global Settings window

The following parameters may be configured.

Parameter	Description
DHCP Server State	Use the Pull-down menu to globally enable or disable the switch as a DHCP server. If DHCP relay is enabled, the DHCP server can not be enabled. The opposite is also true.
Ping Packet (0-10)	Enter a number between 0-10 to denote the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. The default setting is 2 packets.
Ping Timeout (10-2000)	The user may set a time between 10-2000 milliseconds that the Switch will wait before timing out a ping packet. The default setting is 100 milliseconds.

Click **Apply** to implement changes made.

DHCP Server Pool Settings

The following windows will allow users to create and then set the parameters for the DHCP Pool of the switch's DHCP server. Users must first create the pool by entering a name of up to 12 alphanumeric characters into the **Pool Name** field and clicking **Apply**. Once created, users can modify the settings of a poll by clicking its corresponding **Modify** button. To view the following window, click **L3 features > DHCP Server > DHCP Server Pool Settings.**

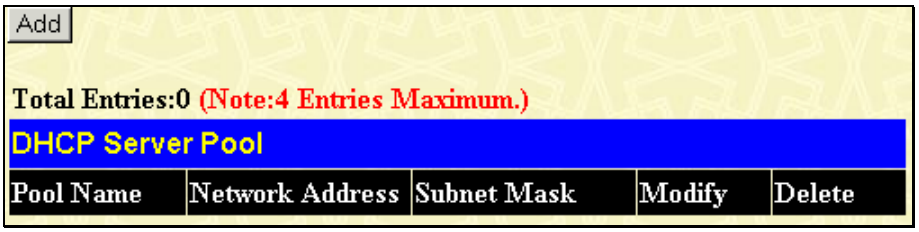


Figure 8- 45. DHCP Pool Table window

Click the **Add** button to add the settings for the specific DHCP pool table.

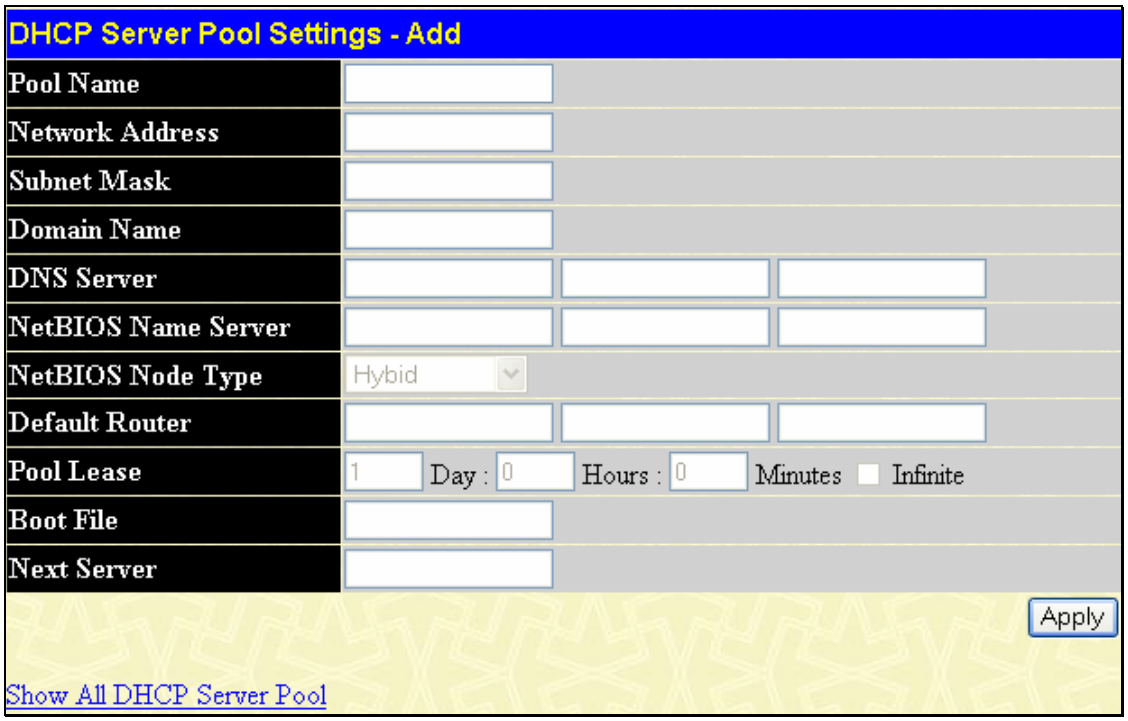


Figure 8- 46. DHCP Server Pool Settings - Add window.

The following parameters may be configured or viewed.

Parameter	Description
Pool Name	Denotes the name of the DHCP pool for which you are currently adjusting the parameters.
Network Address	Enter the Network address to be assigned to requesting DHCP Clients. This address will not be chosen but the first 3 sets of numbers in the Network address will be used for the Network address of requesting DHCP Clients. (ex. If this entry is given the Network address 10.10.10.2, then assigned addresses to DHCP Clients will resemble 10.10.10.x, where x is a number between 1-255 but does not include the assigned 10.10.10.2)
Subnet Mask	Enter the corresponding Subnet Mask of the IP address assigned above.
Domain Name	Enter the domain name for the DHCP client. This domain name represents a general group of networks that collectively make up the domain. The Domain Name may be an alphanumeric string of up to 64 characters.
DNS Server	Enter the IP address of a DNS server that is available to the DHCP client. The DNS Server correlates IP addresses to host names when queried. Users may add up to 3 DNS Server

	addresses.
Net BIOS Name Server	Enter the IP address of a Net BIOS Name Server that will be available to a Microsoft DHCP Client. This Net BIOS Name Server is actually a WINS (Windows Internet Naming Service) Server that allows Microsoft DHCP clients to correlate host names to IP addresses within a general grouping of networks. The user may establish up to 3 Net BIOS Name Servers.
NetBIOS Node Type	This field will allow users to set the type of node server for the previously configured Net BIOS Name server. Using the pull-down menu, the user has for node type choices which are *Broadcast*, *Peer to Peer*, *Mixed* and *Hybrid*.
Default Router	Enter the IP address of the default router for a DHCP Client. Users must configure at least one address here, yet up to three IP addresses can be configured for this field. The IP address of the default router must be on the same subnet as the DHCP client.
Pool Lease	Using this field, the user can specify the lease time for the DHCP client. This time represents the amount of time that the allotted address is valid on the local network. Users may set the time by entering the days into the open field and then use the pull-down menus to precisely set the time by hours and minutes. Users may also use the **Infinite** check box to set the allotted IP address to never be timed out of its lease. The default setting is 1 day.
Boot File	This field is used to specify the Boot File that will be used as the boot image of the DHCP client. This image is usually the operating system that the client uses to load its IP parameters.
Next Server	This field is used to identify the IP address of the device that has the previously stated boot file.

Click **Apply** to implement changes made.

DHCP Server Manual Binding Settings

The following windows will allow users to view and set manual DHCP entries. Manual DHCP entries will bind an IP address with the MAC address of a device within a DHCP pool. These entries are necessary for special devices on the local network which will always require a static IP address that cannot be changed. To view this window, click **L3 features > DHCP Server > DHCP Server Manual Binding Settings.**

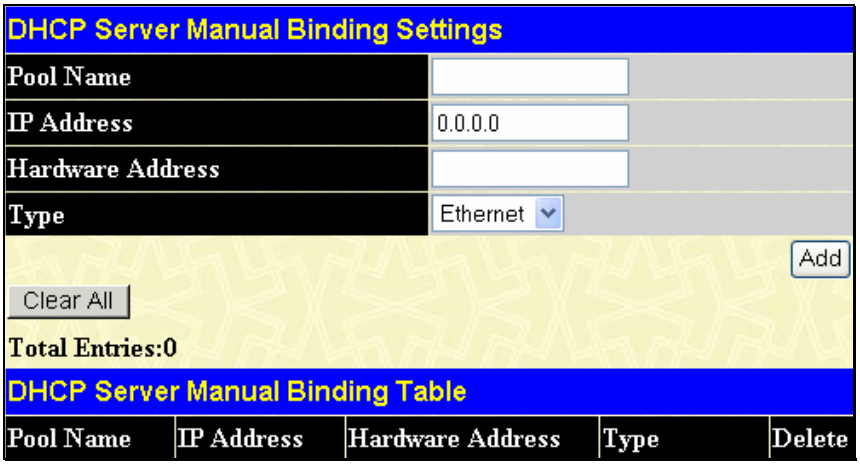


Figure 8- 47. DHCP Server Manual Binding Settings and DHCP Server Manual Binding Table

Users may set a manual DHCP Binding entry by entering the information and clicking **Add**. To clear an entry click the **Clear All** button.

The following parameters may be configured or viewed.

Parameter	Description
Pool Name	Enter the name of the DHCP pool within which will be created a manual DHCP binding entry.
IP Address	Enter the IP address to be statically bound to a device within the local network that will be specified by entering the Hardware Address in the following field.
Hardware Address	Enter the MAC address of the device to be statically bound to the IP address entered in the previous field.
Type	This field is used to specify the type of connection for which this manually bound entry will be set. *Ethernet* will denote that the manually bound device is connected directly to the Switch, while the *IEEE802* denotes that the manually bound device is outside the local network of the Switch.

Click **Apply** to set the entry.

DHCP Server Excluded Address Settings

The following window will allow the user to set an IP address, or a range of IP addresses that are NOT to be included in the range of IP addresses that the Switch will allot to clients requesting DHCP service. To view this window, click **L3 features > DHCP Server > DHCP Server Excluded Address Settings.** To set an IP address or range of IP addresses, enter the **Begin Address** of the range and then the **End Address** of the range and click **Apply**. Set address ranges will appear in the **DHCP Excluded Address Table** in the bottom half of the screen, as shown below.

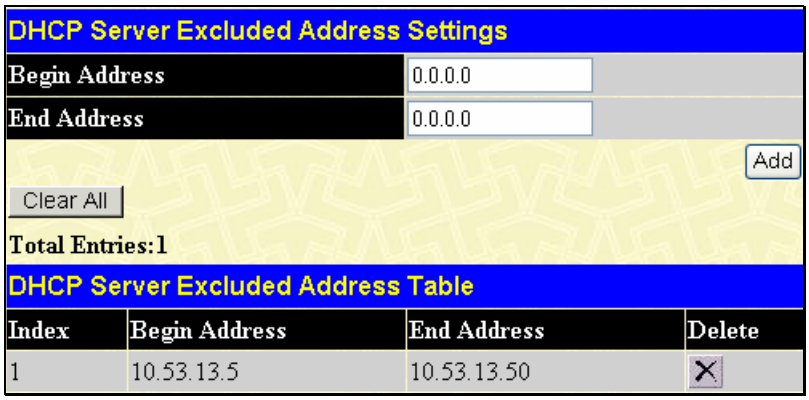


Figure 8- 48. DHCP Server Excluded Address Settings and DHCP Server Excluded Address Table window

DHCP Server Conflict IP Table

The following window will allow users to delete IP addresses that conflict with the DHCP server. To view this window, click **L3 features > DHCP Server > DHCP Server Conflict IP Table.** To delete an entry enter the IP address and click on the **Delete** button, to clear all conflicting IP addresses click the **Clear All** button.

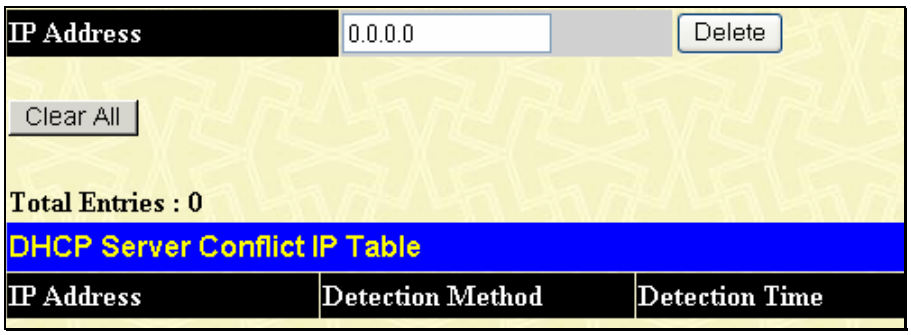


Figure 8- 49. DHCP Server Conflict IP Table

DHCP Server Binding Table

The following window will allow users to view dynamically bound IP addresses of the DHCP server. These IP addresses are ones that were allotted to clients on the local network and are now bound to the device stated by its MAC address. To view this window, click **L3 features > DHCP Server > DHCP Server Binding Table.**

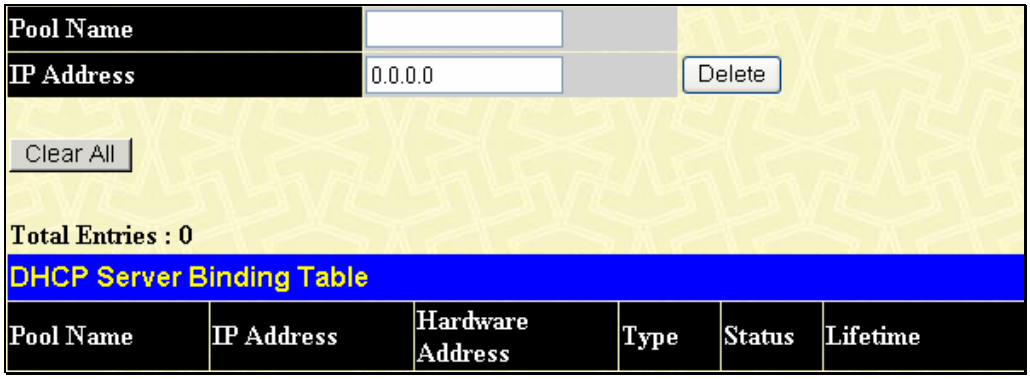


Figure 8- 50. DHCP Server Binding Table window

The DHCP Server Binding window is divided into two sections. The top section allows the administrator to delete an existing DHCP Server Binding Entry and the bottom section displays the DHCP Server Binding Table Entries.

The following parameters may be configured at the top of the window:

Parameter	Description
Pool Name	To find the bound entries of a specific pool, enter the Pool Name into the field.
IP Address	To find the bound entries of a specific pool, enter the IP Address in the field. DHCP Server binding entries of this pool will be displayed in the table. To clear the corresponding Pool Name and IP Address entries of this table, click **Clear**. To clear all entries, click **Clear All**.

The following parameters appear in the DHCP Server Binding Table:

Parameter	Description
Pool Name	This field will denote the Pool Name of the displayed dynamically bound DHCP entry.
IP address	This field will display the IP address allotted to this device by the DHCP Server feature of this Switch.
Hardware Address	This field will display the MAC address of the device that is bound to the corresponding IP address.
Type	This field will display the type of node server being used for the previously configured Net BIOS Name server of this entry.
Status	This field will display the Status of the entry, whether it was dynamically bound or manually bound.
Life Time	This field will display, in seconds, the time remaining on the lease for this IP address.

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 second's 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 **L3 Features > DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Global Settings**:

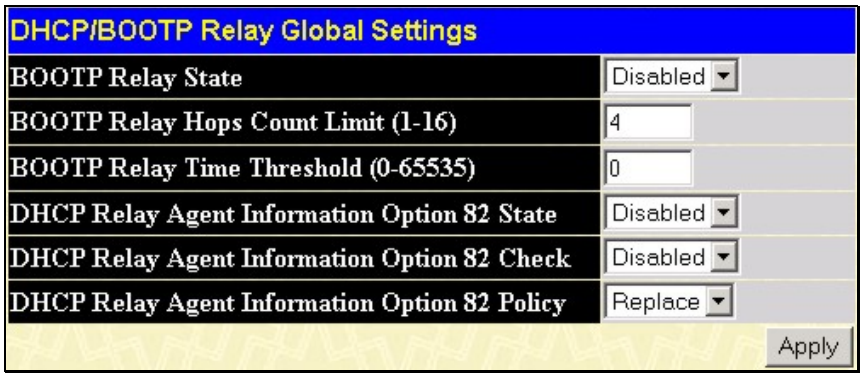


Figure 8- 51. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
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.* If the DHCP server is enabled, DHCP relay can not be enabled. The opposite is also true.
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*.
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 second's 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 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 Agent Information Option 82 Check	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. This 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 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, users may configure a client with the option-82 field. In this situation, disable the information-check feature so that the Switch does not remove the option-82 field from the packet. Users may configure the action that the Switch takes when it receives a packet with existing option-82 information by configuring the **DHCP Agent Information Option 82 Policy.**

The Implementation of DHCP Information Option 82 in DES-3828P/DES-3828DC

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

1. Sub-option type
2. Length
3. Circuit ID type
4. Length
5. VLAN: the incoming VLAN ID of DHCP client packet.
6. Module: For a standalone switch, the Module is always 0; For a stackable switch, the Module is the Unit ID.

7. Port: The incoming port number of 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 8- 52. Circuit ID and Remote ID Sub-option Format

DHCP/BOOTP Relay Interface Settings

The **DHCP/ BOOTP Relay Interface Settings** allow the user to set up a server, by IP address, for relaying DHCP/ BOOTP information. 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 **BOOTP Relay Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking it's corresponding ✕. To enable and configure **DHCP/BOOTP Relay Interface Settings** on the Switch, click **L3 Features > DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Interface Settings**:

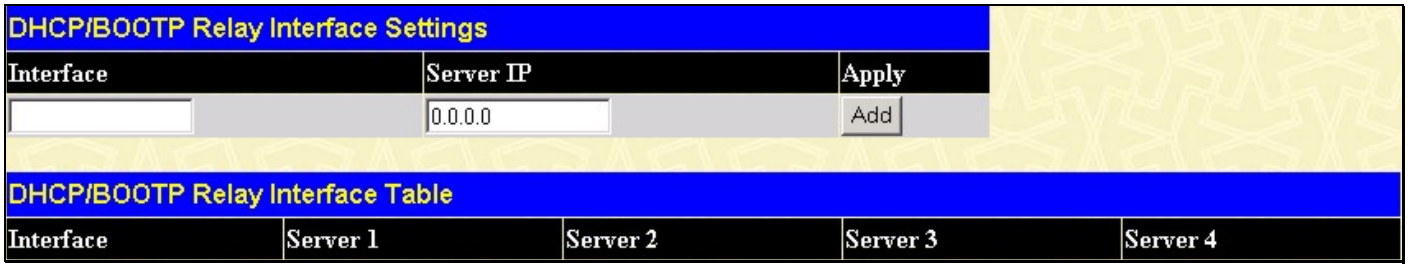


Figure 8- 53. DHCP/BOOTP Relay Interface Settings and DHCP/BOOTP Relay Interface Table window

NOTE: The secondary IP interface does not support DHCP/BOOTP relay. Only the primary IP interface supports DHCP/BootP relay.

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

DNS Relay

Computer users usually prefer to use text names for computers for which they may want to open a connection. Computers themselves, require 32 bit IP addresses. Somewhere, a database of network devices' text names and their corresponding IP addresses must be maintained.

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets.

For two DNS servers to communicate across different subnets, the **DNS Relay** of the Switch must be used. The DNS servers are identified by IP addresses.

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name server. The client program is called a Name resolver. A Name resolver may need to contact several Name servers to translate a name to an address.

The Domain Name System (DNS) servers are organized in a somewhat hierarchical fashion. A single server often holds names for a single network, which is connected to a root DNS server - usually maintained by an ISP.

Domain Name Resolution

The domain name system can be used by contacting the name servers one at a time, or by asking the domain name system to do the complete name translation. The client makes a query containing the name, the type of answer required, and a code specifying whether the domain name system should do the entire name translation, or simply return the address of the next DNS server if the server receiving the query cannot resolve the name.

When a DNS server receives a query, it checks to see if the name is in its sub domain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution and requires the server to contact other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it returns the address of the next DNS server the client should contact.

Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

The address of the machine that supplies domain name service is often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Relay Global Settings

To configure the DNS function on the Switch, click **L3 Features > DNS Relay > DNS Relay Global Settings**, which will open the **DNS Relay Global Settings** window, as seen below:

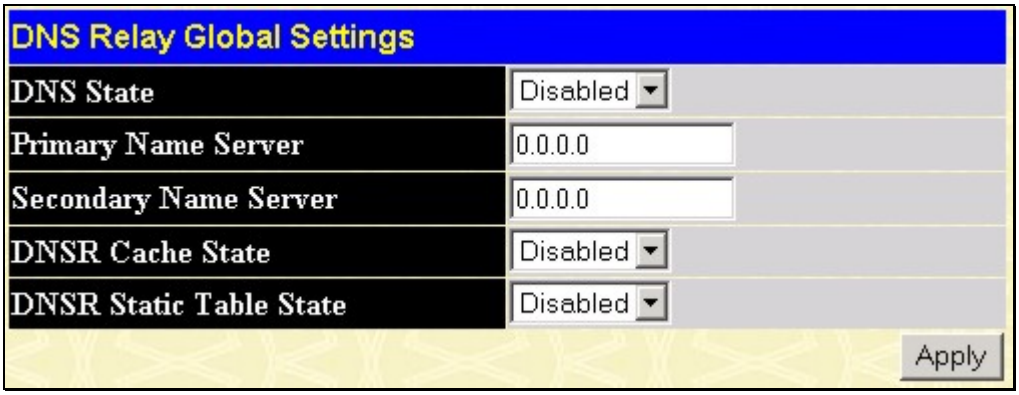


Figure 8- 54. DNS Relay Global Settings window

The following fields can be set:

Parameter	Description
DNS State	This field can be toggled between *Disabled* and *Enabled* using the pull-down menu, and is used to enable or disable the DNS Relay service on the Switch.

Primary Name Server	Allows the entry of the IP address of a primary domain name server (DNS).
Secondary Name Server	Allows the entry of the IP address of a secondary domain name server (DNS).
DNSR Cache Status	This can be toggled between *Disabled* and *Enabled.* This determines if a DNS cache will be enabled on the Switch.
DNSR Static Table State	This field can be toggled using the pull-down menu between *Disabled* and *Enabled.* This determines if the static DNS table will be used or not.

Click **Apply** to implement changes made.

DNS Relay Static Settings

To view the **DNS Relay Static Settings**, click **L3 Features > DNS Relay > DNS Relay Static Settings**, which will open the **DNS Relay Static Settings** window, as seen below:

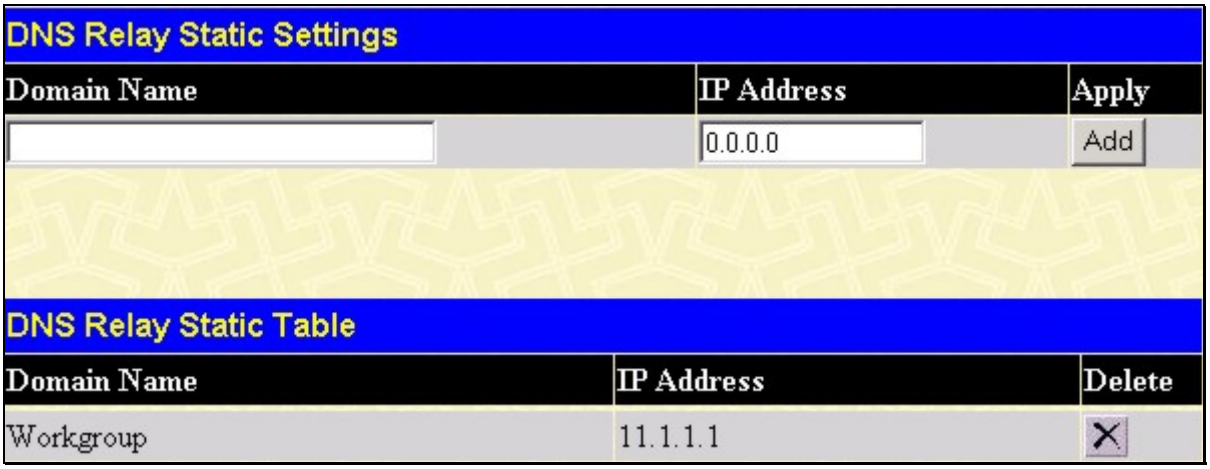


Figure 8- 55. DNS Relay Static Settings

To add an entry into the **DNS Relay Static Table**, simply enter a **Domain Name** with its corresponding IP address and click **Add** under the **Apply** heading. A successful entry will be presented in the table below, as shown in the example above. To erase an entry from the table, click its corresponding ✕ under the Delete heading.

VRRP

VRRP or *Virtual Routing Redundancy Protocol* is a function on the Switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the Switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the Switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

VRRP Global Settings

To enable VRRP globally on the Switch, click **L3 Features > VRRP > VRRP Global Settings**:

Figure 8- 56. VRRP Global Settings window

The following fields can be set:

Parameter	Description
VRRP State	Use the pull-down menu to enable or disable VRRP globally on the Switch. The default is *Disabled*.
Non-Owner Response Ping	Enabling this parameter will allow the virtual IP address to be pinged from other host end nodes to verify connectivity. This will only enable the ping connectivity check function. This command is *Disabled* by default.

Click **Apply** to implement changes made.

VRRP Virtual Router Settings

The following window will allow the user to view the parameters for the VRRP function on the Switch. To view this window, click **L3 Features > VRRP > VRRP Virtual Router Settings**:

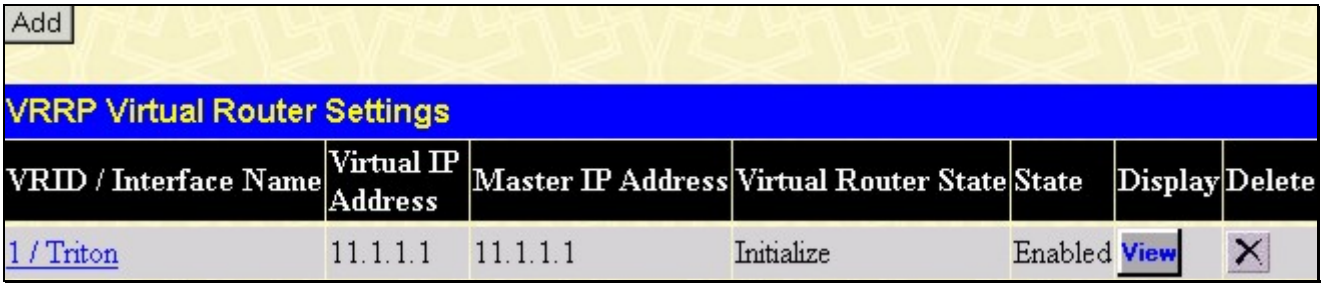


Figure 8- 57. VRRP Virtual Router Settings window

The following fields are displayed in the window above:

Parameter	Description
VRID / Interface Name	*VRID* - Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network. *Interface Name* - An IP interface name that has been enabled for VRRP. This entry must have been previously set in the IP Interfaces table.
Virtual IP Address	The IP address of the Virtual router configured on the Switch.
Master IP Address	Displays the IP address of the Master router for the VRRP function.
Virtual Router State	Displays the current state of the Virtual Router on the Switch. Possible states include *Initialize*, *Master* and *Backup.*
State	Displays the VRRP state of the corresponding VRRP entry.
Display	Click the View button to display the settings for this particular VRRP entry.
Delete	Click the ✕ to delete this VRRP entry.

Click the **Add** button to display the following window to configure a VRRP interface.

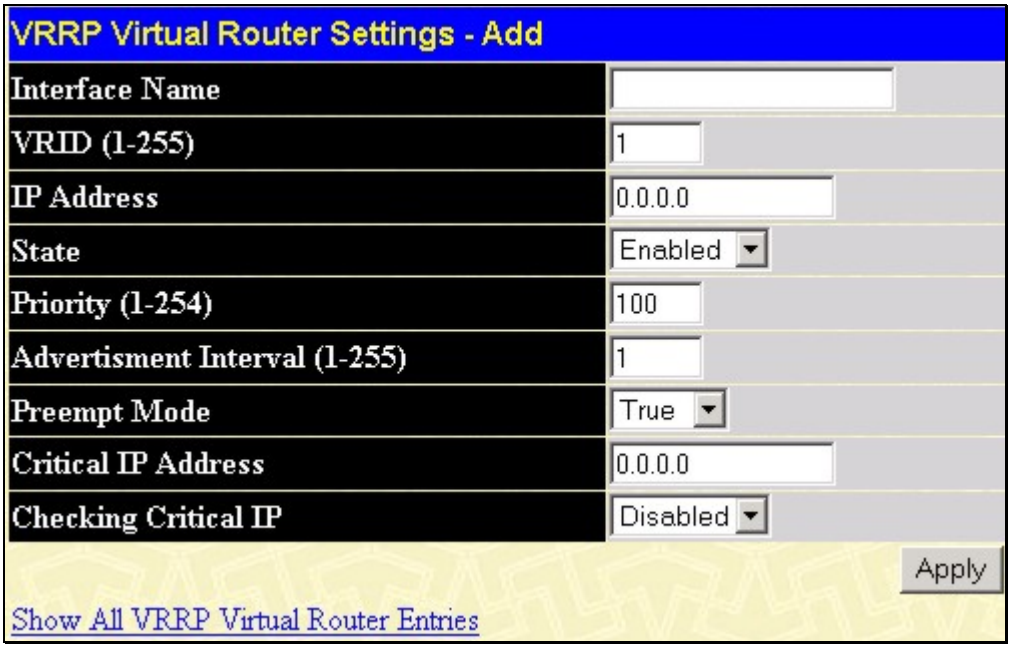


Figure 8- 58. VRRP Virtual Router Settings - Add

Or, the user may click the hyperlinked **Interface Name** to view the same window:

The following parameters may be set to configure an existing or new VRRP interface.

Parameter	Description
Interface Name	Enter the name of a previously configured IP interface for which to create a VRRP entry. This IP interface must be assigned to a VLAN on the Switch.
VRID (1-255)	Enter a value between *1* and *255* to uniquely identify this VRRP group on the Switch. All routers participating in this group must be assigned the same **VRID** value. This value MUST be different from other VRRP groups set on the Switch.
IP Address	Enter the IP address that will be assigned to the VRRP router. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.

State	Used to enable (Up) and disable (Down) the VRRP IP interface on the Switch.
Priority (1-254)	Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.)
Advertisement Interval (1-255)	Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all participating routers. The default is 1 second.
Preempt Mode	This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A *True* entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A *False* entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is *True*.
Critical IP Address	Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.
Checking Critical IP	Use the pull-down menu to enable or disable the Critical IP address entered above.

Click **Apply** to implement changes made.

To view the settings for a particular VRRP setting, click the corresponding View in the **VRRP Interface Table** of the entry, which will display the following:

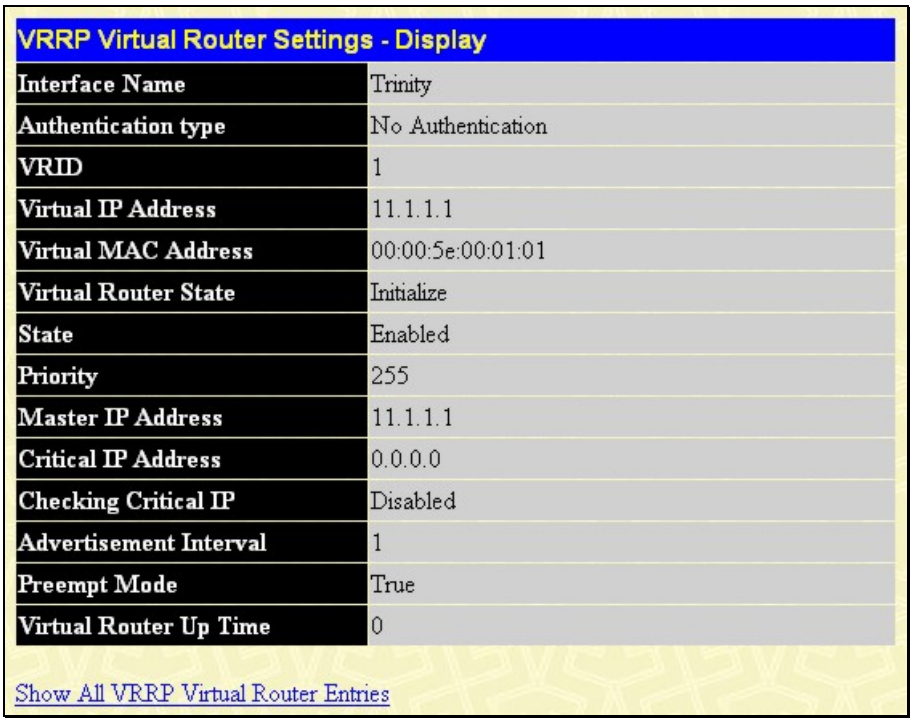


Figure 8- 59. VRRP Virtual Router Settings - Display window

This window displays the following information:

Parameter	Description
Interface Name	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the IP Interface Settings table.
Authentication type	Displays the type of authentication used to compare VRRP packets received by a virtual router. Possible authentication types include: • *No authentication* - No authentication has been selected to compare VRRP packets received by a virtual router. • *Simple Text Password* - A *Simple* password has been selected to compare VRRP packets received by a virtual router, for authentication. • *IP Authentication Header* - An MD5 message digest algorithm has been selected to compare VRRP packets received by a virtual router, for authentication.
VRID	Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.
Virtual IP Address	The IP address of the Virtual router configured on the Switch.
Virtual MAC Address	The MAC address of the device that holds the Virtual router.
Virtual Router State	Displays the current status of the virtual router. Possible states include *Initialize*, *Master* and *Backup.*
Admin. State	Displays the current state of the router. *Up* will be displayed if the virtual router is enabled and *Down,* if the virtual router is disabled.
Priority	Displays the priority of the virtual router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. The lower the number, the higher the priority.
Master IP Address	Displays the IP address of the Master router for the VRRP function.
Critical IP Address	Displays the critical IP address of the VRRP function. This address will judge if a virtual router is qualified to be a master router.
Checking Critical IP	Displays the status of the Critical IP address. May be enabled or disabled.
Advertisement Interval	Displays the time interval, in seconds, which VRRP messages are sent out to the network.
Preempt Mode	Displays the mode for determining the behavior of backup routers set on this VRRP interface. *True* will denote that this will be the backup router, if the routers priority is set higher than the master router. *False* will disable the backup router from becoming the master router.
Virtual Router Up Time	Displays the time, in minutes, since the virtual router has been initialized

VRRP Authentication Settings

The **VRRP Authentication Settings** window is used to set the authentication for each Interface configured for VRRP. This authentication is used to identify incoming message packets received by a router. If the authentication is not consistent with incoming packets, they will be discarded. The **Authentication Type** must be consistent with all routers participating within the VRRP group.

To view the following window, click **L3 Features > VRRP > VRRP Authentication Settings**.

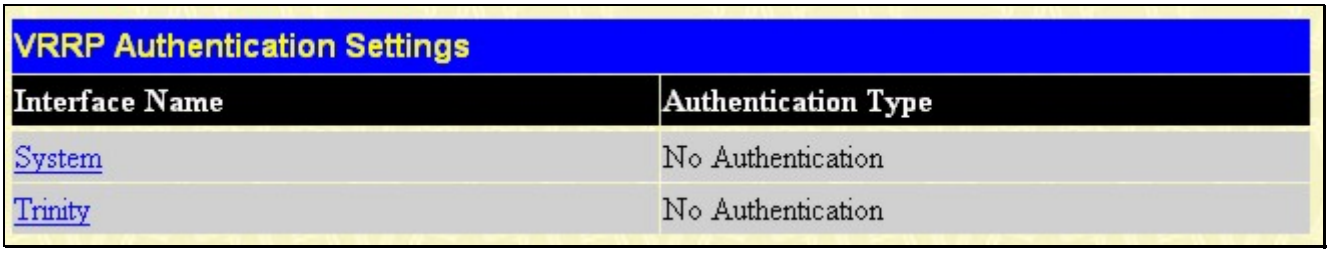


Figure 8- 60. VRRP Authentication Settings window

To configure the authentication for a pre-created interface, click its hyperlinked name, revealing the following window to configure:

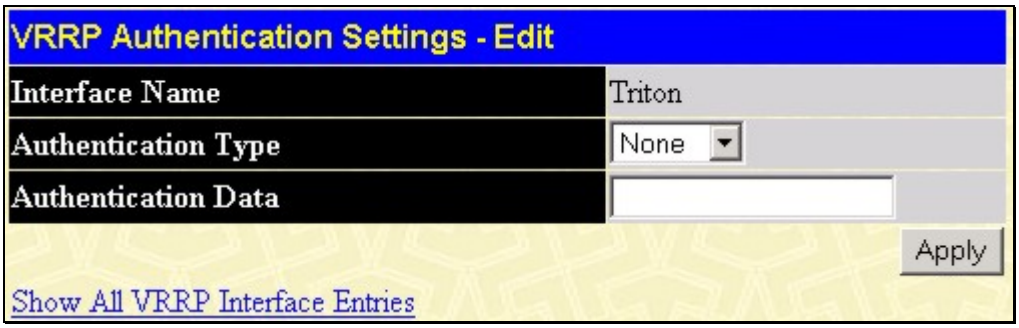


Figure 8- 61. VRRP Authentication Settings – Edit window

The following parameters may be viewed or configured:

Parameter	Description
Interface Name	The name of a previously created IP interface for which to configure the VRRP authentication.
Authentication Type	Specifies the type of authentication used. The **Authentication Type** must be consistent with all routers participating within the VRRP group. The choices are: • *None* - Selecting this parameter indicates that VRRP protocol exchanges will not be authenticated. • *Simple* - Selecting this parameter will require the user to set a simple password in the Auth. Data field for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped. • *IP* - Selecting this parameter will require the user to set a MD5 message digest for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
Authentication Data	This field is only valid if the user selects *Simple* or *IP* in the **Authentication Type** field. • *Simple* will require the user to enter an alphanumeric string of no more than eight characters to identify VRRP packets received by a router. • *IP* will require the user to enter a MD5 message digest for authentication in comparing VRRP messages received by the router. This entry must be consistent with all routers participating in the same IP interface.

Click **Apply** to implement changes made.

IP Multicast Routing Protocol

The functions supporting IP multicasting are added under the **IP Multicast Routing Protocol** folder, from the **L3 Features** folder. **IGMP**, **DVMRP**, and **PIM-DM** can be enabled or disabled on the Switch without changing the individual protocol's configuration by using the **DES-3800 Web Management Tool**.

IGMP

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP**) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active.

In the case where there is more than one multicast router on a sub-network, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub-network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given sub-network. If there are no members on a sub-network, packets will not be forwarded to that sub-network.

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

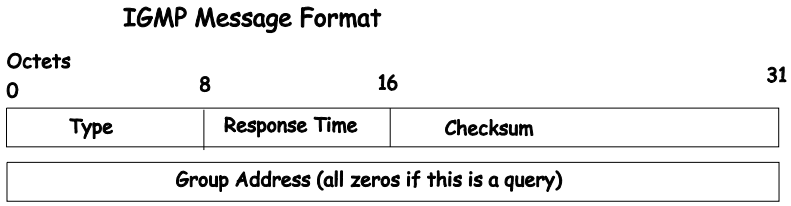


Figure 8- 62. IGMP Message Format

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

Table 8- 4. IGMP Type Codes

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub-networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP "report" to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a "leave" report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub-networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub-networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast querier for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

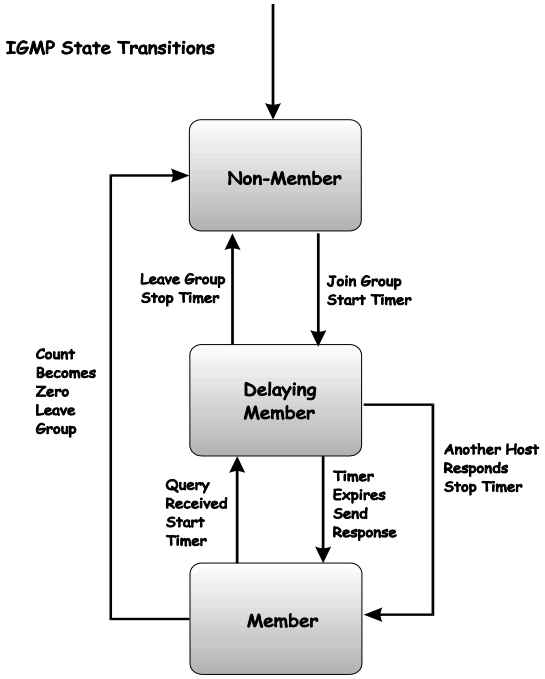


Figure 8- 63. IGMP State Transitions

IGMP Version 3

The current release of the xStack DES-3800 switch series now implements IGMPv3. Improvements of IGMPv3 over version 2 include:

- The introduction of the *SSM* or *Source Specific Multicast*. In previous versions of IGMP, the host would receive all packets sent to the multicast group. Now, a host will receive packets only from a specific source or sources. This is done through the implementation of *include* and *exclude* filters used to accept or deny traffic from these specific sources.
- In IGMP v2, Membership reports could contain only one multicast group whereas in v3, these reports can contain multiple multicast groups and multiple sources within the multicast group.
- Leaving a multicast group could only be accomplished using a specific leave message in v2. In v3, leaving a multicast group is done through a Membership report which includes a block message in the group report packet.
- For version 2, the host could respond to a group query but in version 3, the host is now capable to answer queries specific to the group and the source.

IGMP v3 is backwards compatible with other versions of IGMP.

The IGMPv3 Type supported codes are shown below:

Type	Meaning
0x11	Membership Query
0x12	Version 1 Membership Report
0x16	Version 2 Membership Report
0x17	Version 2 Leave Group
0x22	IGMPv3 Membership Report

Timers

As previously mentioned, IGMPv3 incorporates filters to include or exclude sources. These filters are kept updated using timers. IGMPv3 utilizes two types of timers, one for the group and one for the source. The purpose of the filter mode is to reduce the reception state of a multicast group so that all members of the multicast group are satisfied. This filter mode is dependant on membership reports and timers of the multicast group. These filters are used to maintain a list of multicast sources and groups of multicast receivers that more accurately reflect the actual sources and receiving groups at any one time on the network.

Source timers are used to keep sources present and active within a multicast group on the Switch. These source timers are refreshed if a group report packet is received by the Switch, which holds information pertaining to the active source group record part of a report packet. If the filter mode is set to exclude, traffic is being denied from at least one specific source, yet other hosts may be accepting traffic from the multicast group. If the group timer expires for the multicast group, the filter mode is changed to include and other hosts can receive traffic from the source. If no group report packet is received and the filter mode is include, the Switch presumes that traffic from the source is no longer wanted on the attached network and the source record list is then deleted after all source timers expire. If there is no source list record in the multicast group, the multicast group will be deleted from the Switch.

Timers are also used for IGMP version 1 and 2 members, which are a part of a multicast group when the Switch is running IGMPv3. This timer is based on a host within the multicast group that is running IGMPv1 or v2. Receiving a group report from an IGMPv1 or v2 host within the multicast group will refresh the timer and keep the v1 and/or v2 membership alive in v3.

NOTE: The length of time for all timers utilized in IGMPv3 can be determined using IGMP configurations to perform the following calculation:

(Query Interval x Robustness Variable) + One Query Response Interval

IGMP Interface Settings

The Internet Group Multicasting Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. To view the **IGMP Interface Table**, click **L3 Features > IP Multicast Routing Protocol** > **IGMP Interface Settings.** Each IP interface configured on the Switch is displayed in the below **IGMP Interface Settings** dialog box. To configure IGMP for a particular interface, click the corresponding hyperlink for that IP interface. This will open another **IGMP Interface Settings – Edit** window:

IGMP Interface Settings

Interface Name	IP Address	Version	Query Interval	Max Response Time	Robustness Variable	Last Member Query Interval	State
System	10.53.13.52	3	125	10	2	1	Disabled
Trinity	11.1.1.1	3	125	10	2	1	Disabled

Figure 8- 64. IGMP Interface Settings window

IGMP Interface Settings - Edit

Interface Name	Triton
IP Address	11.1.1.1
Version	3
Query Interval (1- 31744)	125
Max Response Time (1-25)	10
Robustness Variable (1-255)	2
Last Member Query Interval (1-25)	1
State	Disabled

Apply

Show All IGMP Interface Entries

Figure 8- 65. IGMP Interface Settings – Edit window

This window allows the configuration of IGMP for each IP interface configured on the Switch. IGMP can be configured as Version 1, 2 or 3 by toggling the **Version** field using the pull-down menu. The length of time between queries can be varied by entering a value between 1 and 31,744 seconds in the **Query Interval** field. The maximum length of time between the receipt of a query and the sending of an IGMP response report can be varied by entering a value in the **Max Response Time** field.

The **Robustness Variable** field allows IGMP to be 'tuned' for sub-networks that are expected to lose many packets. A high value (max. 255) for the robustness variable will help compensate for 'lossy' sub-networks. A low value (min. 2) should be used for less 'lossy' sub-networks.

The following fields can be set:

Parameter	Description
Interface Name	Displays the name of the IP interface that is to be configured for IGMP. This must be a previously configured IP interface.
IP Address	Displays the IP address corresponding to the IP interface name above.
Version	Enter the IGMP version (1, 2 or 3) that will be used to interpret IGMP queries on the interface.
Query Interval (1-31744)	Allows the entry of a value between *1* and *31744* seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time (1-25)	Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered, with a default of 10 seconds.
Robustness Variable (1-255)	A tuning variable to allow for sub-networks that are expected to lose a large number of packets. A value between 1 and 255 can be entered, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.
Last Member Query Interval (1-25)	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.
State	This field can be toggled between *Enabled* and *Disabled* and enables or disables IGMP for the IP interface. The default is *Disabled*.

Click **Apply** to implement changes made.

DVMRP Interface Configuration

The Distance Vector Multicast Routing Protocol (**DVMRP**) is a hop-based method of building multicast delivery trees from multicast sources to all nodes of a network. Because the delivery trees are 'pruned' and 'shortest path', DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) relatively low bandwidth networks, and can be considered as a 'best-effort' multicasting protocol.

DVMRP resembles the Routing Information Protocol (RIP), but is extended for multicast delivery. DVMRP builds a routing table to calculate 'shortest paths' back to the source of a multicast message, but defines a 'route cost' (similar to the hop count in RIP) as a relative number that represents the real cost of using this route in the construction of a multicast delivery tree to be 'pruned' - once the delivery tree has been established.

When a sender initiates a multicast, DVMRP initially assumes that all users on the network will want to receive the multicast message. When an adjacent router receives the message, it checks its unicast routing table to determine the interface that gives the shortest path (lowest cost) back to the source. If the multicast was received over the shortest path, then the adjacent router enters the information into its tables and forwards the message. If the message is not received on the shortest path back to the source, the message is dropped.

Route cost is a relative number that is used by DVMRP to calculate which branches of a multicast delivery tree should be 'pruned'. The 'cost' is relative to other costs assigned to other DVMRP routes throughout the network.

The higher the route cost, the lower the probability that the current route will be chosen to be an active branch of the multicast delivery tree (not 'pruned') - if there is an alternative route.

DVMRP Global Settings

To enable DVMRP globally on the Switch, click **L3 Features > IP Multicast Routing Protocol > DVMRP Global Settings**. This will give the user access to the following screen:

Figure 8- 66. DVMRP Global Settings window

Use the pull down menu, choose *Enabled*, and click **Apply** to implement the DVMRP function on the Switch.

DVMRP Interface Settings

To view the **DVMRP Interface Table**, click **L3 Features > IP Multicast Routing Protocol > DVMRP Interface Settings**. This menu allows the **Distance-Vector Multicast Routing Protocol (DVMRP)** to be configured for each IP interface defined on the Switch. Each IP interface configured on the Switch is displayed in the below **DVMRP Interface Configuration** dialog box. To configure DVMRP for a particular interface, click the corresponding hyperlink for that IP interface. This will open the **DVMRP Interface Settings** window:

DVMRP Interface Settings

Interface Name	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.53.13.83	35	10	1	Disabled
Triton	11.1.1.1	35	10	1	Disabled

Figure 8- 67. DVMRP Interface Settings window

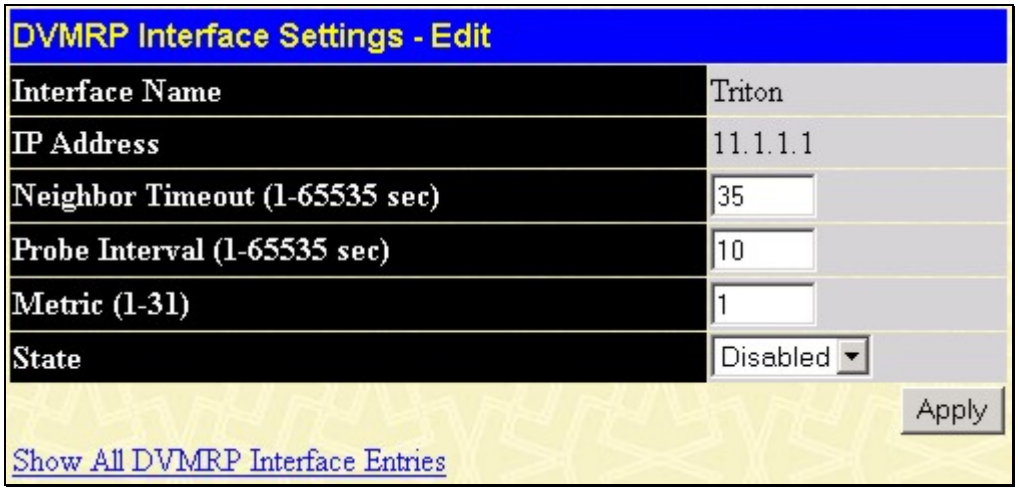


Figure 8- 68. DVMRP Interface Settings - Edit window

The following fields can be set:

Parameter	Description
Interface Name	Displays the name of the IP interface for which DVMRP is to be configured. This must be a previously defined IP interface.
IP Address	Displays the IP address corresponding to the IP Interface name entered above.
Neighbor Timeout Interval (1-65535 sec)	This field allows an entry between *1* and *65,535* seconds and defines the time period DVMRP will hold Neighbor Router reports before issuing poison route messages. The default is *35* seconds.
Probe Interval (1-65535 sec)	This field allows an entry between *1* and *65,535* seconds and defines the interval between 'probes'. The default is *10*.
Metric (1-31)	This field allows an entry between *1* and *31* and defines the route cost for the IP interface. The DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default cost is *1*.
State	This field can be toggled between *Enabled* and *Disabled* and enables or disables DVMRP for the IP interface. The default is *Disabled*.

Click **Apply** to implement changes made. Click Show All DVMRP Interface Entries to return to the **DVMRP Interface Settings** window.

PIM Protocol

PIM or *Protocol Independent Multicast* is a method of forwarding traffic to multicast groups over the network using any pre-existing unicast routing protocol, such as RIP or OSPF, set on routers within a multicast network. The xStack DES-3800 Series supports two types of PIM, Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).

PIM-SM

PIM-SM or *Protocol Independent Multicast – Sparse Mode* is a method of forwarding multicast traffic over the network only to multicast routers who actually request this information. Unlike most multicast routing protocols which flood the network with multicast packets, PIM-SM will forward traffic to routers who are explicitly a part of the multicast group through the use of a Rendezvous Point (RP). This RP will take all requests from PIM-SM enabled routers, analyze the information and then returns multicast information it receives from the source, to requesting routers within its configured network. Through this method, a distribution tree is created, with the RP as the root. This distribution tree holds all PIM-SM enabled routers within which information collected from these router is stored by the RP.

Two other types of routers also exist with the PIM-SM configuration. When many routers are a part of a multiple access network, a Designated Router (DR) will be elected. The DR's primary function is to send Join/Prune messages to the RP. The router with the highest priority on the LAN will be selected as the DR. If there is a tie for the highest priority, the router with the higher IP address will be chosen.

The third type of router created in the PIM-SM configuration is the Boot Strap Router (BSR). The goal of the Boot Strap Router is to collect and relay RP information to PIM-SM enabled routers on the LAN. Although the RP can be statically set, the BSR mechanism can also determine the RP. Multiple Candidate BSRs (C-BSR) can be set on the network but only one BSR will be elected to process RP information. If it is not explicitly apparent which C-BSR is to be the BSR, all C-BSRs will emit Boot Strap Messages (BSM) out on the PIM-SM enabled network to determine which C-BSR has the higher priority and once determined, will be elected as the BSR. Once determined, the BSR will collect RP data emanating from candidate RPs on the PIM-SM network, compile it and then send it out on the land using periodic Boot Strap Messages (BSM). All PIM-SM Routers will get the RP information from the Boot Strap Mechanism and then store it in their database.

Discovering and Joining the Multicast Group

Although Hello packets discover PIM-SM routers, these routers can only join or be "pruned" from a multicast group through the use of Join/Prune Messages exchanged between the DR and RP. Join/Prune Messages are packets relayed between routers that effectively state which interfaces are, or are not to be receiving multicast data. These messages can be configured for their frequency to be sent out on the network and are only valid to routers if a Hello packet has first been received. A Hello packet will simply state that the router is present and ready to become a part of the RP's distribution tree. Once a router has accepted a member of the IGMP group and it is PIM-SM enabled, the interested router will then send an explicit Join/Prune message to the RP, which will in turn route multicast data from the source to the interested router, resulting in a unidirectional distribution tree for the group. Multicast packets are then sent out to all nodes on this tree. Once a prune message has been received for a router that is a member of the RP's distribution tree, the router will drop the interface from its distribution tree.

Distribution Trees

Two types of distribution trees can exist within the PIM-SM protocol, a Rendezvous-Point Tree (RPT) and a Shortest Path Tree (SPT). The RP will send out specific multicast data that it receives from the source to all outgoing interfaces enabled to receive multicast data. Yet, once a router has determined the location of its source, an SPT can be created, eliminating hops between the source and the destination, such as the RP. This can be configured by the switch administrator by setting the multicast data rate threshold. Once the threshold has been passed, the data path will switch to the SPT. Therefore, a closer link can be created between the source and destination, eliminating hops previously used and shortening the time a multicast packet is sent from the source to its final destination.

Register and Register Suppression Messages

Multicast sources do not always join the intended receiver group. The first hop router (DR) can send multicast data without being the member of a group or having a designated source, which essentially means it has no information about how to relay this information to the RP distribution tree. This problem is alleviated through Register and Register-Stop messages. The first multicast packet received by the DR is encapsulated and sent on to the RP which in turn removes the encapsulation and sends the packet on down the RP distribution tree. When the route has been established, a SPT can be created to directly connect routers to the source, or the multicast traffic flow can begin, traveling from the DR to the RP. When the latter occurs, the same packet may be sent twice, one type encapsulated, one not. The RP will detect this flaw and then return a Register Suppression message to the DR requesting it to discontinue sending encapsulated packets.

Assert Messages

At times on the PIM-SM enabled network, parallel paths are created from source to receiver, meaning some receivers will receive the same multicast packets twice. To improve this situation, Assert messages are sent from the receiving device to both multicast sources to determine which single router will send the receiver the necessary multicast data. The source with the shortest metric (hop count) will be elected as the primary multicast source. This metric value is included within the Assert message.

PIM-DM Interface Configuration

The *Protocol Independent Multicast - Dense Mode* (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth as PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

The PIM-DM multicast routing protocol is assumes that all downstream routers want to receive multicast messages and relies upon explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit 'join' messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the **Join/Prune Interval**) or for the downstream routers to transmit explicit 'prune' messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches ('prunes' them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the 'prune' information from its database and floods multicast messages to all interfaces on that branch. The interval for removing 'prune' information is the **Join/Prune Interval**.

PIM Global Settings

To enable PIM globally on the Switch, go to **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Global Settings**. This will give the user access to the following screen:

Figure 8- 69. PIM Global Settings window

Use the pull-down menu, choose *Enabled*, and click **Apply** to set the PIM function on the Switch.

PIM Interface Settings

To configure the settings for the PIM Protocol per IP interface, go to **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Interface Settings**. This will give the user access to the following screen:

PIM Interface Settings

Interface Name	IP Address	Designated Router	Hello Interval	Join/Prune Interval	Mode	State	DR priority
System	10.53.13.30	10.53.13.30	30	60	DM	Disabled	1
Trinity	11.1.1.1	11.1.1.1	30	60	DM	Disabled	1

Figure 8- 70. PIM Interface Settings window

To configure an IP interface for PIM, click its corresponding link which will lead you to the following screen:

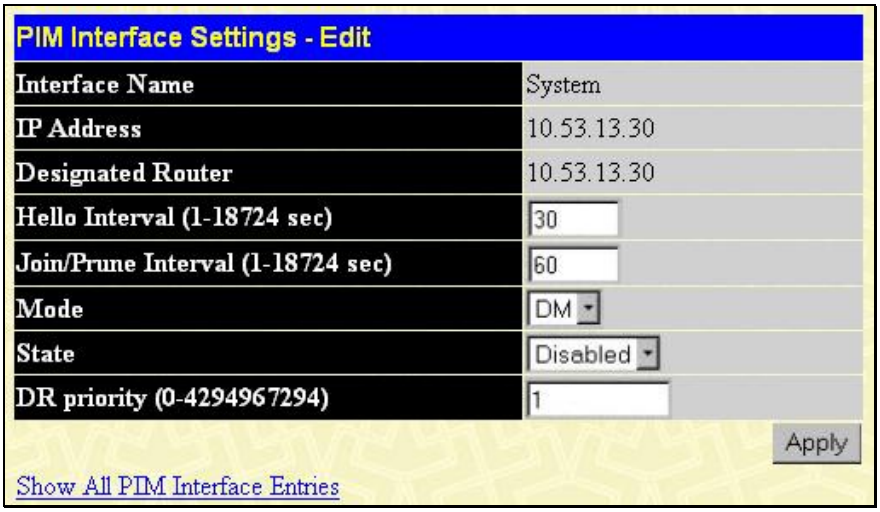


Figure 8- 71. PIM Interface Settings – Edit window

The following fields can be set:

Parameter	Description
Interface Name	This read-only field denotes the IP interface selected to be configured for PIM.
IP Address	This read-only field denotes the IP address of the IP interface selected to be configured for PIM.
Designated Router	This read-only field denotes the IP address of the Designated Router of the distribution tree to which this IP address belongs.
Hello Interval (1-18724 sec)	This field will set the interval time between the sending of Hello Packets from this IP interface to neighboring routers one hop away. These Hello packets are used to discover other PIM enabled routers and state their priority as the Designated Router (DR) on the PIM enabled network. The user may state an interval time between 1 – 18724 seconds with a default interval time of 30 seconds.
Join/Prune Interval (1-18724 sec)	This field will set the interval time between the sending of Join/Prune packets stating which multicast groups are to join the PIM enabled network and which are to be removed or "pruned" from that group. The user may state an interval time between 1 – 18724 seconds with a default interval time of 60 seconds.
Mode	Use the pull-down menu to select the type of PIM protocol to use, select *SM* to use Sparse Mode or select *DM* to use Dense Mode (DM). The default setting is DM.
State	Use the pull-down menu to enable or disable PIM for this IP interface. The default is Disabled.
DR priority (0-429396294)	Enter the priority of this IP interface to become the Designated Router for the multiple access network. The user may enter a DR priority between 0 and 4,294,967,294 with a default setting of 1.

Click **Apply** to implement changes made.

PIM Candidate BSR Settings

The following windows are used to configure the Candidate Boot Strap Router (C-BSR) settings for the switch and the priority of the selected IP interface to become the Boot Strap Router (BSR) for the PIM enabled network. The Boot Strap Router holds the information which determines which router on the network is to be elected as the RP for the multicast group and then to gather and distribute RP information to other PIM-SM enabled routers. To view the Candidate BSR window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Candidate BSR Settings.**

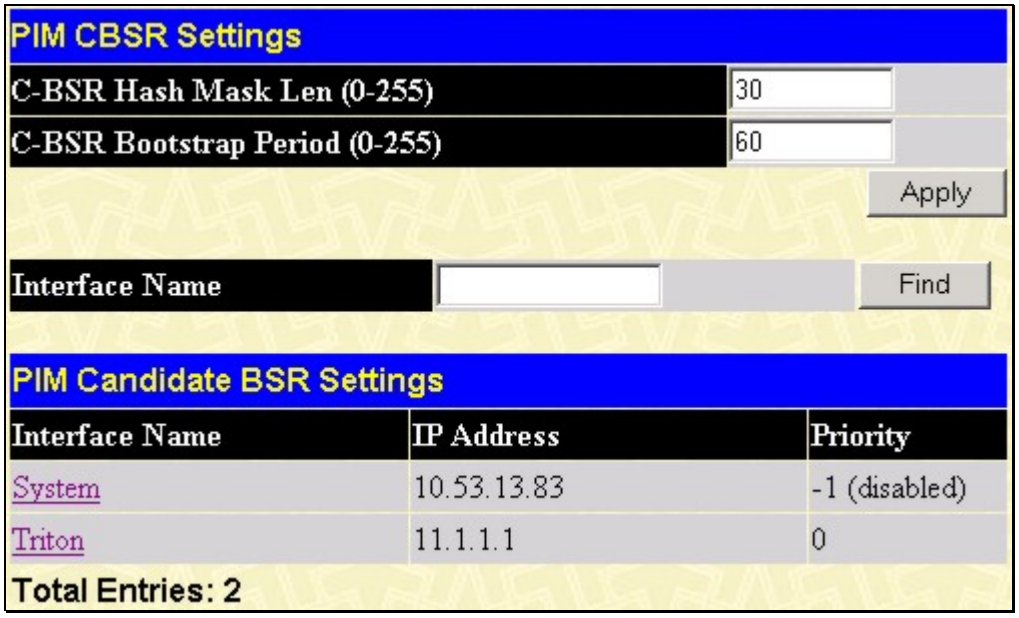


Figure 8- 72. PIM CBSR Settings window

The following fields can be set:

Parameter	Description
C-BSR Hash Mask Len (0-255)	Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which C-RP on the PIM-SM enabled network will be the RP. The user may select a length between 0 –32 with a default setting of 30.
C-BSR Bootstrap Period (0-255)	Enter a time period between 1-255 to determine the interval, the Switch will send out Boot Strap Messages (BSM) to the PIM enabled network. The default setting is 60 seconds.
Interface Name	To find an IP interface on the Switch, enter the interface name into the space provided and click **Find**. If found, the Interface Name will appear alone in the PIM Candidate BSR Settings window below.

To view the CBSR settings for an IP interface and set its BSR priority, click its hyperlinked name, which will lead you to the following window.

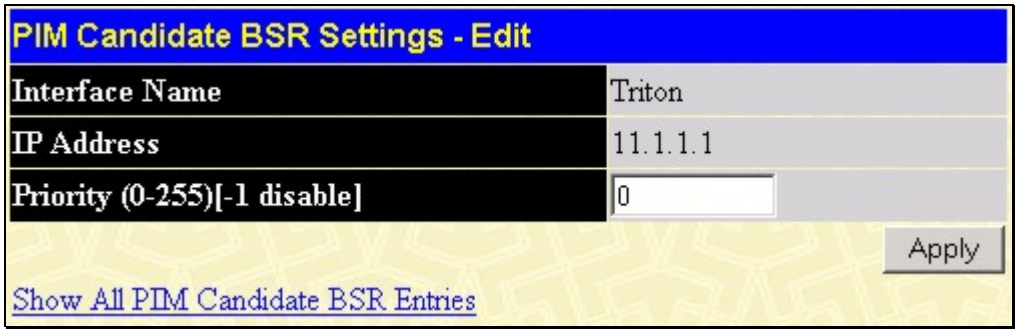


Figure 8- 73. PIM Candidate BSR Settings – Edit

The following fields can be viewed or set:

Parameter	Description
Interface Name	This read-only field denotes the IP Interface Name to be edited for its C-BSR priority.
IP Address	Denotes the IP Address of the IP Interface Name to be edited for its C-BSR priority.
Priority (0-255) [-1 disable]	Used to state the Priority of this IP Interface to become the BSR. The user may select a priority between -1 to 255. An entry of -1 states that the interface will be disabled to be the BSR.

Click **Apply** to set the priority for this IP Interface.

PIM Parameter Settings

The following window will configure the parameter settings for the PIM distribution tree. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Parameter Settings.**

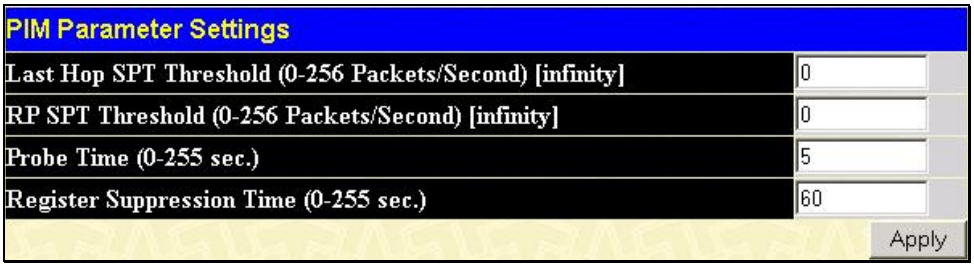


Figure 8- 74. PIM Parameter Settings window

The following fields can be viewed or set:

Parameter	Description
Last Hop SPT Threshold (0-256 Packets/Second) [infinity]	This field is to be configured for the last hop router in the RP tree. When the amount of multicast packets per second reaches the configured threshold, the last hop router will change its distribution tree to a (Shortest Path Tree) SPT. The user may enter a value between 0-256 packets per second. *0* will denote that the last hop router will immediately enter the SPT once a multicast packet has been received. An entry of *infinity* will disable the last hop router from entering the SPT. The default setting is *0*.
RP SPT Threshold (0-256 Packets/Second) [infinity]	This field is to be configured for the RP of the distribution tree. When the amount of register packets per second reaches the configured threshold, it will trigger the RP to switch to an SPT, between the RP and the first hop router. The user may enter a value between 0-256 packets per second. *0* will denote that the RP will immediately enter the SPT once a register packet has been received. An entry of *infinity* will disable the RP from entering an SPT. The default setting is *0*.
Probe Time (0-255 sec.)	This command is used to set a time to send a probe message from the DR to the RP before the Register Suppression time expires. If a Register Stop message is received by the DR, the Register Suppression Time will be restarted. If no Register Stop message is received within the probe time, Register Packets will be resent to the RP. The user may configure a time between 0-255 seconds with a default setting of 5 seconds.
Register Suppression Time (0-255 sec.)	This field is to be configured for the first hop router from the source. After this router sends out a Register message to the RP, and the RP replies with a Register stop message, it will wait for the time configured here to send out another register message to the RP. The user may set a time between 0-255 with a default setting of 60 seconds.

Click **Apply** to implement changes made.

NOTE: The Probe time value must be less than half of the Register Suppression Time value. If not, the administrator will be presented with an error message after clicking Apply.

PIM Candidate RP Global Settings

The following window is used to set the Parameters for this Switch to become the RP of its distribution tree. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Candidate RP Global Settings.**

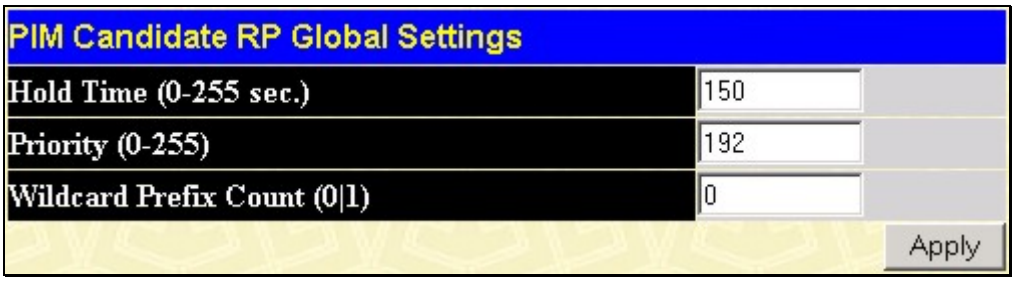


Figure 8- 75. PIM Candidate RP Global Settings

The following fields can be viewed or set:

Parameter	Description
Hold Time (0-255 sec.)	This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. The user may set a time between 0 - 255 seconds with a default setting of 150 seconds. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network.
Priority (0-255)	Enter a priority value to determine which CRP will become the RP for the distribution tree. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP. The user may set a priority between 0 – 255 with a default setting of 0.
Wildcard Prefix Count (0|1)	The user may set the Prefix Count value of the wildcard group address here by choosing a value between 0 and 1 with a default setting of 0.

Click **Apply** to implement changes made.

PIM Candidate RP Settings

The following window will display the parameters for the switch to become a CRP. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Candidate RP Settings.**

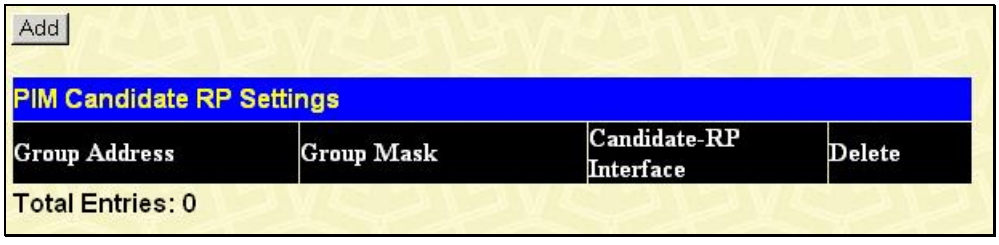


Figure 8- 76. PIM Candidate RP Settings window

To configure the settings for this window, click the Add button, which will reveal the following window for the administrator to configure.

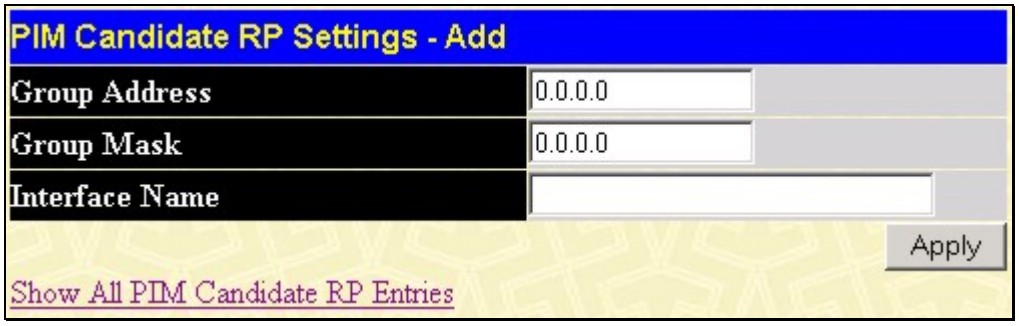


Figure 8- 77. PIM Candidate RP Settings – Add window

The following fields can be viewed or set:

Parameter	Description
Group Address	Enter the multicast group address for this CRP. This address must be a class D address.
Group Mask	Enter the mask for the multicast group address stated above.
Interface Name	Enter the name of the PIM-SM enabled interface the switch administrator wishes to become the CRP for this group.

Click **Apply** to implement changes made.

PIM Register Checksum Settings

This window is used to set a first hop router to create checksums to be included with the data in Registered packets. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Register Checksum Settings.**

Figure 8- 78. PIM Register Checksum Include Data RP List Settings window

To configure the settings for this window, click the **Add** button, which will reveal the following window for the administrator to configure.

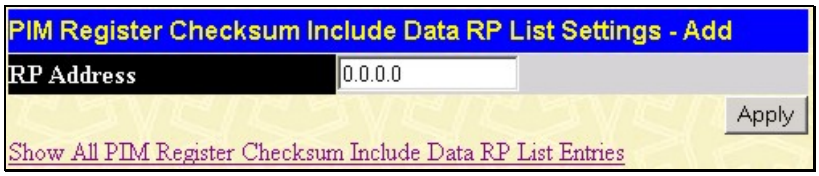


Figure 8- 79. PIM Register Checksum Include Data RP List Settings - Add window

The following fields can be set:

Parameter	Description
RP Address	Enter the IP address of the RP that will verify checksums included with Registered packets.

Click **Apply** to set the RP as a checksum enabled router.

PIM Static RP Settings

This window is used to view the Static RP settings for this router. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Static RP Settings.**

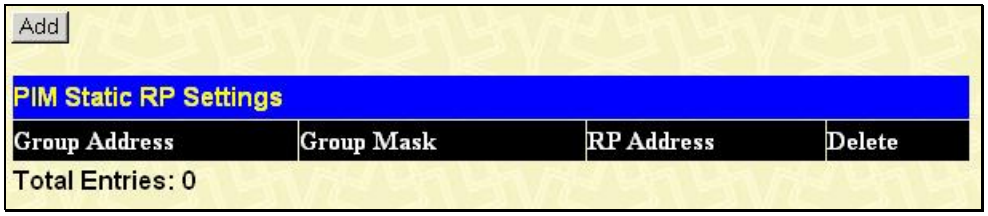


Figure 8- 80. PIM Static RP Settings window

To configure the settings for this window and set this router as the Static RP, click the **Add** button, which will reveal the following window for the administrator to configure.

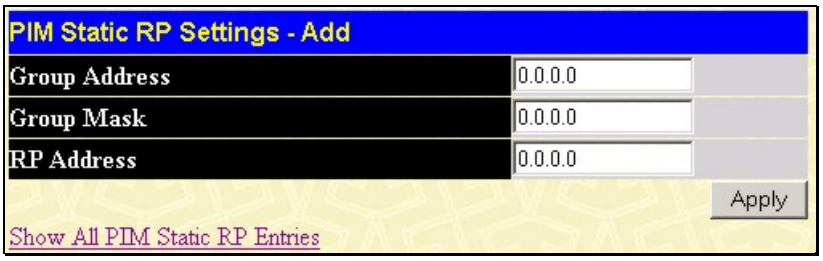


Figure 8- 81. PIM Static RP Settings – Add window

The following fields can be set:

Parameter	Description
Group Address	Enter the multicast group IP address to identify who is the RP. This address must be a class D address.
Group Mask	Enter the mask for the Group address stated above.
RP Address	Enter the RP's IP address to be set for the Group Address stated above.

Click **Apply** to set the static RP.

Section 9

QoS

Bandwidth Control

QoS Scheduling Mechanism

QoS Output Scheduling

802.1P Default Priority

802.1P User Priority

WRED Settings

The DES-3800 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-3800 Series implements 802.1P priority queuing.

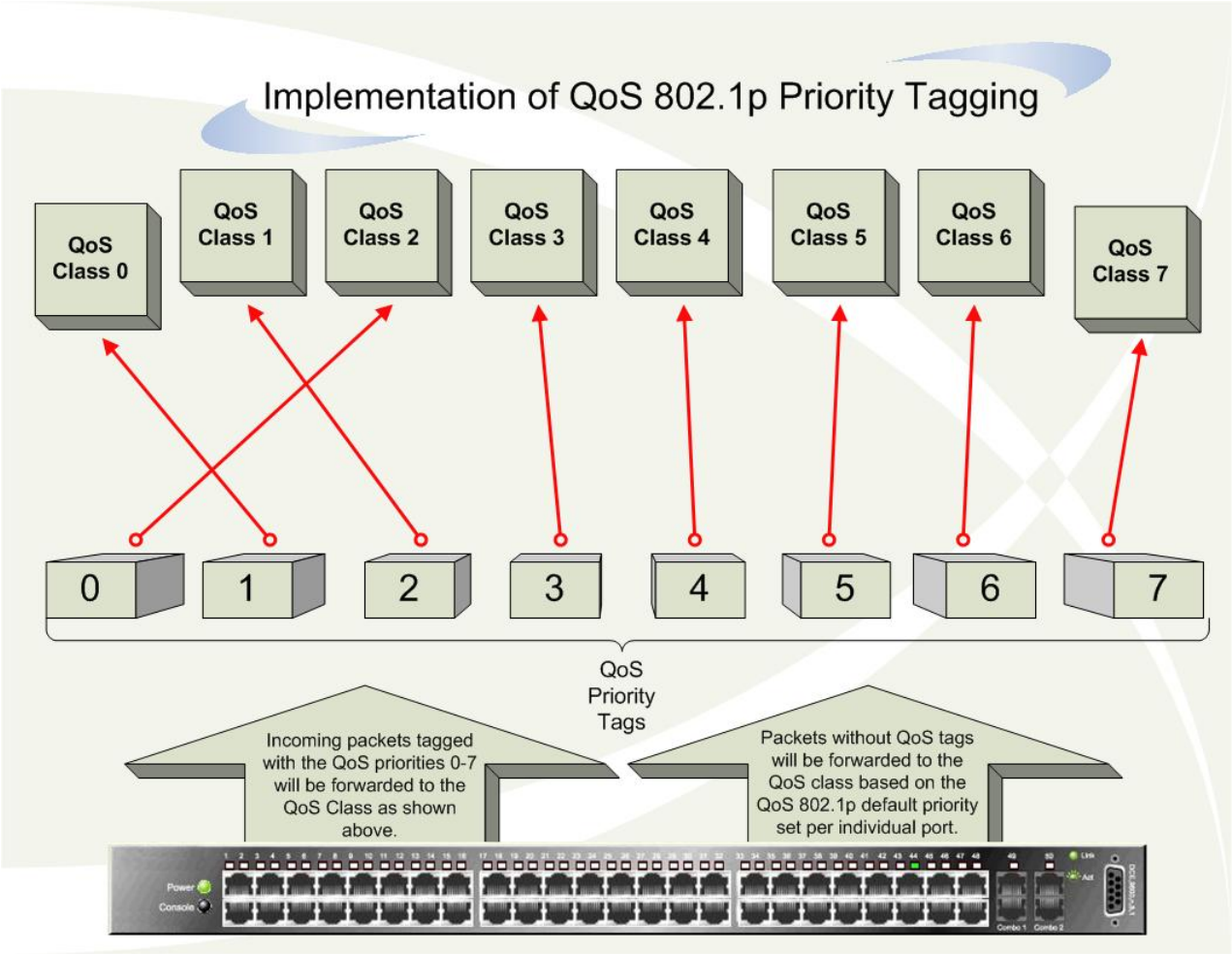


Figure 9- 1. Mapping QoS on the Switch

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 as 7, the high queue to 0, the lowest queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

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

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

For weighted round robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, 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-3800 Series has eight priority queues (and eight Classes of Service) for each port on the Switch.

Bandwidth Control

To access the Bandwidth Settings window, click **QoS > Bandwidth Control**.

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port. In the **QoS** folder, click **Bandwidth Control**, to view the window shown to the left.

Bandwidth Settings

From	To	Type	No Limit	Rate (64-1000000) (Kbit/sec)	Apply
Port 1	Port 1	Both	Disabled	1	Apply

Port Bandwidth Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX Rate (Kbit/sec)	Effective TX Rate (Kbit/sec)
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
7	No Limit	No Limit	No Limit	No Limit
8	No Limit	No Limit	No Limit	No Limit
9	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit
11	No Limit	No Limit	No Limit	No Limit
12	No Limit	No Limit	No Limit	No Limit
13	No Limit	No Limit	No Limit	No Limit
14	No Limit	No Limit	No Limit	No Limit
15	No Limit	No Limit	No Limit	No Limit
16	No Limit	No Limit	No Limit	No Limit
17	No Limit	No Limit	No Limit	No Limit
18	No Limit	No Limit	No Limit	No Limit
19	No Limit	No Limit	No Limit	No Limit
20	No Limit	No Limit	No Limit	No Limit
21	No Limit	No Limit	No Limit	No Limit
22	No Limit	No Limit	No Limit	No Limit
23	No Limit	No Limit	No Limit	No Limit
24	No Limit	No Limit	No Limit	No Limit
25	No Limit	No Limit	No Limit	No Limit
26	No Limit	No Limit	No Limit	No Limit
27	No Limit	No Limit	No Limit	No Limit
28	No Limit	No Limit	No Limit	No Limit

Figure 9- 2. Bandwidth Settings window

The following parameters can be set in the Bandwidth Settings section:

Parameter	Description
From/To	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, which will be the limit for the selected port. The value must be a multiple of 64, between 64 and 1000000.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured Bandwidth Settings will be displayed in the **Port Bandwidth Table**.

The following fields are displayed in the *Port Bandwidth Table*:

Parameter	Description
Port	Displays the ports of the Switch in sequential order.
RX Rate (Kbit/sec)	Displays the Receiving Rate (Kbit/sec) that the administrator configured for the port.
TX Rate (Kbit/sec)	Displays the Transmission Rate (Kbit/sec) the administrator configured for the port.
Effective RX Rate (Kbit/sec)	Displays the running Receiving Rate (Kbit/sec) for the port. The user can assign ingress bandwidth through the RADIUS server. When doing this, the Effective RX Rate will display the rate assigned by the Radius server. For more details, please refer to the 'Port Access Entity (802.1X)' chapter.
Effective TX Rate (Kbit/sec)	Displays the running Transmission Rate (Kbit/sec) for the port. The user can assign ingress bandwidth through the RADIUS server. When doing this, the Effective TX Rate will display the rate assigned by the Radius server. For more details, please refer to the 'Port Access Entity (802.1X)' chapter.

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 is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. 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. In the **QoS** folder, click **QoS Scheduling Mechanism**, to view the window shown below.

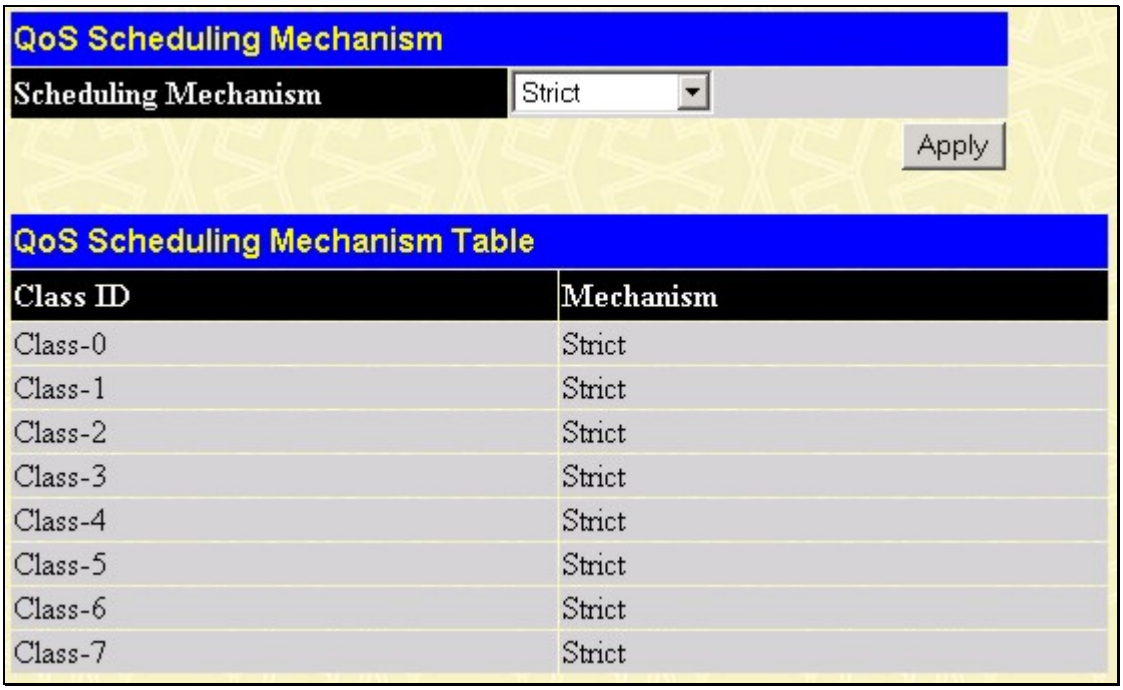


Figure 9- 3. QoS Output Scheduling window

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.
Weight Robin	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.

QoS Output Scheduling

QoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority classes of service is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If choosing 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 Output Scheduling**.

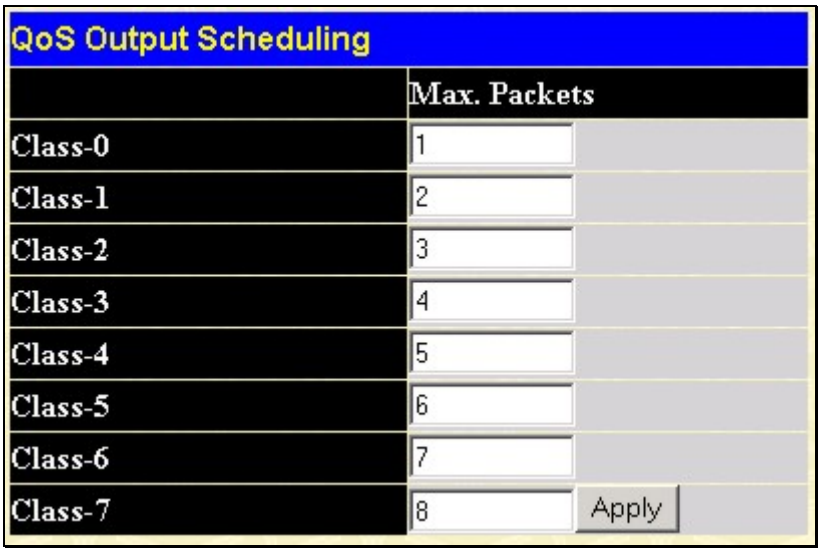


Figure 9- 4. QoS Output Scheduling window

The following values may be assigned to the QoS classes to set the scheduling.

Parameter	Description
Max. Packets	Specifies the maximum number of packets the above specified hardware priority class of service will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 15 can be specified.

Click **Apply** to implement changes made.

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. Click **QoS** > **802.1p Default Proiriry**, to view the window shown below.

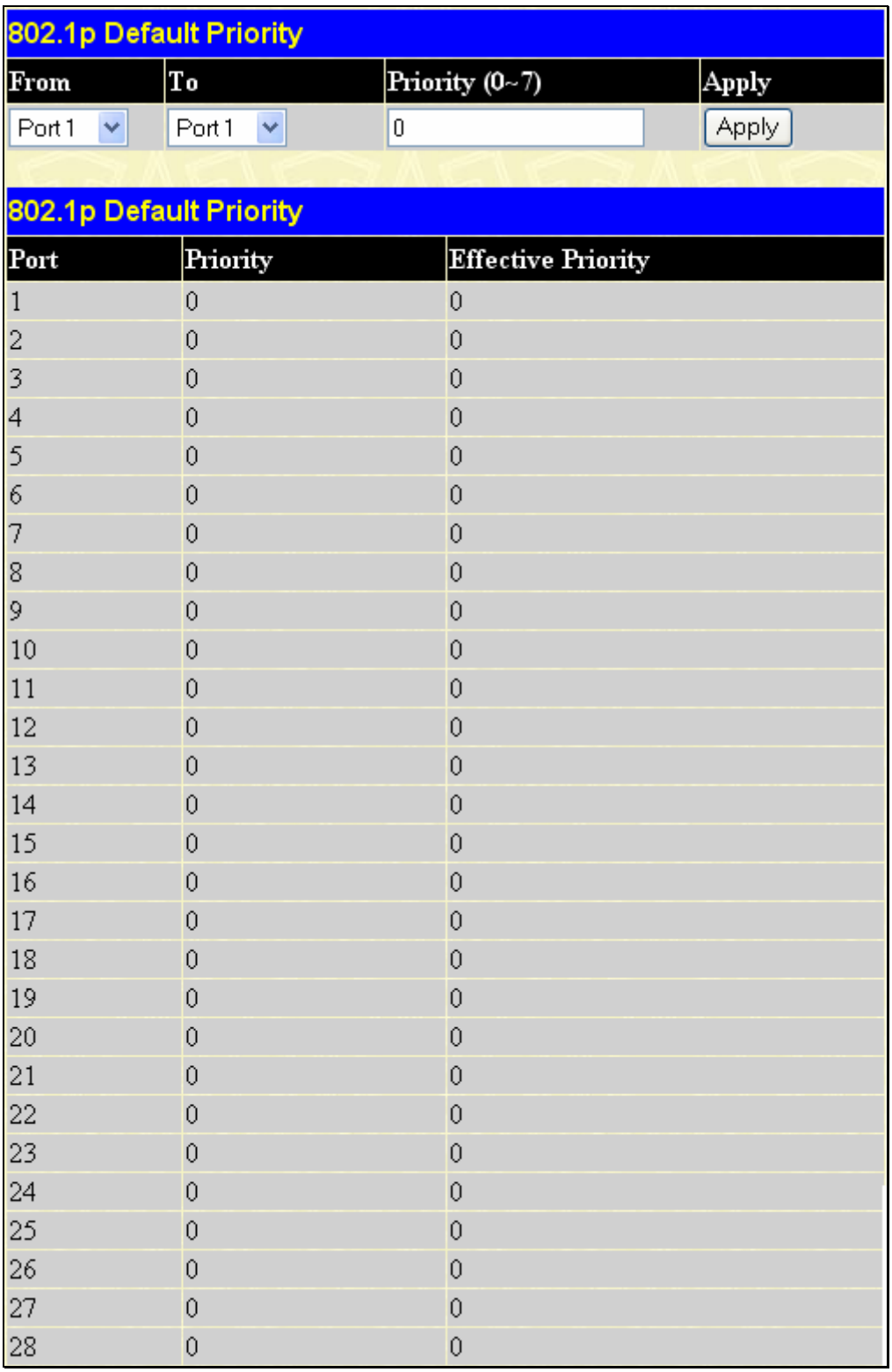


Figure 9- 5. 802.1p Default Priority Settings window

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.

The following information is displayed in the *802.1p Default Priority* table:

Parameter	Description
Port	Displays the ports of the Switch in sequential order.
Priority	Displays the Priority level the administrator configured for the port
Effective Priority	Displays the actual Priority level for the port.  **NOTE:** You can assign 802.1p priority through the RADIUS server. When doing this, the Effective Priority will display the priority assigned by the Radius server. For details, please refer to the 'Port Access Entity (802.1X)' chapter

802.1p User Priority

The DES-3800 Series allows the assignment of a user priority to each of the 802.1p priorities. Click **QoS** > **802.1p User Priority**, to view the screen shown below.

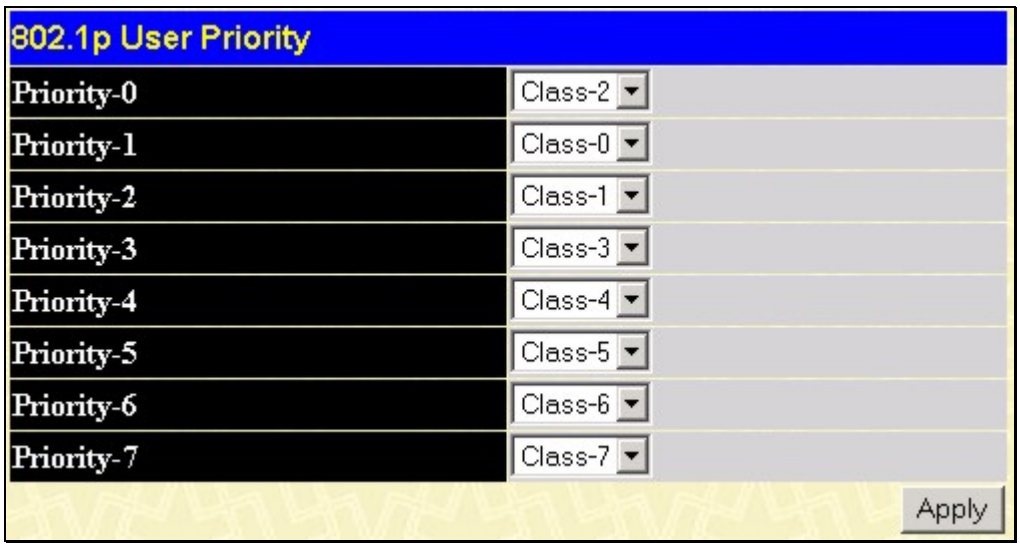


Figure 9- 6. QoS Class of Traffic window

Once you have assigned a priority to the port groups on the Switch, you can then assign this Class to each of the 8 levels of 802.1p priorities. Click **Apply** to set your changes.

WRED Settings

WRED or Weighted Random Early Discard is another implementation for QoS that will help the overall throughput for your QoS queues. Based on the egrees queue of the QoS function set on the Switch, this method will analyze these packets and their QoS queue to determine if there will be an overflow of packets entering the QoS queues and consequentially, minimize the packet flow into these queues by dropping random packets. WRED employs two methods of avoiding congestion within the QoS queue.

1. Every QoS queue has a minimum and a maximum level for acceptance of packets. Once the maximum threshold has been reached for this queue, the switch will begin discarding all ingress packets, this minimizing the allotted bandwidth for QoS. When below the minimum threshold, the switch will accept all ingress packets.
2. When the ingress packets are somewhere between the maximum and minimum queue, the Switch will use a slope probability function to determine a random method of dropping packets based on the fill percentage of the QoS queue. If queues are closer to being full, the Switch will increase the discarding of random packets to even out the flow to the queues and avoid overflows to higher priority queues.

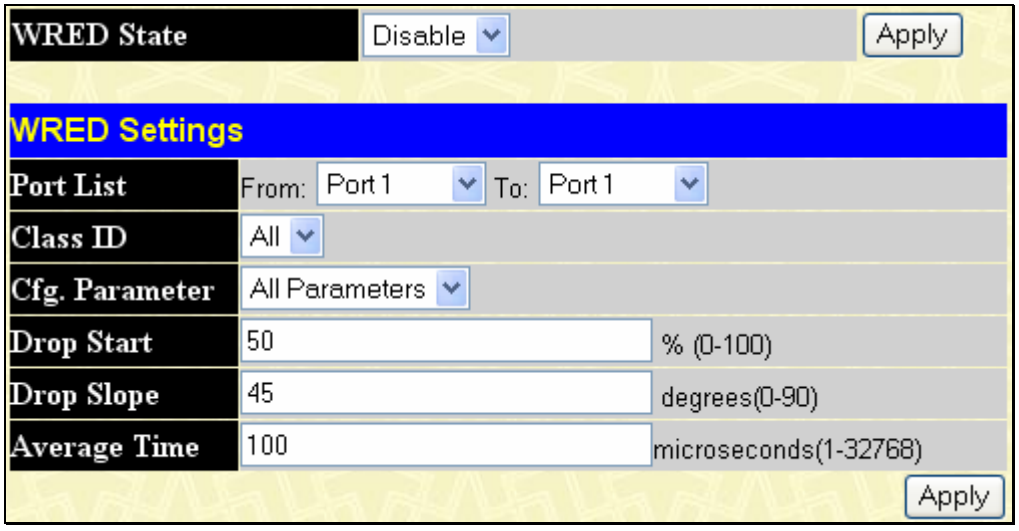


Figure 9- 7. WRED Settings window

To configure WRED settings for the Switch, configure the following fields and click **Apply**. Note that WRED State may be separately globally enabled and disabled and has its own **Apply** button for this reason.

Parameter	Description
WRED State	Allows the user to globally enable and disable the WRED function on this switch without altering previously made configurations. Use the pull-down menu and click the **Apply** button, located directly adjacent to the WRED State configuration field.
Port List	Use the pull-down menus to select a port or range of ports to be configured for WRED.
Class ID	Select the CoS ID, from *0*-*7*, to configure for the WRED parameters. Selecting *All* will set the parameters configured here for all CoS queues.
Cfg. Parameter	Use the pull-down menu if you desire to configure a particular parameter of the WRED settings for a specified queue or port. The user may choose *All Parameters,* which will allow the user to configure *Drop Start*, *Drop Slope* and *Average Time,* simultaneously for a desired CoS queue, or select a specific parameter only to be configured. These parameters can be configured in the following three fields.
Drop Start	Select a percentage between 0 and 100 to initialize the discarding of random packets. This percentage is based on the fill percentage of the egress QoS queue stated in the Class ID field. (Once the specified queue reaches the target percentage specified here, the Switch will begin randomly discarding packets)
Drop Slope	The drop slope is a formula resulting in a degree which compares the average size of a queue to the percentage of the maximum and minimum Drop Start function previously stated. A value closer to 90° will wait a longer time before dropping packets than a value set closer to 0°.
Average Time	Enter a time, in microseconds, that the Switch will check the CoS queues to determine abnormalities in the settings and boundaries which will trigger the WRED function to initialize.

Click **Apply** to implement changes made.

Section 10

ACL

Access Profile Table

Flow Metering Table

CPU Interface Filtering

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 9 access profiles. The rules used to define the access profiles are limited to a total of 800 rules for the Switch.

There is an additional limitation on how the rules are distributed among the Fast Ethernet and Gigabit Ethernet ports. This limitation is described as follows: Fast Ethernet ports are limited to 200 rules for each of the three sequential groups of eight ports. That is, 200 ACL profile rules may be configured for ports 1 to 8. Likewise, 200 rules may be configured for ports 9 to 16, and another 200 rules for ports 17 to 24. Up to 100 rules may be configured for each Gigabit Ethernet port. The table below provides a summary of the maximum ACL profile rule limits.

DES-3828/DES-3828DC/DES-3828P

Port Numbers	Maximum ACL Profile Rules per Port Group
1 - 8	200
9 – 16	200
17 - 24	200
25 (Gigabit)	100
26 (Gigabit)	100
27(Gigabit)	100
28(Gigabit)	100
Total Rules	800

DES-3852

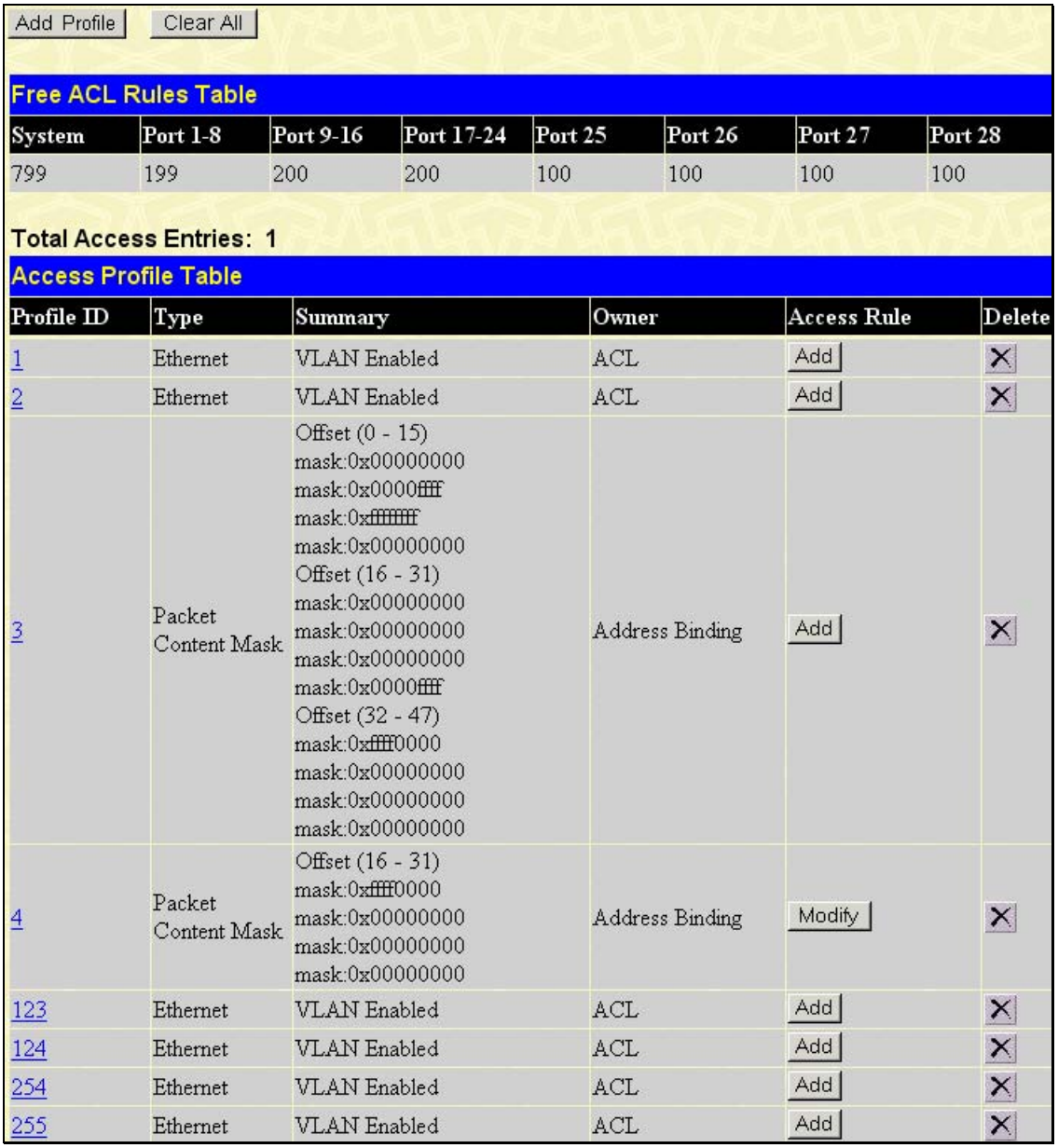
Port Numbers	Maximum ACL Profile Rules per Port Group
1 - 8	200
9 - 16	200
17 - 24	200
25 - 32	200
33 - 40	200
41 - 48	200
49 (Gigabit)	100
50 (Gigabit)	100
51(Gigabit)	100
52(Gigabit)	100
Total Rules	800

It is important to keep this in mind when setting up VLANs as well. Access rules applied to a VLAN require that a rule be created for each port in the VLAN. For example, let's say VLAN10 contains ports 2, 11 and 12. If users create an access profile specifically for VLAN10, users must create a separate rule for each port. Now take into account the rule limit. The rule limit applies to both port groups 1-8 and 9-16 since VLAN10 spans these groups. One less rule is available for port group 1-8. Two less rules are available for port group 9-16. In addition, a total of three rules apply to the 800 rule Switch limit.

In the example used above - config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny – a single access rule was created. This rule will subtract one rule available for the port group 1 – 8, as well as one rule from the total available rules.

Access Profile Table

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



Add Profile | Clear All

Free ACL Rules Table

System	Port 1-8	Port 9-16	Port 17-24	Port 25	Port 26	Port 27	Port 28
799	199	200	200	100	100	100	100

Total Access Entries: 1

Access Profile Table

Profile ID	Type	Summary	Owner	Access Rule	Delete
1	Ethernet	VLAN Enabled	ACL	Add	X
2	Ethernet	VLAN Enabled	ACL	Add	X
3	Packet Content Mask	Offset (0 - 15) mask:0x00000000 mask:0x0000ffff mask:0xffffffff mask:0x00000000 Offset (16 - 31) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x0000ffff Offset (32 - 47) mask:0xffff0000 mask:0x00000000 mask:0x00000000 mask:0x00000000	Address Binding	Add	X
4	Packet Content Mask	Offset (16 - 31) mask:0xffff0000 mask:0x00000000 mask:0x00000000 mask:0x00000000	Address Binding	Modify	X
123	Ethernet	VLAN Enabled	ACL	Add	X
124	Ethernet	VLAN Enabled	ACL	Add	X
254	Ethernet	VLAN Enabled	ACL	Add	X
255	Ethernet	VLAN Enabled	ACL	Add	X

Figure 10- 1. Access Profile Table

To add an entry to the **Access Profile Table**, click the **Add Profile** button. This will open the **Access Profile Configuration** page, as shown below. There are four **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration, one for the **Packet Content Mask** and one for **IPv6**. You can switch between the four **Access Profile Configuration** pages by using the **Type** drop-down menu. 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.

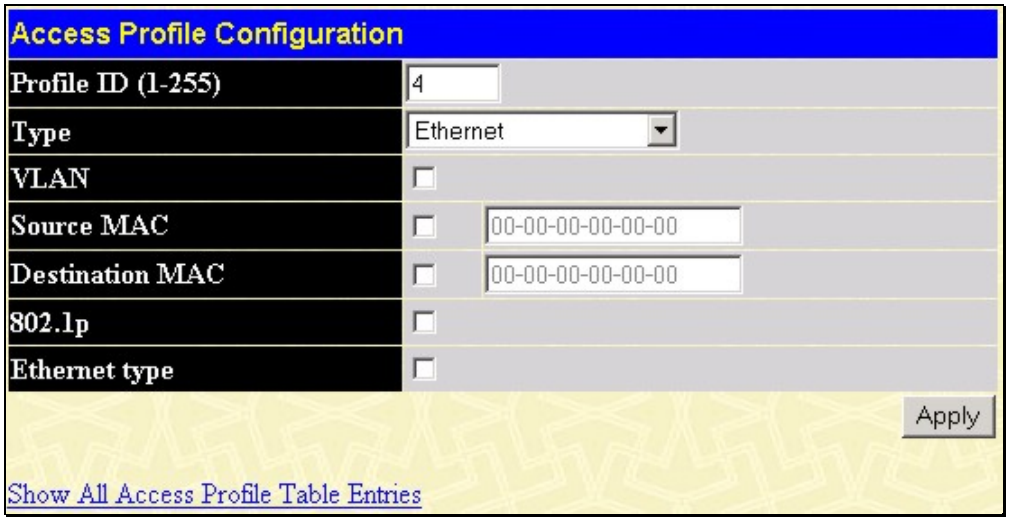


Figure 10- 2. Access Profile Table (Ethernet)

The following parameters can be set, for the **Ethernet** type:

Parameter	Description
Profile ID (1-255)	Type in a unique identifier number for this profile set. This value can be set from 1 – 255, yet only 9 access profiles can be created on the Switch.
Type	Select profile based on Ethernet (MAC Address), IP address, or packet content mask. This will change the menu according to the requirements for the type of profile. • Select *Ethernet* to instruct the Switch to examine the layer 2 part of each packet header. • Select *IP* 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. • Select *IPv6* to instruct the Switch to examine the IPv6 address in each frame's header.
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.
Source MAC	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
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.

NOTE: IP-MAC Binding ACL entries can only be removed form the Access Profile table by using the IP-MAC Binding window, mentioned earlier in this manual. The Clear All button will only remove entries created in the Access Profile window.

The page shown below is the **IP Access Profile Configuration** page:

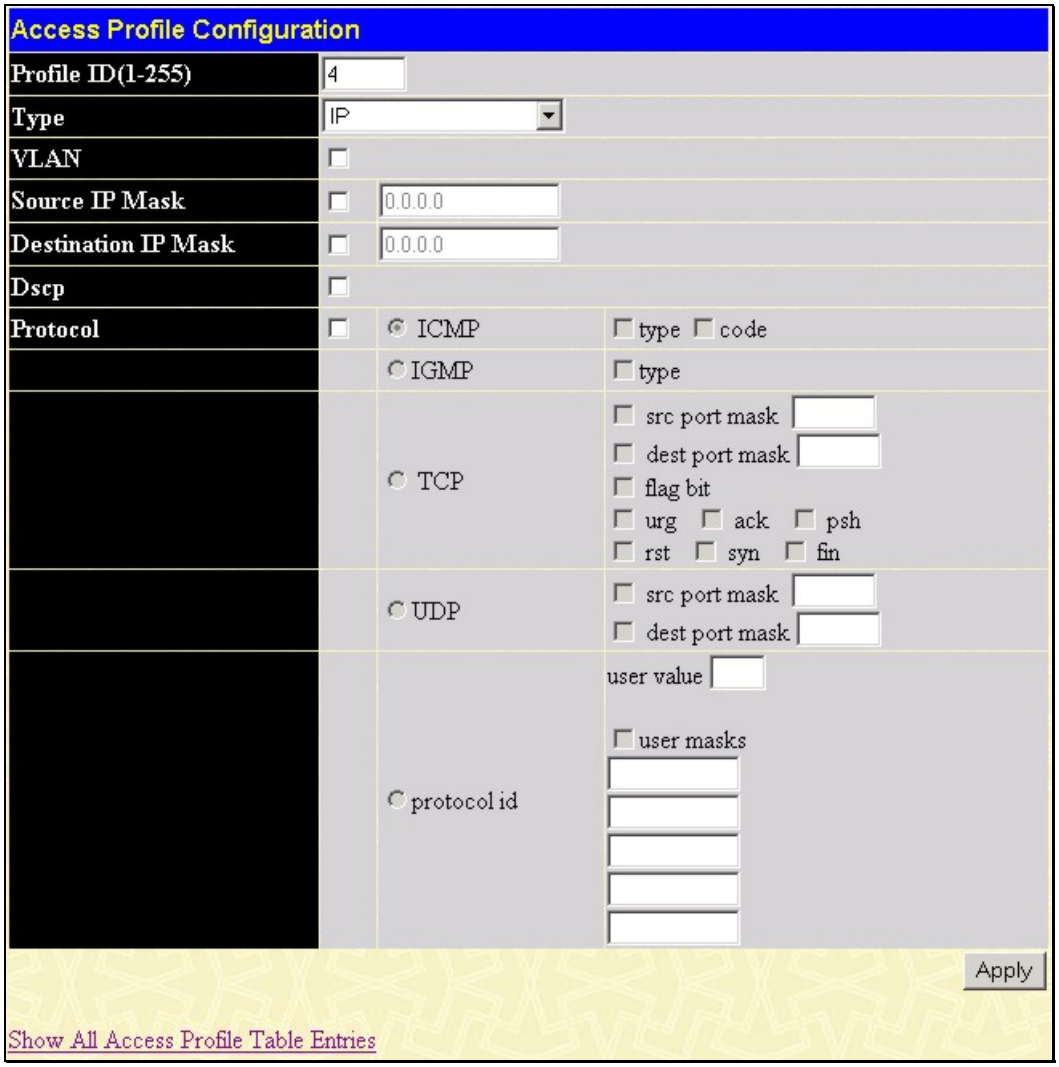


Figure 10- 3. Access Profile Configuration (IP)

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

Parameter	Description
Profile ID (1-255)	Type in a unique identifier number for this profile set. This value can be set from 1 – 255, yet only 9 access profiles can be created on the Switch.
Type	Select profile based on Ethernet (MAC Address), IP address, 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 *Packet Content Mask* to specify a mask to hide the content of the packet header. • Select *IPv6* to instruct the Switch to examine the IPv6 address in each frame's header.
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.
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.

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.
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. • **dest 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). • **dest port mask** - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff). **protocol id** - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xffffffff) or a user value.

Click **Apply** to implement changes made.

The page shown below is the **ACL Packet Content Mask** configuration window.

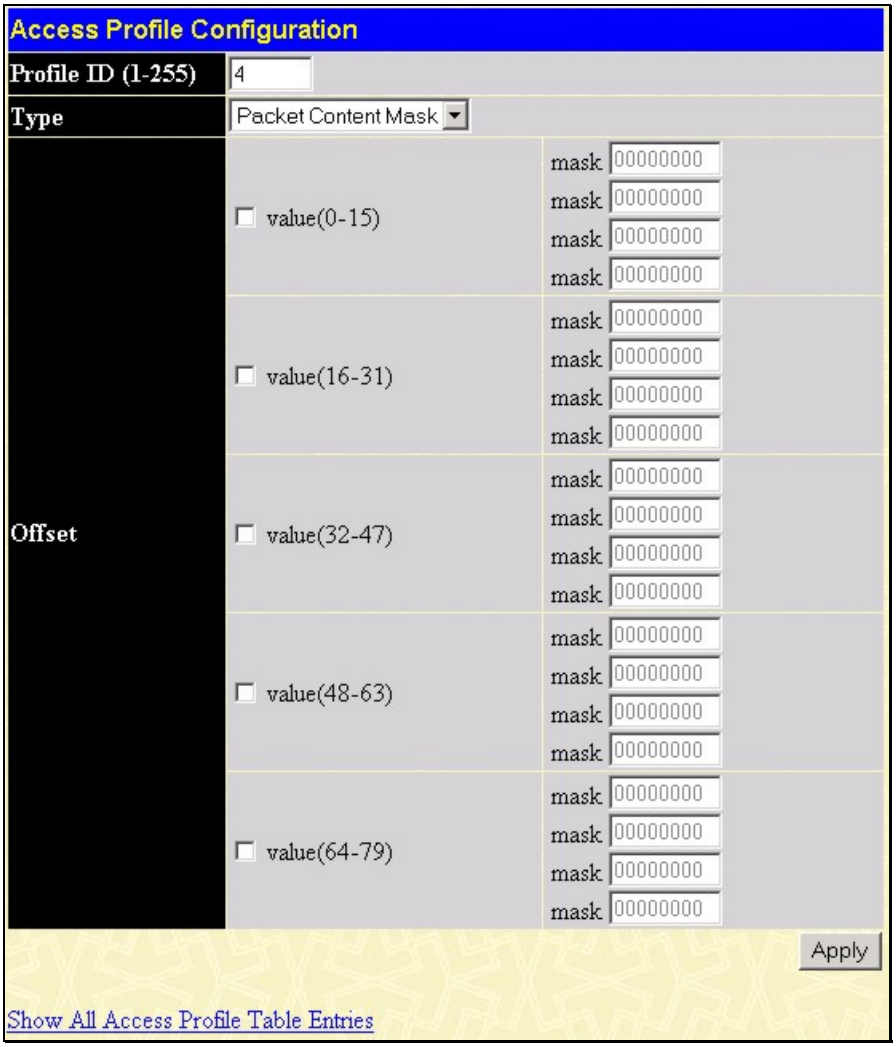


Figure 10- 4. Access Profile Configuration (Packet Content Mask)

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **Packet Content Mask**:

Parameter	Description
Profile ID (1-255)	Type in a unique identifier number for this profile set. This value can be set from 1 – 255, yet only 9 access profiles can be created on the Switch.
Type	Select profile based on Ethernet (MAC Address), IP address, or packet content mask. This will change the menu according to the requirements for the type of profile. • Select *Ethernet* to instruct the Switch to examine the layer 2 part of each packet header. • Select *IP* 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. • Select *IPv6* to instruct the Switch to examine the IPv6 address in each frame's header.
Offset	This field will allow users to examine any specified content up to 80 bytes within a packet at one time and instruct the Switch to mask the packet header beginning with the offset value specified: • *value (0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • *value (16-31)* – Enter a value in hex form to mask the packet from byte 16 to byte 31. • *value (32-47)* – Enter a value in hex form to mask the packet from byte 32 to byte 47.

	• *value (48-63)* – Enter a value in hex form to mask the packet from byte 48 to byte 63. • *value (64-79)* – Enter a value in hex form to mask the packet from byte 64 to byte 79. With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link xStack switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is the reason why Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click **Apply** to implement changes made.

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 F, at the end of this manual.

The page shown below is the **IPv6 Access Profile** configuration window.

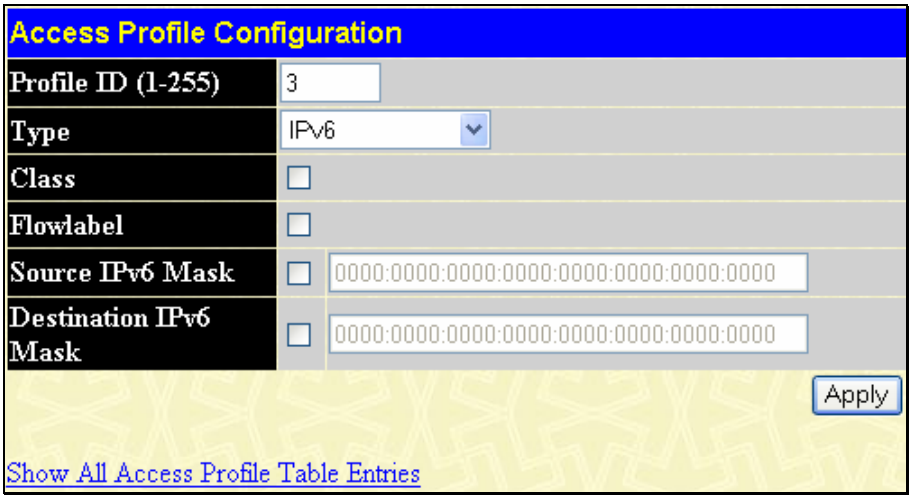


Figure 10- 5. Access Profile Configuration (IPv6)

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **IPv6**:

Parameter	Description
Profile ID (1-255)	Type in a unique identifier number for this profile set. This value can be set from *1* to *255*. Yet only 9 access profiles can be created on the Switch.
Type	Select profile based on *Ethernet* (MAC Address), *IP Address, Packet Content* or *IPv6* address. 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 *Packet Content Mask* to specify a mask to hide the content of the packet header. • Select *IPv6* to instruct the Switch to examine the IPv6 address in each frame's header.
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.
Flowlabel	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.
Source IPv6 Mask	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
Destination IPv6 Mask	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.

Click **Apply** to implement changes made.

To view the configurations set for a previously created access profile, click the hyperlinked **Show All Access Profile Table Entries**. A window similar to the one below will be displayed.

Click **ACL** > **Access Profile Table**, the window shown below will appear.

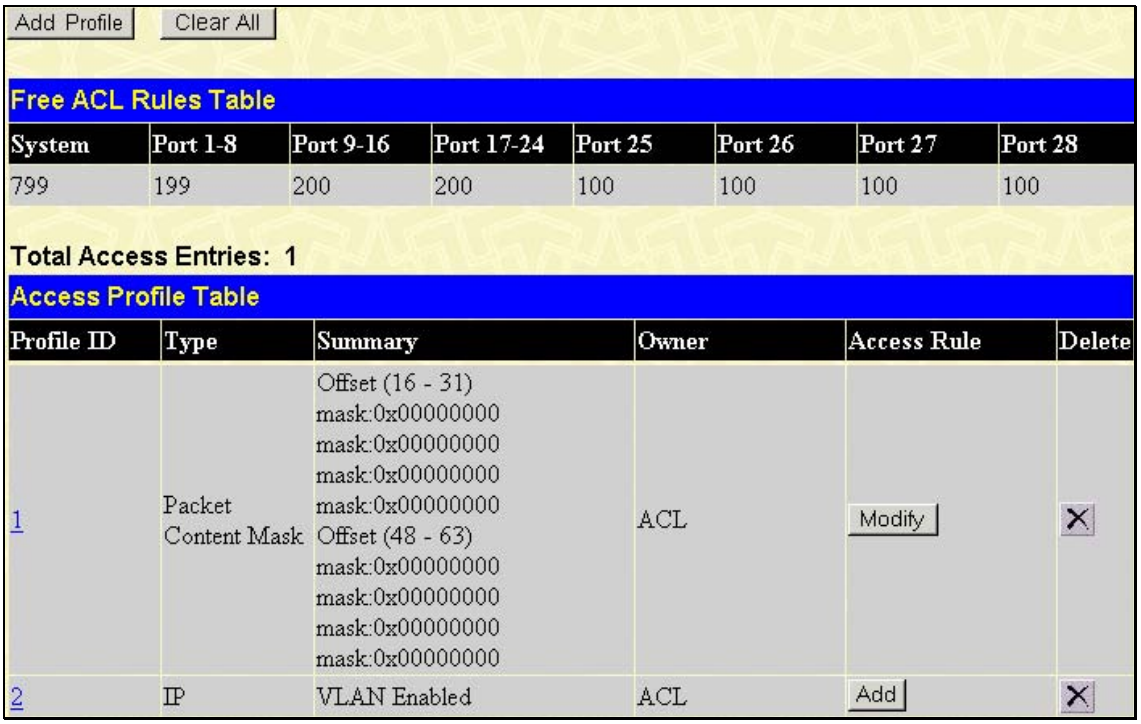


Figure 10- 6. Access Profile Table window

To create a new rule set for an access profile click the **Add** button. To modify an existing access rule click the **Modify** button and to remove a previously created rule click the corresponding ✕ button. To view the settings of a previously correctly configured profile, click the hyperlinked Profile ID in the **Access Profile Table** to view the following screen:

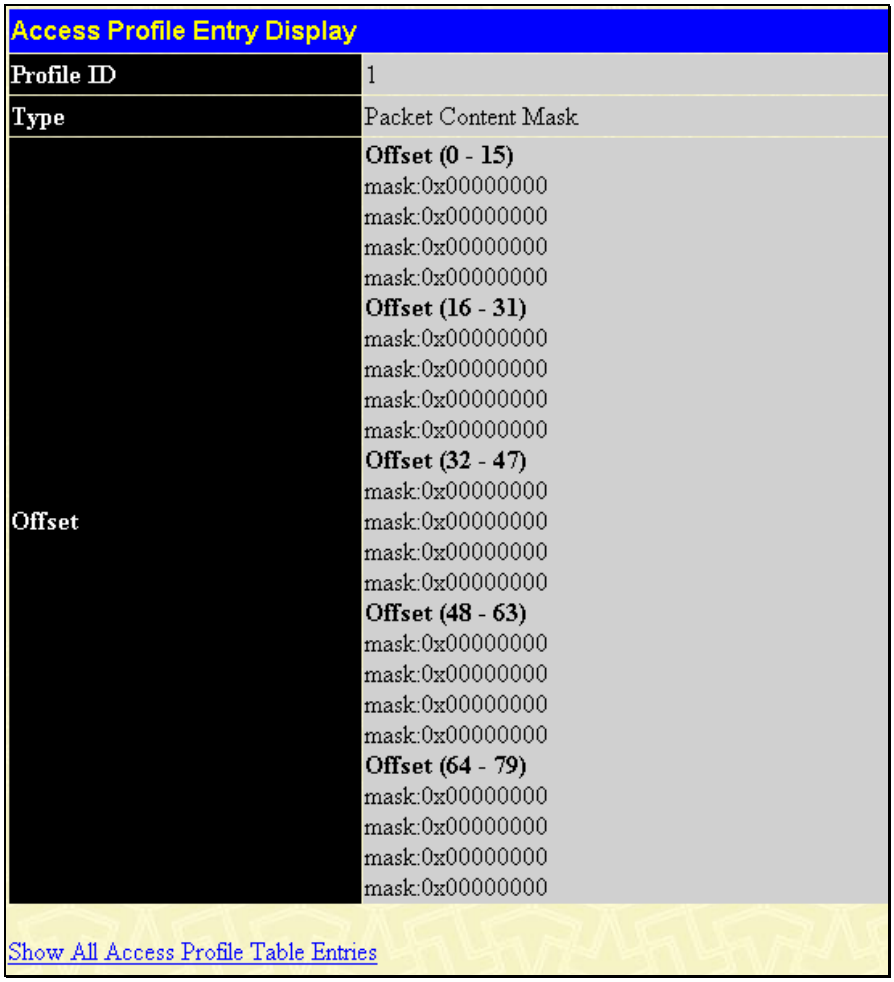


Figure 10- 7. Access Profile Entry Display window (Packet Content Mask)

By clicking **Modify** on the **Access Profile Table** it will bring you to the Access Rule Table where you can configure the Flow Metering for the each entry.

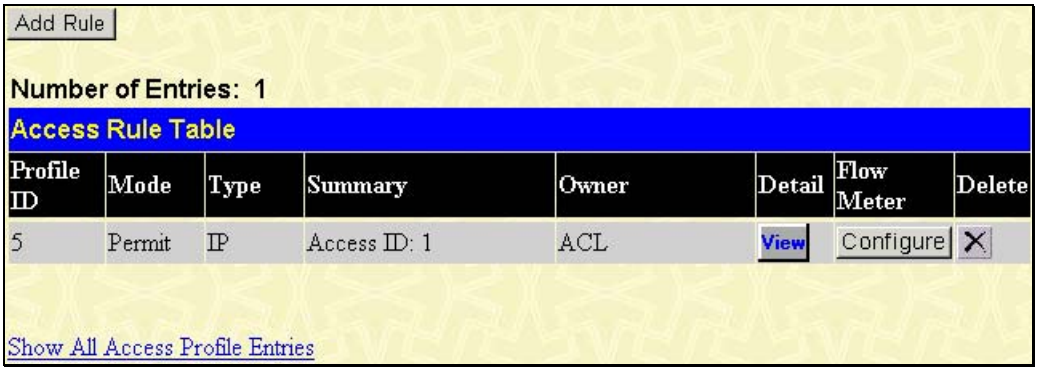


Figure 10- 8. Access Profile Table window

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button. To configure the Flow Meter Settings click the **Configure** button.

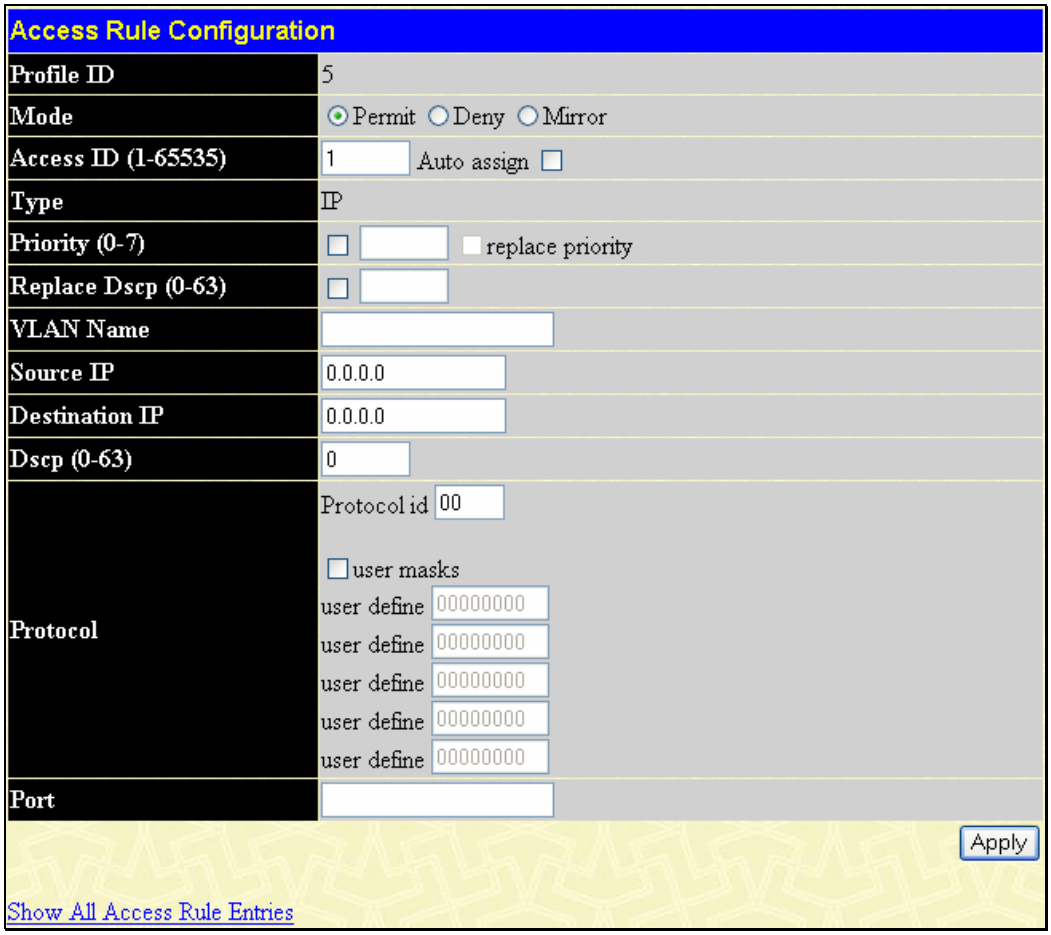


Figure 10-9. Access Rule Configuration window (IP)

Configure the following Access Rule Configuration settings:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the Switch, according to any additional rule, forward the packets that match the access profile 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 monitor the packets forwarded by the switch.
Access ID (1-65535)	Type in a unique identifier number for this access or use **Auto Assign**.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header. • *IPv6* instructs the switch to examine the IPv6 address in each frame's header.
Priority (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. *Replace Priority with* – Click the corresponding box if you want to re-write 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.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address - Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address - Enter an IP Address mask for the destination IP address.
DSCP (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*.
Protocol	This field allows the user to modify the protocol used to configure the Access Rule Table; depending on which protocol the user has chosen in the Access Profile Table.
Port	The user may set the Access Rule to *Permit* or *Deny* on a per-port basis by entering a port number in this field. Any other specified criteria applies as well.

To view the settings of a previously correctly configured rule, click View in the Access Rule Table to view the following window:

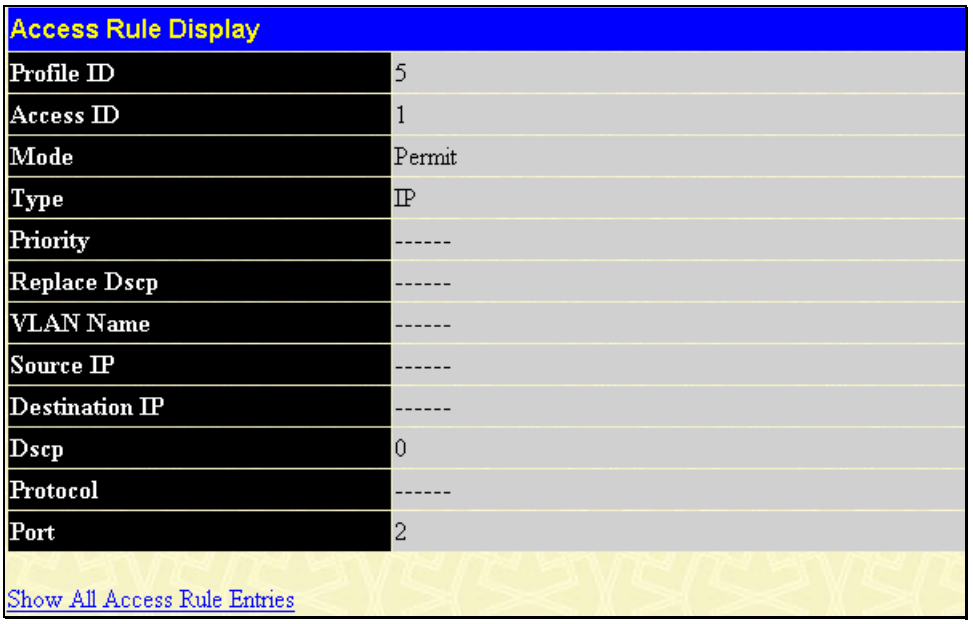


Figure 10- 10. Access Rule Display window (IP)

To configure the Access Rule for Ethernet, open the Access Profile Table and click **Modify** for an Ethernet entry. This will open the following window:

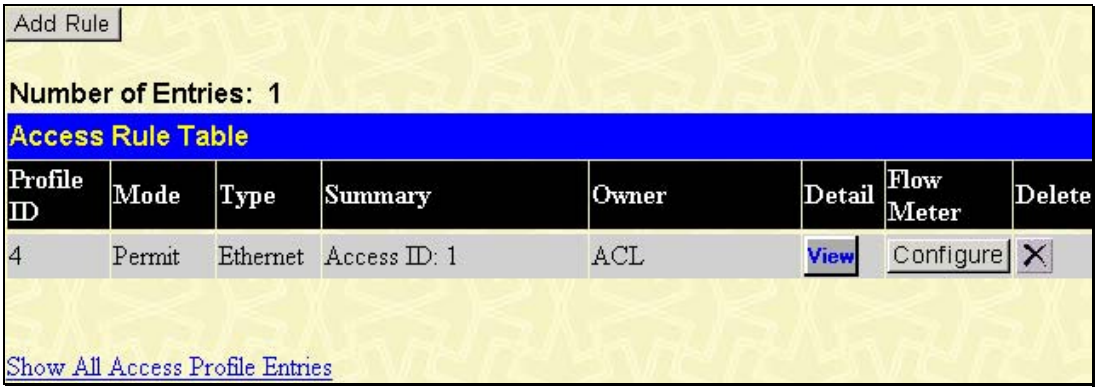


Figure 10- 51. Access Rule Table window

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button. To configure the Flow Meter Settings click the **Configure** button.

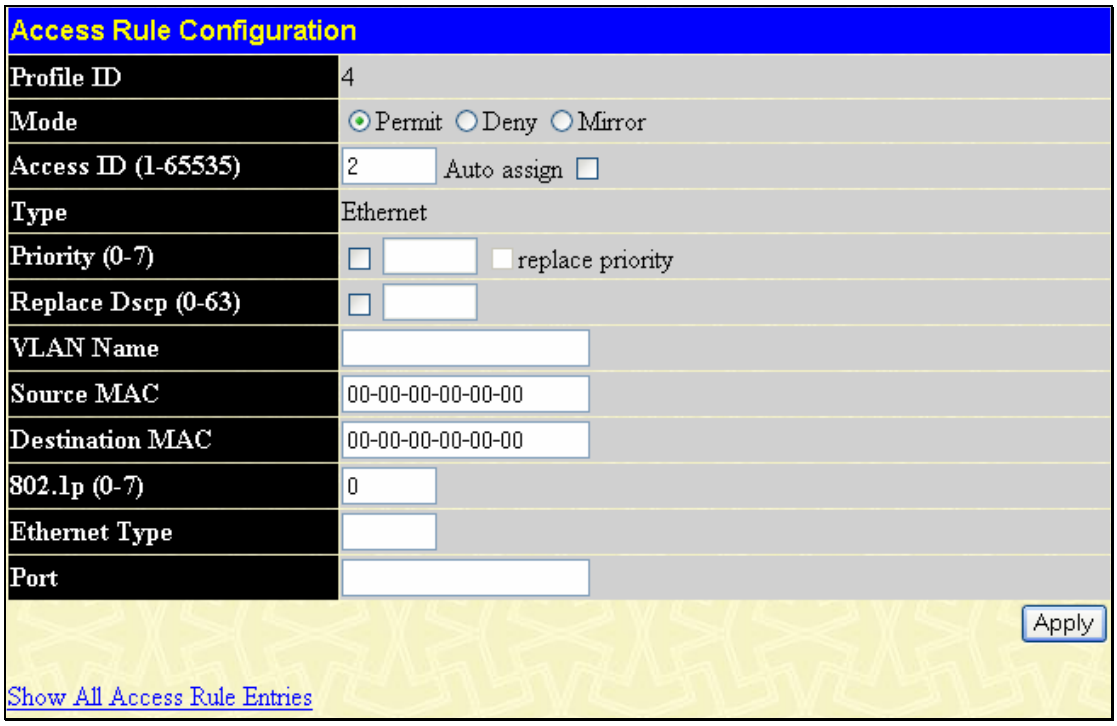


Figure 10- 52. Access Rule Configuration window (Ethernet)

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

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the Switch, according to any additional rule, forwards the packets that match the access profile 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 monitor and copy the packets forwarded by the switch.
Access ID (1-65535)	Type in a unique identifier number for this access or use **Auto Assign**.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6.

	• *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header. • *IPv6* instructs the switch to examine the IPv6 address in each frame's header.
Priority (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. *Replace Priority with* – Click the corresponding box if you want to re-write 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.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source MAC	Source MAC Address - Enter a MAC Address for the source MAC address.
Destination MAC	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.
Port	The user may set the Access Rule to *Permit* or *Deny* on a per-port basis by entering a port number in this field. Any other specified criteria applies, as well.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following window:

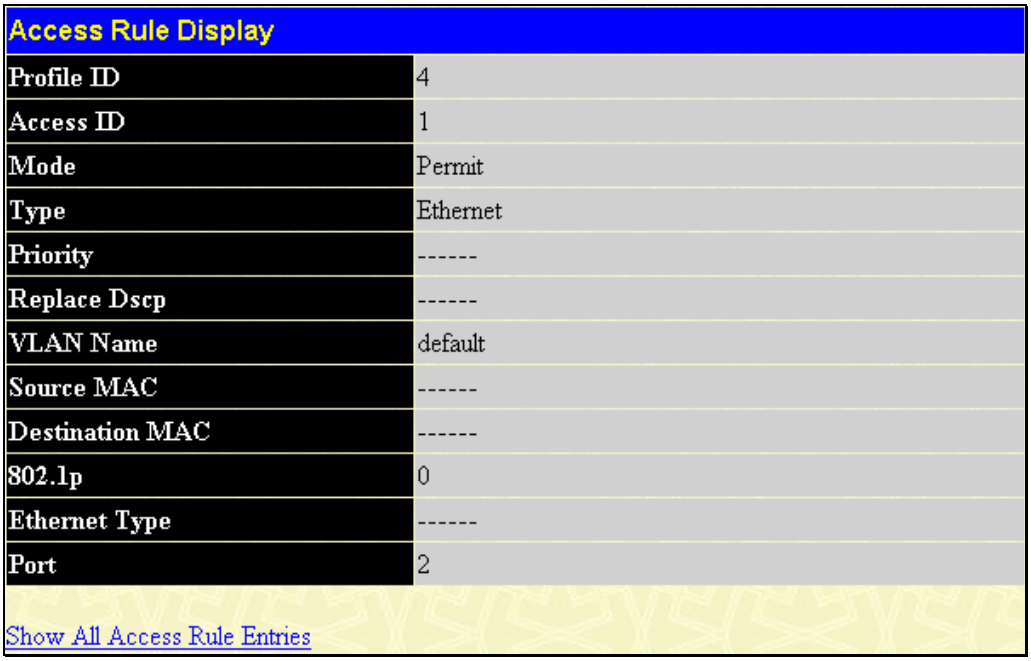


Figure 10- 53. Access Rule Display window (Ethernet)

To configure the Access Rule for Packet Content Mask, open the Access Profile Table and click **Modify** for a Packet Content Mask entry. This will display the Access Rule Table.

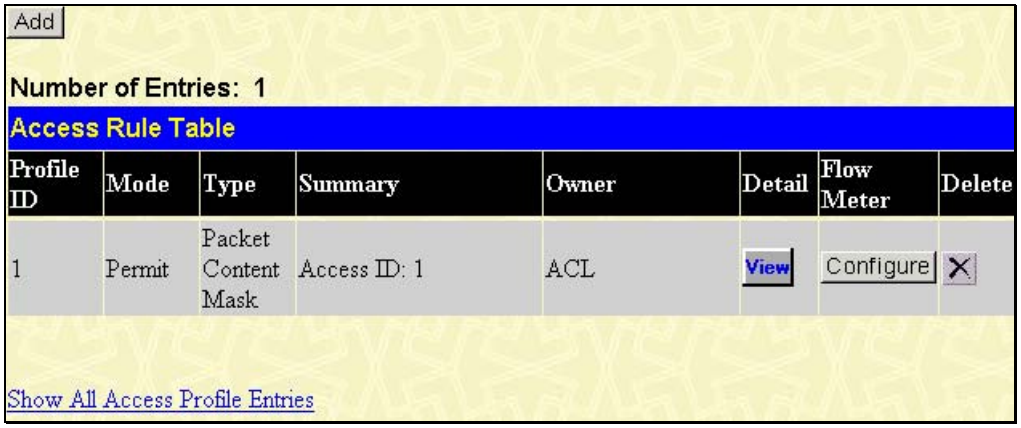


Figure 10- 54. Access Rule Table window

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding button. To configure the Flow Meter Settings click the **Configure** button. To display all rules in the table, click the **Show All Access Profile Entries** button.

To add a new Access Rule, click the **Add** button above the Access Rule Table to view the Access Rule Configuration menu.

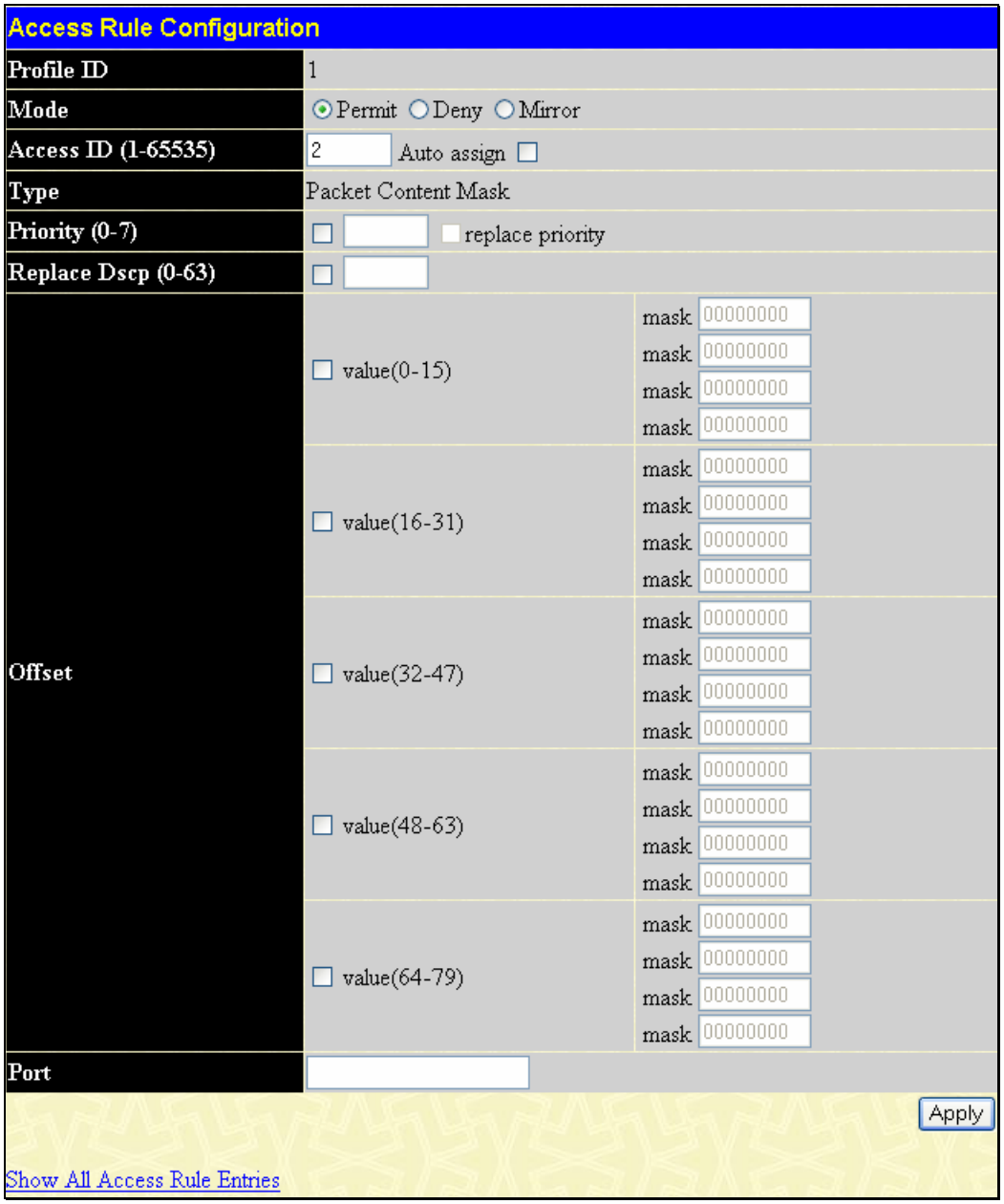


Figure 10- 55. Access Rule Configuration window (Packet Content Mask)

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

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the Switch, according to any additional rule, forwards the packets that match the access profile 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 monitor and copy the packets forwarded by the switch.
Access ID (1-65535)	Type in a unique identifier number for this access or use **Auto Assign**.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header.

	• *Packet Content Mask* instructs the Switch to examine the packet header. • *IPv6* instructs the switch to examine the IPv6 address in each frame's header.
Priority (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. *Replace Priority with* – Click the corresponding box if you want to re-write 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.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Offset	This field will allow users to examine any specified content up to 80 bytes within a packet at one time and instruct the Switch to mask the packet header beginning with the offset value specified: • *value (0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte. • *value (16-31)* - Enter a value in hex form to mask the packet from byte 16 to *byte 31.* • *value (32-47)* - Enter a value in hex form to mask the packet from byte 32 to byte 47. • *value (48-63)* - Enter a value in hex form to mask the packet from byte 48 to byte 63. • *value (64-79)* - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Port	The user may set the Access Rule to *Permit* or *Deny* on a per-port basis by entering a port number in this field. Any other specified criteria applies as well.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following window:

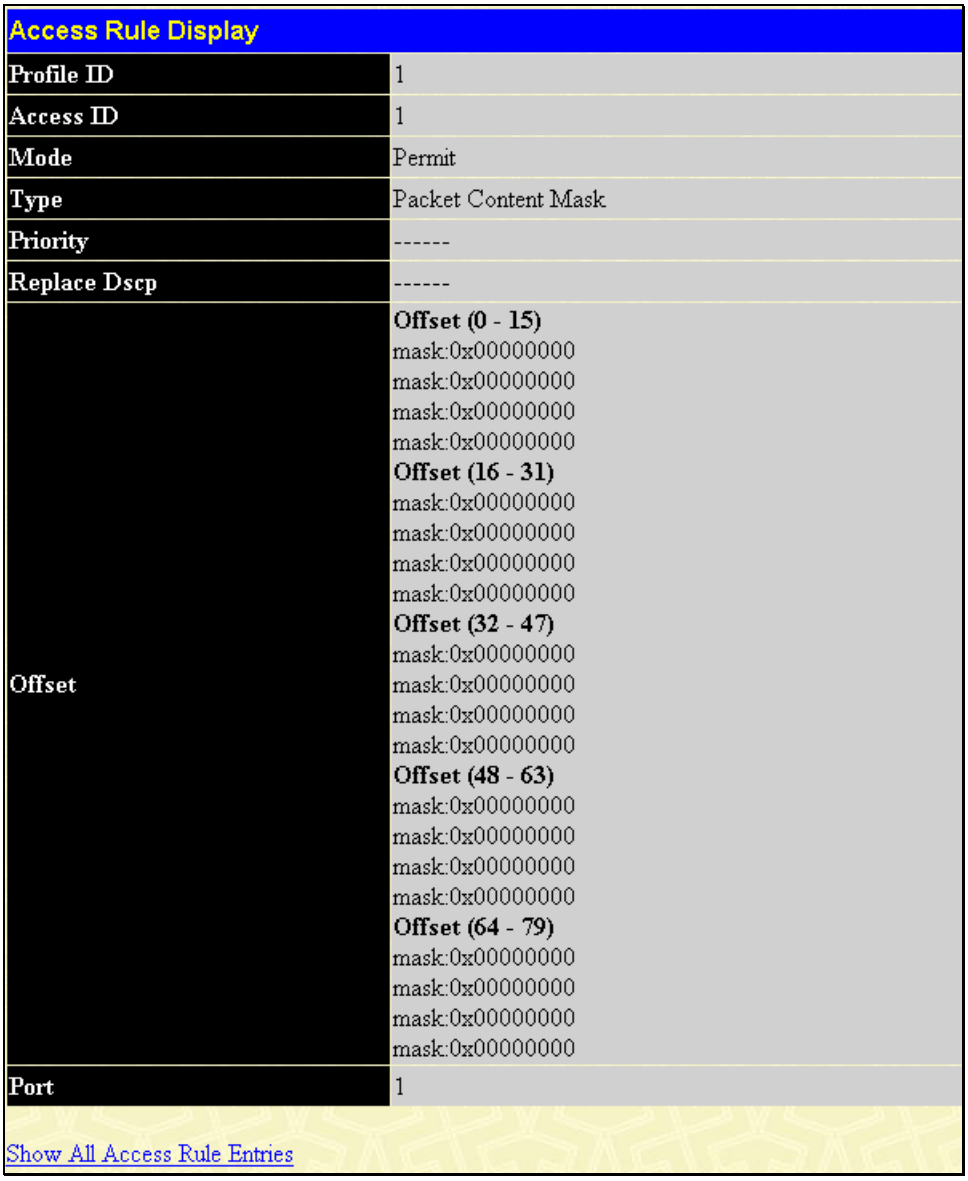


Figure 10- 56. Access Rule Display window (Packet Content)

To configure the Access Rule for IPv6, open the Access Profile Table and click **Modify** for an IPv6 entry. This will display the Access Rule Table.

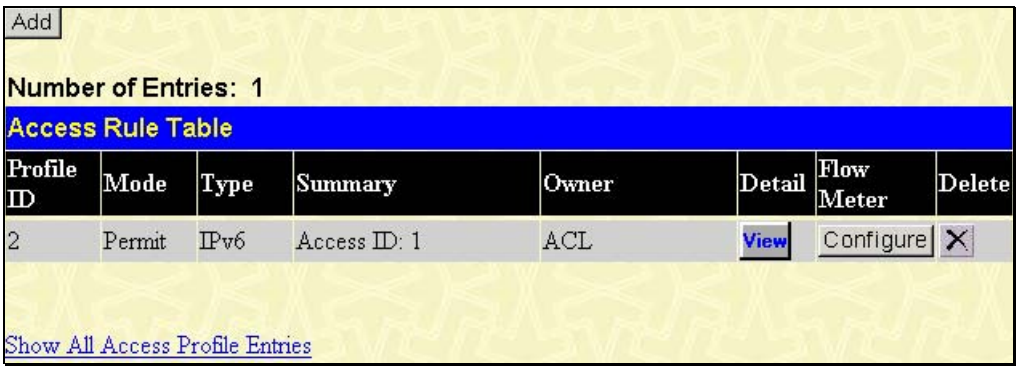


Figure 10- 57. Access Rule Table window

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding button. To configure the Flow Meter Settings click the **Configure** button. To display all rules in the table, click the **Show All Access Profile Entries** button.

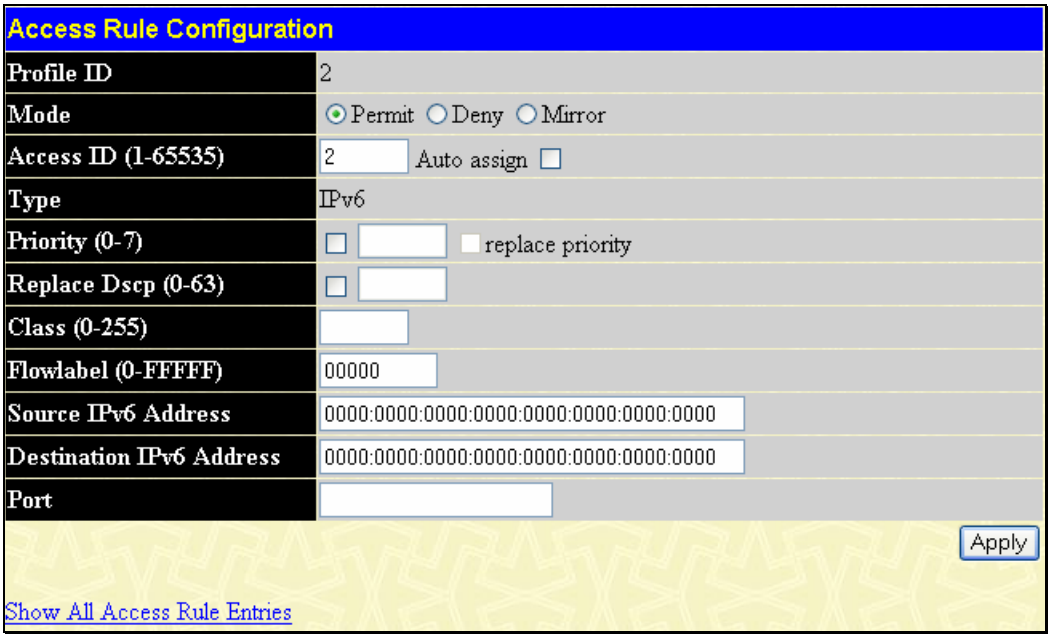


Figure 10- 58. Access Rule Configuration window (IPv6)

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

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the Switch, according to any additional rule, forwards the packets that match the access profile 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 monitor and copy the packets forwarded by the switch.
Access ID (1-65535)	Type in a unique identifier number for this access or use **Auto Assign**.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header. • *IPv6* instructs the switch to examine the IPv6 address in each frame's header.
Priority (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. *Replace Priority with* – Click the corresponding box if you want to re-write 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.

Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Class (0-255)	The user may enter a value for the Class to instruct the Switch to examine the *class* field of the IPv6 header.
Flowlabel (0-FFFFF)	The user may 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.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.
Port	The user may set the Access Rule to *Permit* or *Deny* on a per-port basis by entering a port number in this field. Any other specified criteria applies as well.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following window:

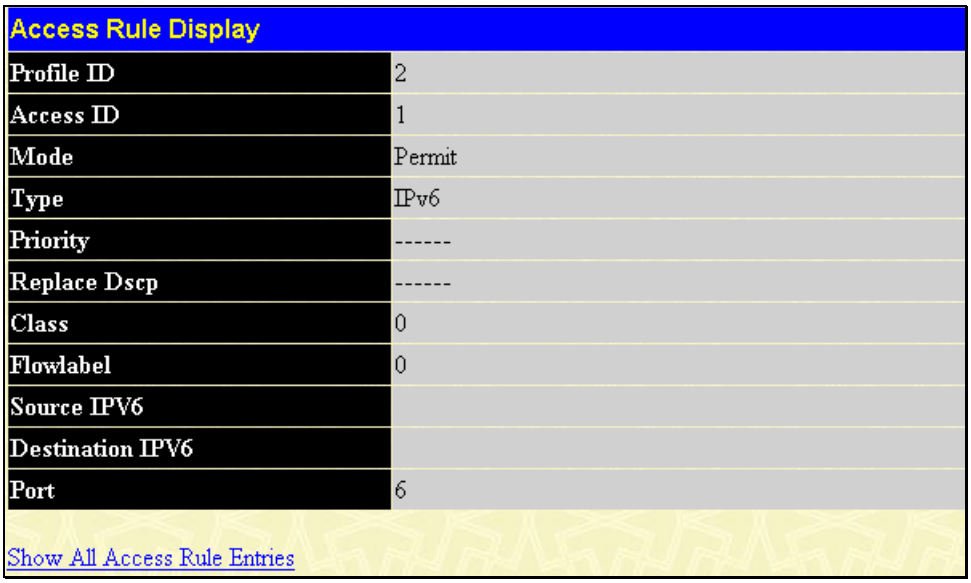


Figure 10- 59. Access Rule Display window (IPv6)

Flow Metering Table

Flow Metering Table is a per flow bandwidth control used to limit the bandwidth of the ingress traffic. When the users create an ACL rule to filter packets, a metering rule can be created to associate with this ACL rule to limit traffic. The step of bandwidth is 64kbps. Due to limited metering rules, not all ACL rules can associate with a metering rule.

To view the **Flow Metering Table**, click **ACL > Flow Metering Table**.

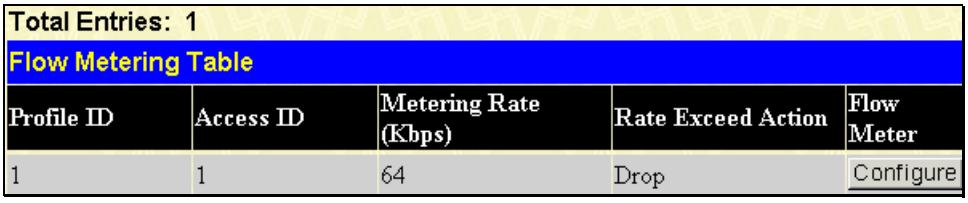


Figure 10- 20. Flow Metering Table

To edit an existing entry click the configure button which will open the **Flow Metering Table** page, as shown below.

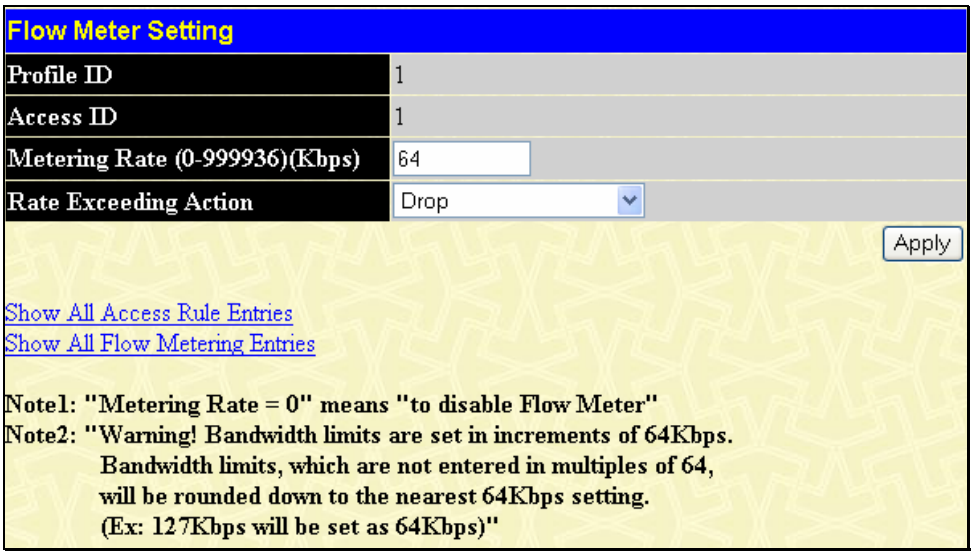


Figure 10- 9. Flow Meter Setting

To enter a new rule set for an access profile click the **Apply** button. To view an existing access rule entry click the hyperlinked **Show All Access Rule Entries**, to view existing flow metering entries click the hyperlinked **Show All Flow Metering Entries**.

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.
Metering Rate (0-999936) (Kbps)	Users may set the rate of packets flowing into the switch between *0* and *999936* Kbps, a value of *0* will disable the Flow Meter.
Rate Exceeding Action	This field denotes the course of action the packet will take. • *Drop* – drops the packets. • *Set Drop Precedence* – the packet will not be dropped right away. However, when the traffic is busy, it has the higher probability to be dropped in the later stage.

CPU Interface Filtering

Due to a chipset limitation and the need for extra switch security, the xStack DES-3800 switch series 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 Interface Filtering Profile Table

Click **ACL** > **CPU Interface Filtering** > **CPU Interface Filtering Table** to display the CPU Access Profile Table entries created on the Switch. To view the configurations for an entry, click the hyperlinked **Profile ID** number.

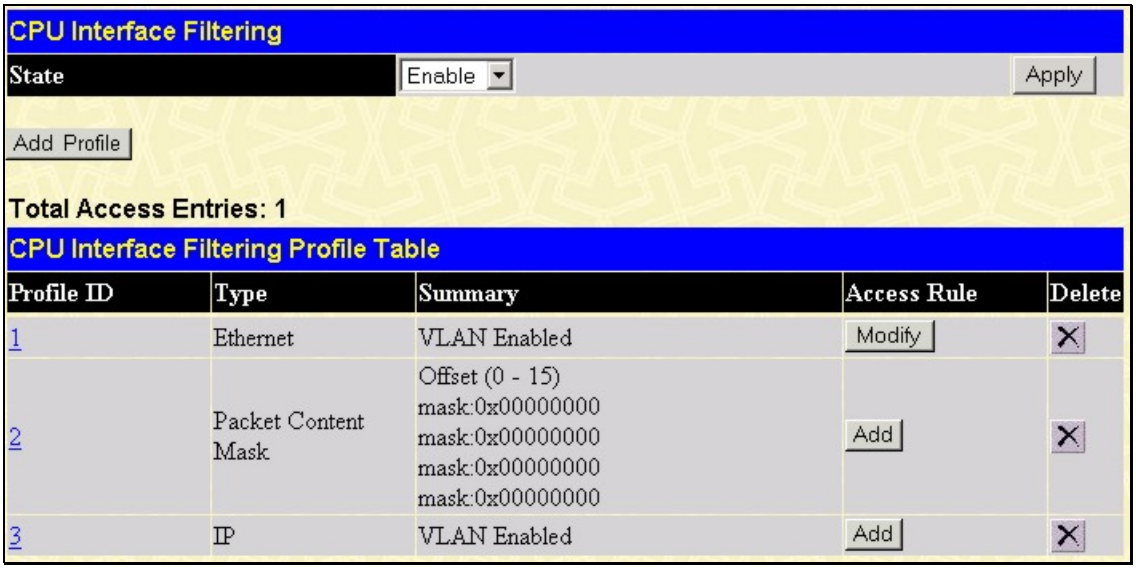


Figure 10- 10. CPU Interface Filtering Table

The user may globally enable or disable the CPU Interface Filtering function by using the pull down menu in the **State** field. Disabling the CPU Interface Filtering function will not alter or destroy any configurations; it will only disable the function.

To add an entry to the **CPU Interface Filtering Profile Table**, click the **Add Profile** button. This will open the **CPU Interface Filtering Profile Configuration** page, as shown below. There are three **CPU Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration and one for the **Packet Content Mask**. You can switch between the three **CPU Access Profile Configuration** pages by using the **Type** drop-down menu. The page shown below is the **Ethernet CPU Interface Filtering Configuration** page.

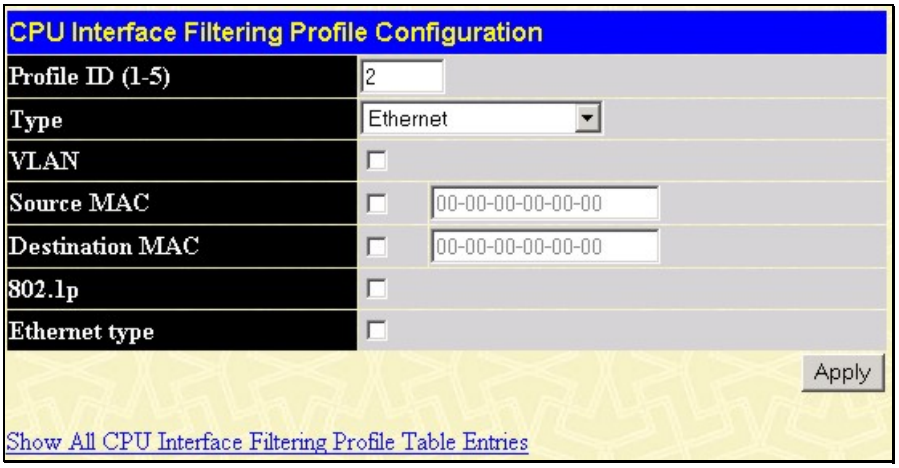


Figure 10- 11. CPU Interface Filtering Profile Configuration – Ethernet

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile. • Select *Ethernet* to instruct the Switch to examine the layer 2 part of each packet header. • Select *IP* 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.
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.
Source MAC	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
802.1p	Enter a value from 0-7 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.

The page shown below is the **CPU Interface Filtering Profile Configuration** for **IP** page.

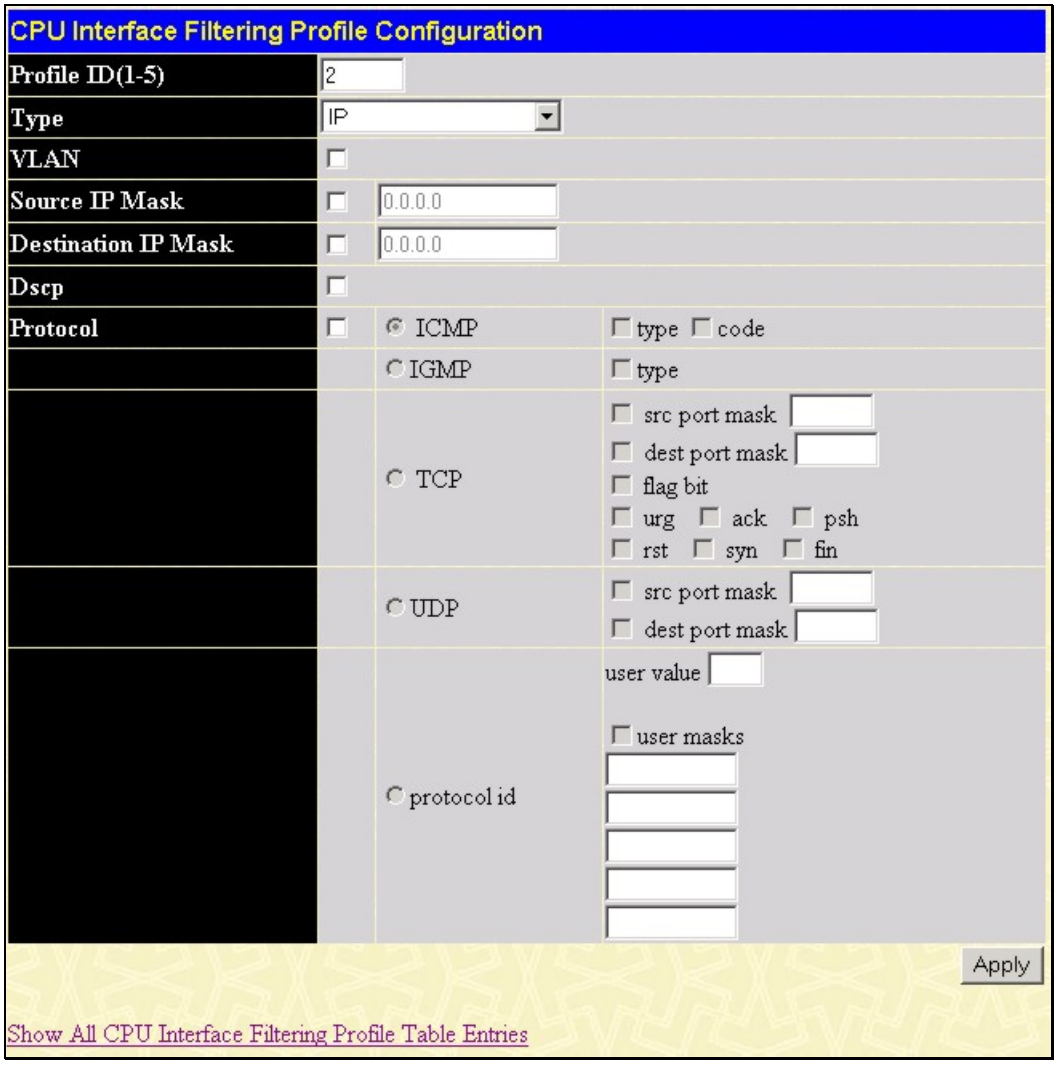


Figure 10- 12. CPU Interface Filtering Configuration window - IP

The following parameters can be modified:

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or Packet Content Mask. This will change the menu according to the requirements for the type of profile. • Select *Ethernet* to instruct the Switch to examine the layer 2 part of each packet header. • Select *IP* 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.
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.
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.
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.
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. • **dest 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). • **dest port mask** - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff). **protocol id** - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xffffffff).

Click **Apply** to set this entry in the Switch's memory.

The page shown below is the **CPU Interface Filtering Profile Configuration** window for the **Packet Content Mask**.

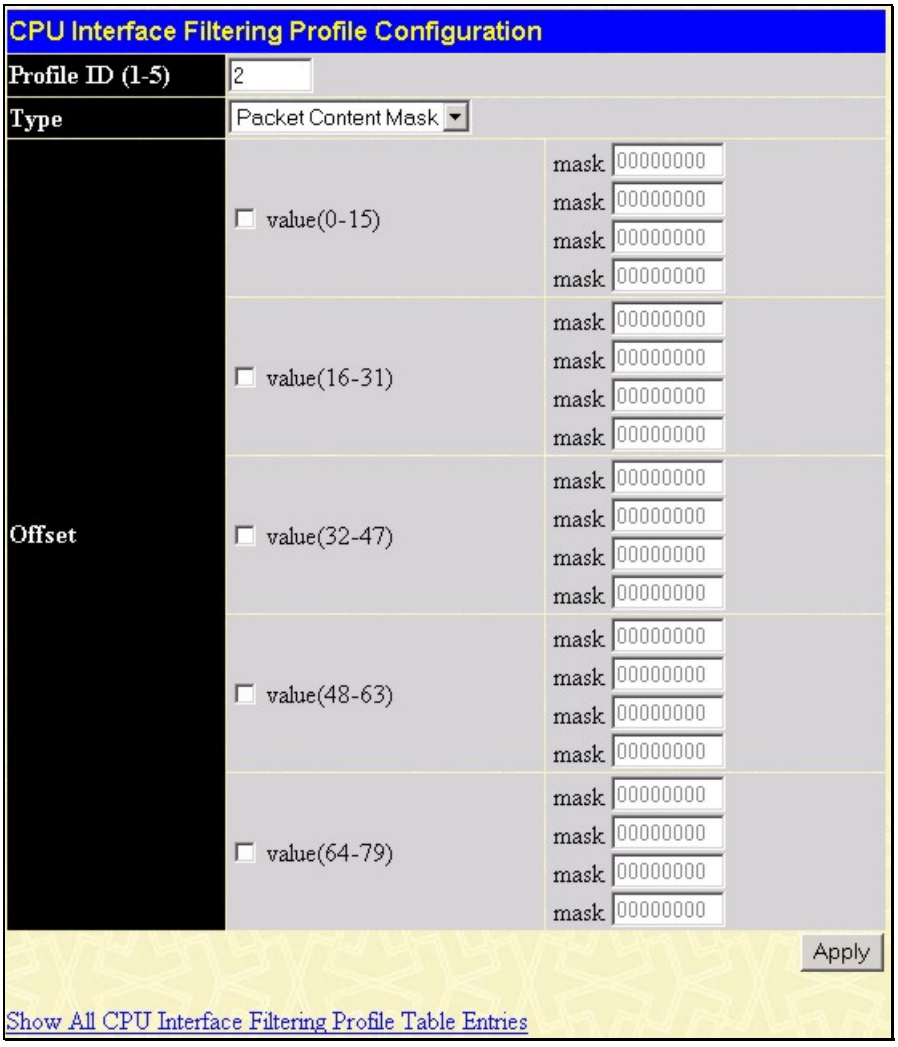


Figure 10- 13. CPU Interface Filtering Configuration window- Packet Content

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **Packet Content Mask**:

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile. • Select *Ethernet* to instruct the Switch to examine the layer 2 part of each packet header. • Select *IP* 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: • *value (0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • *value (16-31)* – Enter a value in hex form to mask the packet from byte 16 to byte 31. • *value (32-47)* – Enter a value in hex form to mask the packet from byte 32 to byte 47. • *value (48-63)* – Enter a value in hex form to mask the packet from byte 48 to byte 63. • *value (64-79)* – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click **Apply** to implement changes made.

To establish the rule for a previously created CPU Access Profile:

Click **ACL** > **CPU Interface Filtering** to view the following window:

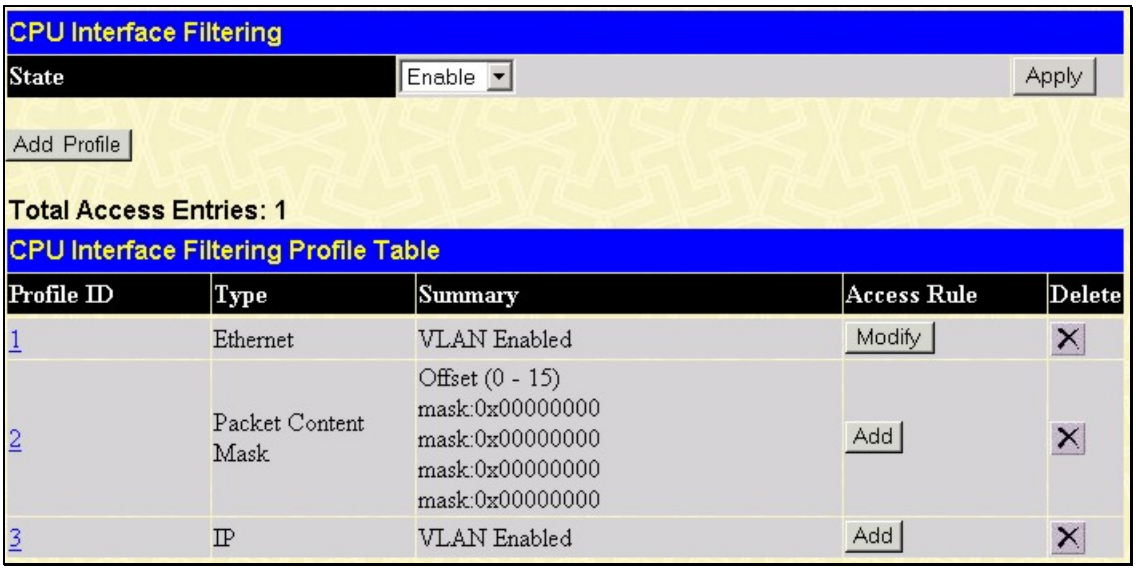


Figure 10- 14. CPU Interface Filtering Profile Table - Add

In this window, the user may add an **Access Rule** to a previously created CPU access profile by clicking the corresponding **Modify** button of the entry to configure **Ethernet, IP** or **Packet Content Mask**.

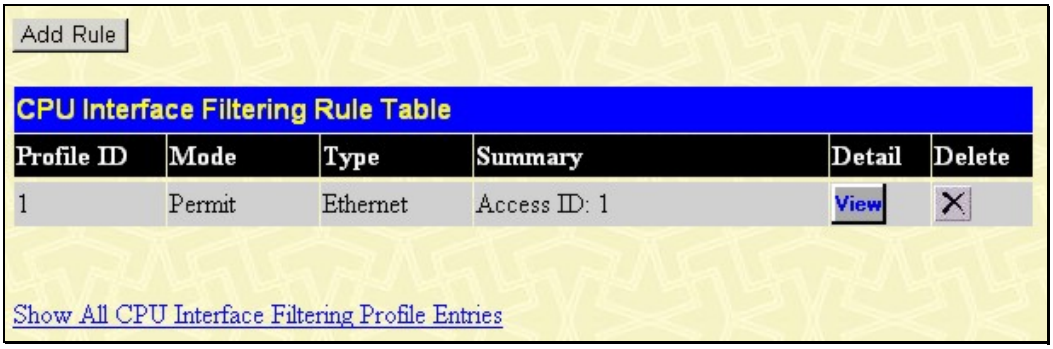


Figure 10- 15. CPU Interface Filtering Rule Table

Click the **Add Rule** button to continue on to the **CPU Interface Filtering Rule Table** window. A new and unique window, for Ethernet, IP and Packet Content will open as shown in the examples below.

To change a rule for a previously created CPU Access Profile Rule:

In this window, the user may change a rule that has been previously created by clicking the corresponding **Modify** button of the entry.

The **CPU Interface Filtering Rule Configuration** allows the user to create a rule for a previously created CPU Access Profile.

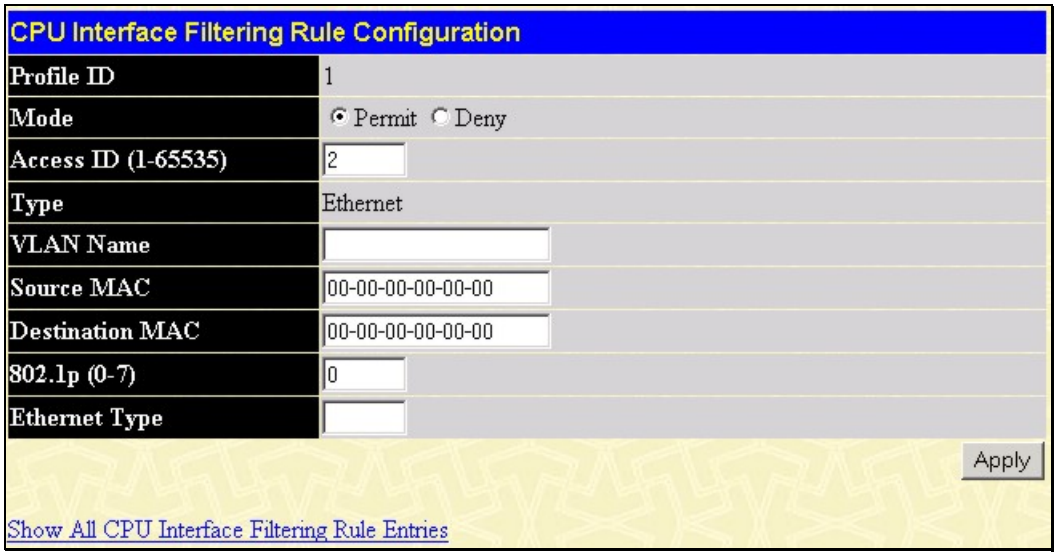


Figure 10- 16. CPU Interface Filtering Rule Configuration – Ethernet

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

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select **Deny** to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access and priority. This value can be set from 1 - 65535.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source MAC	Source MAC Address - Enter a MAC Address for the source MAC address.
Destination MAC	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
802.1P (0-7)	Enter a value from 0-7 to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.

To view the settings of a previously configured rule, click View in the **Access Rule Table** to view the following screen:

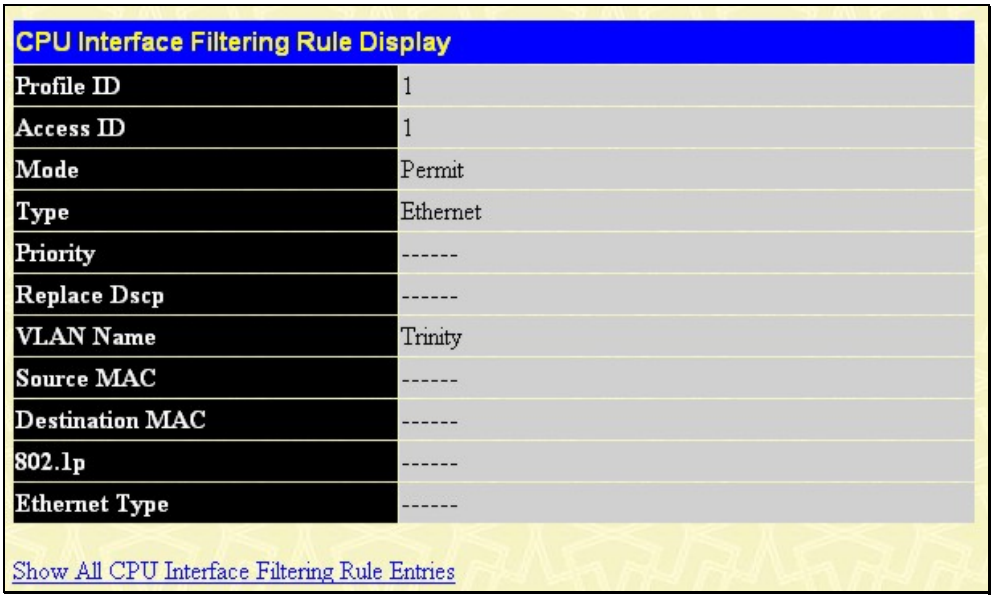


Figure 10- 17. CPU Interface Filtering Rule Display – Ethernet

The following window is the **CPU Interface Filtering Rule Table** for IP.

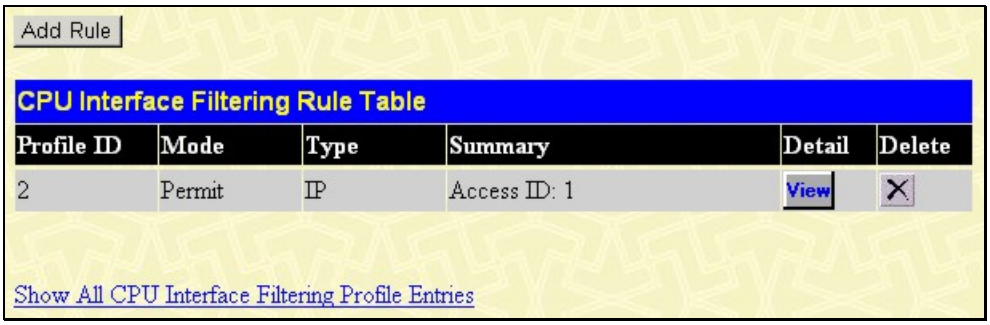


Figure 10- 18. CPU Interface Filtering Rule Table – IP

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding button. The following window is used for the CPU IP Rule configuration.

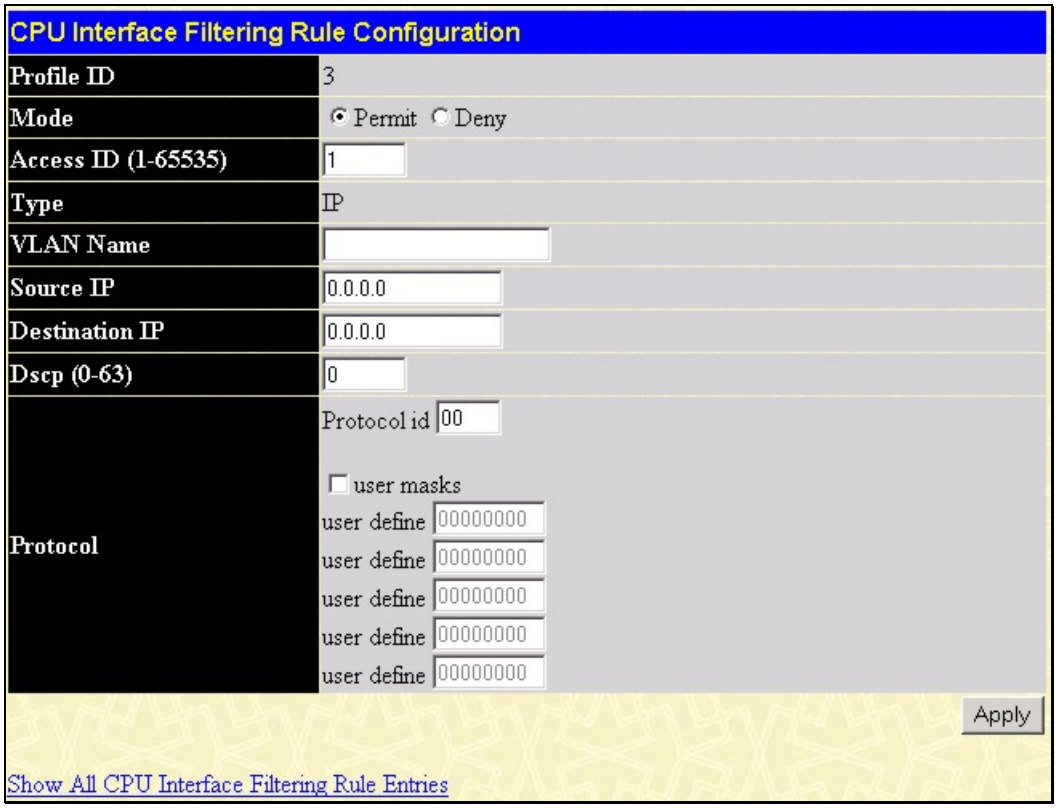


Figure 10- 19. CPU Interface Filtering Rule Configuration – IP

Configure the following **Access Rule Configuration** settings for IP:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select **Deny** to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 -65535.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address - Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address- Enter an IP Address mask for the destination IP address.
Dscp (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.
Protocol	This field allows the user to modify the protocol used to configure the **Access Rule Table;** depending on which protocol the user has chosen in the **Access Profile Table**.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following screen:

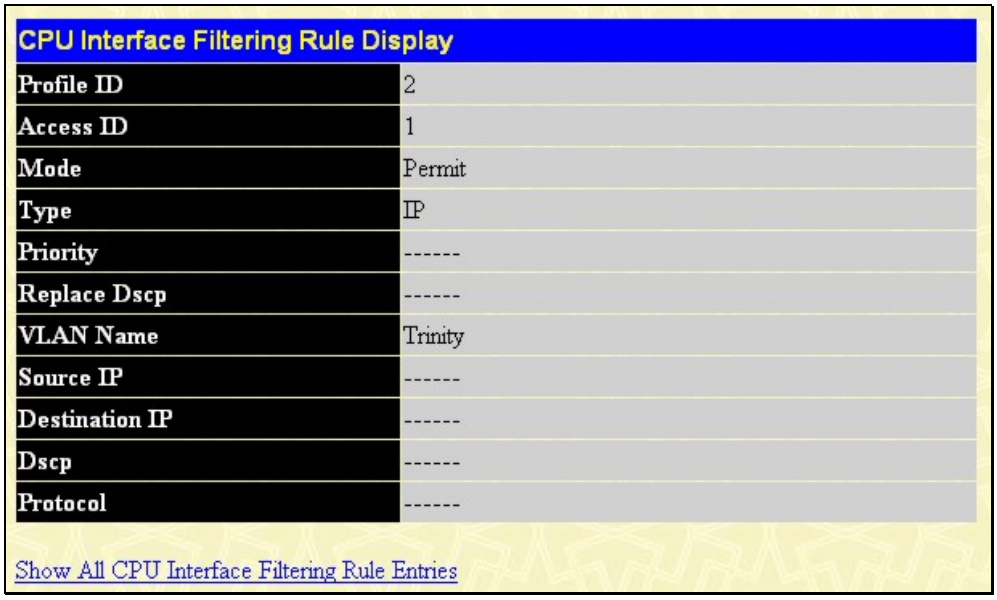


Figure 10- 20. CPU Interface Filtering Rule Display - IP

The following window is the **CPU Interface Filtering Rule Table** for Packet Content.

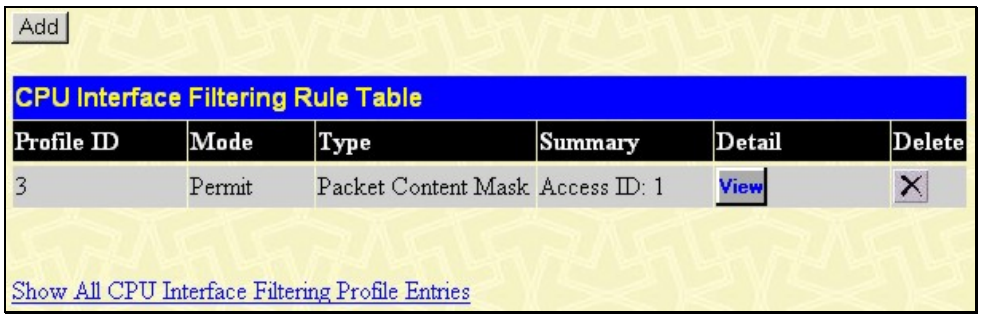


Figure 10- 21. CPU Interface Filtering Rule Table – Packet Content

To remove a previously created rule, select it and click the ✕ button. To add a new CPU Access Rule, click the **Add** button:

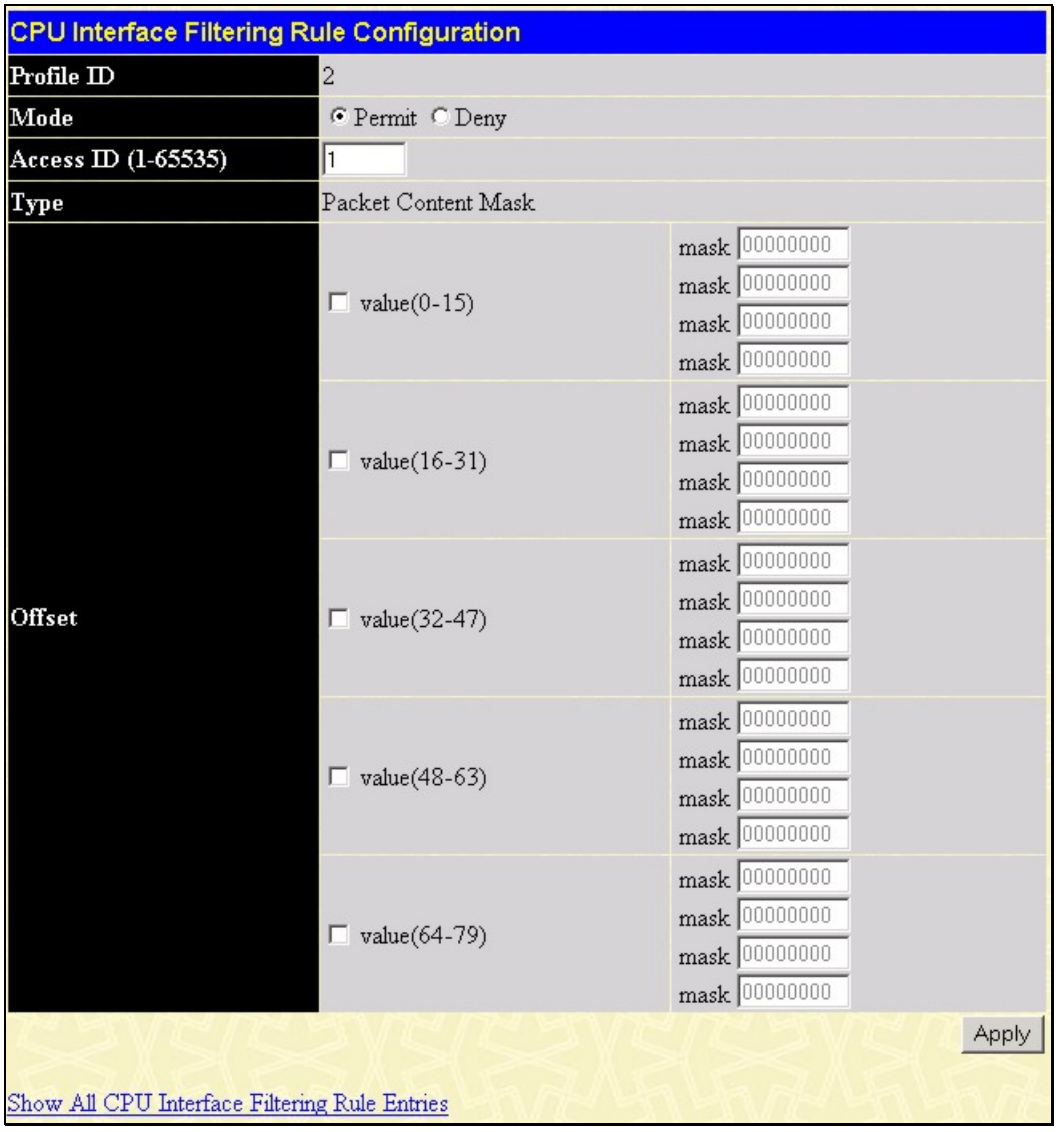


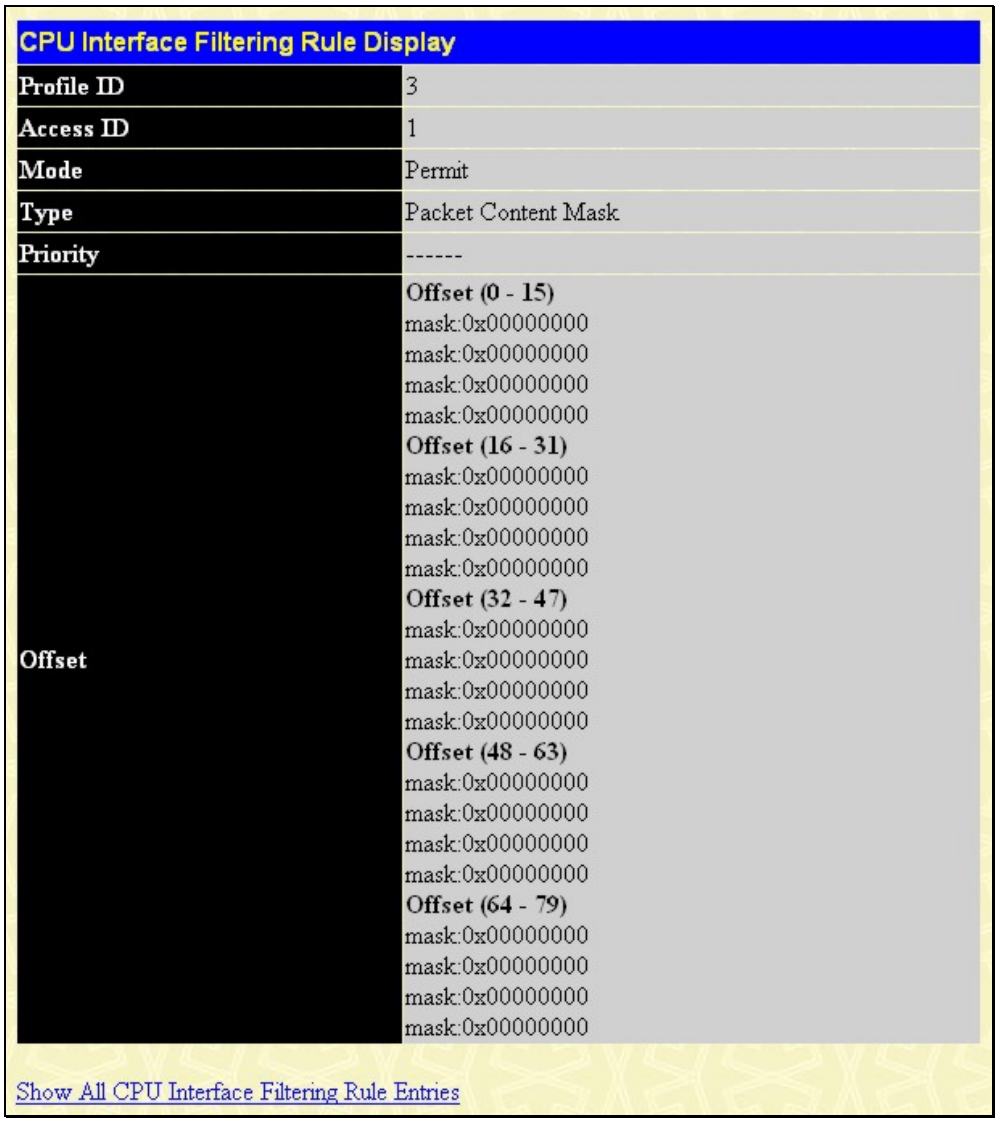
Figure 10- 22. CPU Interface Filtering Rule Configuration - Packet Content Mask

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

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select **Deny** to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 65535.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: • *value (0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte.

	• *value (16-31)* - Enter a value in hex form to mask the packet from byte 16 to *byte 31.* • *value (32-47)* - Enter a value in hex form to mask the packet from byte 32 to byte 47. • *value (48-63)* - Enter a value in hex form to mask the packet from byte 48 to byte 63. • *value (64-79)* - Enter a value in hex form to mask the packet from byte 64 to byte 79.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following screen:



CPU Interface Filtering Rule Display

Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content Mask
Priority	------
Offset	Offset (0 - 15) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 Offset (16 - 31) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 Offset (32 - 47) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 Offset (48 - 63) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 Offset (64 - 79) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000

Show All CPU Interface Filtering Rule Entries

Figure 10- 60. CPU Interface Filtering Rule Display – Packet Content

Section 11

Security

Traffic Control

Port Security

Port Lock Entries

802.1X

Trusted Host

Access Authentication Control

Traffic Segmentation

Broadcast Segmentation

SSL

SSH

IP MAC Binding

Limited IP Multicast Range

Web-based Access Control

MAC-based Access Control

Safeguard Engine

Filter

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 the following window to configure Traffic Control, click **Security** > **Traffic Control**.

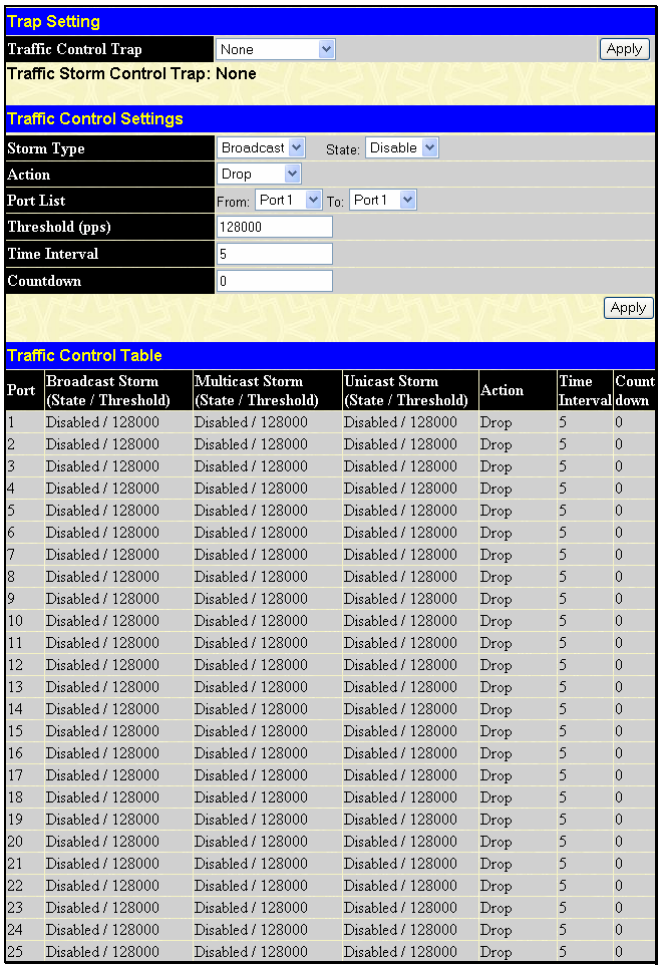


Figure 11- 1. Traffic Control Table window

Parameter	Description
Trap Setting	
Traffic Control Trap	Enable the sending of Traffic Control Trap messages when the type of action taken by the Traffic Control function is handling a Traffic Storm in one of the following situations: • *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 Hardware mode. (When *Drop* is chosen from the **Action** field.

Traffic Control Settings	
Storm 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 the specified type of storm detection.
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.
Port List	Use the *From* and *To* drop-down menus to select the ports that need to be manually recovered from the Shutdown state.
Threshold (pps)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from 0-255000 with a default setting of 128000.
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.
Countdown	The Countdown 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 the default setting for this field and 0 will denote that the port will immediately shutdown.

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

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

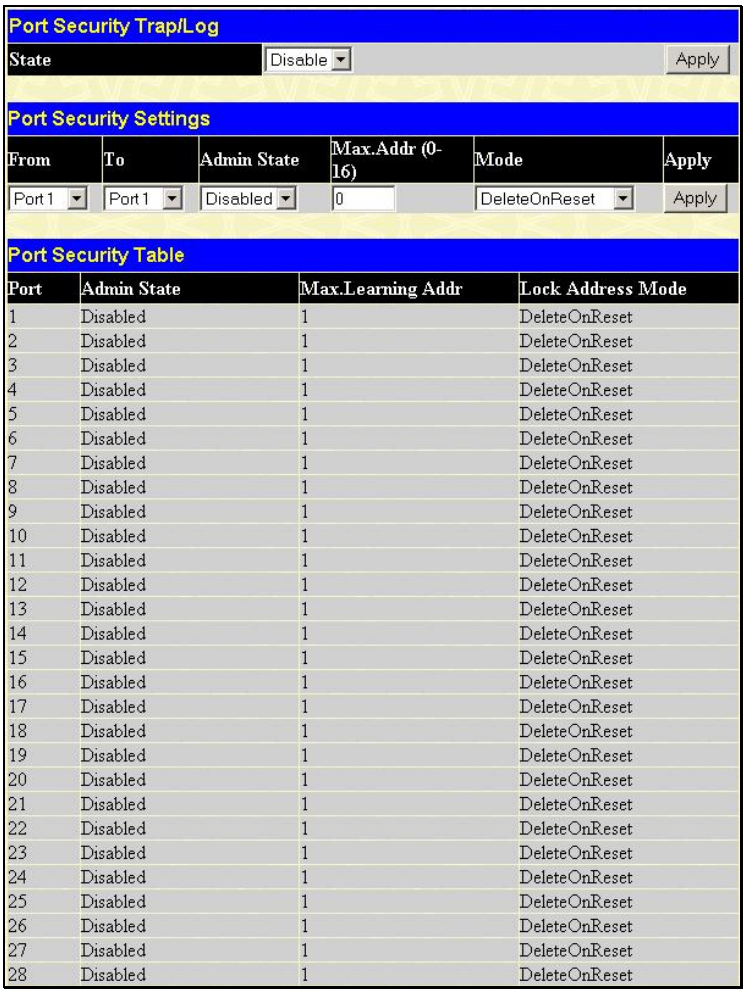
NOTE: Ports that are in the Shutdown forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

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.

Port Security

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 Trap/Log

State: Disable — Apply

Port Security Settings

From	To	Admin State	Max.Addr (0-16)	Mode	Apply
Port 1	Port 1	Disabled	0	DeleteOnReset	Apply

Port Security Table

Port	Admin State	Max.Learning Addr	Lock Address Mode
1	Disabled	1	DeleteOnReset
2	Disabled	1	DeleteOnReset
3	Disabled	1	DeleteOnReset
4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Disabled	1	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset
13	Disabled	1	DeleteOnReset
14	Disabled	1	DeleteOnReset
15	Disabled	1	DeleteOnReset
16	Disabled	1	DeleteOnReset
17	Disabled	1	DeleteOnReset
18	Disabled	1	DeleteOnReset
19	Disabled	1	DeleteOnReset
20	Disabled	1	DeleteOnReset
21	Disabled	1	DeleteOnReset
22	Disabled	1	DeleteOnReset
23	Disabled	1	DeleteOnReset
24	Disabled	1	DeleteOnReset
25	Disabled	1	DeleteOnReset
26	Disabled	1	DeleteOnReset
27	Disabled	1	DeleteOnReset
28	Disabled	1	DeleteOnReset

Figure 11- 2. Port Security Settings window

The following parameters can be set:

Parameter	Description
From/To	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 Addr. (0-16)	The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.
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 Lock Entries

The **Port Lock Entries Table** window is used to remove an entry from the port security entries learned by the Switch and entered into the forwarding database. To view the following window, click **Security > Port Lock Entries**:

Figure 11- 3. Port Lock Entries Table

This function is only operable if the **Mode** in the **Port Security** window is selected as **Permanent** or **DeleteOnReset,** or in other words, only addresses that are permanently learned by the Switch can be deleted. Once the entry has been defined by entering the correct information into the window above, click the ✕ under the **Delete** heading of the corresponding MAC address to be deleted. Click the **Next** button to view the next page of entries listed in this table. This window displays the following information:

Parameter	Description
VID	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
VLAN NAME	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
Port	The ID number of the port that has permanently learned the MAC address.
Type	The type of MAC address in the forwarding database table. Only entries marked *Secured_Permanent* can be deleted.
Delete	Click the ✕ in this field to delete the corresponding MAC address that was permanently learned by the Switch.

Port Access Entity (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:

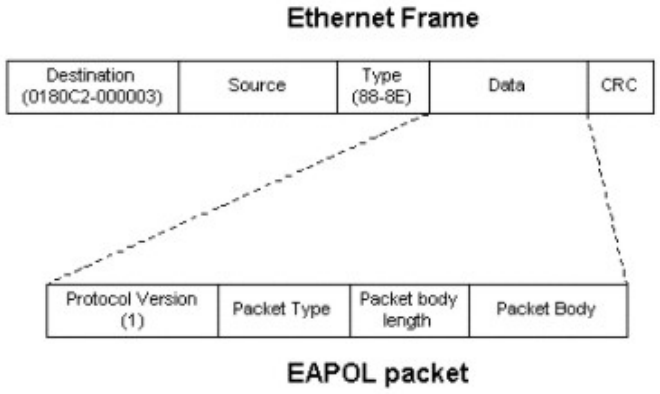


Figure 11- 4. The EAPOL Packet

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 up keeping a stable and working Access Control security method.

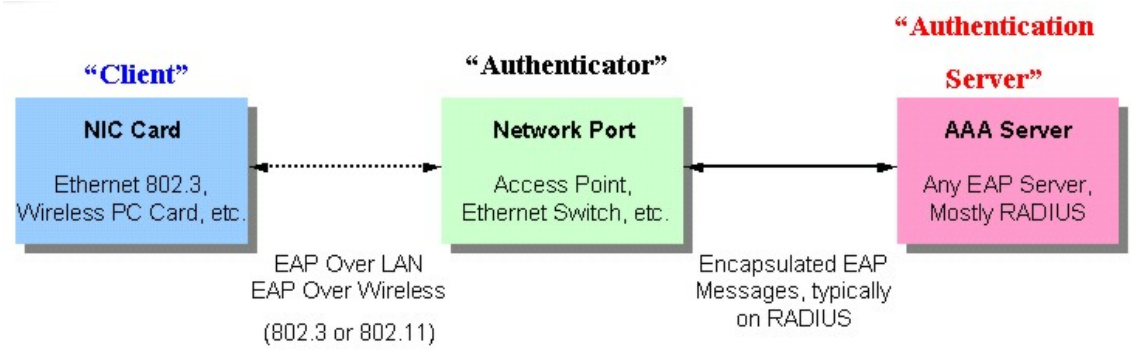


Figure 11- 5. The three roles of 802.1x

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.

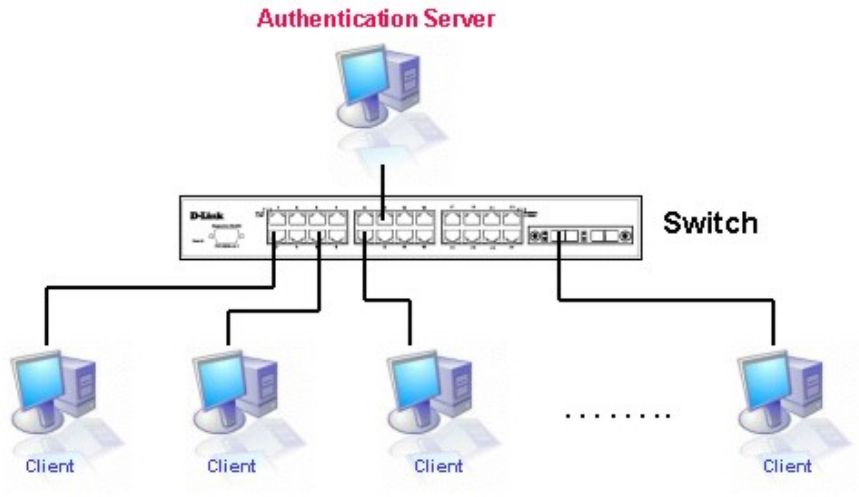


Figure 11- 6. The Authentication Server

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*. (**DES-3800 Web Management Tool**)
2. The 802.1x settings must be implemented by port (**Security** / **802.1x** / **Configure 802.1X Authenticator Parameter**)
3. A RADIUS server must be configured on the Switch. (**Security** / **802.1x** / **Authentic RADIUS Server**)

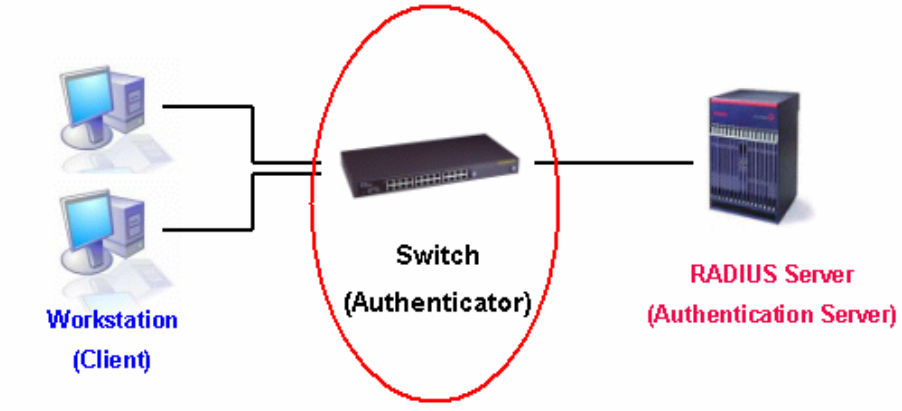


Figure 11- 7. The Authenticator

Client

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

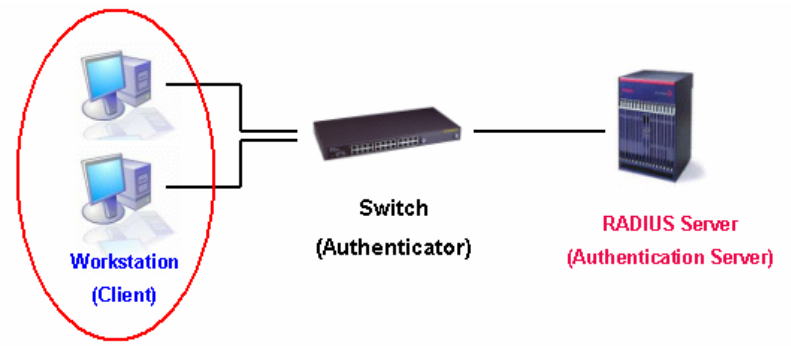


Figure 11- 8. The Client

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.

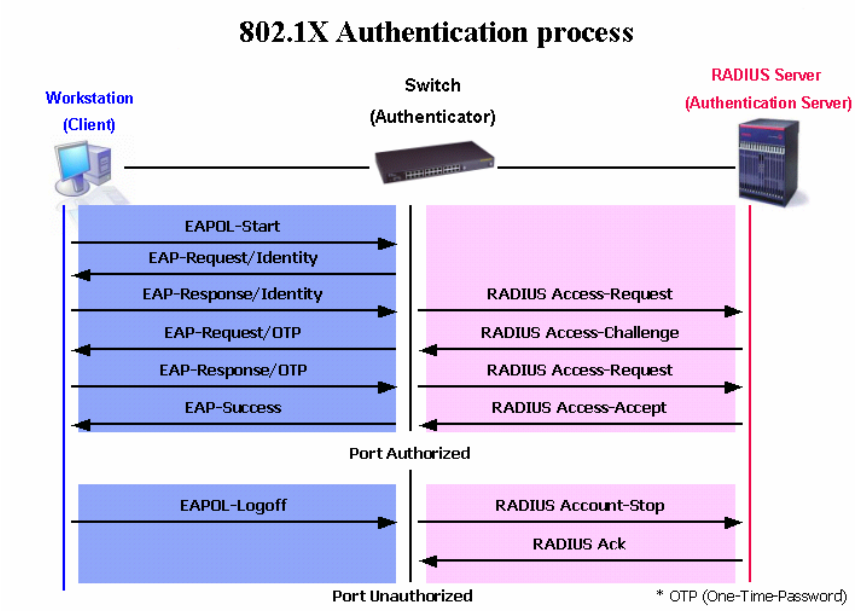


Figure 11- 9. The 802.1x Authentication Process

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

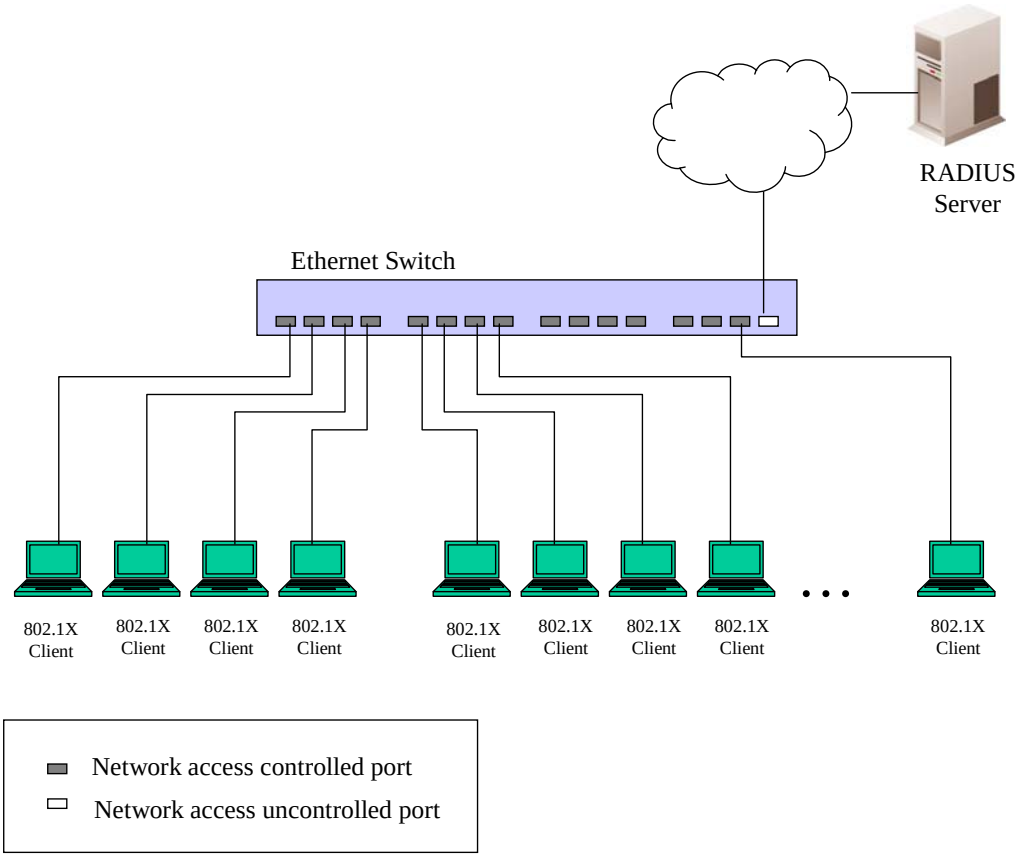


Figure 11- 10. Example of Typical Port-Based Configuration

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

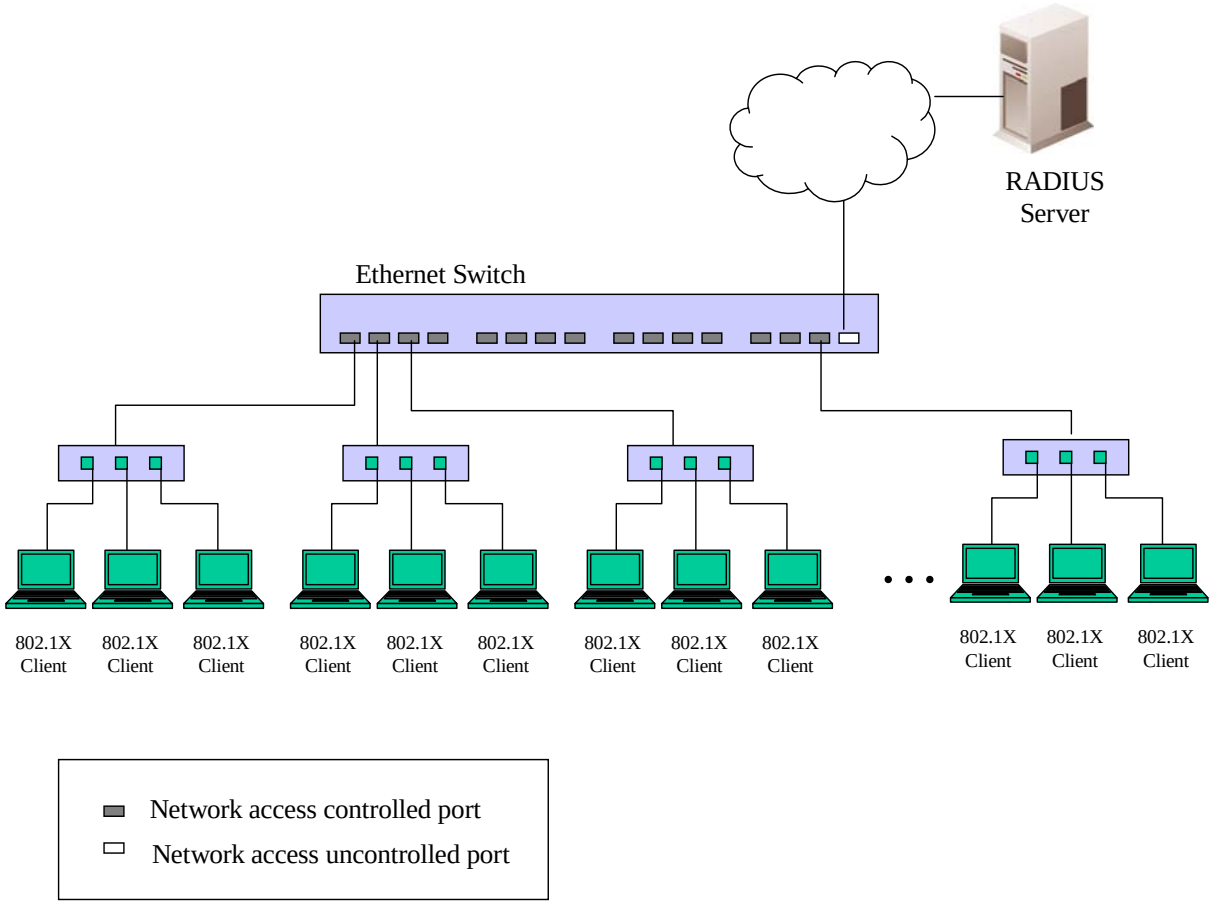


Figure 11- 11. Example of Typical MAC-Based Configuration

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.

Configure 802.1x Authenticator Parameter

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

Configure 802.1X Authenticator Parameter

Port	AdmDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled	Capability
1	both	Auto	30	60	30	30	2	3600	No	None
2	both	Auto	30	60	30	30	2	3600	No	None
3	both	Auto	30	60	30	30	2	3600	No	None
4	both	Auto	30	60	30	30	2	3600	No	None
5	both	Auto	30	60	30	30	2	3600	No	None
6	both	Auto	30	60	30	30	2	3600	No	None
7	both	Auto	30	60	30	30	2	3600	No	None
8	both	Auto	30	60	30	30	2	3600	No	None
9	both	Auto	30	60	30	30	2	3600	No	None
10	both	Auto	30	60	30	30	2	3600	No	None
11	both	Auto	30	60	30	30	2	3600	No	None
12	both	Auto	30	60	30	30	2	3600	No	None
13	both	Auto	30	60	30	30	2	3600	No	None
14	both	Auto	30	60	30	30	2	3600	No	None
15	both	Auto	30	60	30	30	2	3600	No	None
16	both	Auto	30	60	30	30	2	3600	No	None
17	both	Auto	30	60	30	30	2	3600	No	None
18	both	Auto	30	60	30	30	2	3600	No	None
19	both	Auto	30	60	30	30	2	3600	No	None
20	both	Auto	30	60	30	30	2	3600	No	None
21	both	Auto	30	60	30	30	2	3600	No	None
22	both	Auto	30	60	30	30	2	3600	No	None
23	both	Auto	30	60	30	30	2	3600	No	None
24	both	Auto	30	60	30	30	2	3600	No	None
25	both	Auto	30	60	30	30	2	3600	No	None
26	both	Auto	30	60	30	30	2	3600	No	None
27	both	Auto	30	60	30	30	2	3600	No	None
28	both	Auto	30	60	30	30	2	3600	No	None

Figure 11- 12. 802.1X Authenticator Settings window

To configure the settings by port, click on the hyperlinked port number under the Port heading, which will display the following table to configure:

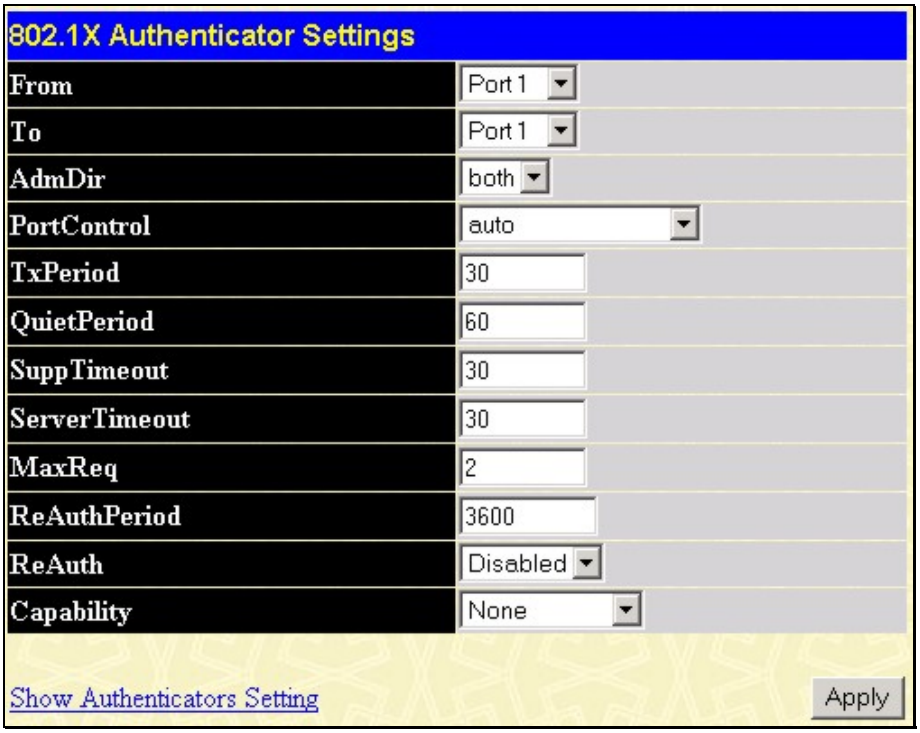


Figure 11- 13. 802.1X Authenticator Settings window (Modify)

This window allows you to set the following features:

Parameter	Description
From [ ] To [ ]	Enter the port or ports to be set.
AdmDir	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.
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*.
TxPeriod	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.
QuietPeriod	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	This value determines timeout conditions in the exchanges between the Authenticator and the

	client. The default setting is *30* seconds.
ServerTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq	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*.
ReAuthPeriod	A constant that defines a nonzero number of seconds between periodic re-authentication of the client. The default setting is *3600* seconds.
ReAuth	Determines whether regular re-authentication will take place on this port. The default setting is *Disabled*.
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.

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

Initializing Ports for Port Based 802.1x

Existing 802.1x port and MAC settings are displayed and can be configured using the window below.

Click **Security > 802.1X > Initialize Port(s)** to open the following window:

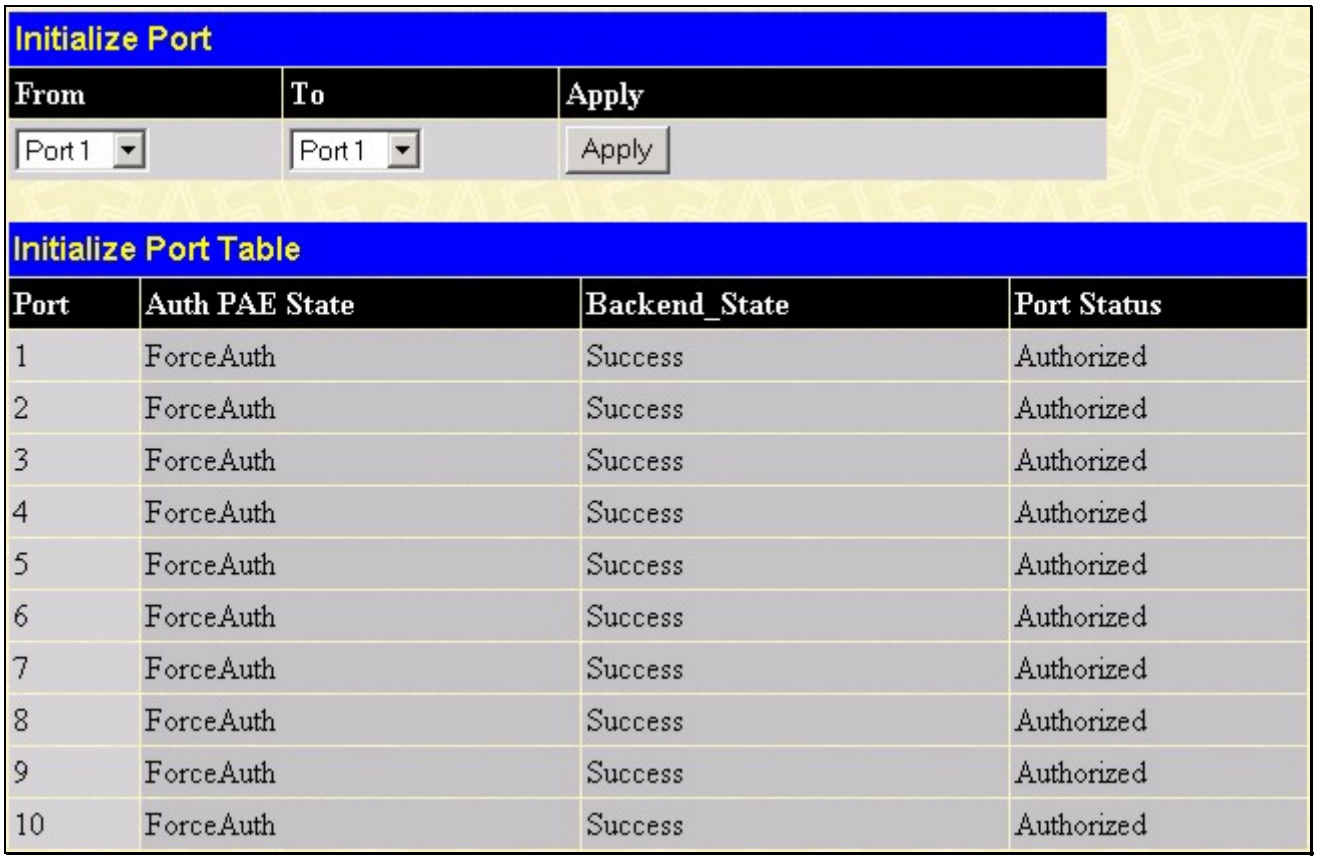


Figure 11- 14. Initialize Port window

This window allows initialization of a port or group of ports. The **Initialize Port Table** in the bottom half of the window displays the current status of the port(s).

This window displays the following information:

Parameter	Description
From / To	Use the drop-down menus to select the ports that need to be initialized.
Port	A read-only field indicating a port on the Switch.
MAC Address	The MAC address of the Switch connected to the corresponding port, if any.
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
Backend State	The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*
Port Status	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A.*

Initializing Ports for MAC Based 802.1x

To initialize ports for the MAC side of 802.1x, the user must first enable 802.1x by MAC address in the **Advanced Settings** window. Click **Security > 802.1X > Initialize Port(s)** to open the following window:

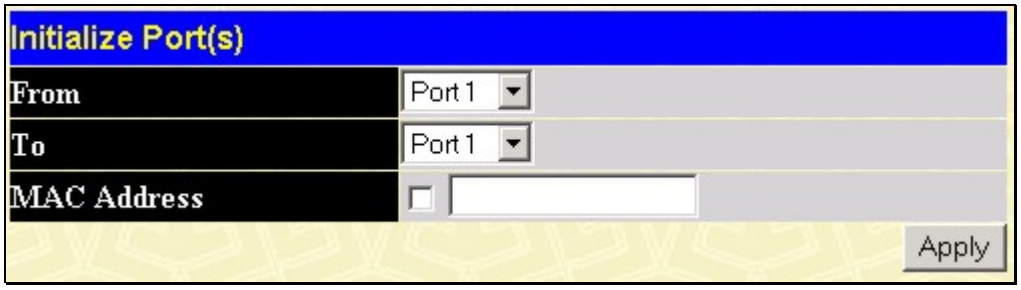


Figure 11- 15. Initialize Ports (MAC based 802.1x)

To initialize ports, first choose the switch in the switch stack by using the **Unit** pull-down menu, then the range of ports in the **From** and **To** field. Then the user must specify the MAC address to be initialized by entering it into the **MAC Address** field and checking the corresponding check box. To begin the initialization, click **Apply**.

NOTE: The user must first globally enable 802.1X in the **Advanced Settings** window in the **Configuration** folder before initializing ports. Information in the **Initialize Ports Table** cannot be viewed before enabling 802.1X.

Reauthenticate Port(s) for Port Based 802.1x

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

Click **Security > 802.1X > Reauthenticate Port(s)** to open the **Reauthenticate Port(s)** window:

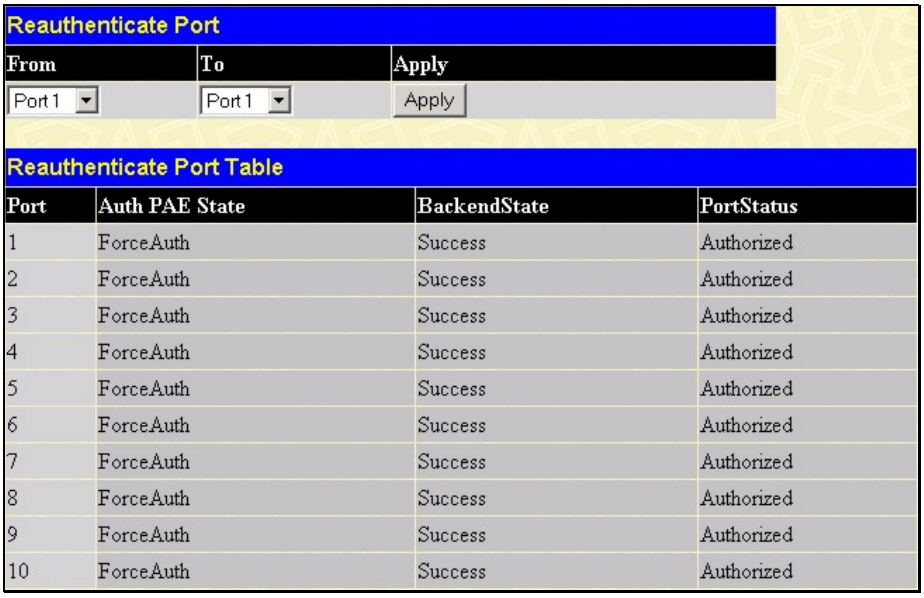


Figure 11- 16. Reauthenticate Port and Reauthenticate Port Table window

This window displays the following information:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
Port	The port number of the reauthenticated port.
MAC Address	Displays the physical address of the Switch where the port resides.
Auth PAE State	The Authenticator State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth*, *ForceUnauth*, and *N/A.*
BackendState	The Backend State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize*, and *N/A.*
PortStatus	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A*.

Reauthenticate Port(s) for MAC-based 802.1x

To reauthenticate ports for the MAC side of 802.1x, the user must first enable 802.1x by MAC address in the **Advanced Settings** window. Click **Security > 802.1X > Reauthenticate Port(s)** to open the following window:

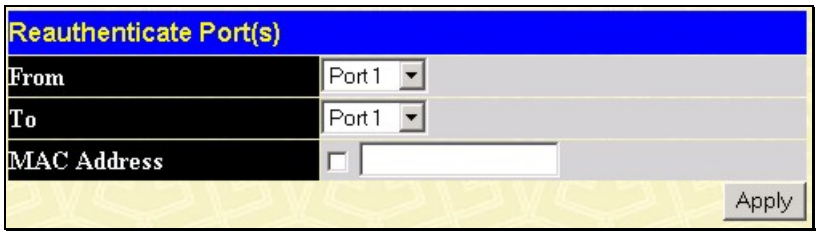


Figure 11- 17. Reauthenticate Ports window – MAC based 802.1x

To reauthenticate ports, first choose the range of ports in the **From** and **To** field. Then the user must specify the MAC address to be reauthenticated by entering it into the **MAC Address** field and checking the corresponding check box. To begin the reauthentication, click **Apply**.

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. The Web Manager offers three windows.

Click **Security** > **802.1x** > **Authentication RADIUS Server** to open the **Authentic RADIUS Server** window shown below:

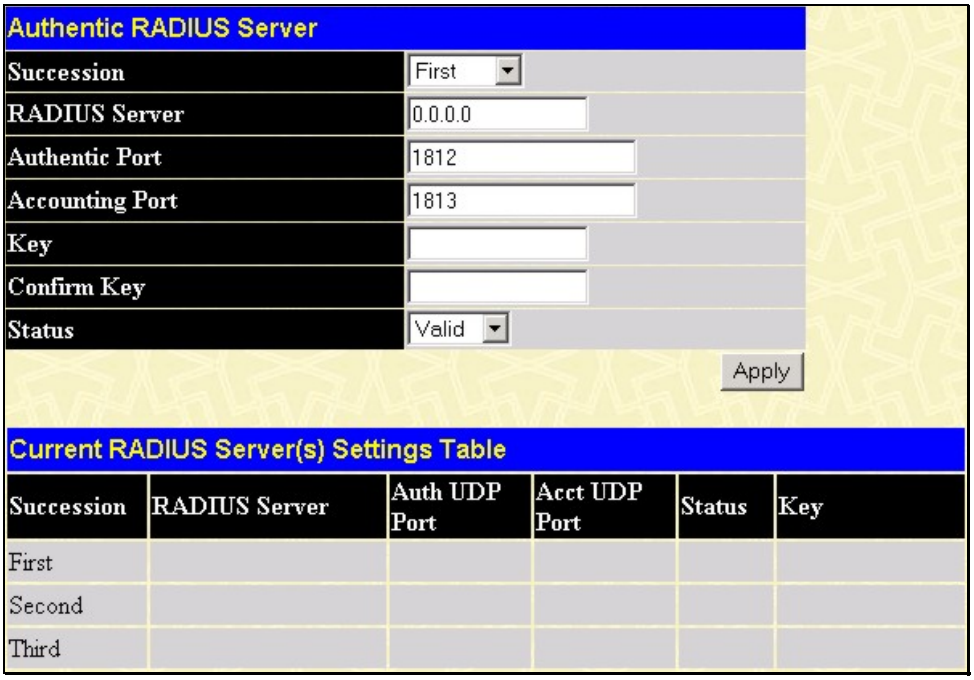


Figure 11- 18. Authentic RADIUS Server window

The window is divided into two main sections. The top section allows the administrator to configure the RADIUS Server settings. The parameters used are explained below:

Parameter	Description
Succession	Choose the desired RADIUS server to configure: *First, Second* or *Third*.
RADIUS Server	Set the RADIUS server IP.
Auth UDP Port	Set the RADIUS authentic server(s) UDP port. The default port is 1812.
Accounting Port	Set the RADIUS account server(s) UDP port. The default port is 1813.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Status	This allows you to set the RADIUS Server as *Valid* (Enabled) or *Invalid* (Disabled).

The bottom of the window displays the settings of the RADIUS servers that are currently setup on the system.

RADIUS Attributes Assignment

1. To assign Ingress/Egress bandwidth by RADIUS server, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth and default priority:

The parameters of the Vendor-Specific attribute are:

Vendor-Specific attribute	Description	Value	Usage
Vendor-ID	Defines the vendor	171 (DLINK)	Required
Vendor-Type	The definition of this attribute	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific field	Used to assign the bandwidth of the port	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1x authentication is successful, the device will assign the correct bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign bandwidth to the port. If the bandwidth attribute is configured on the RADIUS with a value of "0" or more then the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to no_limited.

2. To assign 802.1p default priority by RADIUS server, proper parameters should be configured on the RADIUS Server. Below are the parameters of a user account

The parameters of the Vendor-Specific attribute are:

Vendor-Specific attribute	Description	Value	Usage
Vendor-ID	Defines the vendor	171 (DLINK)	Required
Vendor-Type	The definition of this attribute	4	Required
Attribute-Specific field	Used to assign the 802.1p default priority of the port	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1x authentication is successful, the device will assign the correct 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute configured on the RADIUS is a value out of range (>7), it will not set to the device.

Guest VLANs

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 Guest 802.1x VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement Guest 802.1x 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.

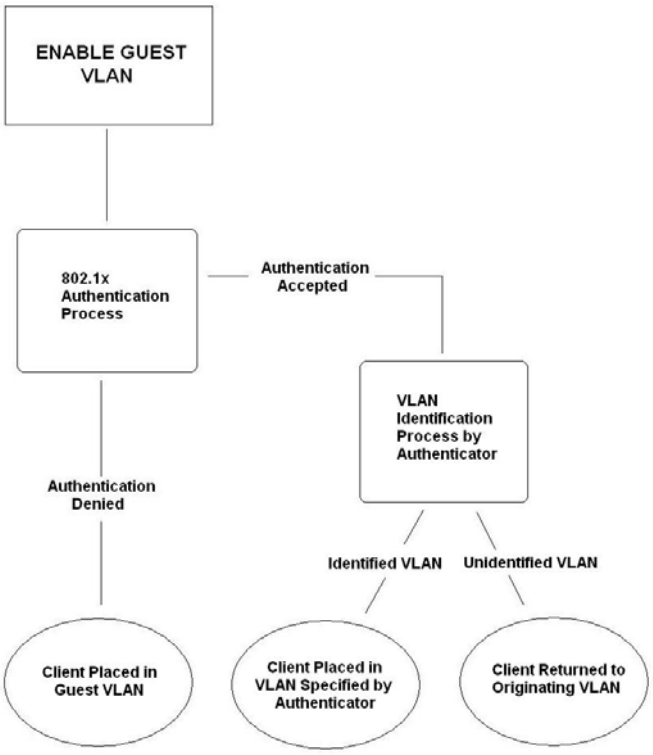


Figure 11- 19. Guest VLAN Authentication Process

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

Click **Security** > **802.1X** > **Guest VLAN**, which will display the following window for the user to configure. Remember, to set a guest 802.1x VLAN, the user must first configure a normal VLAN which can be enabled here for Guest VLAN status. Guest VLANs cannot be configured unless 802.1x is first globally enabled.

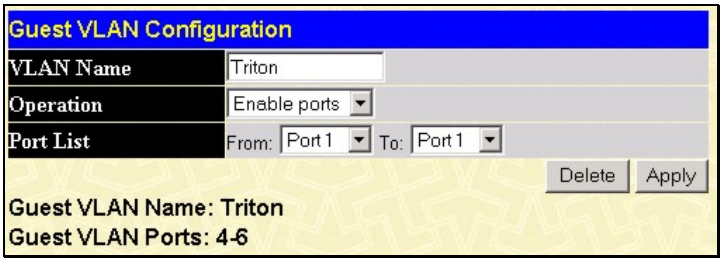


Figure 11- 20. Guest VLAN Configuration window

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

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a guest 802.1x VLAN.
Operation	Allows the user to enable or disable ports for the 802.1x VLAN, using the Port List stated below.
Port List	Set the port list of ports to be enabled for the guest 802.1x VLAN using the pull down menus.

Click **Apply** to implement the guest 802.1x VLAN. Once properly configured, the **Guest VLAN Name** and associated ports will be listed in the lower part of the window, as seen in the example above.

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.

Trusted Host

The Trusted Host window allows the administrator to restrict access to the Switch to up to three specific hosts. To add a new Trusted Host, click **Security >Trusted Host**. The following window will appear:

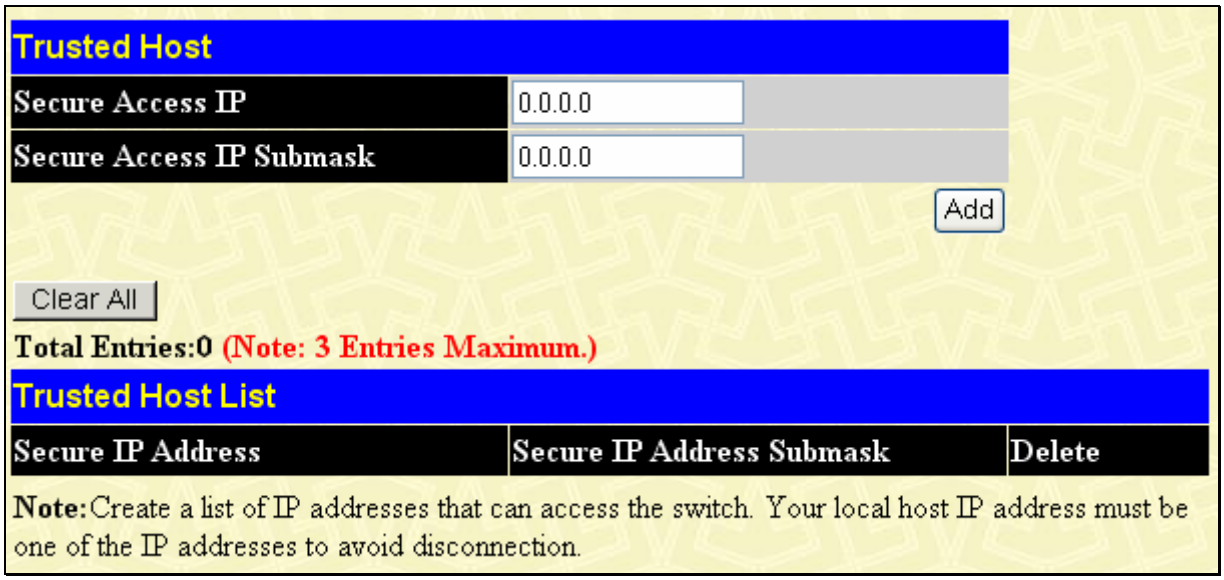


Figure 11- 21. Trusted Host window

The Trusted Host window is divided into two sections. The top section allows the administrator to add a new Trust Host and the bottom section contains a table that displays information about the Trusted Hosts that have been configured in the Switch.

To add a new Trusted Host, configure the parameters as described below:

Parameter	Description
Secure Access IP	Enter the IP address of the host that requires access to the Switch.
Secure Access IP Submask	Enter the Subnet Mask of the host that requires access to the Switch

Click the **Add** button to add the host to the **Trusted Host List**.

To remove all Trusted Hosts, click the **Clear All** button.

Access Authentication Control

The TACACS/XTACACS/TACACS+/RADIUS commands allow users to secure access to the Switch using the TACACS/XTACACS/TACACS+/RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS/XTACACS/TACACS+/RADIUS authentication is enabled on the Switch, it will contact a TACACS/XTACACS/TACACS+/RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- **TACACS** (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- **Extended TACACS (XTACACS)** - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- **TACACS+ (Terminal Access Controller Access Control System plus**) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS/XTACACS/TACACS+/RADIUS security function to work properly, a TACACS/XTACACS/TACACS+/RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS/XTACACS/TACACS+/RADIUS server to verify, and the server will respond with one of three messages:

- The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- The server will not accept the username and password and the user is denied access to the Switch.
- The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in ***Authentication Server Groups***, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set ***Authentication Server Hosts*** in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS/XTACACS/TACACS+/RADIUS/local/none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that when the user logins to the device successfully through TACACS/XTACACS/TACACS+server or none method, the “user” privilege level is the only level assigned. If the user wants to get the administration privilege level, the user must use the “enable admin” command to promote his privilege level. However when the user 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 and Parameter 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 and Parameter Settings**:

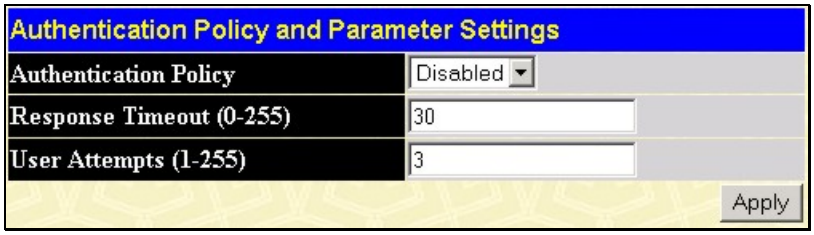


Figure 11- 22. Policy & Parameters Settings window

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 an authentication response 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**:

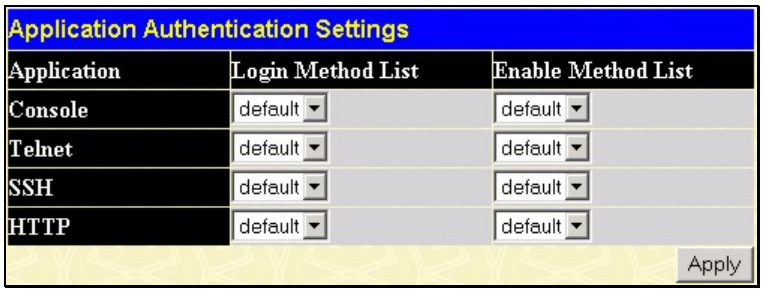


Figure 11- 23. Application's Authentication Settings window

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**:

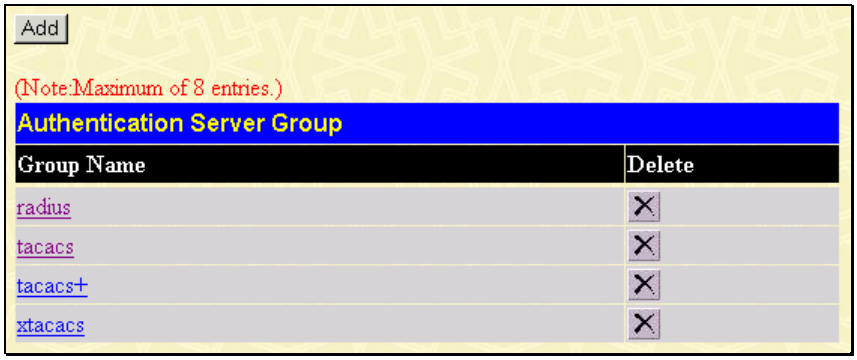


Figure 11- 24. Authentication Server Group Settings window

This screen displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click its hyperlinked Group Name, which will then display the following 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 Group** to add this Authentication Server Host to the group.

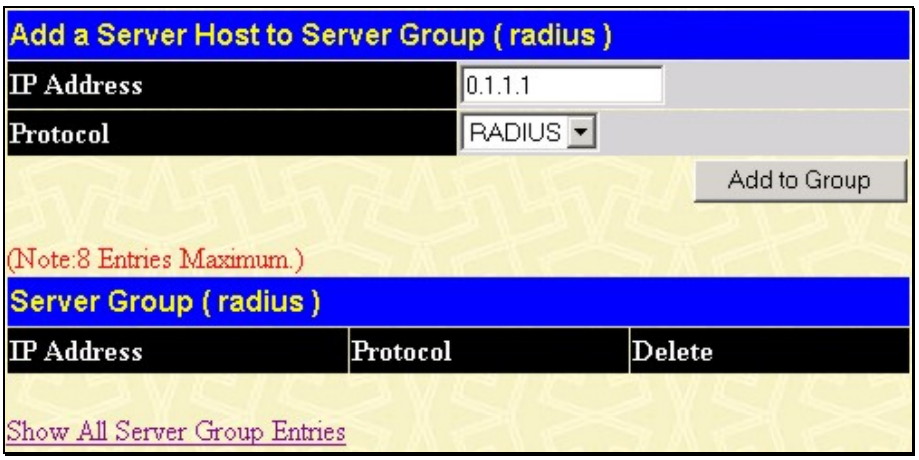


Figure 11- 25. Add a Server Host to Server Group (RADIUS) window

To add a user-defined group to the list, click the Add button in the **Authentication Server Group** window, which will display the following window.

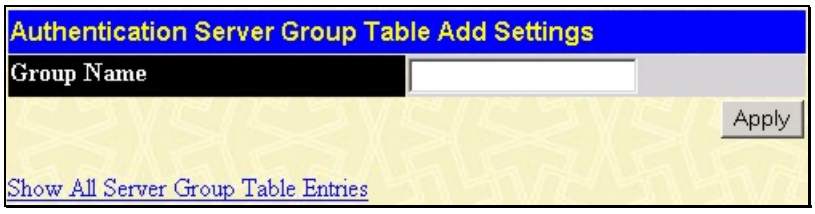


Figure 11- 26. Authentication Server Group Table Add Settings

Simply enter a group name of no more than 15 alphanumeric characters to define the user group to add. After clicking **Apply**, the new user-defined group will be displayed in the **Authentication Server Group** window. Here, it can be configured as the user desires.

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 Host

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 Host**:

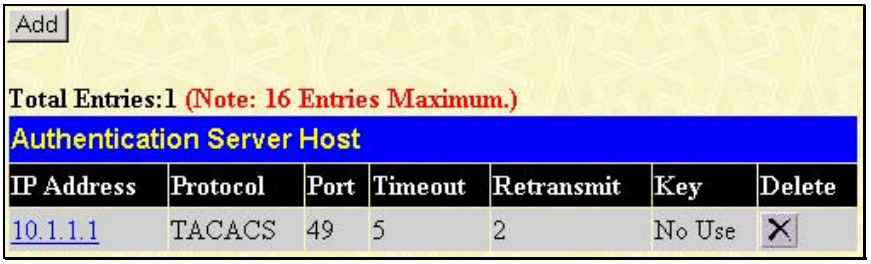


Figure 11- 27. Authentication Server Host Settings window

To add an Authentication Server Host, click the **Add** button, revealing the following window:

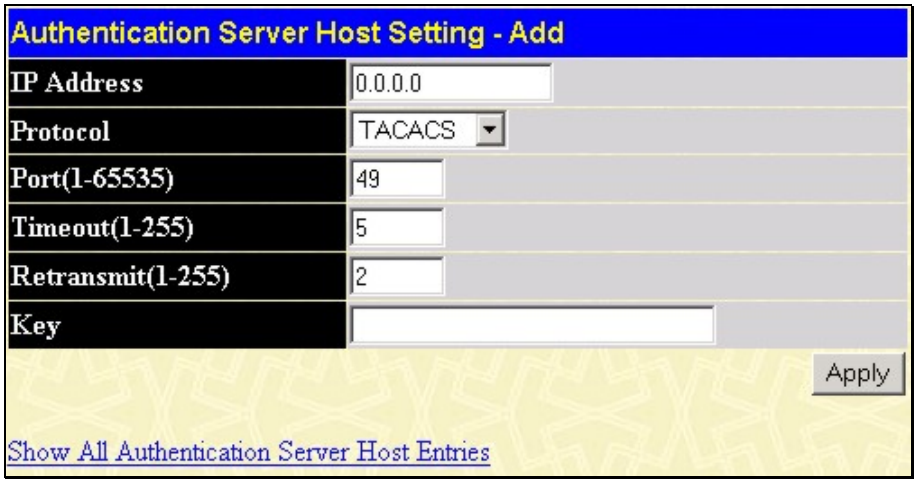


Figure 11- 28. Authentication Server Host Settings – Add window

To edit an Authentication Server Host, click the IP address hyperlink, revealing the following window:

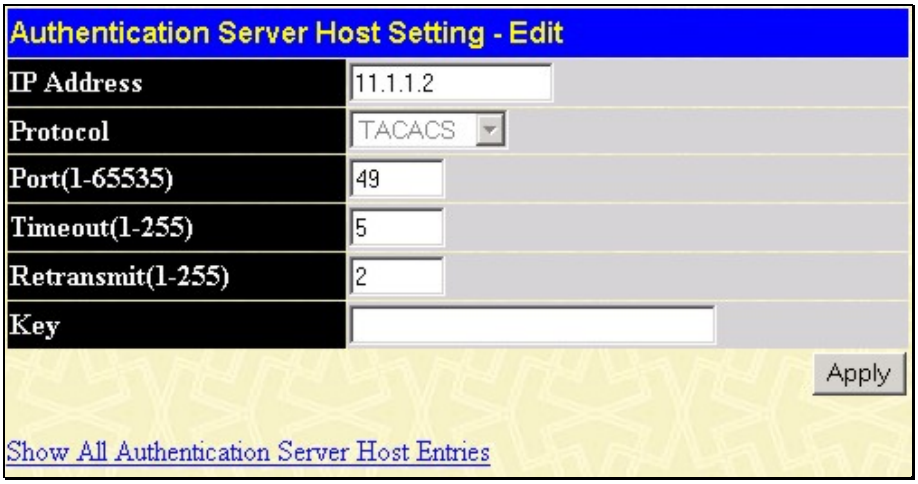


Figure 11- 29. Authentication Server Host Setting –Edit window

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.
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.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Retransmit (1-255)	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.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.

Click **Apply** to add the server host.

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.

頁: 255

When the user logins to the device successfully through 頁: 255

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**:

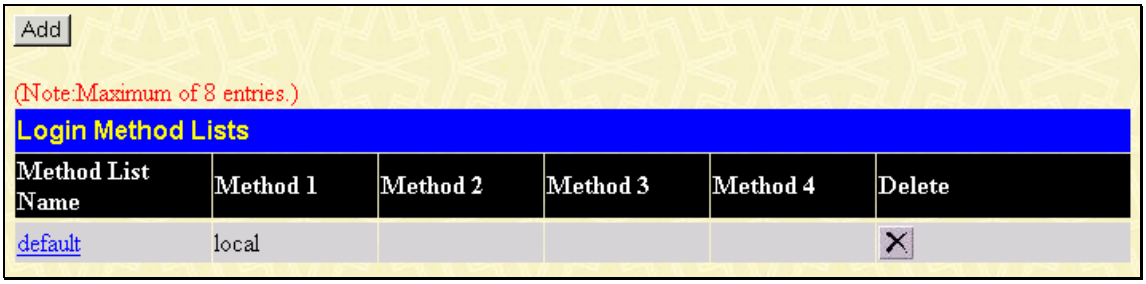


Figure 11- 30. Login Method Lists Settings window

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 ✕ under the Delete heading corresponding to the entry desired to be deleted. To modify a Login Method List, click on its hyperlinked Method List Name. To configure a new Method List, click the **Add** button.

Both actions will result in the same window to configure:

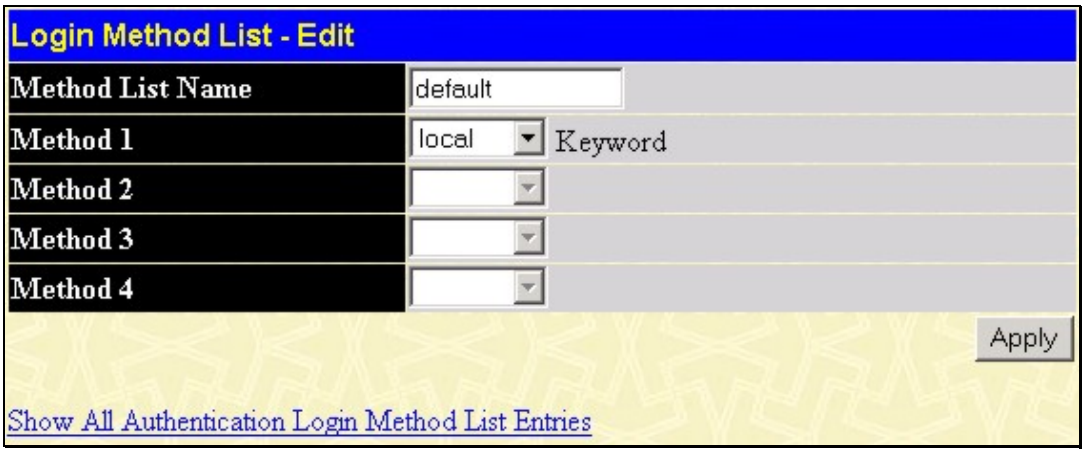


Figure 11- 31. Login Method List - Edit window (default)

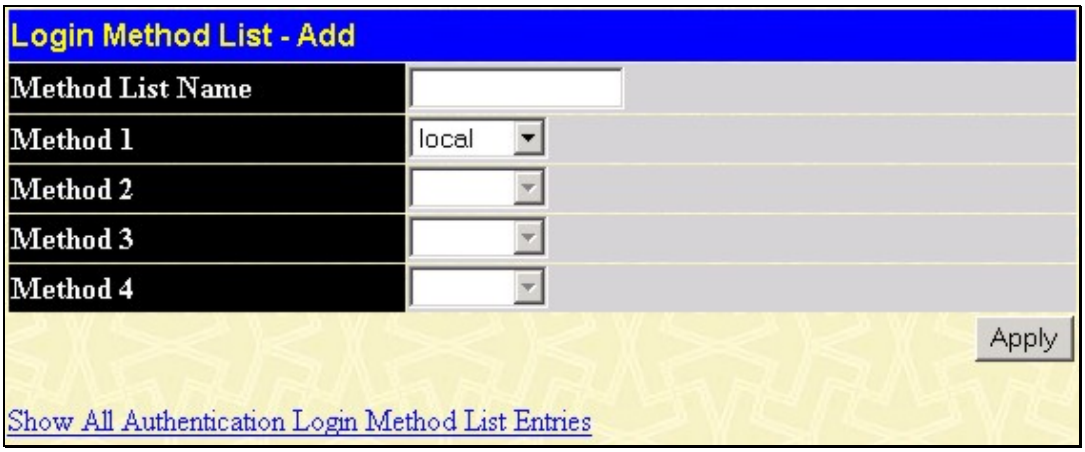


Figure 11- 32. Login Method List – Add window

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.
Method 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**:

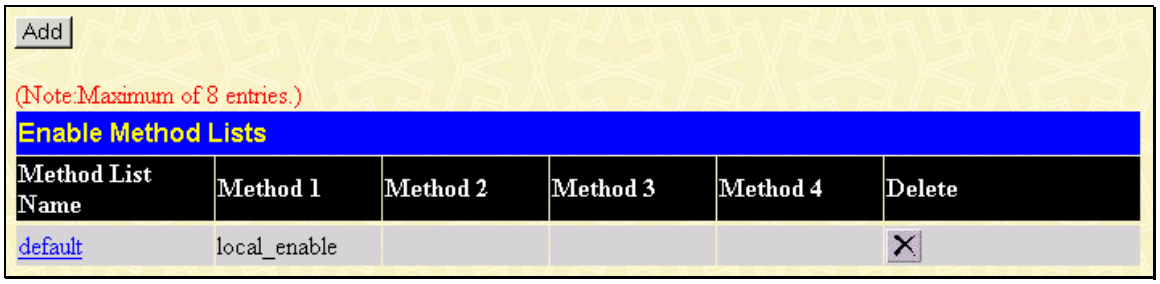


Figure 11- 33. Enable Method List Settings window

To delete an Enable Method List defined by the user, click the ✕ under the Delete heading corresponding to the entry desired to be deleted. To modify an Enable Method List, click on its hyperlinked Method List Name. To configure a Method List, click the **Add** button.

Both actions will result in the same window to configure:

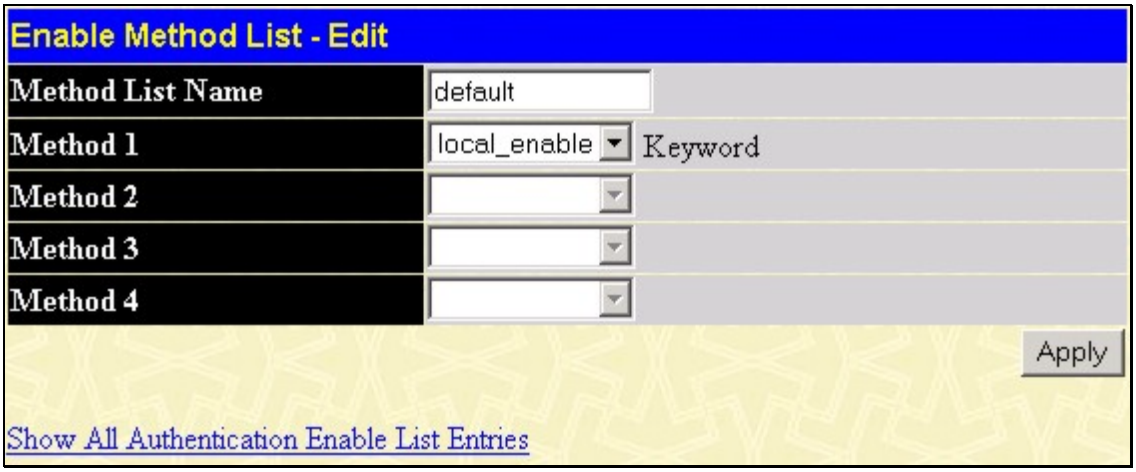


Figure 11- 34. Enable Method List - Edit window

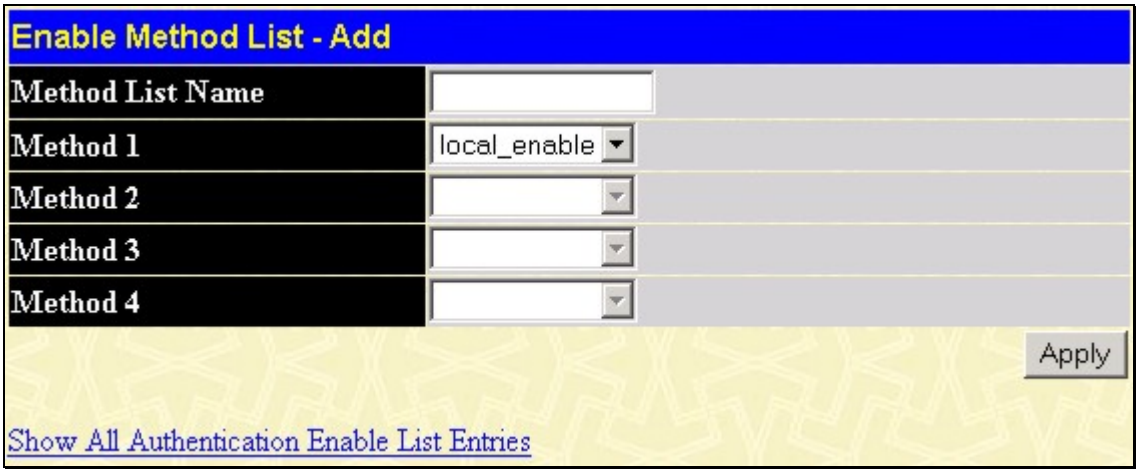


Figure 11- 35. Enable Method List - Add window

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.
Method 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.

Configure Local Enable Password

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 > Configure Local Enable Password**:

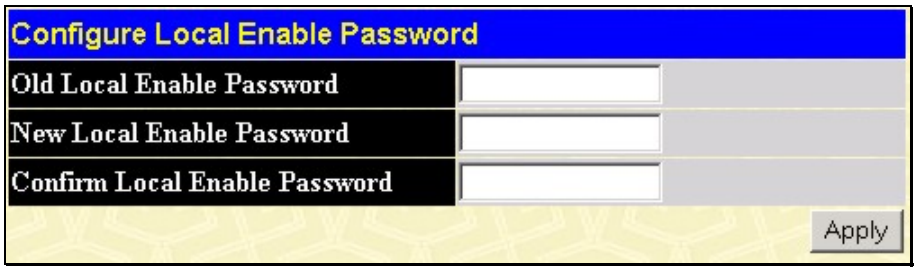


Figure 11- 36. Configure Local Enable Password window

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

Parameter	Description
Old Local Enabled	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enabled	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 Enabled	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.

Enable Admin

When the user logins to the device successfully through TACACS/XTACACS/TACACS+ server or none method, the “User” privilege level is assigned only. If the user wants to get “Admin” privilege level, the user must open the Enable Admin window to promote his privilege level. But when the user logins to the device successfully through RADIUS server or local method, 3 kinds of privilege level can be assigned to the user and the user can not use the Enable Admin window to promote to “Admin” privilege level. When the Enable Method List is set to TACACS, XTACACS, or RADIUS, the user must create a special account with the username “enable” in order to support the Enable Admin function. This function becomes inoperable when the authentication policy is disabled.

When this window appears, click the **Enable Admin** button revealing a dialog box for the user to enter authentication (password, username), as seen below. A successful entry will promote the user to Administrator level privileges on the Switch.

To view the following window, click **Security > Access Authentication Control > Enable Admin**:

Figure 11- 37. Enable Admin Screen

Figure 11- 38. Enter Network Password dialog box

Three Level User Accounts

When the user logins to the device successfully through TACACS/XTACACS/TACACS+ server or none method, “User” privilege level is the only level assigned. If the user wants to get “Admin” privilege level, the user must use the **Enable Admin** window to promote his privilege level. However when the user logins to the device successfully through the RADIUS server or through the local method, three kinds of privilege levels can be assigned to the user and the user can not use the **Enable Admin** window to promote to “Admin” privilege level.

To assign user privilege by RADIUS server, proper parameters should be configured on the RADIUS Server. Below are the parameters of a user account:

RADIUS Server Attribute	Description	Usage
Username(1)	Name of the user account	Required
Password(2)	Password of the user account	Required
Vendor-Specific(26)	Used to assign the privilege of the user account	Required

The parameters of the Vendor-Specific attribute

Vendor-Specific attribute	Description	Value	Usage
Vendor-ID	To define the vendor	171 (DLINK)	Required
Vendor-Type	The definition of the this attribute	1 (for user privilege)	Required
Attribute-Specific filed	Used to assign the privilege of the user account	3 (User privilege) 4 (Operator privilege) 5 (Admin privilege)	Required

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

Accounting

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 two types of Accounting that can be enabled on the Switch.

Exec – 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 configure the Accounting types on the switch, click **Security** > **Access Authentication Control** > **Accounting**, which will display the following window. Use the pull-down menu to enable or disable **Exec** accounting, **System** Accounting or both. Click **Apply** to implement changes made.

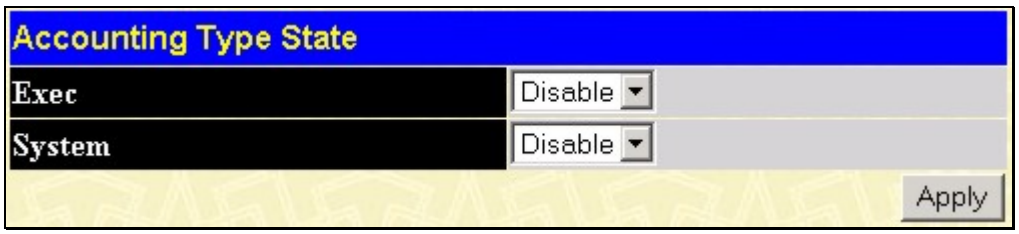


Figure 11- 39. Accounting Type State window

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. Click **Security** > **Traffic Segmentation** to view the table below.

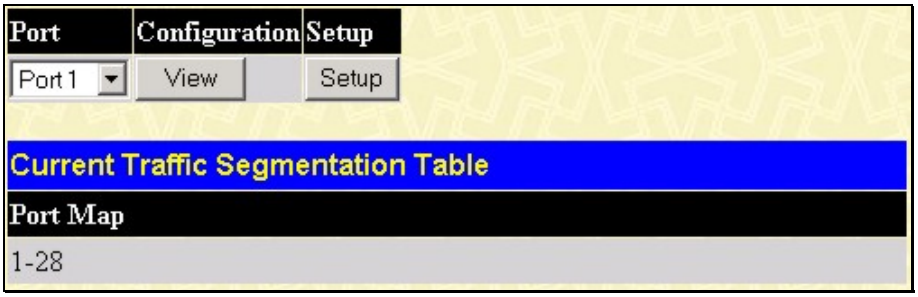


Figure 11- 40. Current Traffic Segmentation Table

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 and click the **View Setting** link to display the forwarding ports. To configure new forwarding ports for a particular port, select a port from the drop down menu and click **Setup**. The window shown below will appear.

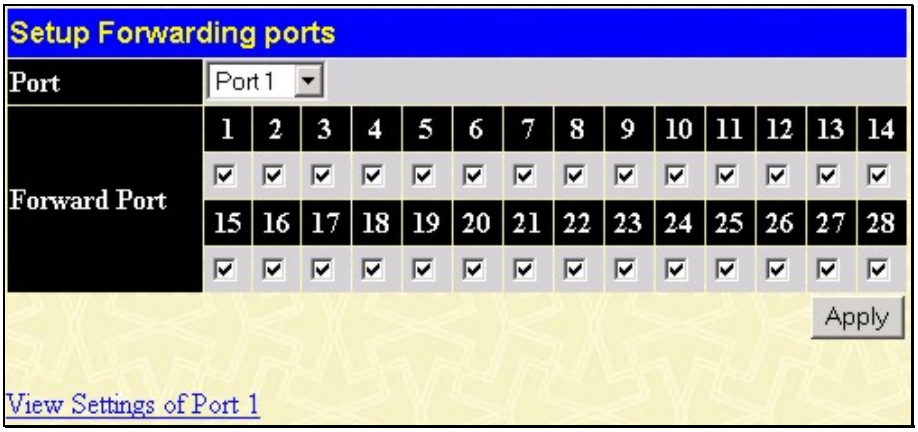


Figure 11- 41. Setup Forwarding Ports window

The user may set the following parameters:

Parameter	Description
Port	Check the corresponding boxes to configure the port(s) to isolate broadcast or L2 unknown multicast traffic
Forward Port	Check the boxes to select which of the ports on the Switch will be able to forward ARP requests.

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

Broadcast Segmentation

Broadcast Segmentation can isolate layer 2 broadcast domains between ports, while keeping IP traffic forwarded between ports. This feature is particularly useful in an Ethernet-to-the-Home environment where broadcasts need to be blocked between each house-hold, while allowing IP communication between them. This method of segmenting the flow of traffic is similar to cross-VLAN routing, but can save the number of IP addresses used for configuring IP interfaces/subnets per VLAN.

Click **Security > Broadcast Segmentation** to view the screen shown below:

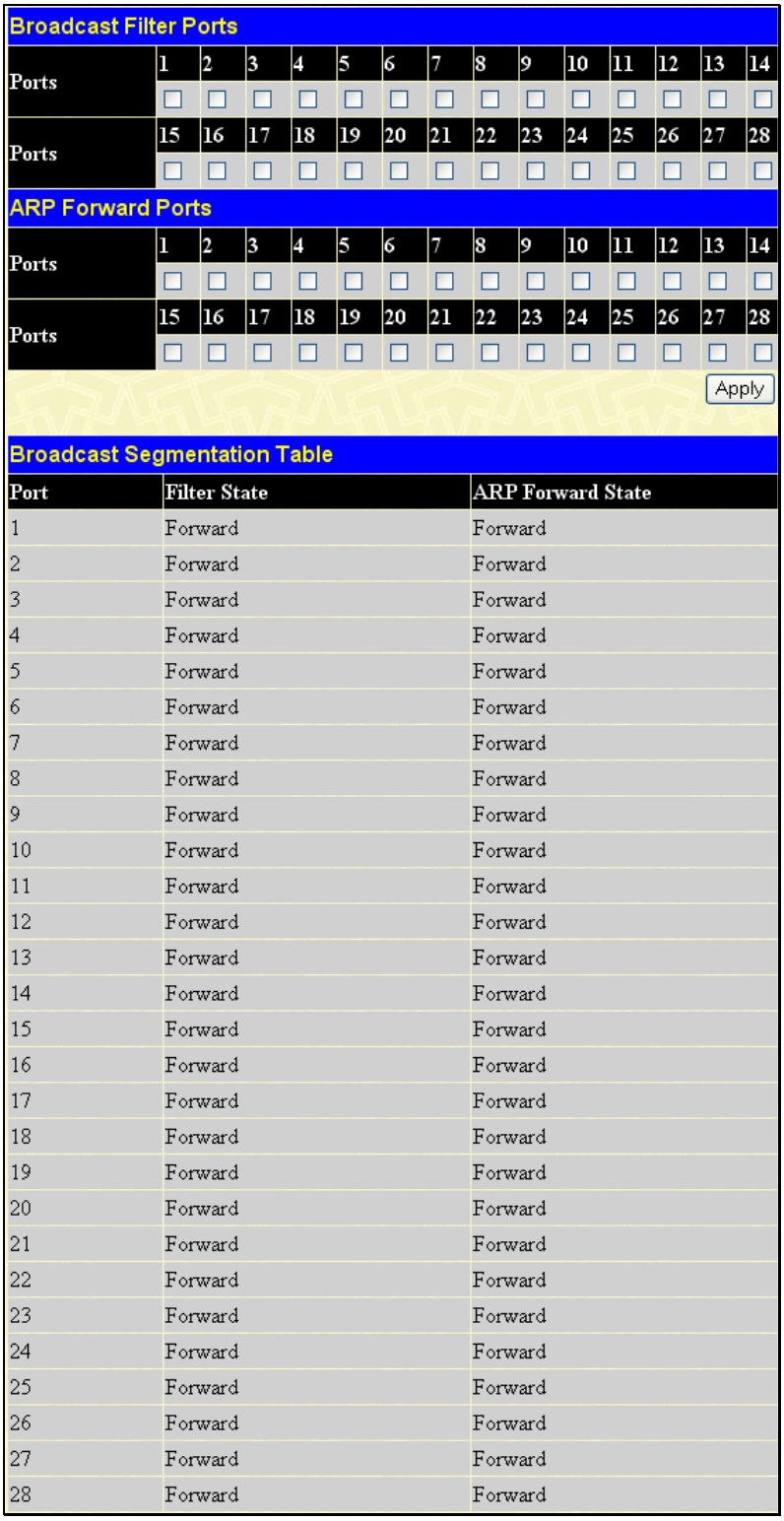


Figure 11- 43. Broadcast Segmentation Table

The *Broadcast Segmentation* window is divided into three main sections, *Broadcast Filter Ports*, *ARP Forward Ports* and *Broadcast Segmentation Table*.

The user may set the following parameters for the *Broadcast Filter Ports* section:

Parameter	Description
Ports	Check the corresponding boxes for the port(s) that you want to apply the Broadcast Filter to. When a port is checked, the broadcast, unknown multicast from other ports to this port will be dropped; the broadcast, unknown multicast from this port to other un-checked ports will still be forwarded.

The user may set the following parameters for the *ARP Forward Ports* section:

Parameter	Description
Ports	Check the corresponding boxes for the port(s) that you want to enable ARP Forwarding on. When a port is checked, the ARP packets, which are broadcast packets, from other ports to this port will be forwarded.

Click the **Apply** button to save the changes.

The following parameters are displayed in the *Broadcast Segmentation Table*:

Parameter	Description
Port	Displays each of the switches ports in sequential order.
Filter State	Displays the Filter State of the switch port.
ARP Forward State	Displays the ARP Forward State of the switch port.

Secure Socket Layer (SSL)

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 the windows for **Download Certificate** and **Ciphersuite**, click **Security > SSL**:

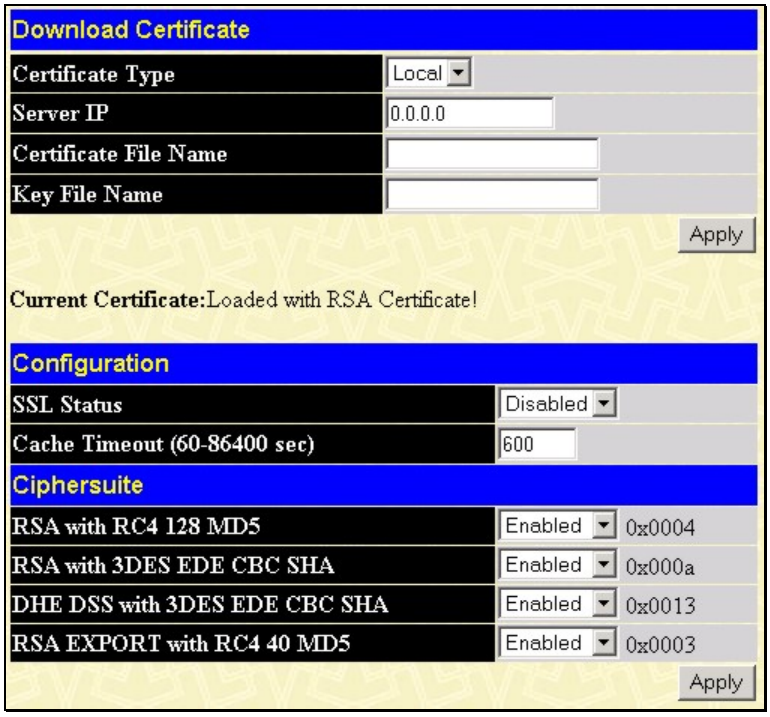


Figure 11- 42. Download Certificate and Ciphersuite window

To download certificates, set the following parameters and click **Apply**.

Parameter	Description
Certificate Type	Choose the type of certificate to be downloaded from the drop-down menu. This type refers to the server responsible for issuing certificates. This field has been limited to *local* for this firmware release.
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)

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

Parameter	Description
Configuration	
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.

Ciphersuite	
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.
DHS 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.

NOTE: Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface. For more information on SSL and its functions, see the xStack DES-3800 Series CLI Manual, located on the documentation CD of this product.

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 Server Configuration

The following window is used to configure and view settings for the SSH server and can be opened by clicking **Security > SSH > SSH Server Configuration**:

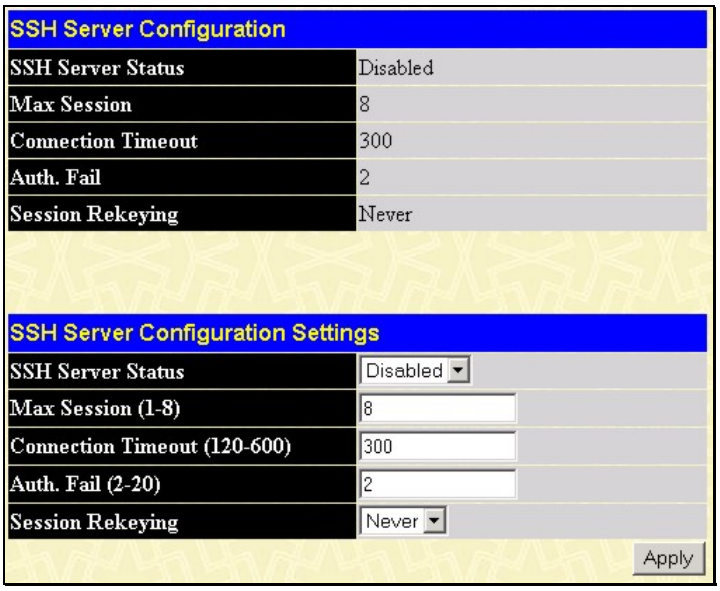


Figure 11- 43. SSH Server Configuration Settings

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

Parameter	Description
SSH Server Status	Use the pull-down menu to enable or disable SSH on the Switch. The default is *Disabled*.
Max Session (1-8)	Enter a value between *1* and *8* to set the number of users that may simultaneously access the Switch. The default setting is *8*.
Time Out (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 *300* seconds.

Auth. Fail (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*.
Session Rekeying	Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.

SSH Authentication Mode 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 using their corresponding pull-down menus. All algorithms are enabled by default. To open the following window, click **Security > SSH > SSH Authentication Mode and Algorithm Settings**:

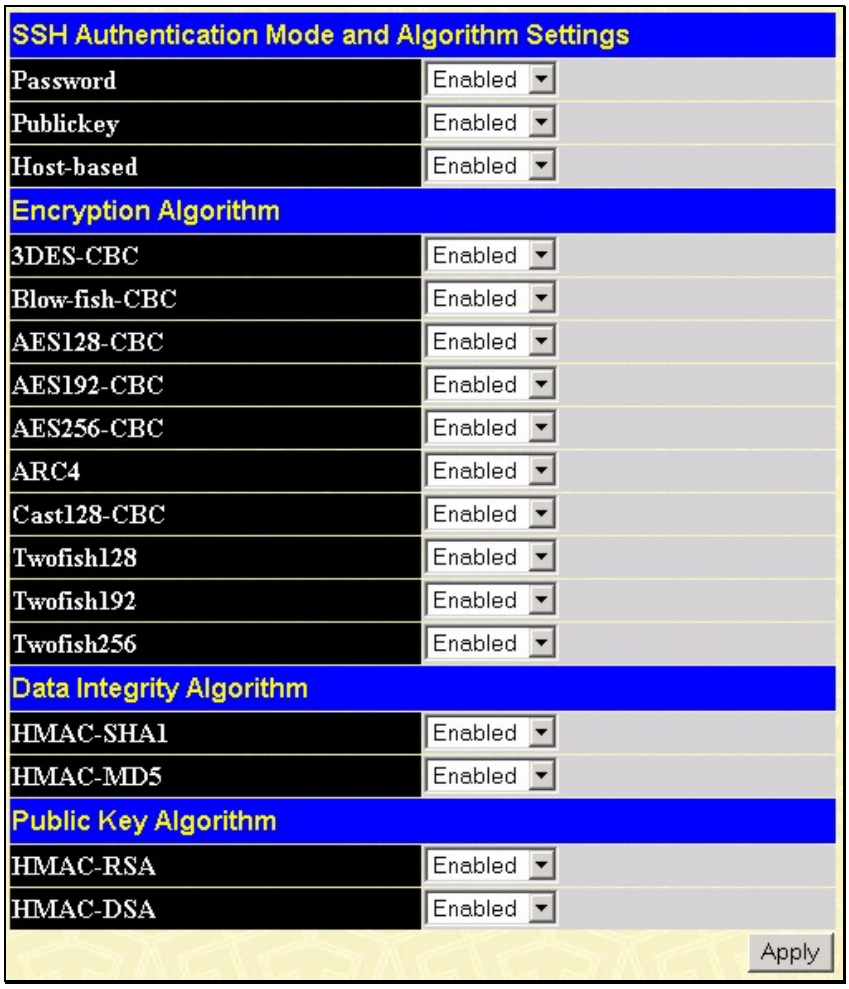


Figure 11- 44. Encryption Algorithm window

The following algorithms may be set:

Parameter	Description
SSH Authentication Mode and Algorithm 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

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**.

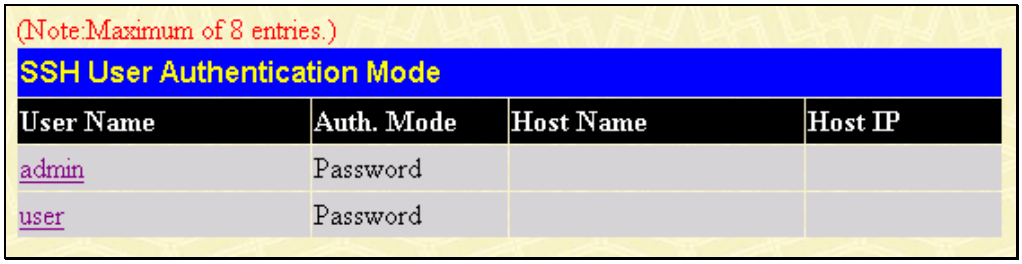


Figure 11- 45. SSH User Authentication Mode window

In the example screen to the right, the User Account "admin" has been previously set using the User Accounts window in the **Security Management** folder. A User Account MUST be set in order to set the parameters for the SSH user. To configure the parameters for a SSH user, click on the hyperlinked User Name in the **Current Accounts** window, which will reveal the following window to configure.

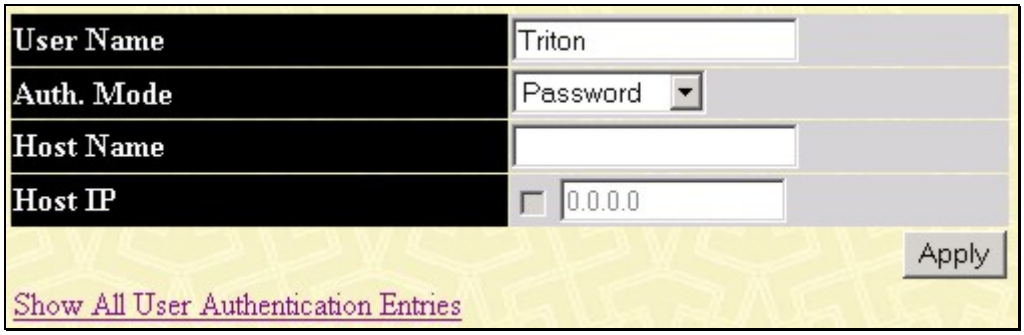


Figure 11- 46. SSH User modify window

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 Administration section.

IP-MAC 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-3800 Series switches, Active and inactive entries use the same database. The maximum entry number is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with the IP-MAC binding, this Switch has been equipped with a special ACL Mode for IP-MAC Binding, which should alleviate this problem for users. When enabled in the **IP-MAC Binding Port** window, the Switch will create two entries in the Access Profile Table as shown below. The entries may only be created if there are at least two Access Profile IDs available on the Switch. If not, when the ACL Mode is enabled, an error message will be prompted to the user. When the ACL Mode is enabled, the Switch will only accept IP packets from a created entry in the IP-MAC Binding Setting window. All others will be discarded.

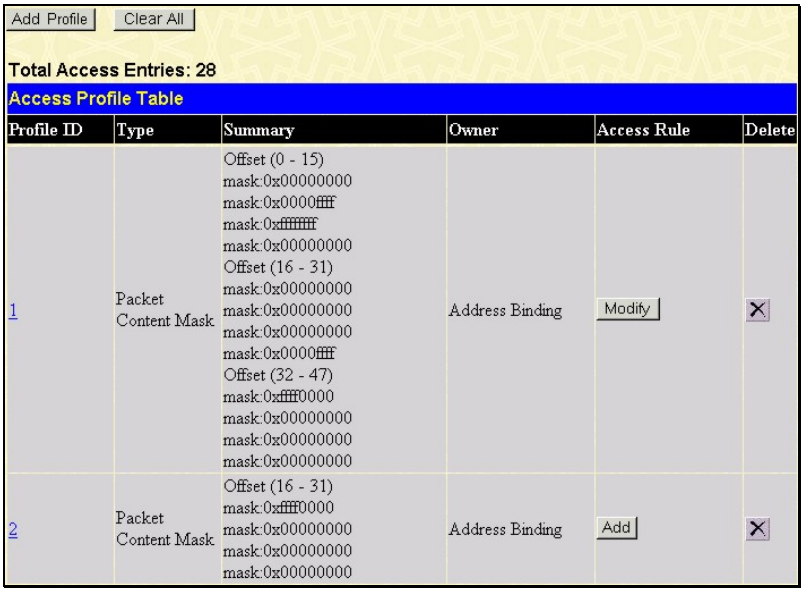


Figure 11- 47. Access Profile Table – IP-MAC ACL Mode Enabled

To view the particular configurations associated with these two entries, click their corresponding hyperlinked Profile IDs, which will display the following:

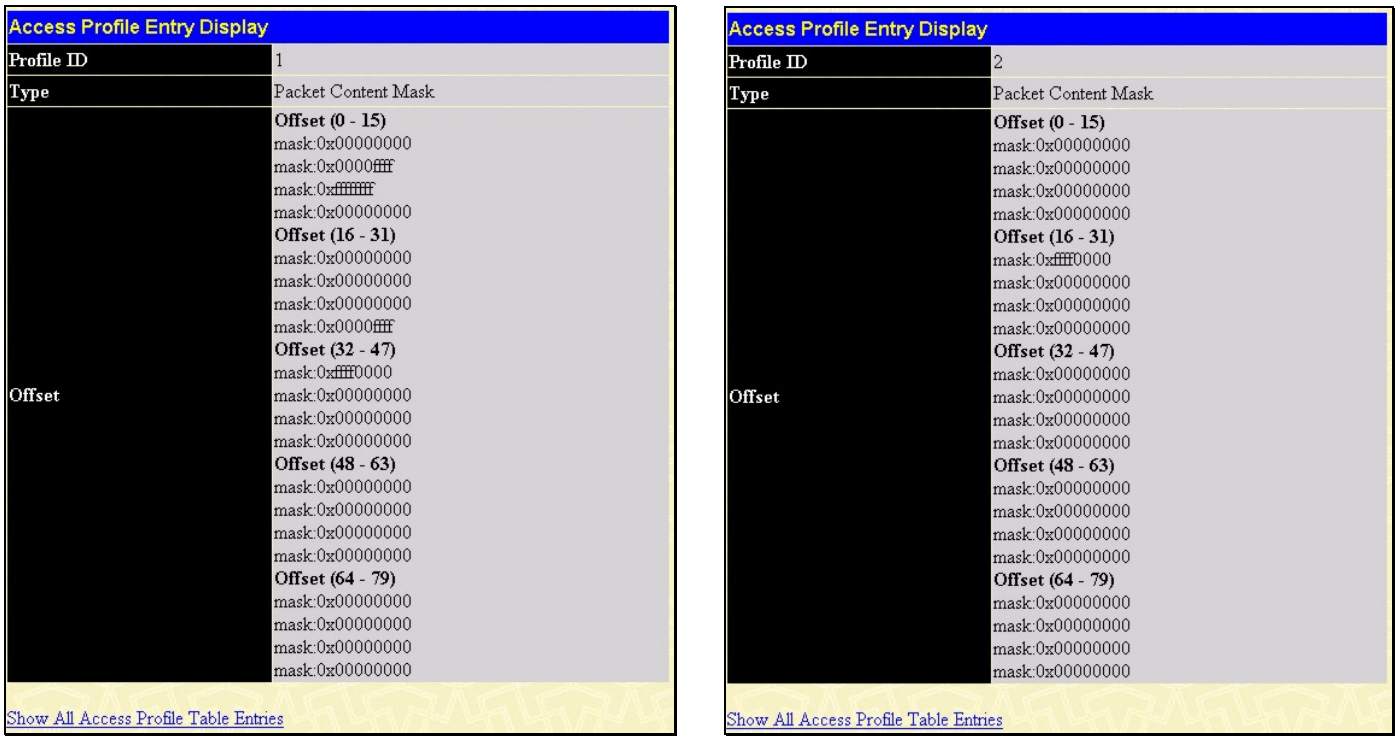


Figure 11- 48. Access Profile Entry Display for IP-MAC ACL Mode Enabled Entries

These two entries cannot be modified or deleted using the Access Profile Table, and any attempt to do so will result in failure. The user may only remove these two entries by disabling the ACL Mode in the IP-MAC Binding Port window.

Also, rules will be created for every port on the Switch. To view the ACL rule configurations set for the ACL mode, click the corresponding modify button of the entry in the Access Profile Table, which will produce a window similar to the example to the right. The user may view the configurations on a port-by-port basis by clicking the **View** button under the Display heading of the corresponding port entry. These entries cannot be modified or deleted, and new rules cannot be added. Yet, these windows will offer vital information to the user when configuring other access profile entries. Click **Next** to view the next page of rules. The user may also search for an entry by **Access ID** by entering that ID into the field and clicking **Find**.


Add

Number of Entries: 28

Access Rule Table

Profile ID	Mode	Type	Summary	Owner	Detail	Delete
1	Permit	Packet Content Mask	Access ID: 1	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 2	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 3	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 4	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 5	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 6	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 7	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 8	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 9	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 10	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 11	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 12	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 13	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 14	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 15	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 16	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 17	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 18	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 19	Address binding	View	X
1	Permit	Packet Content Mask	Access ID: 20	Address binding	View	X

Next

Figure 11- 49. Access Rule Table for IP-MAC Binding rule

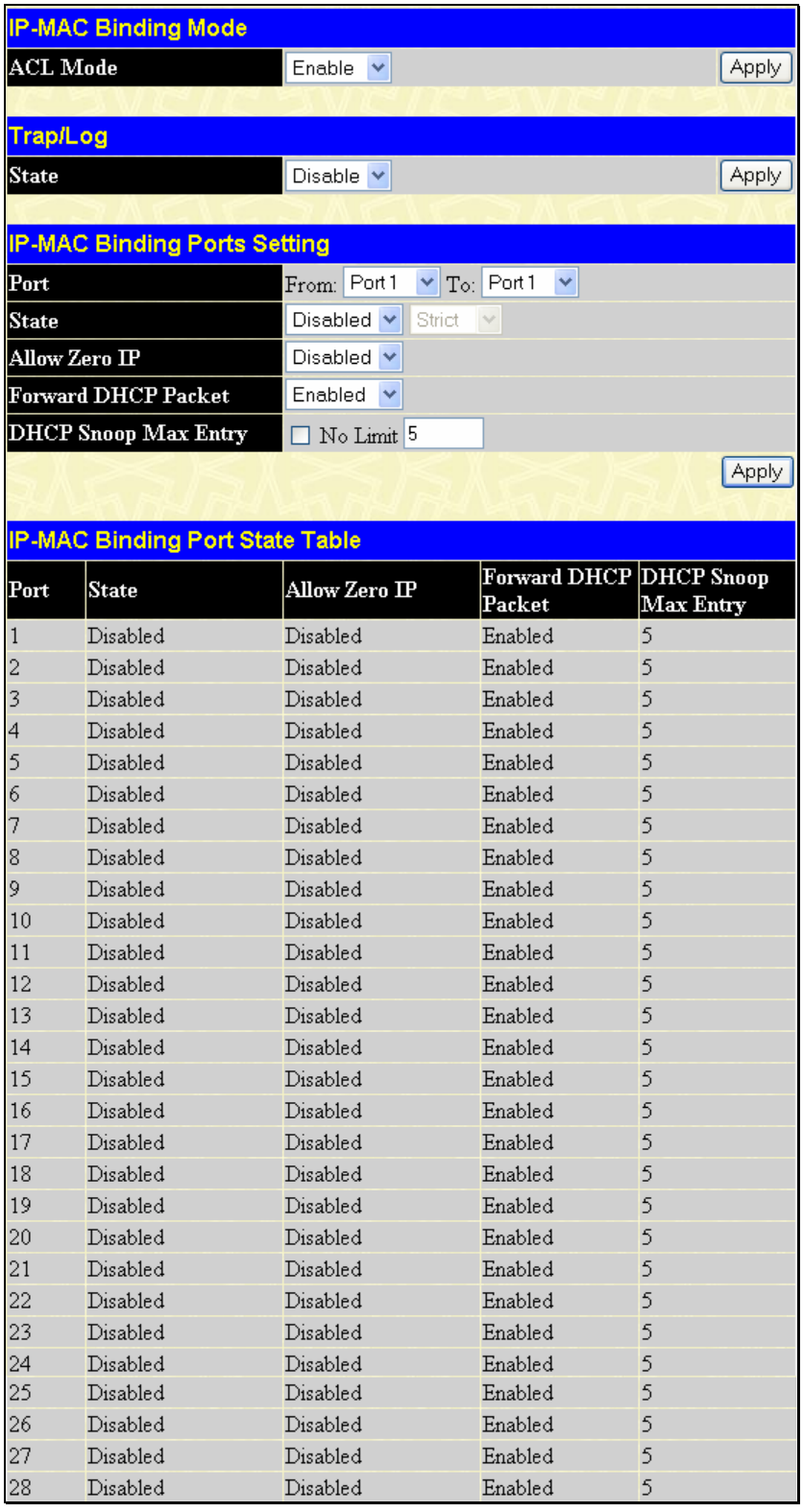
NOTE: When configuring the ACL mode for the IP-MAC binding function, please pay close attention to previously set ACL entries. Since the ACL mode entries will fill the first two available access profiles and access profile IDs denoting the ACL priority, the ACL mode entries may take precedence over other configured ACL entries. This may render some user-defined ACL parameters inoperable due to the overlap of settings combined with the ACL entry priority (defined by profile ID). For more information on ACL settings, please see "Configuring the Access Profile" section mentioned previously in this chapter.

NOTE: Once ACL profiles have been created by the Switch through the IP-MAC binding function, the user cannot modify, delete or add ACL rules to these ACL mode access profile entries. Any attempt to modify, delete or add ACL rules will result in a configuration error as seen in the previous figure.

NOTE: When downloading configuration files to the Switch, be aware of the ACL configurations loaded, as compared to the ACL mode access profile entries set by this function, which may cause both access profile types to experience problems.

IP-MAC Binding Port

To enable or disable IP-MAC binding on specific ports, click **Security** > **IP-MAC Binding** > **IP-MAC Binding Port** to view the **IP-MAC Binding Ports Setting** window. Select a port or a range of ports with the **From** and **To** fields. Enable or disable the port with the **State, allow_zero_IP** and **forward_DHCP packet** field, and configure the port's **maximum entry**. The user may also enable the ACL Mode for IP-MAC Binding which will create two Access Profile Entries on the Switch, as previously stated. 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 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. Click **Apply** to save changes.



Port	State	Allow Zero IP	Forward DHCP Packet	DHCP Snoop Max Entry
1	Disabled	Disabled	Enabled	5
2	Disabled	Disabled	Enabled	5
3	Disabled	Disabled	Enabled	5
4	Disabled	Disabled	Enabled	5
5	Disabled	Disabled	Enabled	5
6	Disabled	Disabled	Enabled	5
7	Disabled	Disabled	Enabled	5
8	Disabled	Disabled	Enabled	5
9	Disabled	Disabled	Enabled	5
10	Disabled	Disabled	Enabled	5
11	Disabled	Disabled	Enabled	5
12	Disabled	Disabled	Enabled	5
13	Disabled	Disabled	Enabled	5
14	Disabled	Disabled	Enabled	5
15	Disabled	Disabled	Enabled	5
16	Disabled	Disabled	Enabled	5
17	Disabled	Disabled	Enabled	5
18	Disabled	Disabled	Enabled	5
19	Disabled	Disabled	Enabled	5
20	Disabled	Disabled	Enabled	5
21	Disabled	Disabled	Enabled	5
22	Disabled	Disabled	Enabled	5
23	Disabled	Disabled	Enabled	5
24	Disabled	Disabled	Enabled	5
25	Disabled	Disabled	Enabled	5
26	Disabled	Disabled	Enabled	5
27	Disabled	Disabled	Enabled	5
28	Disabled	Disabled	Enabled	5

Figure 11- 50. IP-MAC Binding Ports window

The following fields can be set or modified:

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 9 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.
From…To	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 zero IP packets to bypass.
Forward_dhcppkt	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.

IP-MAC Binding Table

The window shown below can be used to create IP-MAC binding entries. Click **Security** > **IP-MAC Binding** > **IP-MAC Binding Table** to view the **IP-MAC Binding Setting** window. Enter the IP and MAC addresses of the authorized users in the appropriate field, choose the designated ports, and click **Add**. To modify either the IP address or the MAC address of the binding entry, make the desired changes in the appropriate field and Click **Modify**. To find an IP-MAC binding entry, enter the IP and MAC addresses and click **Find**. To delete an entry click **Delete**. To clear all the entries from the table click **Delete All**.

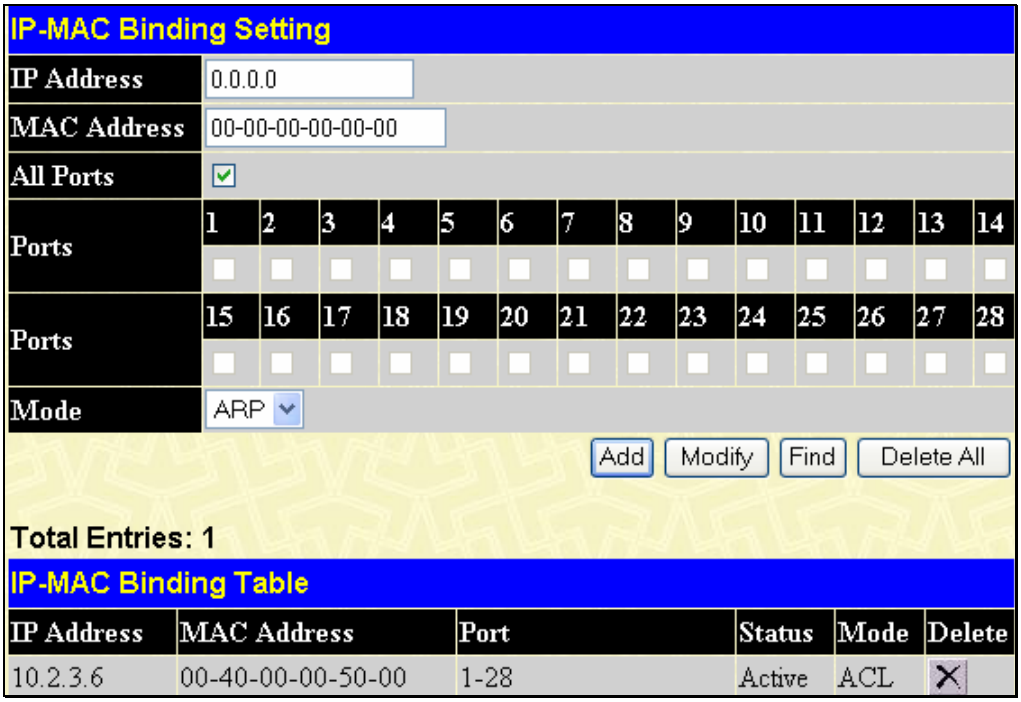


Figure 11- 51. IP-MAC Binding Table window

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.
All Ports	Click this check box to configure this IP-MAC binding entry (IP Address + MAC Address) for all ports on the Switch.
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.
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 IP-MAC Binding Ports window as seen previously.

IP-MAC Binding Blocked

To view unauthorized devices that have been blocked by IP-MAC binding restrictions open the **IP-MAC Binding Blocked** window shown below. Click **Security** > **IP-MAC Binding** > **IP-MAC Binding Blocked** to open the **IP-MAC Binding Blocked** window.

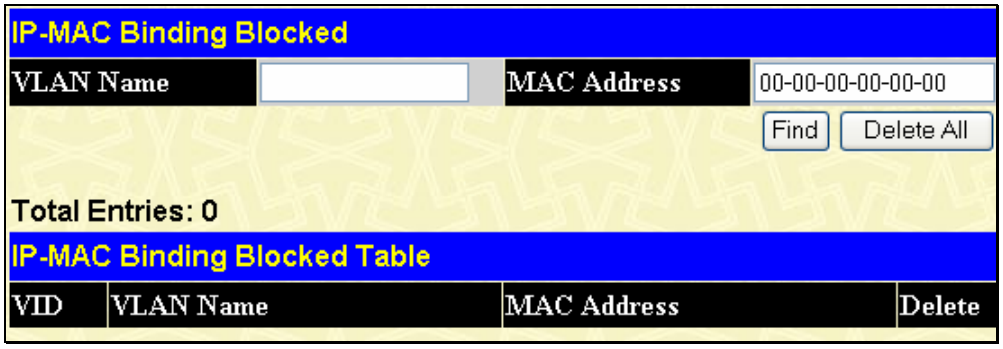


Figure 11- 52. IP-MAC Binding Blocked window

To find an unauthorized device that has been blocked by the IP-MAC binding restrictions, enter the **VLAN** name and **MAC Address** in the appropriate fields and click **Find**. To delete an entry click the delete button next to the entry's MAC address. To delete all the entries in the **IP-MAC Binding Blocked Table** click **Delete All**.

IP-MAC Binding DHCP Snooping Table

The window shown below can be used to show or delete IP-MAC binding auto entries. Click **Security** > **IP-MAC Binding** > **IP-MAC Binding DHCP Snooping** to view the **IP-MAC Binding DHCP Snooping Settings** and the **IP-MAC Binding DHCP Snoop Table**. Adjust the **Address Binding DHCP Snoop Mode** to *enabled.* Select a port or a range of ports with the **From** and **To** fields. Delete the port's IP MAC Binding auto enteries.

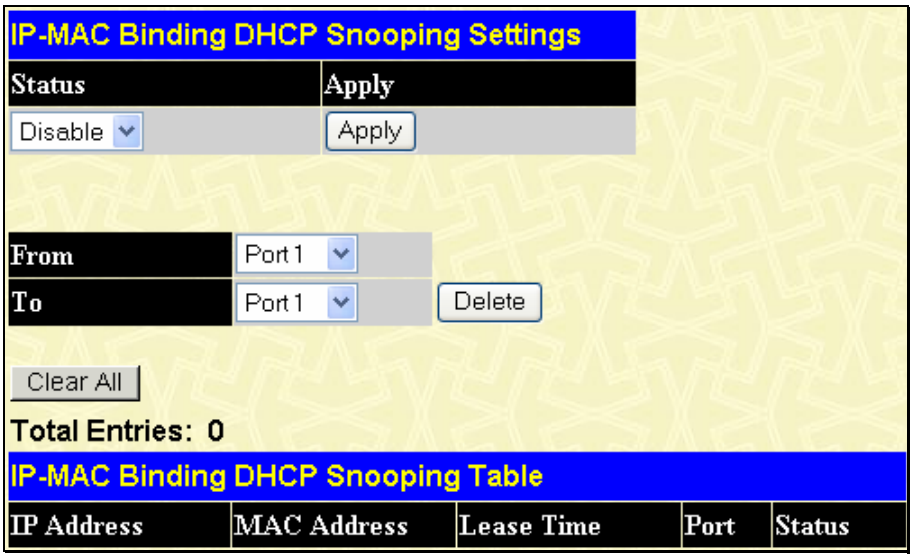


Figure 11- 53. IP-MAC DHCP Snooping window

Limited IP Multicast Range

The **Limited IP Multicast Range Profile Settings** window allows the user to add a profile where multicast address(es) reports will 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 address or range of IP addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports. Click **Security** > **Limited IP Multicast Range** > **Limited IP Multicast Range Profile Settings** to view the window shown below:

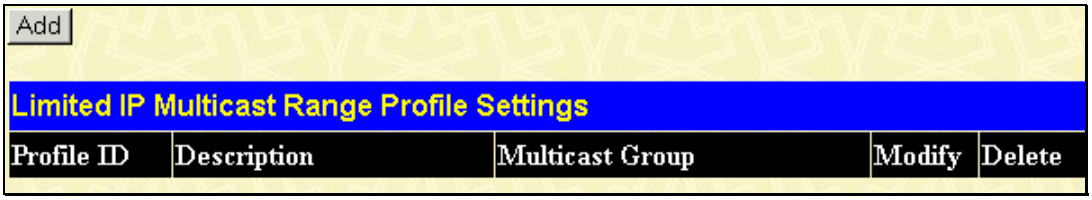


Figure 11- 54. Limited IP Multicast Range Profile Settings Window

To configure a Limited IP Multicast Range Profile Click the **Add** button, which will reveal the following window:

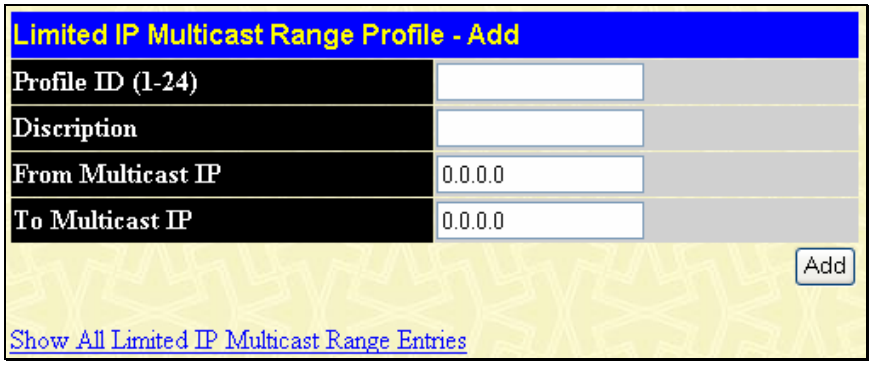


Figure 11- 55. Limited IP Multicast Range Profile - Add Window

Parameter	Description
Profile ID (1-24)	Enter a Profile ID between 1 - 24.
Description	Enter a description for the IP Multicast Range Profile.
From Multicast IP	Enter the lowest multicast IP address of the range.
To Multicast IP	Enter the highest multicast IP address of the range.

Click **Add** to implement the new profile on the Switch.

Limited IP Multicast Range Port Settings

The **Limited IP Multicast Range Port 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 **Security** > **Limited IP Multicast Range** to open the **Limited IP Multicast Range Port Settings** window shown below:

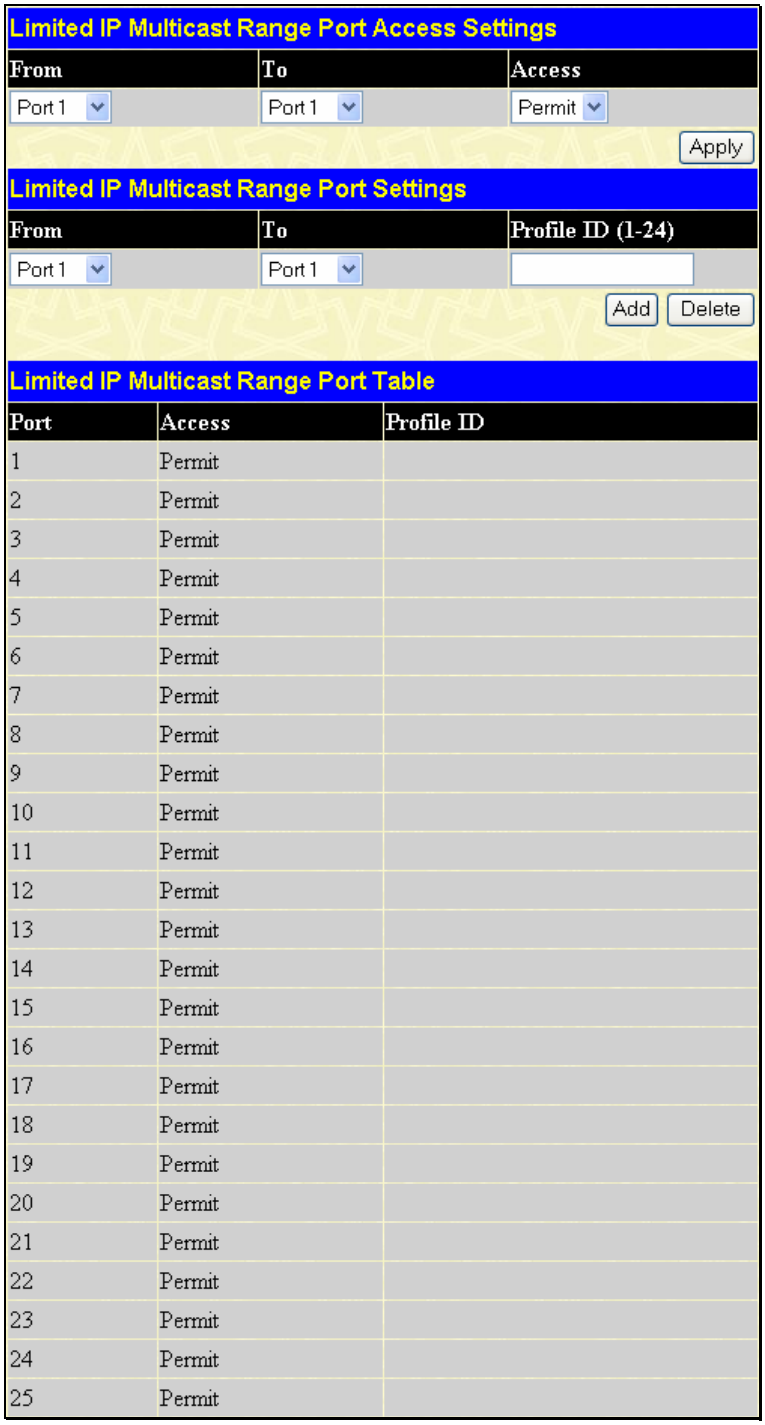


Figure 11- 56. Limited IP Multicast Range Port Access Settings Window

Limited IP Multicast Max Group Settings

The **Limited IP Multicast Max 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 **Security > Limited IP Multicast Range** to open the **Limited IP Multicast Max Group Settings** window shown below:

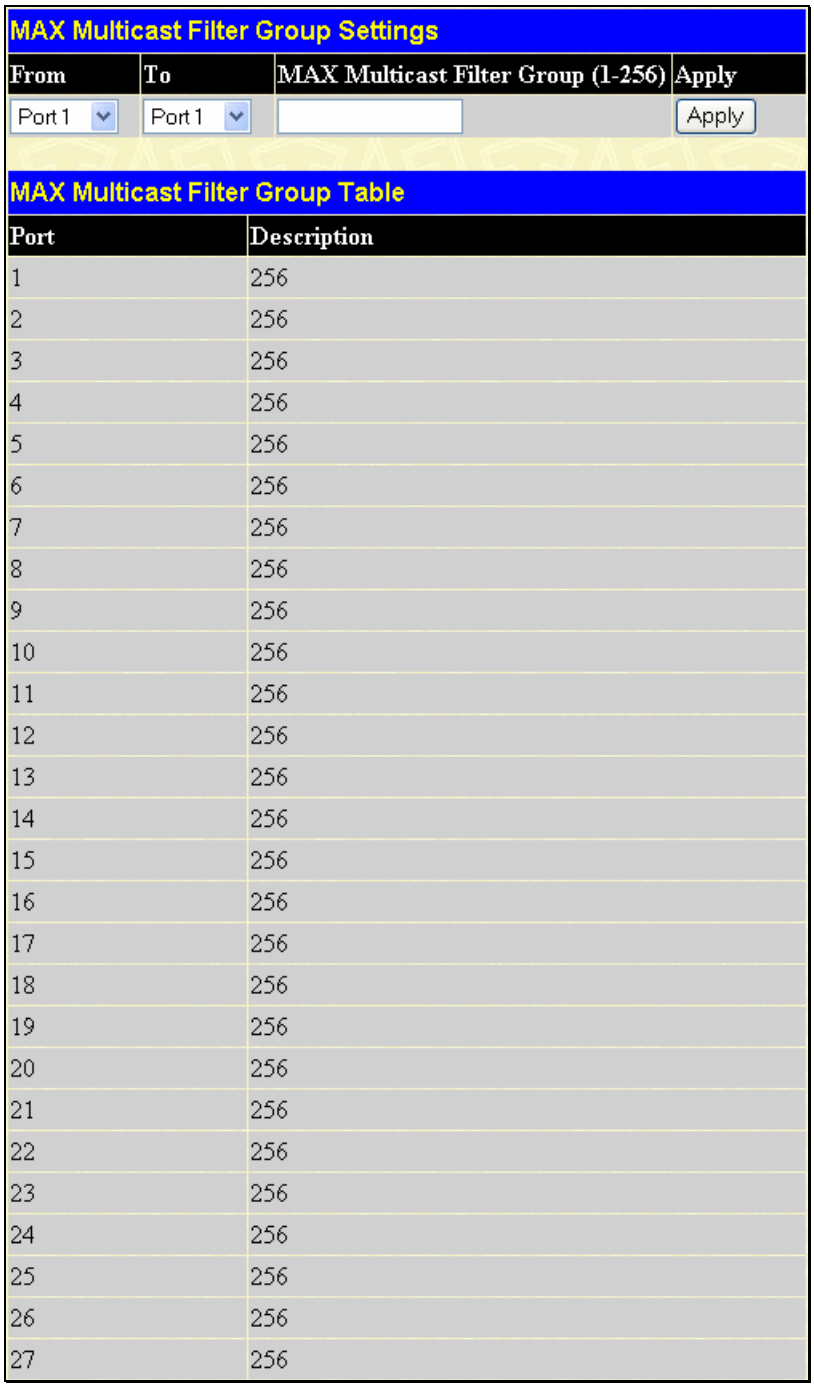


Figure 11- 57. Limited IP Multicast Max Group Setting Window

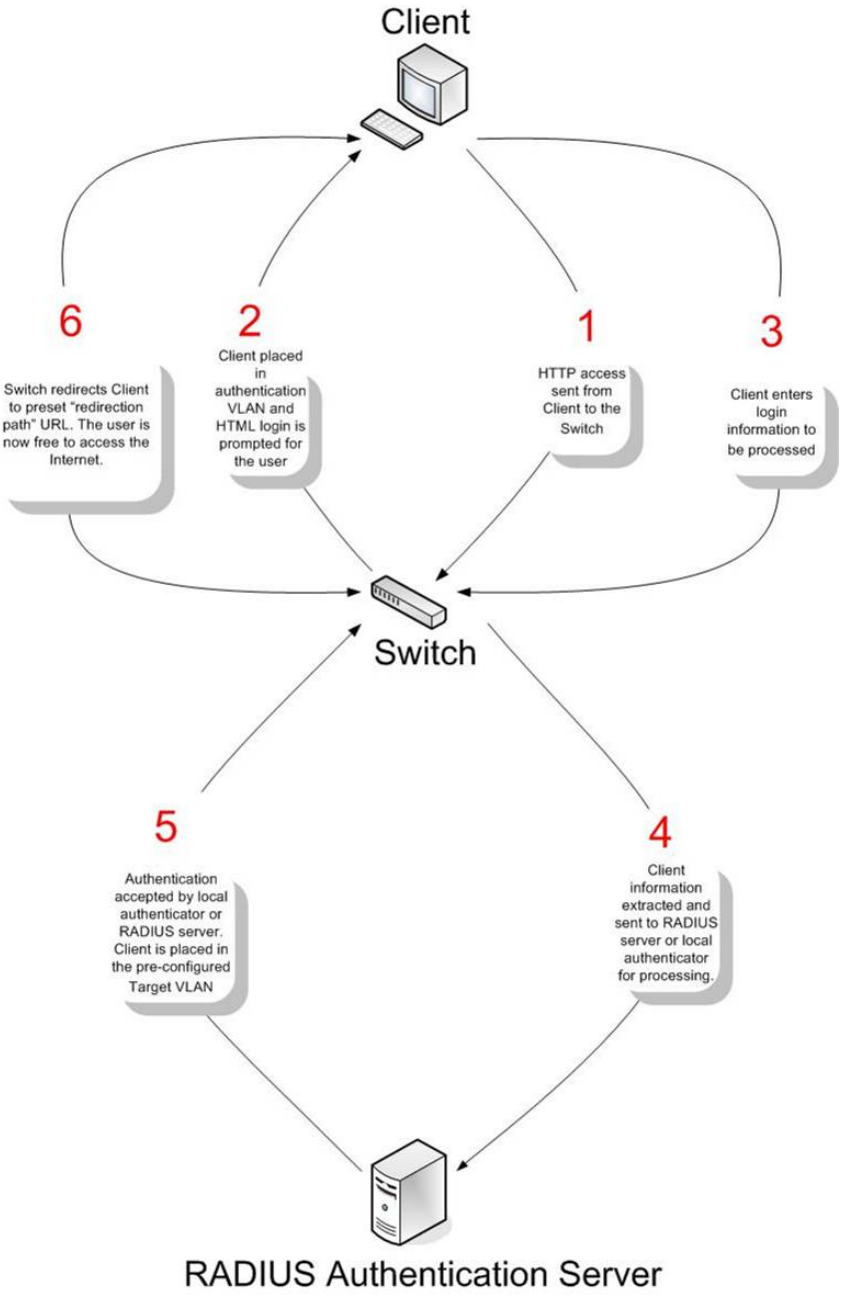
Web-based Access Control

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.

To configure the Switch for WAC, click **Security** > **WAC Configuration**, which will open the following screen.

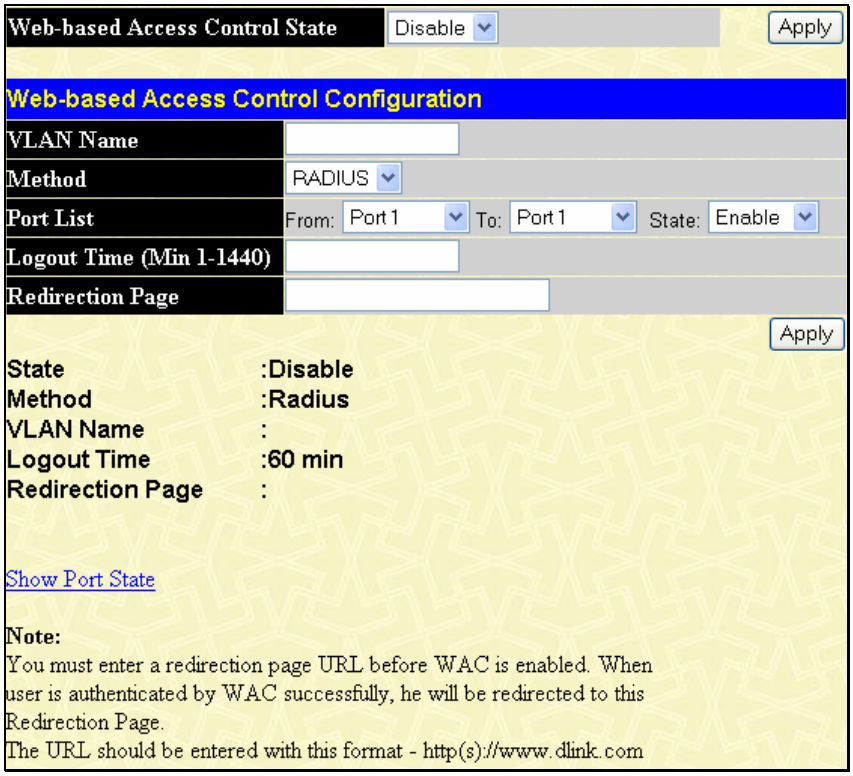


Figure 11- 58. Web-based Access Control Configuration window

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

Parameter	Description
Web-based Access Control State	Use the **drop-down menu** to either *Enable* or *Disable* the Web-based Access Control settings of the Switch.
VLAN Name	Enter the VLAN name which users will be placed while authenticated by the Switch or a RADIUS server. This VLAN should be pre-configured to have limited access rights to web based authenticated users.
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.
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.
Logout Time (Min 1 – 1440)	You can set the logout time by entering a value between *1* and *1440* minutes.
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.

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 which attempt 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.

To view Web-based Access Control status of individual ports, click the Show port state link to open the window seen below.

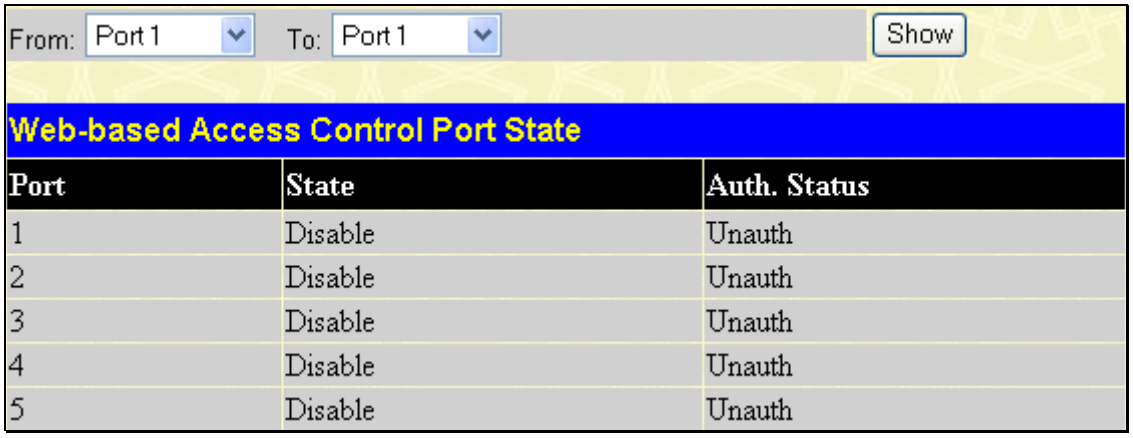


Figure 11- 59. Web-based Access Control Port State window

Use the pull-down menu in the **From** and **To** fields to select a port or range of ports to be viewed for their Web-based Access Control status. In the previous window, ports 1-10 have been selected to be viewed.

To set user accounts for the Web-based Access Control click **Security** > **Web-based Access Control** > **User Account Management** which will open the following screen for the user to configure:

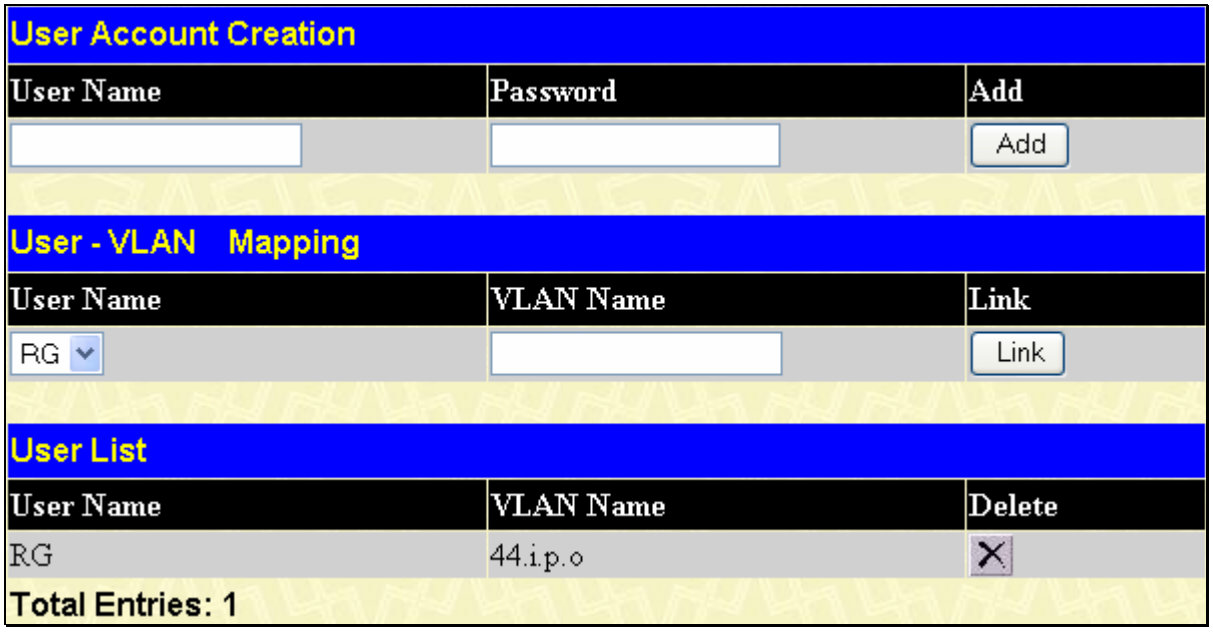


Figure 11- 60. Web-based User Account Settings window

To set the User Account settings for the Web-based Access Control by the Switch, complete the following fields.

Parameter	Description
User Account Creation	
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.
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.
Link	Click the Link button to map the user name and VLAN stated in the previous 2 fields. Users will be linked directly to the VLAN upon successful authentication.
User List	This section displays users and their associated VLAN configured for Web-based Access Control. Click the corresponding ✕ to delete the user.

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 Global Settings

The following window is used to set the parameters for the MAC-Based Access Control function on the Switch. Here the user can set the running state, method of authentication, RADIUS password and view the Guest VLAN configuration to be associated with the MAC-Based Access Control function of the Switch. To view this window, click **Security** > **MAC-Based Access Control** > **MAC-Based Access Control Global Settings**.

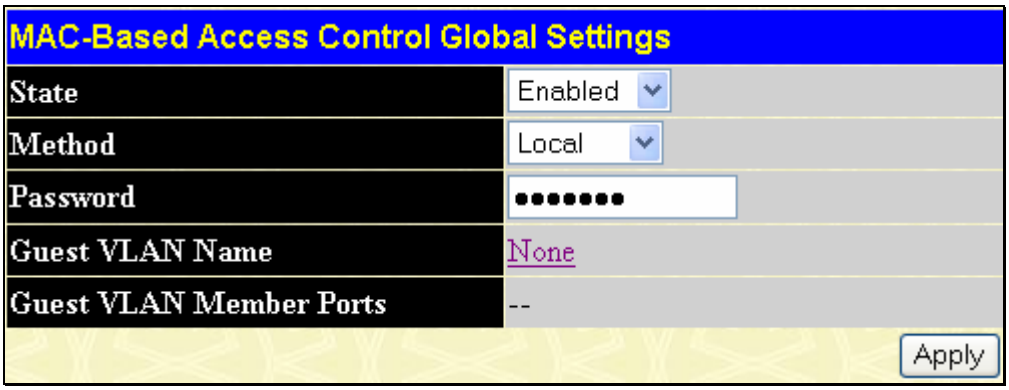


Figure 11- 61. MAC-Based Access Control Global Settings

The following parameters may be viewed or set:

Parameter	Description
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 Name	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.

Clicking the hyperlinked Guest VLAN Name in the window above will display the following window, in which the user can configure ports to be used for MAC-Based Access Control within the Guest VLAN.

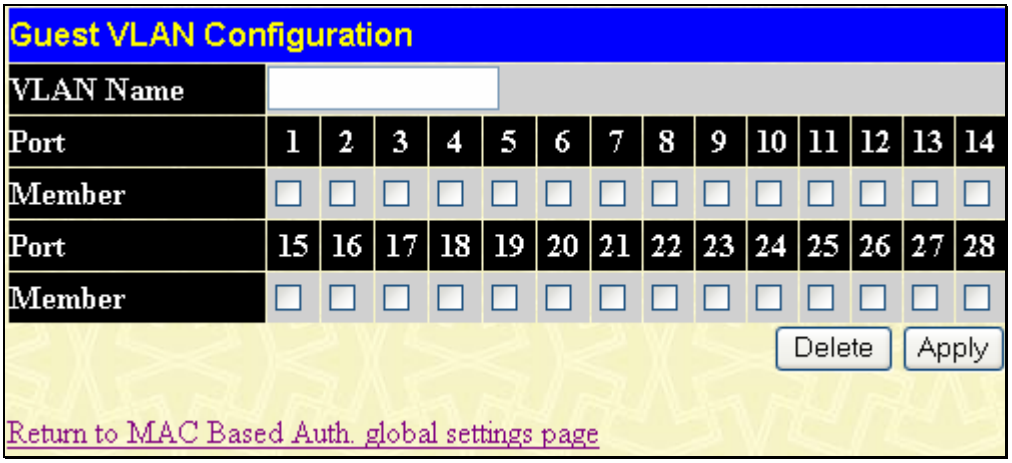


Figure 11- 62. Guest VLAN Configuration window for MAC-Based Access Control

Simply click the ports to be used for MAC-Based Access Control within the Guest VLAN. Web-Based Authentication and 802.1X Guest VLAN ports cannot be set for MAC-Based Access Control and any attempt to do so will result in an error message. Click **Apply** to set the clicked ports. Click the **Delete** button to remove this VLAN as a MAC-Based Access Control Guest VLAN.

MAC-Based Access Control Port Settings

Use the following window to configure ports to be enabled or disabled for the MAC-Based Access Control feature of the Switch. Remember, ports enabled for certain other features, listed previously (#5 Notes About MAC-Based Access Control) cannot be enabled for MAC-Based Access Control. To view this window, click **Security** > **MAC-Based Access Control** > **MAC-Based Access Control Port Settings**.

MAC-Based Access Control Port Setting

From	To	State	Apply
Port 1	Port 1	Disabled	Apply

MAC-Based Access Control Port State Table

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

Figure 11- 63. MAC-Based Access Control Port Setting and State Table

To configure a port or range of ports for the MAC-Based Access Control feature, use the **From** and **To** pull-down menus to choose the ports, and then use the **State** pull-down menu to enable them. To view the MAC address authentication on a port-by-port basis, click the hyperlinked port number, which will display the following window listing that pertinent information, as seen below.

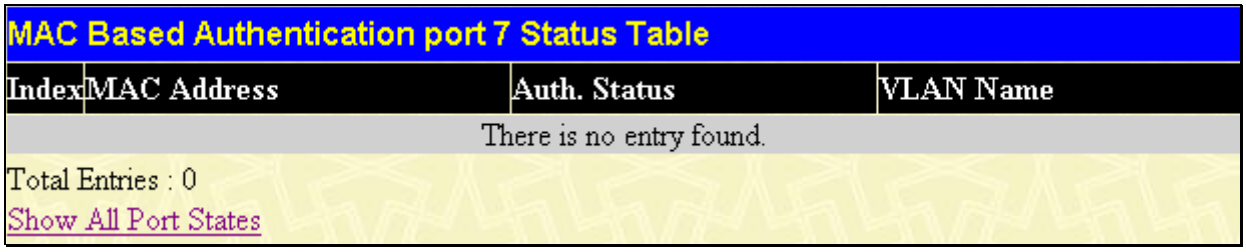


Figure 11- 64. MAC-Based Authentication port 1 Status Table

MAC-Based Access Control Local Database 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 view this window, click **Security** > **MAC-Based Access Control > MAC-Based Access Control Local Database Settings**.

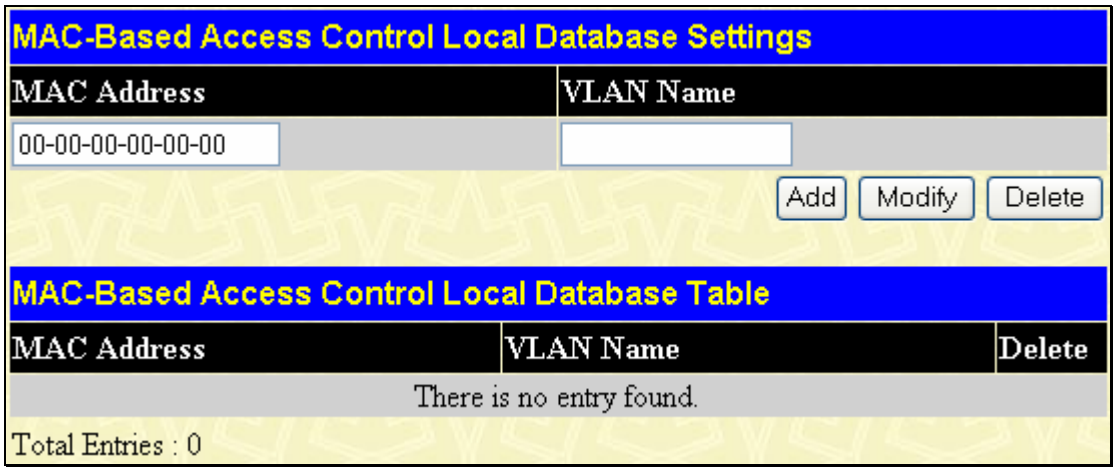


Figure 11- 65. MAC-Based Access Control Local Database Settings

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 **Add**. To change a MAC address or a VLAN in the list, enter its parameters into the appropriate fields and click **Modify**. To delete a MAC address entry, enter its parameters into the appropriate fields and click **Delete**, or click the corresponding ✕ of the entry in the **MAC-Based Access Control Local Database Table.**

Safeguard Engine

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

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

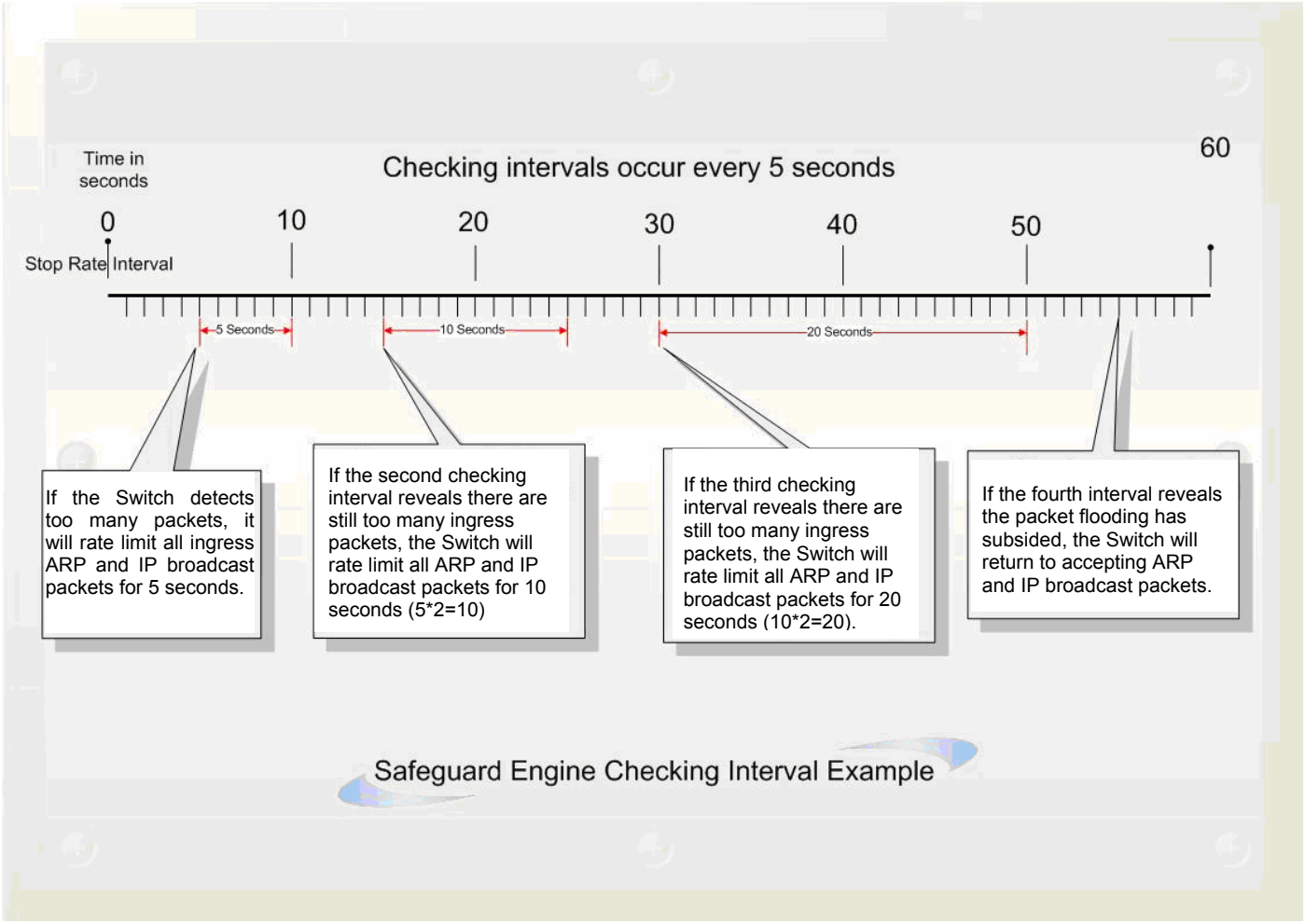


Figure 11- 66. Safeguard Engine example

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:

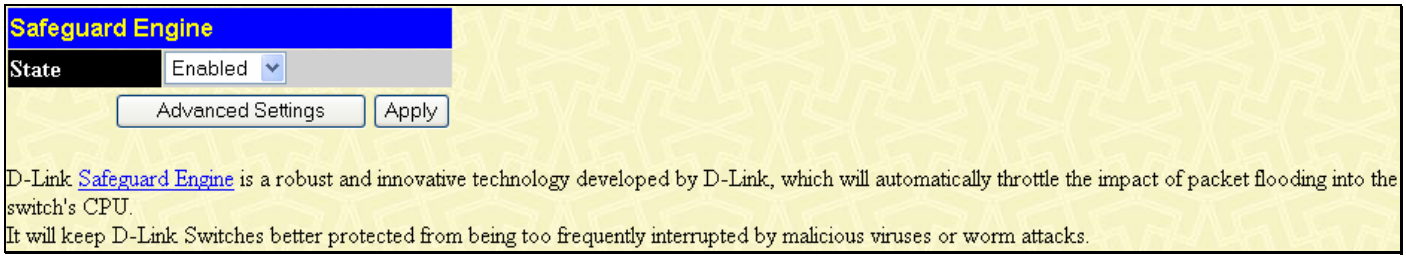


Figure 11- 67. Safeguard Engine window

To configure the Switch's Safeguard Engine, change the **State** to *Enabled*. To configure the parameters for the Safeguard Engine, click the **Advanced Settings** button which will alter the previous screen to look like this:

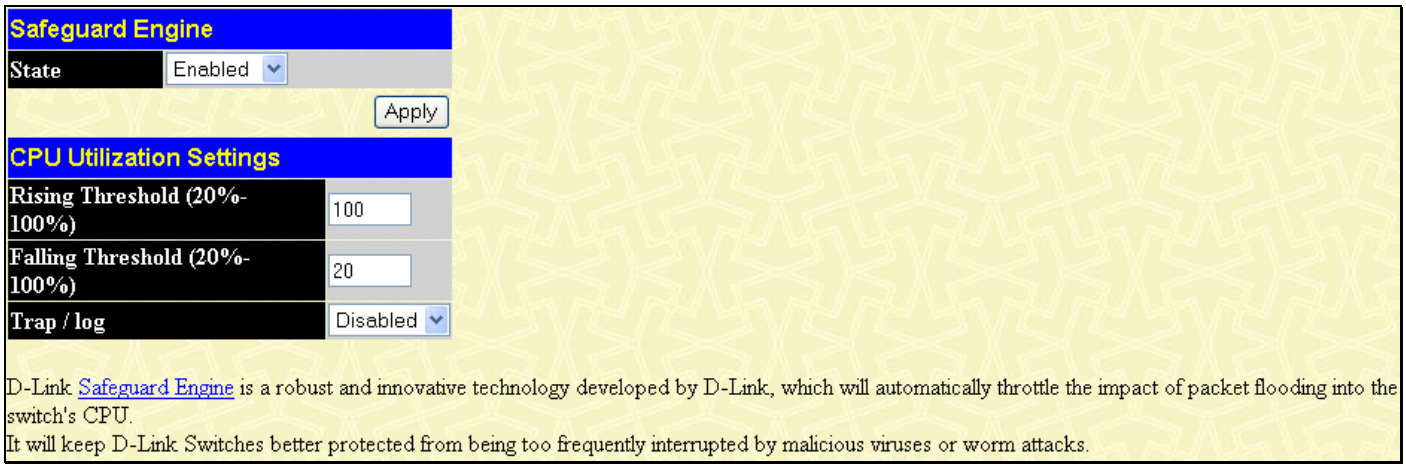


Figure 11- 68. Safeguard Engine window - Advanced Settings

To set the Safeguard Engine for the Switch, complete the following fields:

Parameter	Description
State	Toggle the **State** field to either *Enabled* or *Disabled* for the Safeguard Engine of the Switch.
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.

Filter

CPU Filtering Settings

The CPU Filtering Settings window is divided into two sections. The top section allows the settings of the CPU Filtering Settings to be changed. The bottom section displays the CPU Filtering Status of each port on the Switch.

To configure the CPU Filtering Settings for the Switch, click **Security > Filter > CPU Filtering Settings** which will open the following window:

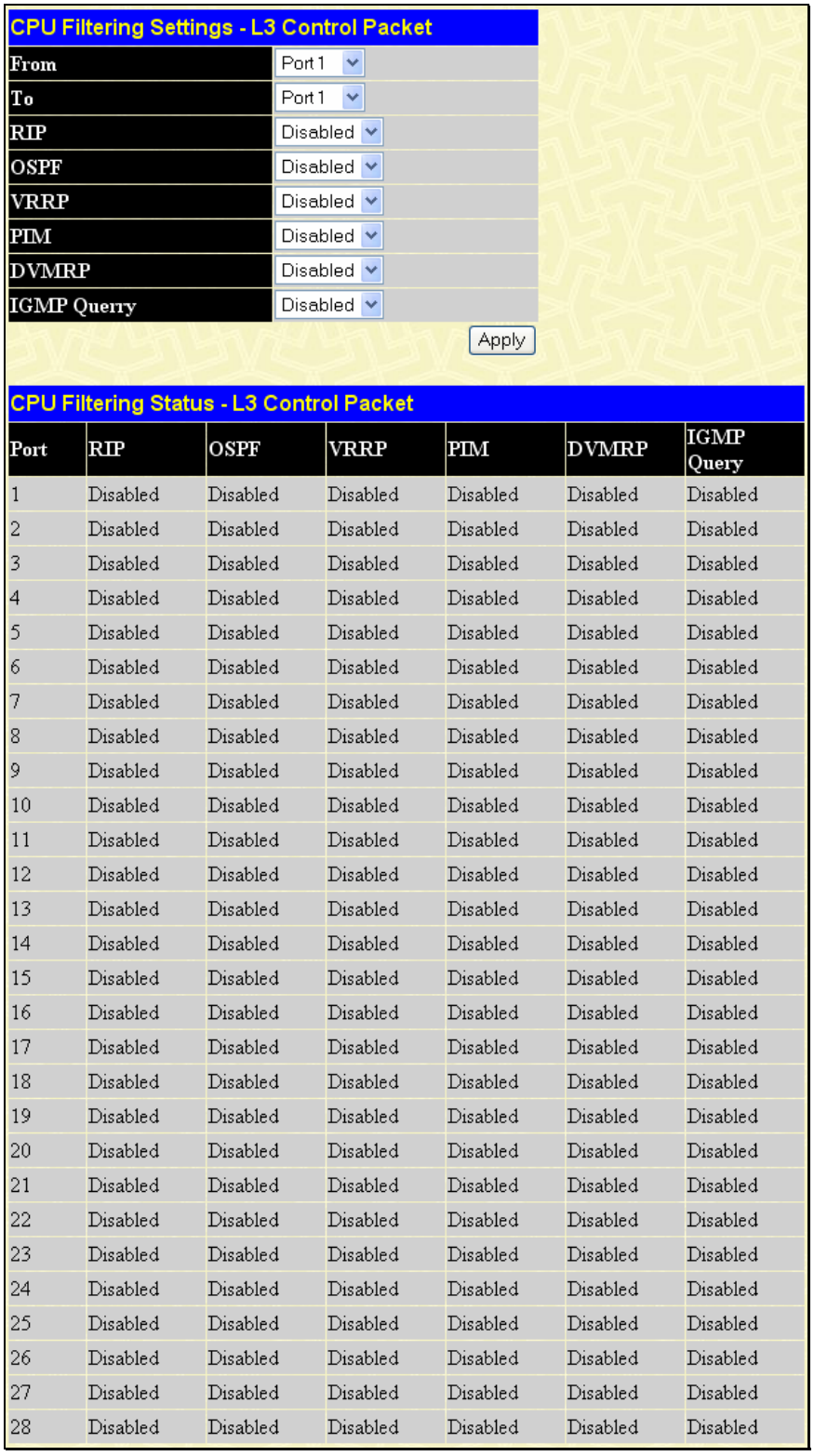


Figure 11- 691. CPU Filtering window

The following parameters can be configured for CPU Filtering:

Parameter	Description
From / To	Use the drop-down menus to select the ports that require the CPU Filter applied to.
RIP	Select *Enabled* from the drop-down menu to discard RIP l3 control packets sent to the CPU from the specified ports.
OSPF	Select *Enabled* from the drop-down menu to discard OSPF l3 control packets sent to the CPU from the specified ports.
VRRP	Select *Enabled* from the drop-down menu to discard VRRP l3 control packets sent to the CPU from the specified ports.
PIM	Select *Enabled* from the drop-down menu to discard PIM l3 control packets sent to the CPU from the specified ports.
DVRMP	Select *Enabled* from the drop-down menu to discard DVRMP l3 control packets sent to the CPU from the specified ports.
IGMP Query	Select *Enabled* from the drop-down menu to discard IGMP Query l3 control packets sent to the CPU from the specified ports.

Click the **Apply** button to save any changes made.

Section 12

Monitoring

Device Status
CPU Utilization
Safeguard Engine Status
Port Utilization
Packets
Errors
Packet Size
Browse Router Port
Port Access Control
MAC Address Table
IP Address Table
Browse Routing Table
Browse ARP Table
Browse IP Multicast Forwarding Table
IGMP Snooping Group
IGMP Snooping Forwarding
Browse IGMP Group Table
DVMRP Monitor
PIM Monitor
OSPF Monitor
Browse WRED Settings
Switch Log

Device Status

The Device Status window displays status information for Internal Power, External Power, Side Fan, and Back Fan.

Device Status

ID	Internal Power	External Power	Side Fan	Back Fan
1	Active	Fail	Fail	OK

Figure 12- 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**.

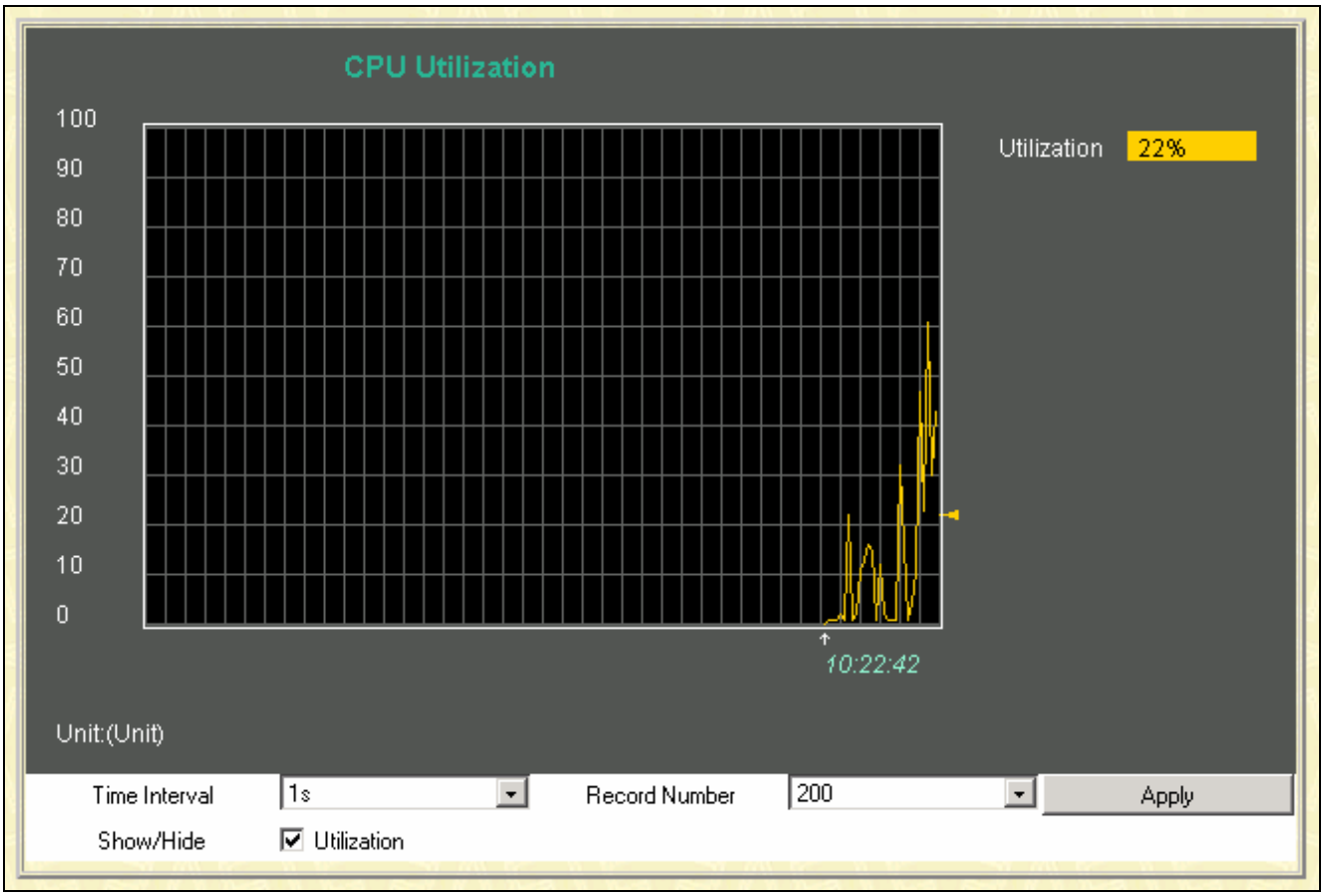


Figure 12- 2. CPU Utilization window

Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics

The information is described 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 *20*.
Utilization	Check whether or not to display Utilization.

Safeguard Engine Status

The following window displays parameters configured for and about the **Safeguard Engine Status** currently set on the Switch.

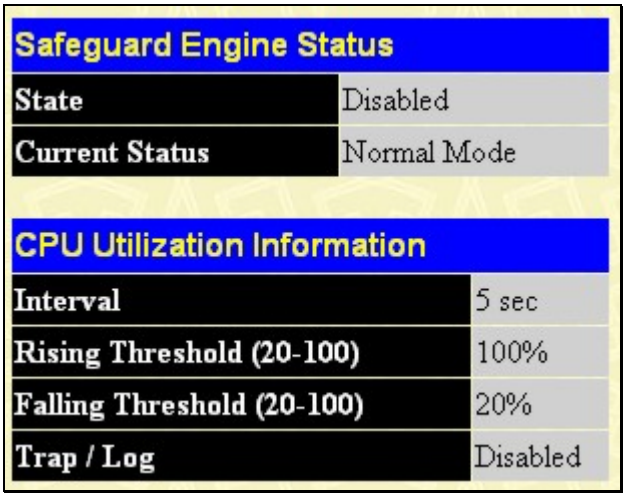


Figure 12- 3. Safeguard Engine Status and CPU Utilization Information window

The information is described as follows:

Parameter	Description
State	Displays the current running state of the Safeguard Engine, whether enabled or disabled.
Current Status	Displays the current running status of the Safeguard Engine, whether engaged or in normal mode.
Interval	Displays the time interval between the checking of the rising and falling threshold of packets entering the Switch. The default setting is 5 seconds.
Rising Threshold	Displays the set percentage of the rising threshold of packets determinant of the Safeguard Engine.
Falling Threshold	Displays the set percentage of the falling threshold of packets determinant of the Safeguard Engine.
Trap/log	Displays the status of the sending of messages to the switch's log or SNMP trap. Enabled will denote the switch will send trap messages in the event of a Safeguard Engine engagement.

Port Utilization

The **Utilization** window displays the percentage of the total available bandwidth being used on the port. To view the port utilization, click **Monitoring** > **Port Utilization**:

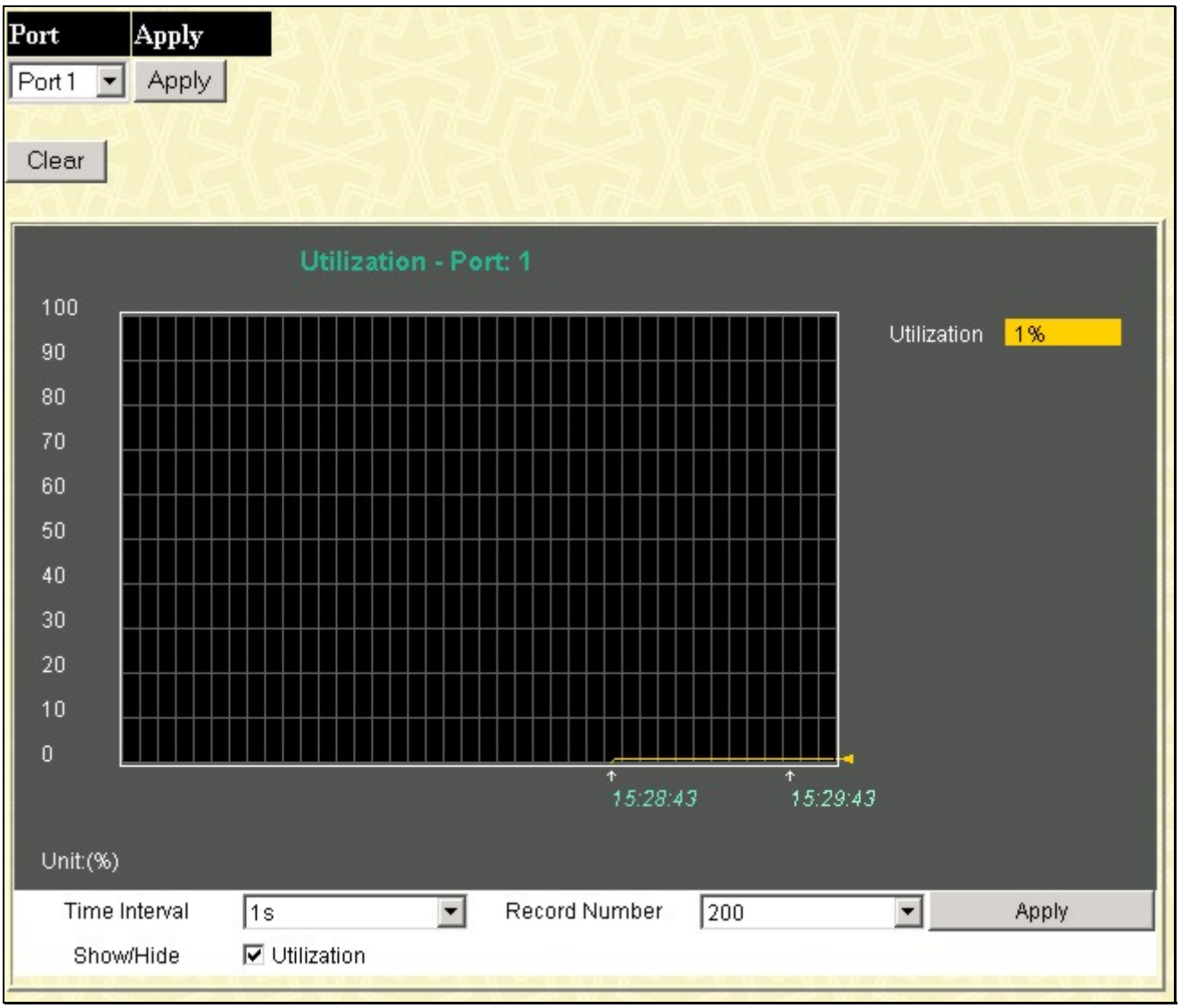


Figure 12- 4. Port Utilization window

Select a port number from the drop down menu and click apply to display the Port Utilization for a particular port. The following fields can be set:

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*.

Click **Clear** to refresh the graph. Click **Apply** to set changes implemented.

Packets

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

Received (RX)

To view this window, click **Monitoring** > **Packets** > **Received (RX)** to display the following graph of packets received on the Switch.

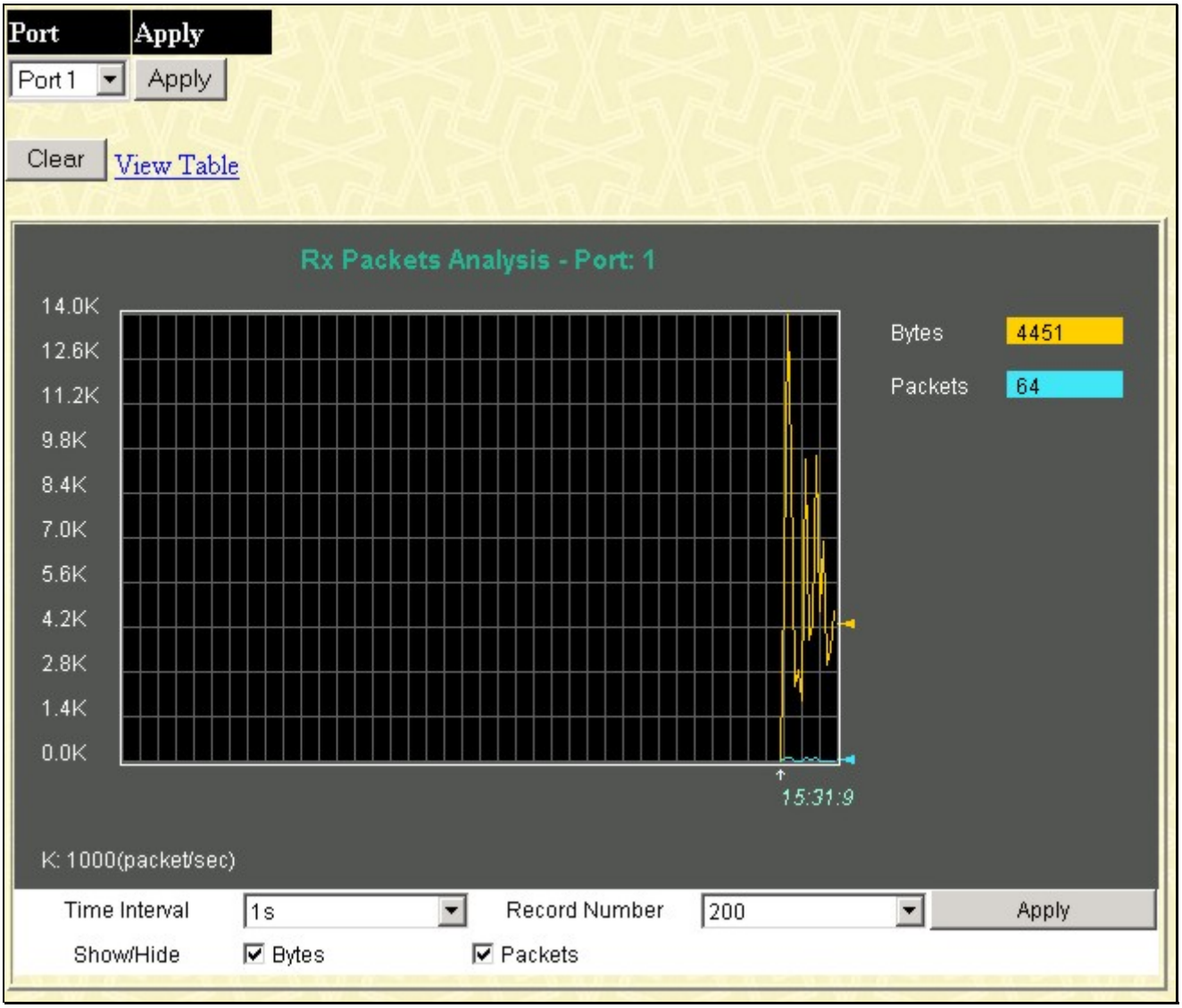


Figure 12- 5. Rx Packets Analysis window (line graph for Bytes and Packets)

Select a Port number from the drop down menu and click **Apply** to display the Rx Packet analysis for a particular port. To view the **Received Packets Table**, click the link View Table, which will show the following table:

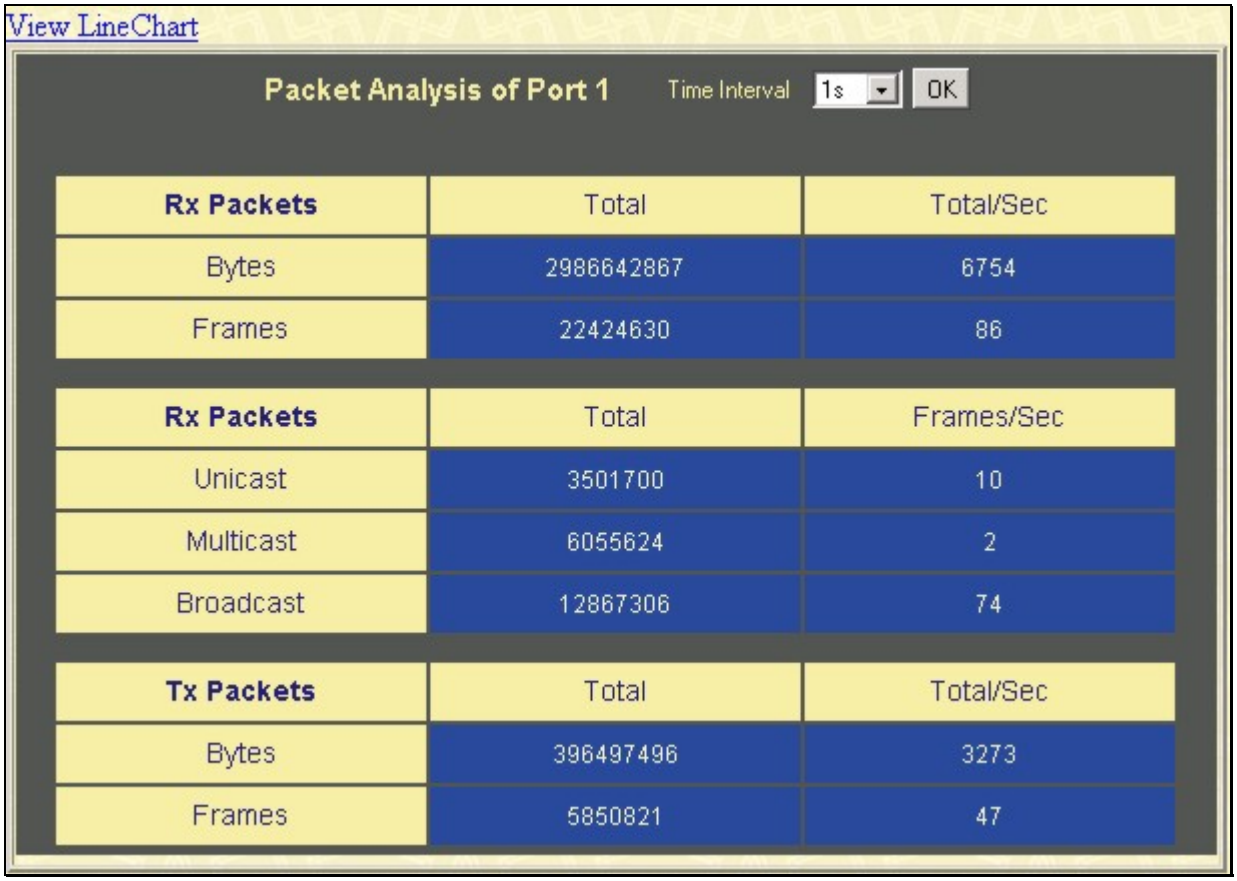


Figure 12- 6. Rx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

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 *20*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
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 Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB Cast (RX)

To view this window, click **Monitoring** > **Packets** > **UMB Cast (RX)** to display the following graph of UMB cast packets received on the Switch.

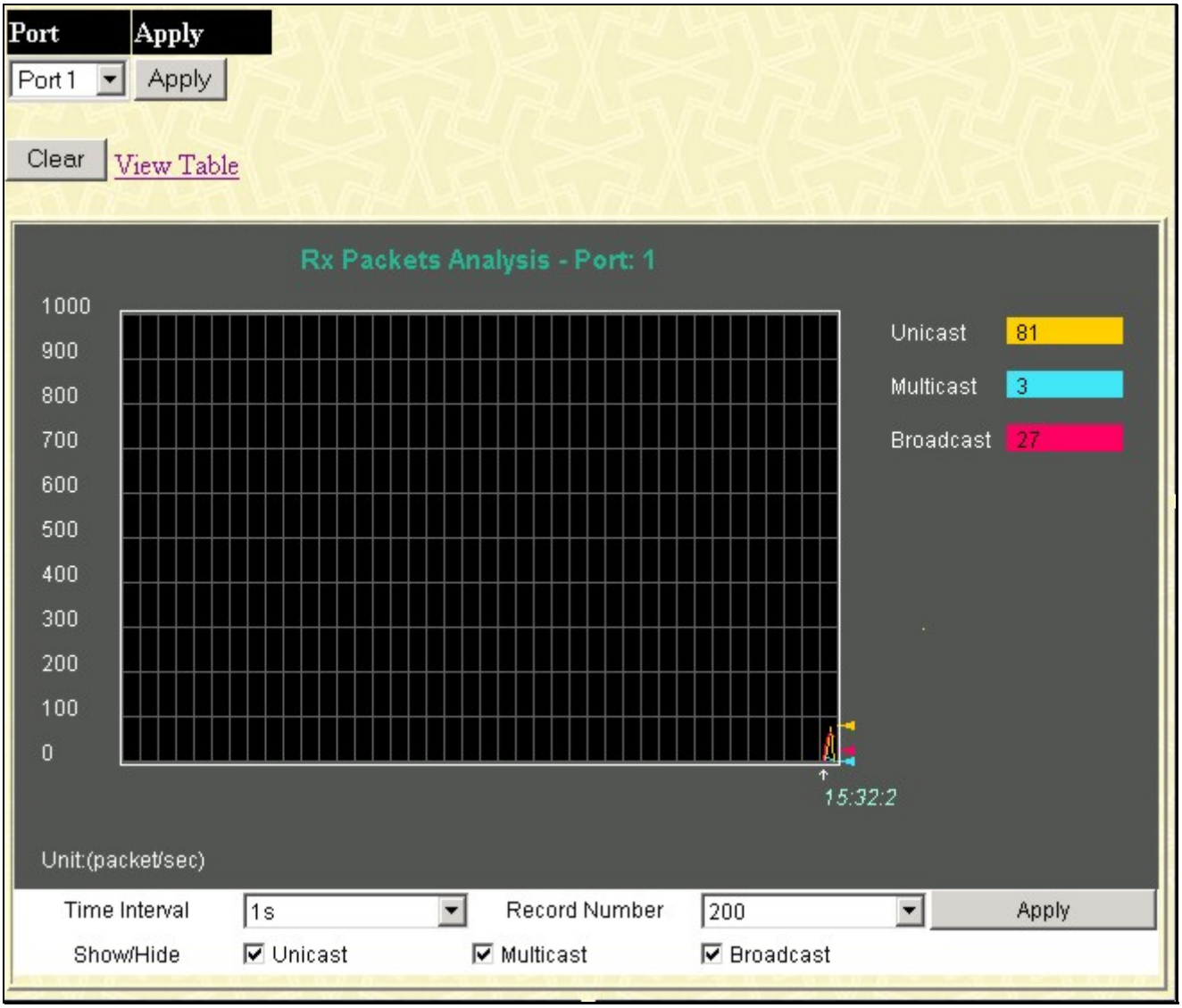


Figure 12- 7. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)

To view the **UMB Cast Table**, click the View Table link, which will show the following table:

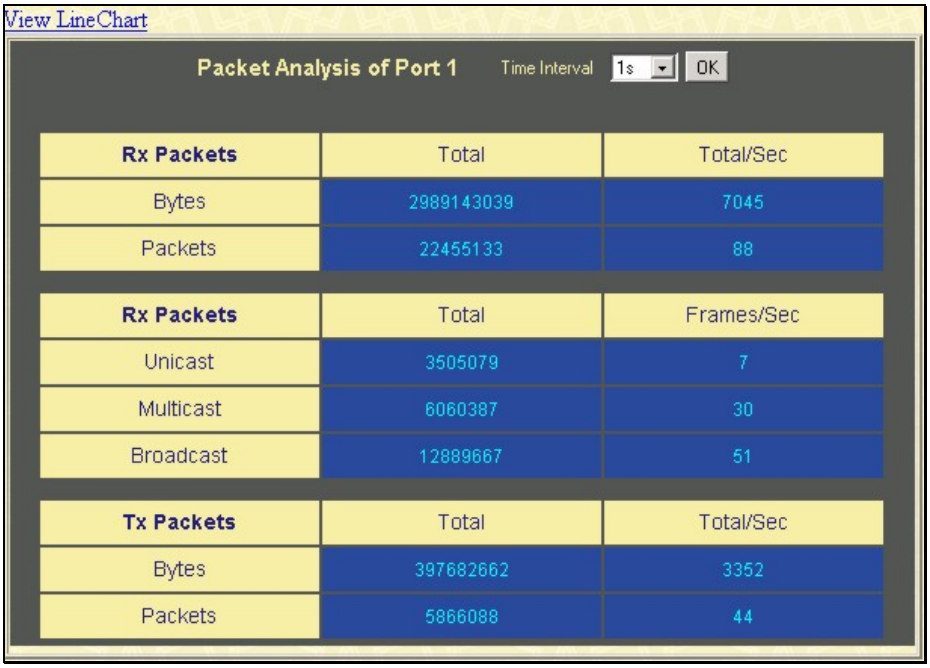


Figure 12- 8. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

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 *20*.
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 Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To view this window, click **Monitoring** > **Packets** > **Transmitted (TX)** to display the following graph of packets transmitted from the Switch.

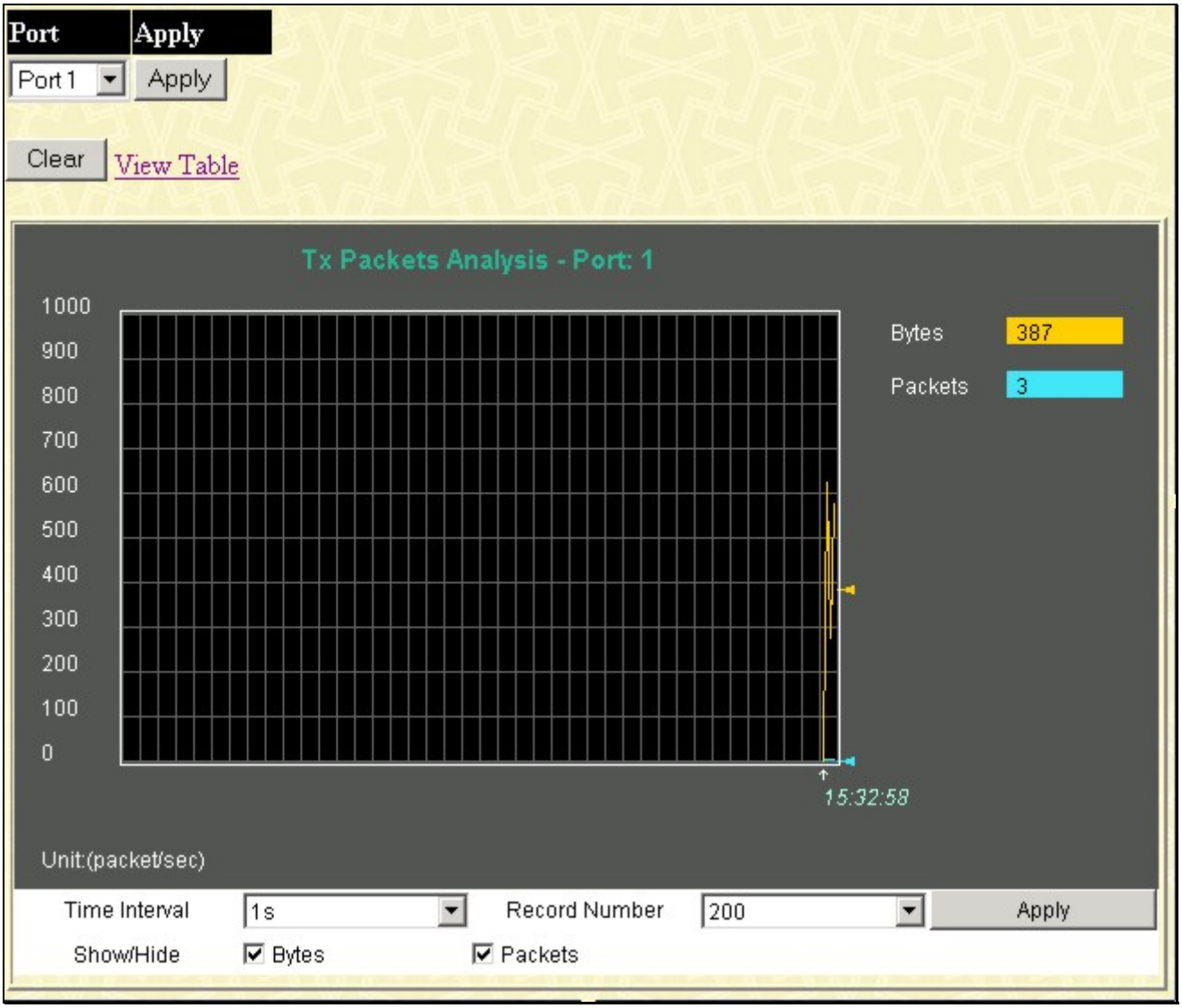


Figure 12- 9. Tx Packets Analysis window (line graph for Bytes and Packets)

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

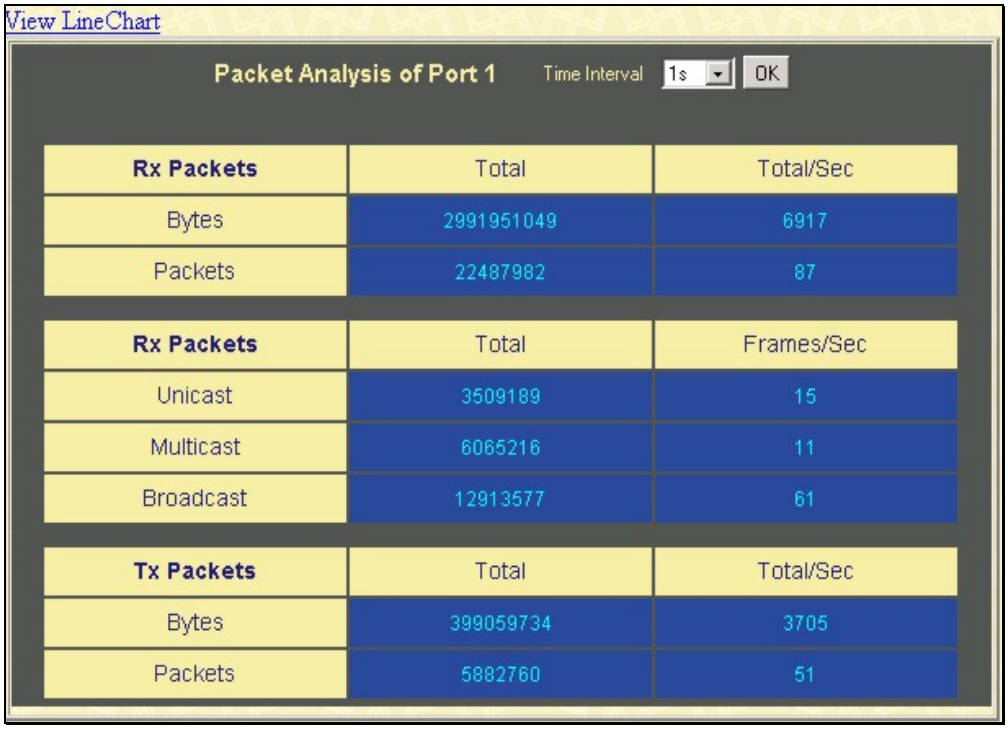


Figure 12- 10. Tx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

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 *20*.
Bytes	Counts the number of bytes successfully sent from the port.
Packets	Counts the number of packets successfully sent on the port.
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 Line Chart	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 view this window, click **Monitoring** > **Errors** > **Received (RX)** to display the following graph of error packets received on the Switch.

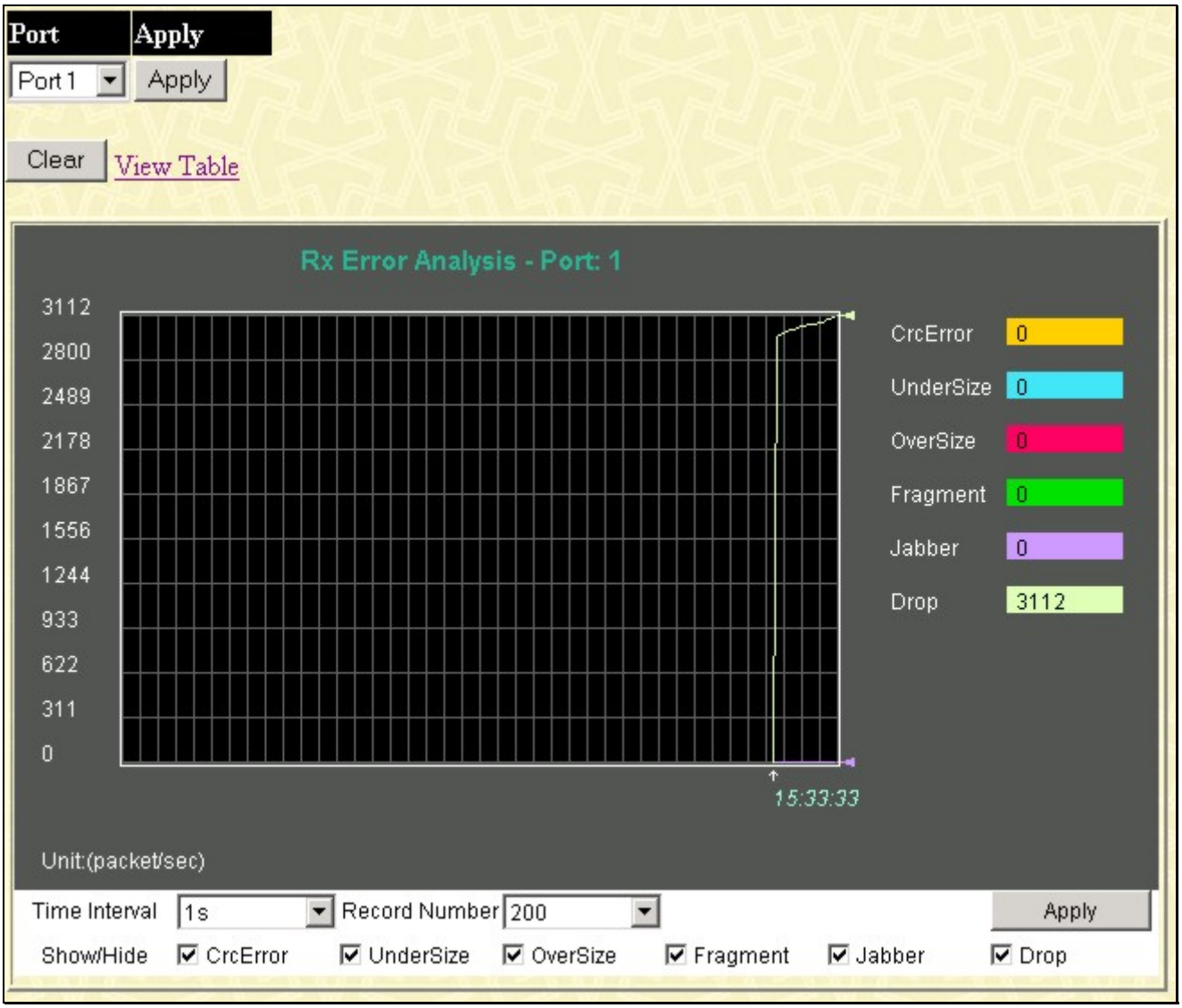


Figure 12- 11. Rx Error Analysis window (line graph)

To view the **Received Error Packets Table**, click the link **View Table**, which will show the following table:

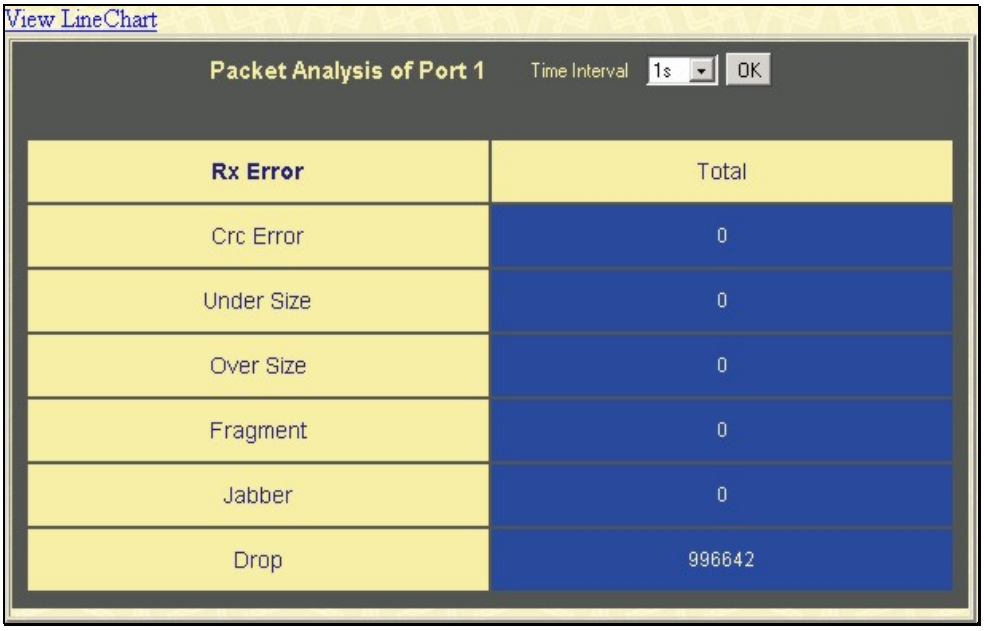


Figure 12- 12. Rx Error Analysis window (table)

The following fields can be set:

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 *20*.
Crc Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
Under Size	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.
Over Size	Counts packets received that were longer than 1518 octets, or if a VLAN frame is 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
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	The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display Crc Error, Under Size, Over Size, Fragment, Jabber, and Drop 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 Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To view this window, click **Monitoring** > **Errors** > **Transmitted (TX)** to display the following graph of error packets received on the Switch.

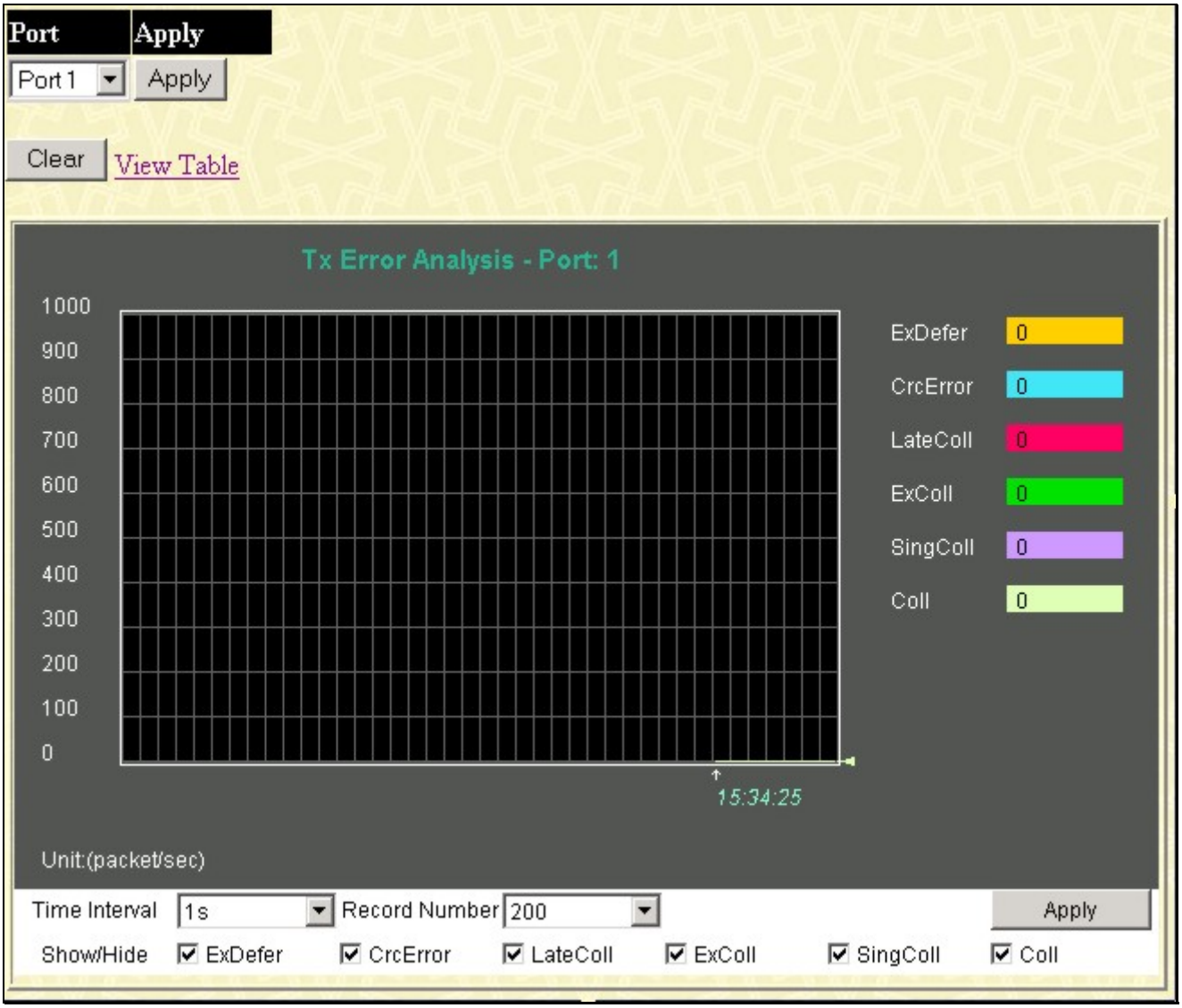


Figure 12- 13. Tx Error Analysis window (line graph)

To view the **Transmitted Error Packets Table**, click the link View Table, which will show the following table:

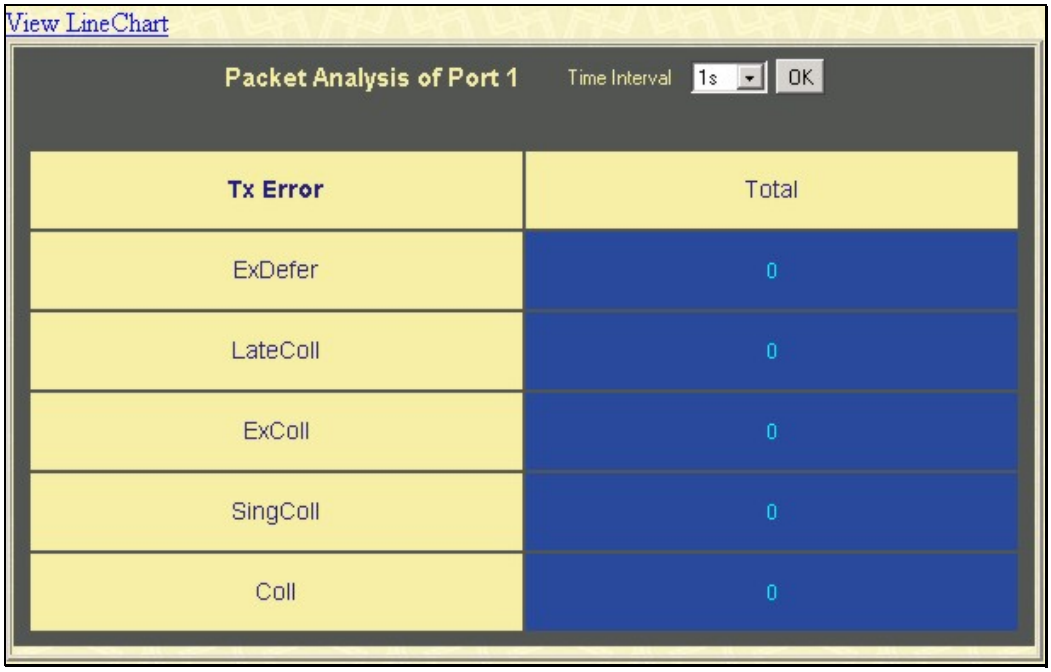


Figure 12- 14. Tx Error Analysis window (table)

The following fields may be set or viewed:

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 *20*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
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.
Coll	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll 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 Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

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.

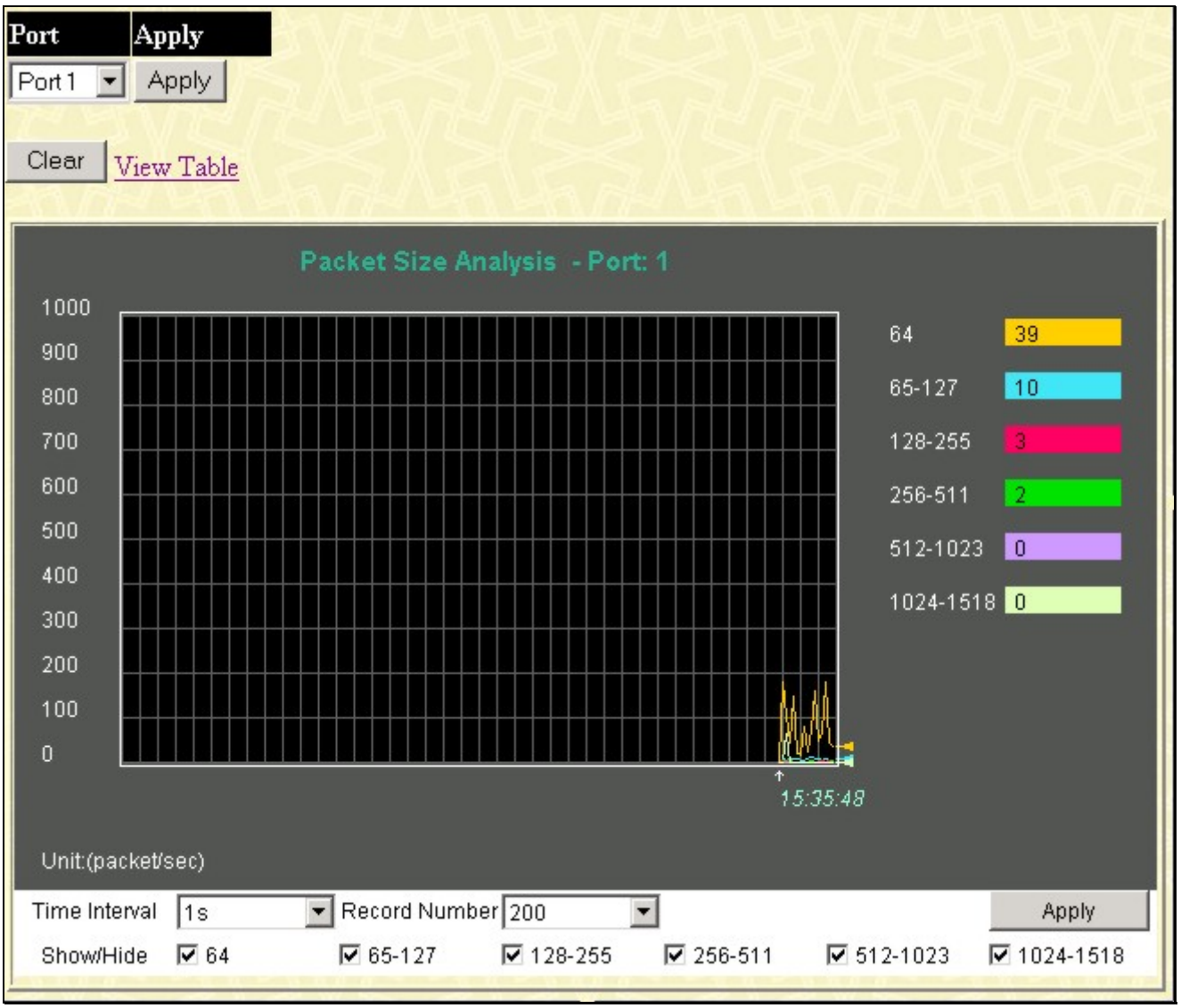


Figure 12- 15. Rx Size Analysis window (line graph)

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

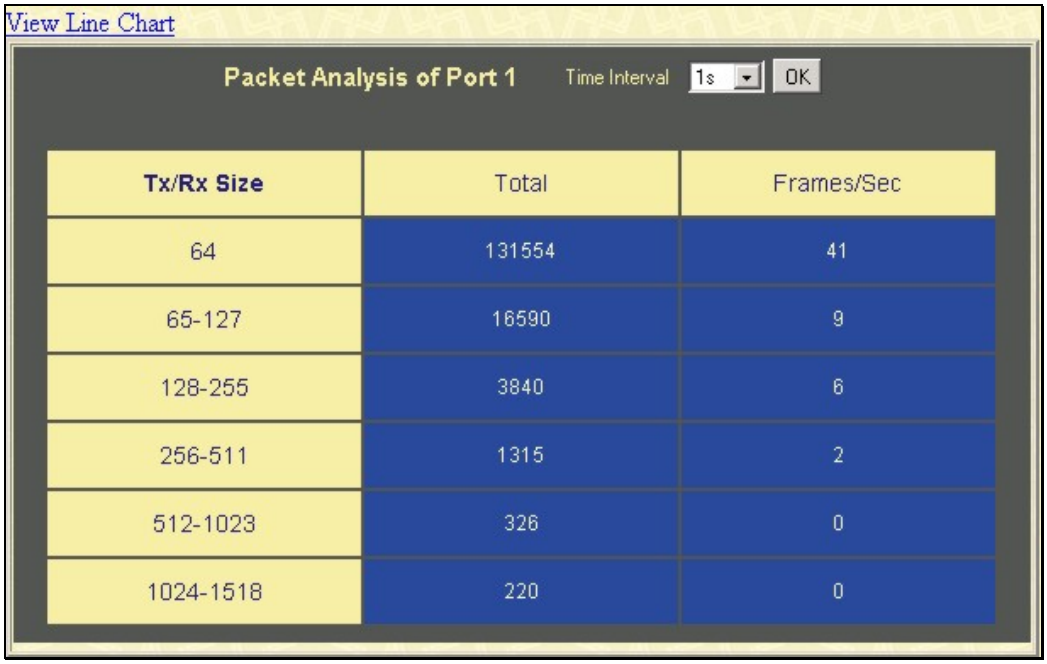


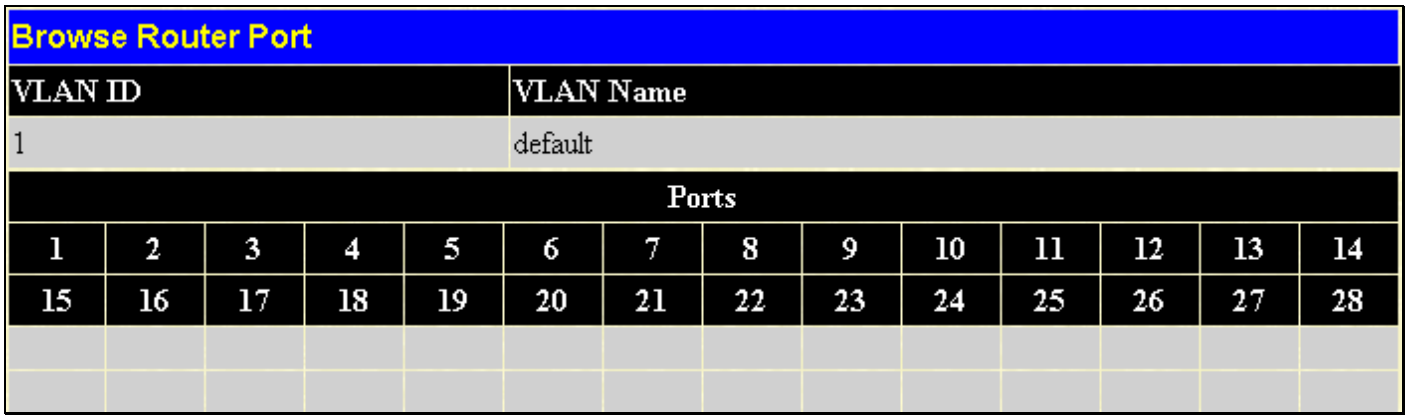
Figure 12- 16. Tx/Rx Packet Size Analysis window (table)

The following fields can be set or viewed:

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 *20*.
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 Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Browse Router Port

This 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. D designates a router port that is dynamically configured by the Switch. To view the following window, click **Monitoring** > **Browse Router Port**.



Browse Router Port

VLAN ID	VLAN Name
1	default

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

Figure 12- 17. Router Port window

Port Access Control

The following screens are used to monitor 802.1x statistics of the Switch, on a per port basis. To view the **Port Access Control** screens, open the monitoring folder and click the **Port Access Control** folder. There are six screens to monitor.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. It has one row for each RADIUS authentication server with which the client shares a secret. To view the **RADIUS Authentication**, click **Monitoring > Port Access Control > RADIUS Authentication**.

Figure 12- 18. RADIUS Authentication window

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

The following fields can be viewed:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
InvalidServerAddr	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.)
AuthServerAddr	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.
AccessRetrans	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 Accounting

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. It has one row for each RADIUS authentication server that the client shares a secret with. To view the **RADIUS Accounting**, click **Monitoring** > **Port Access Control** > **RADIUS Accounting**.

Figure 12- 19. RADIUS Accounting 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.

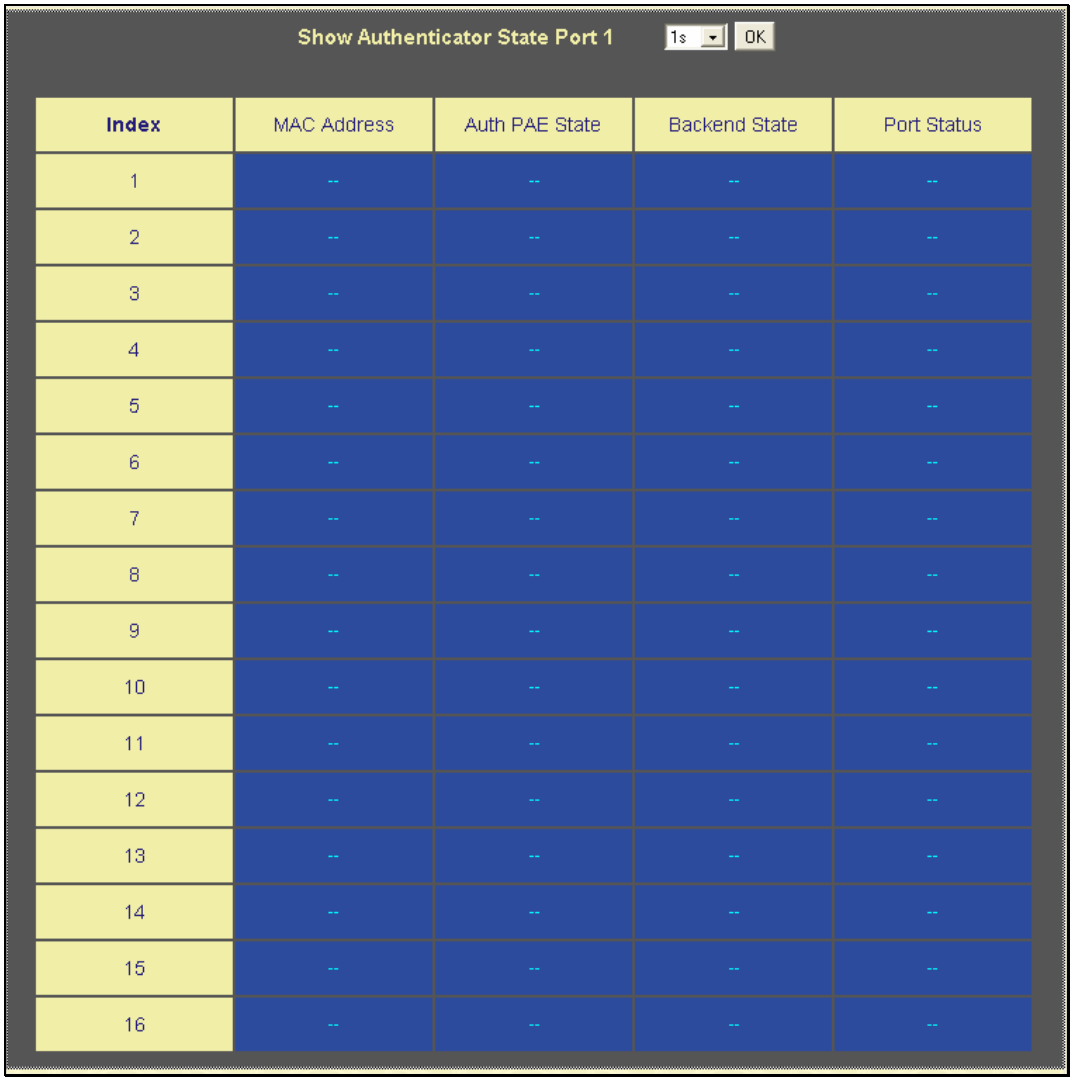
The following fields can be viewed:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS accounting client. (This is not necessarily the same as sysName in MIB II.)
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.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.

Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

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.**



This window displays the **Authenticator State** for individual ports on a selected device. To select unit within the switch stack, use the pull-down menu at the top of the window and click **Apply**. A polling interval between *1* and *60* 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
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*.

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 forwarding table, click **Monitoring** > **MAC Address Table**:

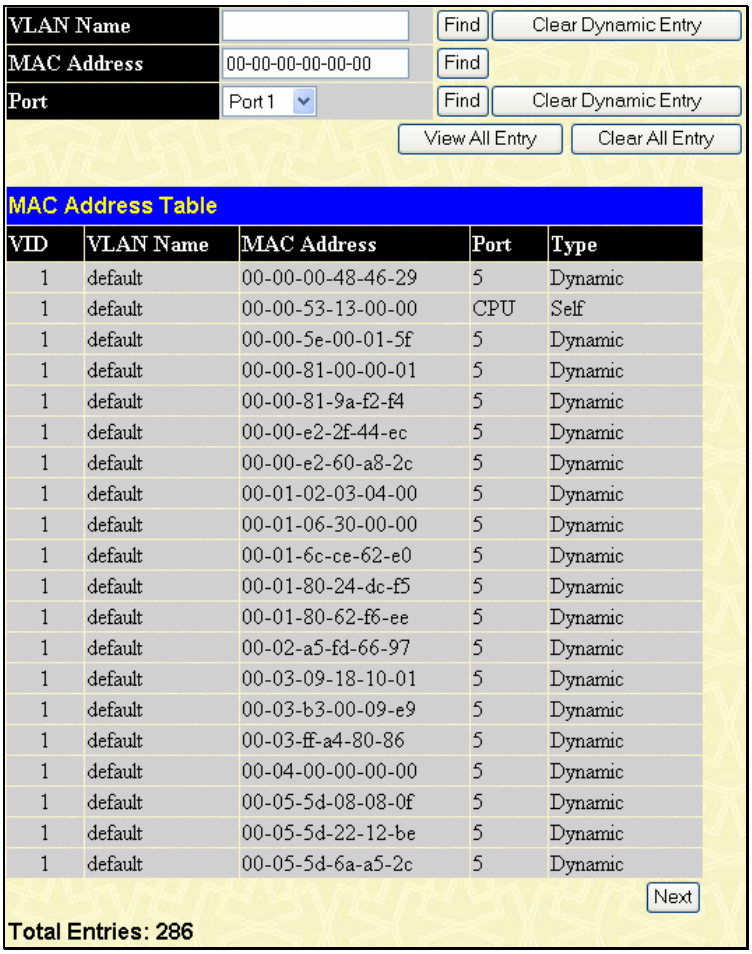


Figure 12- 20. MAC Address Table window

The following fields can be viewed or set:

Parameter	Description
VLAN Name	Enter a VLAN Name for which to browse the forwarding table.
MAC Address	Enter a MAC address for which to browse the forwarding table.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
VID	The VLAN ID of the VLAN the port is a member of.
MAC Address	The MAC address entered into the address table.
Port	The port that the MAC address above corresponds to.
Type	How the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.
Next	Click this button to view the next page of the address table.
Clear Dynamic Entry	Clicking this button will clear Dynamic entries learned by the Switch. This may be accomplished by VLAN Name or by Port.
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.

IP Address Table

The **IP Address Table** is a read only screen where the user may view IP addresses discovered by the Switch. To search a specific IP address, enter it into the field labeled **IP Address** at the top of the screen and click **Find** to begin your search. To view the following table, click **Monitoring > IP Address Table**.

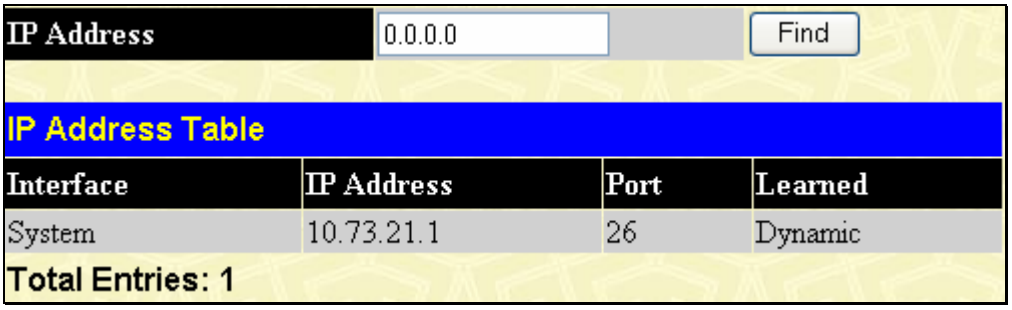


Figure 12- 21. IP Address Table windowBrowse Routing Table

This screen shows the current IP routing table of the Switch. To find a specific IP route, enter an IP address into the **Destination Address** field along with a proper subnet mask into the **Mask** field and click **Find**. To view this table, click **Monitoring > Browse Routing Table**.

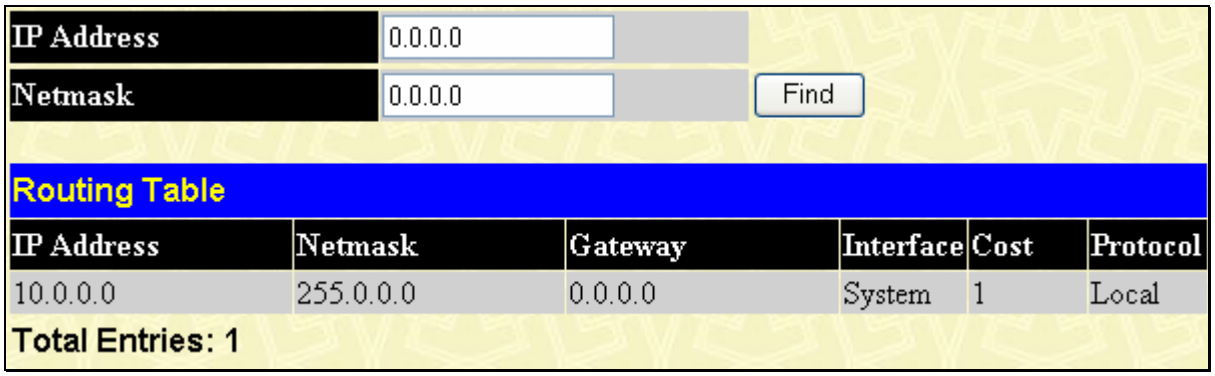


Figure 12- 22. Browse Routing Table window

Browse ARP Table

This window will show current ARP entries on the Switch. To search a specific ARP entry, enter an interface name into the **Interface Name** or an **IP address** and click **Find.** To clear the **ARP Table**, click **Clear All.** To view this table, click **Monitoring > Browse ARP Table**.

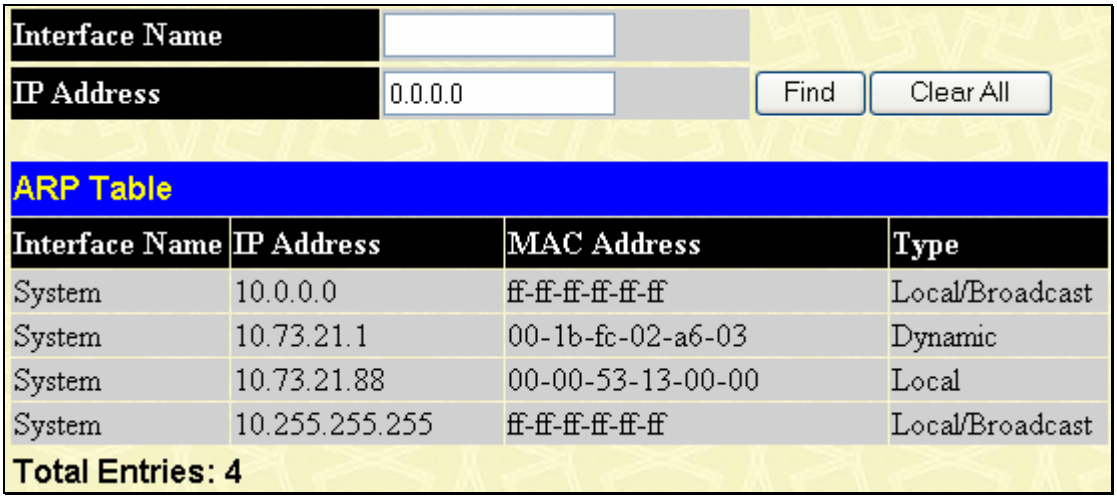


Figure 12- 23. Browse ARP Table window

Browse IP Multicast Forwarding Table

This window will show current IP multicasting information on the Switch. To search a specific entry, enter a multicast group IP address into the **Multicast Group** field or a **Source IP** address and click **Find**. To view this table, click **Monitoring > Browse IP Multicast Forwarding Table**.

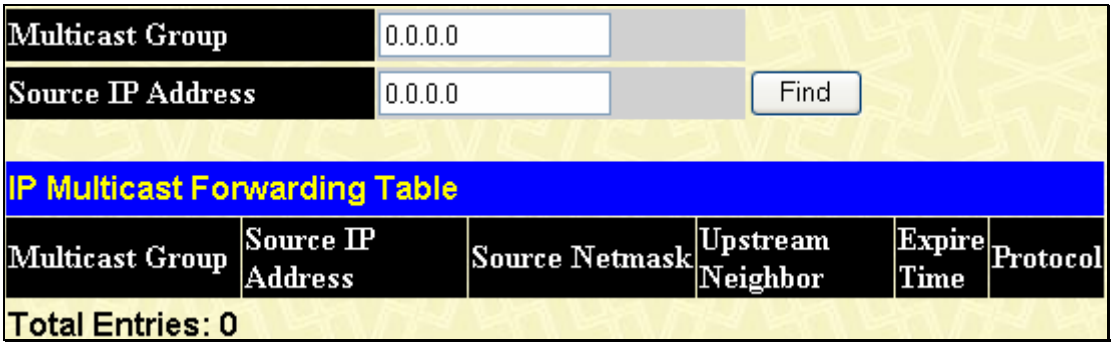


Figure 12- 24. Browse IP Multicast Forwarding Table

IGMP Snooping Group

IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The number of IGMP reports that were snooped is displayed in the Reports field. To view this table, click **Monitoring > IGMP Snooping Group**.

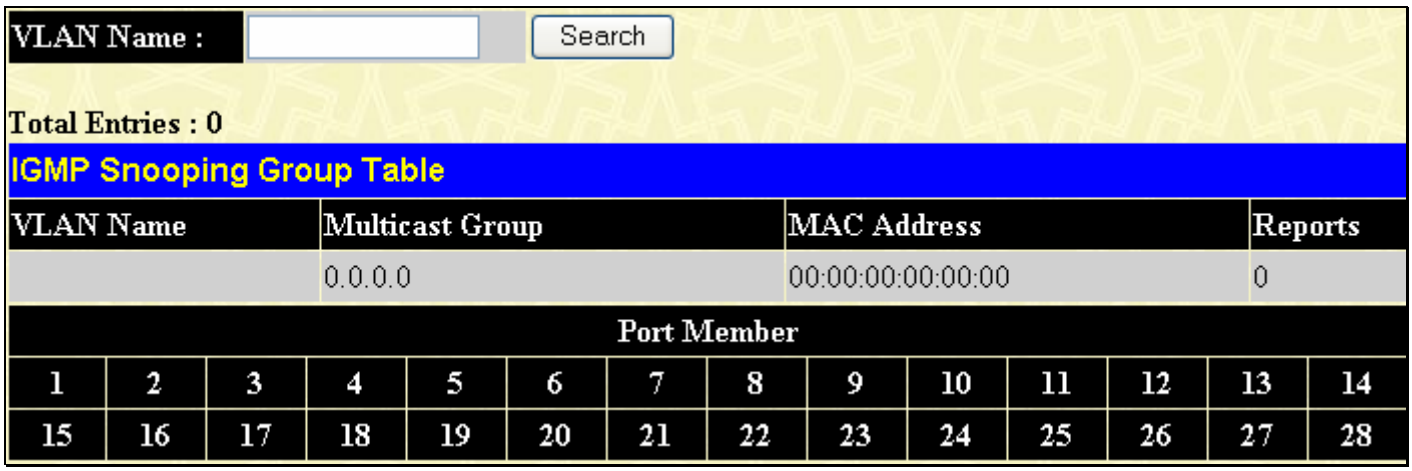


Figure 12- 25. IGMP Snooping Group Table

The user may search the IGMP Snooping Table by entering the VLAN Name in the top left hand corner and clicking **Search**.

NOTE: The Switch supports up to 256 IGMP Snooping groups.

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name 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.
Port Member	These are the ports where the IGMP packets that were snooped are displayed.

IGMP Snooping Forwarding

This window will display the current IGMP snooping forwarding table entries currently configured on the Switch. To view the following window, click **Monotoring** > **IGMP Snooping Forwarding**.

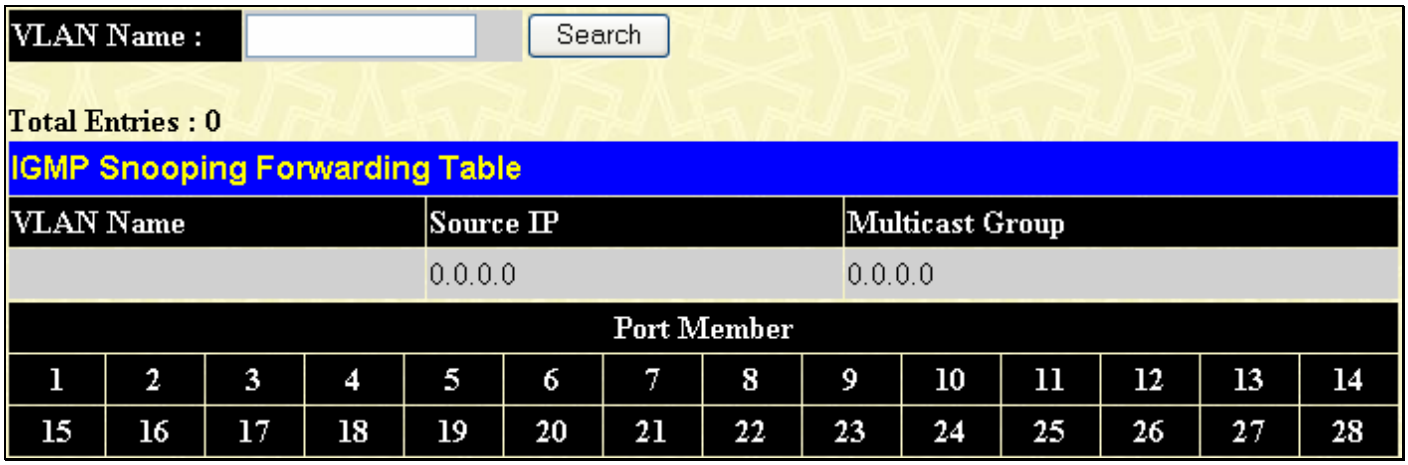


Figure 12- 26. IGMP Snooping Forwarding Table

The user may search the **IGMP Snooping Forwarding Table** by entering the VLAN Name in the top left hand corner and clicking the **Search** button.

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
Source IP	The IP address of the multicast Source.
Multicast Group	The IP address of the multicast group.
Port Member	These are the ports where the IGMP packets that were snooped are displayed.

Browse IGMP Group Table

This window will show current IGMP group entries on the Switch. To search a specific IGMP group entry, enter an interface name into the **Interface Name** field or a **Multicast Group** IP address and click **Find**. To view this window, click **Monitoring** > **Browse IGMP Group Table**.

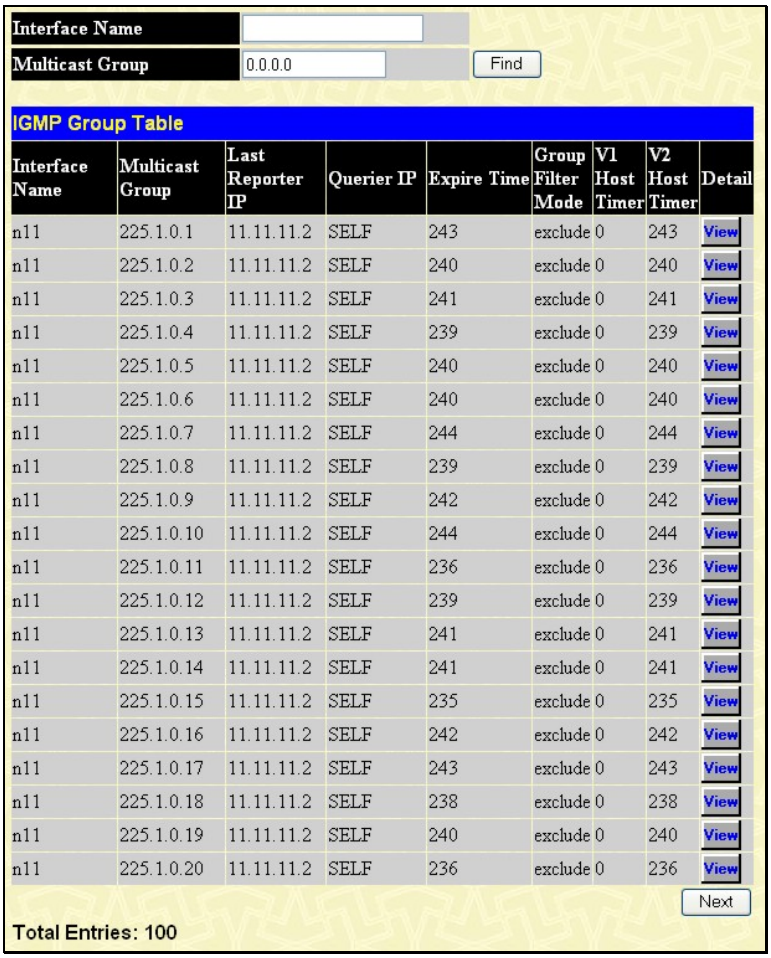


Figure 12- 27. Browse IGMP Group Table

To view the details about a particular IGMP Group entry, click the corresponding View button, which will display the following window.

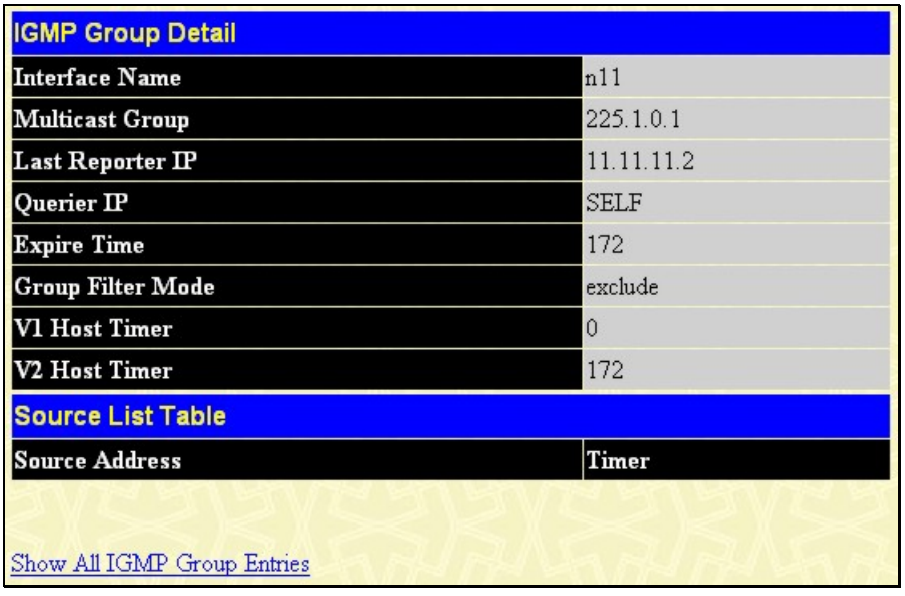


Figure 12- 28. IGMP Group Detail window

DVMRP Monitoring

This menu allows the **DVMRP** (Distance-Vector Multicast Routing Protocol) to be monitored for each IP interface defined on the Switch. This folder, found in the **Monitoring** folder, offers 4 screens for monitoring: **Browse DVMRP Routing Table**, **Browse DVMRP Neighbor Address Table**, **Browse DVMRP Routing Next Hop Table** and **Browse PIM Neighbor Table**.

Browse DVMRP Routing Table

Multicast routing information is gathered and stored by DVMRP in the **DVMRP Routing Table**, this table contains one row for each port in a DVMRP mode. Each routing entry contains information about the source and multicast group, and incoming and outgoing interfaces. You may define your search by entering a **Source IP Address** and its subnet mask into the fields at the top of the page. To view this window, click **Monitoring** > **Browse DVMRP Monitoring**,

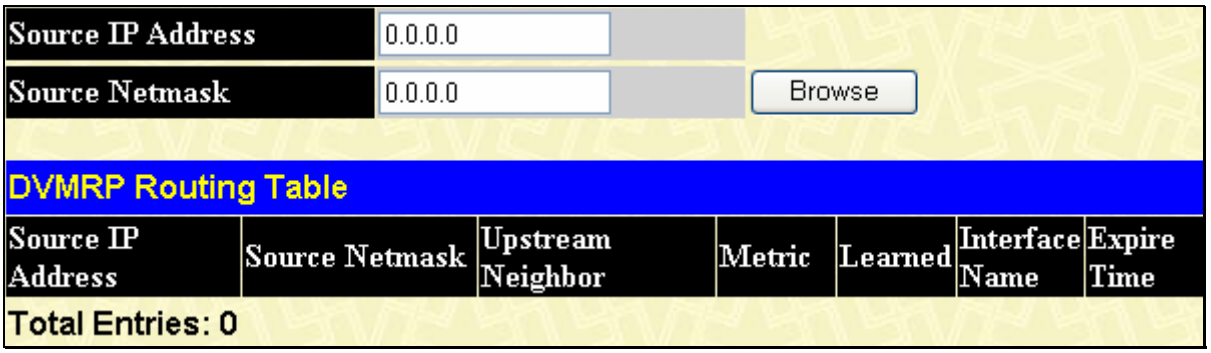


Figure 12- 29. DVMRP Routing Table

Browse DVMRP Neighbor Table

This table contains information about DVMRP neighbors of the Switch. To search this table, enter either an **Interface Name** or **Neighbor Address** into the respective field and click the **Find** button. DVMRP neighbors of that entry will appear in the **DVMRP Neighbor Table** below. To view this table, click **Monitoring > DVMRP Monitor > Browse DVMRP Neighbor**.

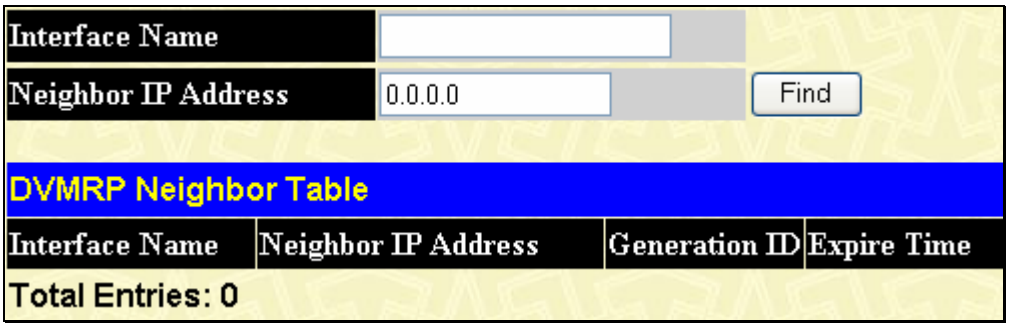


Figure 12- 30. DVMRP Neighbor Table

Browse DVMRP Routing Next Hop Table

The **DVMRP Routing Next Hop Table** contains information regarding the next-hop for forwarding multicast packets on outgoing interfaces. Each entry in the **DVMRP Routing Next Hop Table** refers to the next-hop of a specific source to a specific multicast group address. To search this table, enter either an **Interface Name** or **Source IP Address** into the respective field and click the **Find** button. The next hop of that DVMRP Routing entry will appear in the **DVMRP Routing Next Hop Table** below. To view this table, click **Monitoring > DVMRP Monitor > Browse DVMRP Routing Next Hop Table**.

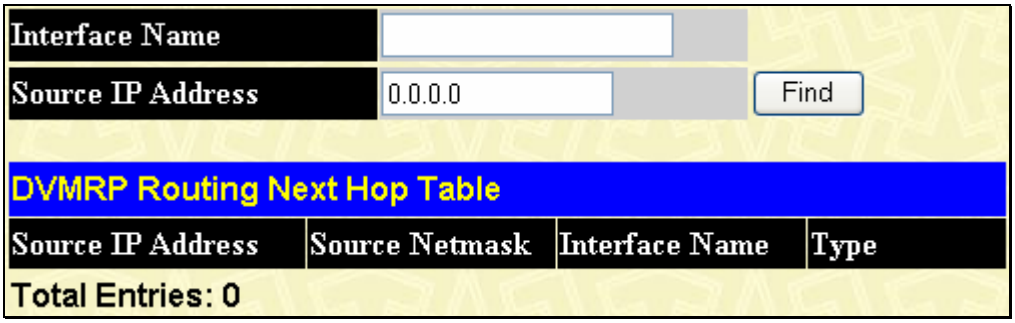


Figure 12- 31. DVMRP Routing Next Hop Table

PIM Monitoring

Multicast routers use **Protocol Independent Multicast (PIM)** to determine which other multicast routers should receive multicast packets. To find out more information concerning PIM and its configuration on the Switch, see the **IP Multicast Routing Protocol** chapter of Section 6, **Configuration**.

Browse PIM Neighbor Table

The **PIM Neighbor Table** contains information regarding each of a router's PIM neighbors. To search this table, enter either an **Interface Name** or **Neighbor Address** into the respective field and click the **Find** button. PIM neighbors of that entry will appear in the **PIM Neighbor Table** below. This screen may be found by clicking **Monitoring** > **PIM Monitor > Browse PIM Neighbor Table**.

Figure 12- 32. PIM Neighbor Table

PIM IP MRoute Table

The PIM IP MRoute Table is used to view information regarding the multicast data route entries in the Switch. This screen may be found by clicking **Monitoring > Layer 3 Feature > PIM Monitor > Browse PIM IP MRoute Table.**

PIM IP MRoute Table

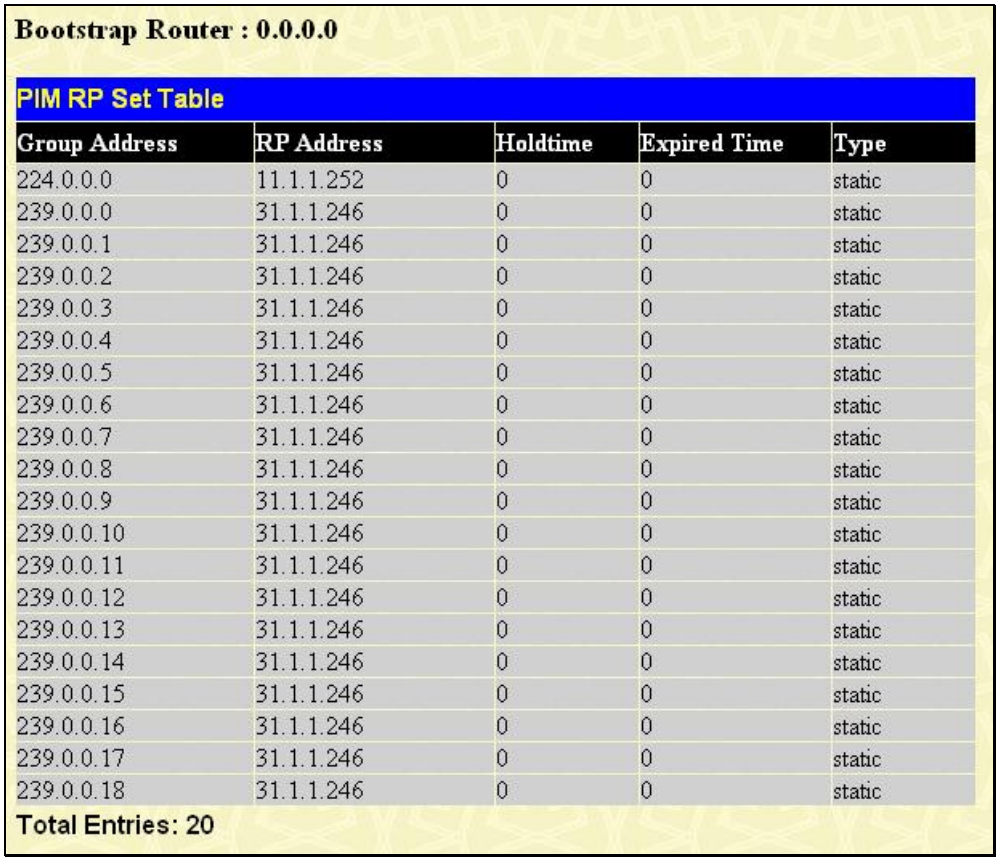
Group Address	Source Address	Upstream Assert Timer	Assert Metric	Assert Metric Pref	Assert RPT Bit	Flag	Type
225.10.10.15	10.62.58.78	0	0	0	0	spt	(S,G)
229.55.150.208	10.6.51.1	0	0	0	0	spt	(S,G)
229.55.150.208	10.38.45.151	0	0	0	0	spt	(S,G)
229.55.150.208	10.38.45.192	0	0	0	0	spt	(S,G)
229.55.150.208	10.51.16.1	0	0	0	0	spt	(S,G)
229.55.150.208	10.59.23.10	0	0	0	0	spt	(S,G)
239.255.255.250	10.26.66.3	0	0	0	0	spt	(S,G)
239.255.255.250	10.48.75.101	0	0	0	0	spt	(S,G)
239.255.255.250	10.60.97.12	0	0	0	0	spt	(S,G)

Total Entries: 9

Figure 12- 33. PIM IP MRoute Table

Browse PIM RP Set Table

The following window is used to assess information regarding the Rendezvous Point (RP) Set on the Switch. This screen may be found by clicking **Monitoring > Layer 3 Feature > PIM Monitor > Browse PIM RP Set Table.**



Bootstrap Router : 0.0.0.0

PIM RP Set Table

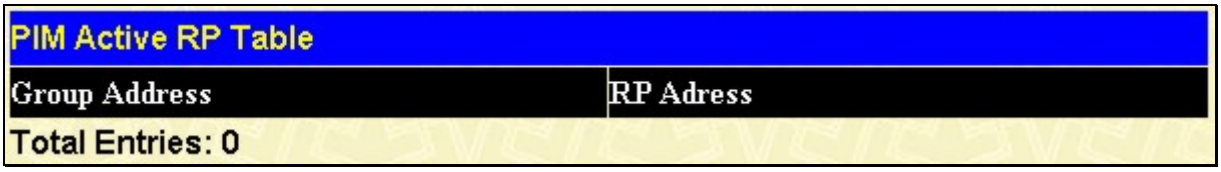
Group Address	RP Address	Holdtime	Expired Time	Type
224.0.0.0	11.1.1.252	0	0	static
239.0.0.0	31.1.1.246	0	0	static
239.0.0.1	31.1.1.246	0	0	static
239.0.0.2	31.1.1.246	0	0	static
239.0.0.3	31.1.1.246	0	0	static
239.0.0.4	31.1.1.246	0	0	static
239.0.0.5	31.1.1.246	0	0	static
239.0.0.6	31.1.1.246	0	0	static
239.0.0.7	31.1.1.246	0	0	static
239.0.0.8	31.1.1.246	0	0	static
239.0.0.9	31.1.1.246	0	0	static
239.0.0.10	31.1.1.246	0	0	static
239.0.0.11	31.1.1.246	0	0	static
239.0.0.12	31.1.1.246	0	0	static
239.0.0.13	31.1.1.246	0	0	static
239.0.0.14	31.1.1.246	0	0	static
239.0.0.15	31.1.1.246	0	0	static
239.0.0.16	31.1.1.246	0	0	static
239.0.0.17	31.1.1.246	0	0	static
239.0.0.18	31.1.1.246	0	0	static

Total Entries: 20

Figure 12- 34. PIM RP Set Table

Browse PIM Active RP Table

The following window is used to view information regarding active Rendezvous Points on the PIM-SM enabled network. This screen may be found by clicking **Monitoring > Layer 3 Feature > PIM Monitor > Browse PIM Active RP Table.**



PIM Active RP Table

Group Address	RP Adress

Total Entries: 0

Figure 12- 35. PIM Active RP Table

OSPF Monitor

This section offers windows regarding OSPF (Open Shortest Path First) information on the Switch, including the **OSPF LSDB Table**, **OSPF Neighbor Table** and the **OSPF Virtual Neighbor Table**. To view these tables, open the **Monitoring** folder and click **OSPF Monitor**.

Browse OSPF LSDB Table

The **OSPF Link-State Database Table** displays the current link-state database in use by the OSPF routing protocol on a per-OSPF area basis. To view this table, click **Monitoring** > **OSPF Monitor** > **Browse OSPF LSDB Table**.

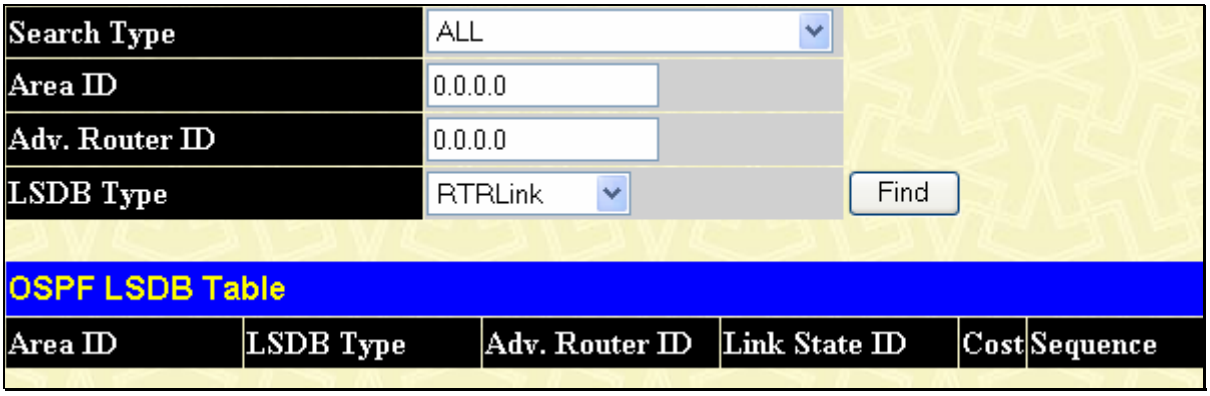


Figure 12- 36. Browse OSPF LSDB Table

The user may search for a specific entry by entering the following information into the fields at the top of the screen:

To browse the **OSPF LSDB Table**, you first must select which browse method you want to use in the **Search Type** field. The choices are *All*, *Area ID*, *Advertise Router ID*, *LSDB*, *Area ID & Advertise Router ID*, *Area ID & LSDB*, and *Advertise Router ID & LSDB*.

If *Area ID* is selected as the browse method, you must enter the IP address in the **Area ID** field, and then click *Find*.

If *Adv. Router ID* is selected, you must enter the IP address in the **Adv. Router ID** field, and then click *Find*.

If *LSDB* is selected, you must select the type of link state (*RtrLink*, *NetLink*, *Summary*, *ASSummary* and *ASExtLink*) in the **LSDB Type** field, and then click *Find*.

The following fields are displayed in the **OSPF LSDB Table**:

Parameter	Description
Area ID	Allows the entry of an OSPF Area ID. This Area ID will then be used to search the table, and display an entry – if there is one.
LSDB Type	Displays which one of eight types of link advertisements by which the current link was discovered by the Switch: *All*, Router link (*RTRLink*), Network link (*NETLink*), Summary link (*Summary*), Autonomous System link (*ASSummary*), Autonomous System external link (*ASExternal)*, MCGLink (*Multicast Group*) and NSSA (*Not So Stubby Area*).
Adv. Router ID	Displays the Advertising Router's ID.
Link State ID	This field identifies the portion of the Internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's LS type. **LS Type** — **Link State ID** 1 — The originating router's Router ID. 2 — The IP interface address of the network's Designated Router. 3 — The destination network's IP address. 4 — The Router ID of the described AS boundary router.
Cost	Displays the cost of the table entry.

Sequence	Displays a sequence number corresponding to number of times the current link has been advertised as changed.

Browse OSPF Neighbor Table

Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two-neighbor routers. This table displays OSPF neighbors of the Switch. To view this table, click **Monitoring** > **OSPF Monitoring** > **Browse OSPF Neighbor Table**.

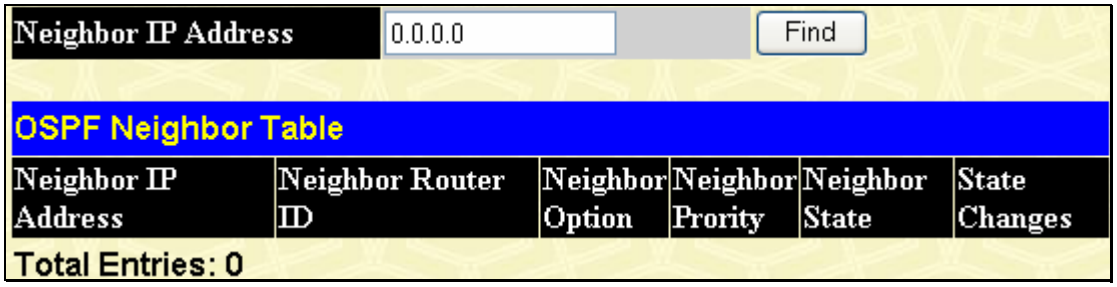


Figure 12- 37. OSPF Neighbor Table

To search for OSPF neighbors, enter an IP address and click **Find**. Valid OSPF neighbors will appear in the **OSPF Neighbor Table** below.

Browse OSPF Virtual Neighbor Table

This table displays a list of **Virtual OSPF Neighbors** of the Switch. To view this table click **Monitoring** > **Browse OSPF Virtual Neighbor Table** > **OSPF Monitoring**. The user may choose to specifically search a virtual neighbor by using one of the two search options at the top of the screen, which are:

Parameter	Description
Transit Area ID	Allows the entry of an OSPF Area ID – previously defined on the Switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
Virtual Neighbor Router ID	The OSPF router ID for the remote router. This IP address uniquely identifies the remote area's Area Border Router.

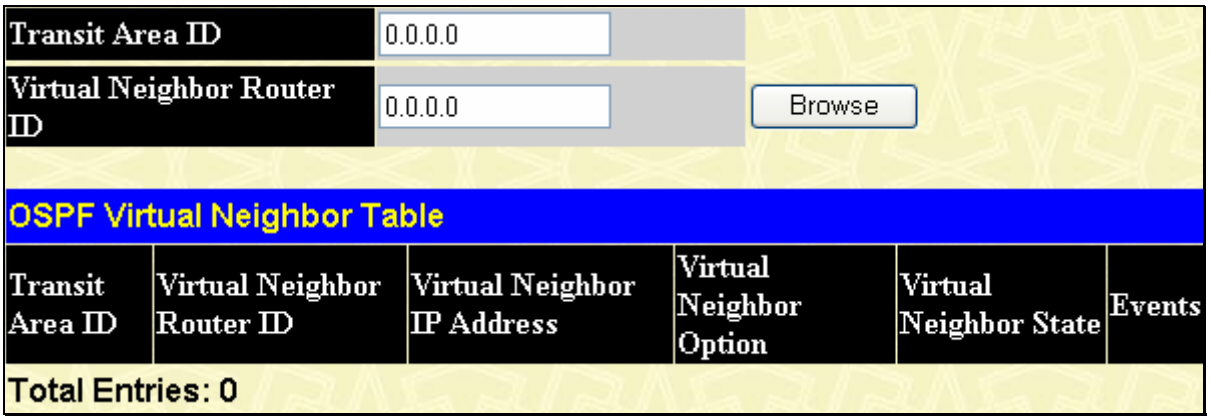


Figure 12- 38. OSPF Virtual Neighbor Table

Browse WRED Settings

The following window displays the WRED settings currently employed on the Switch. To view this window, click **Monitoring** > **Browse WRED Settings**.

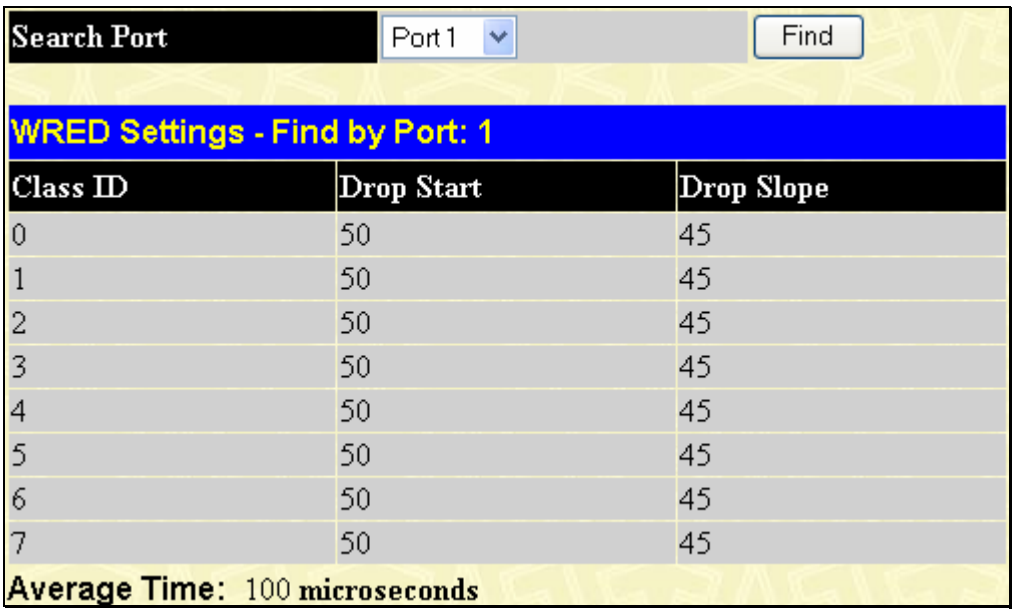


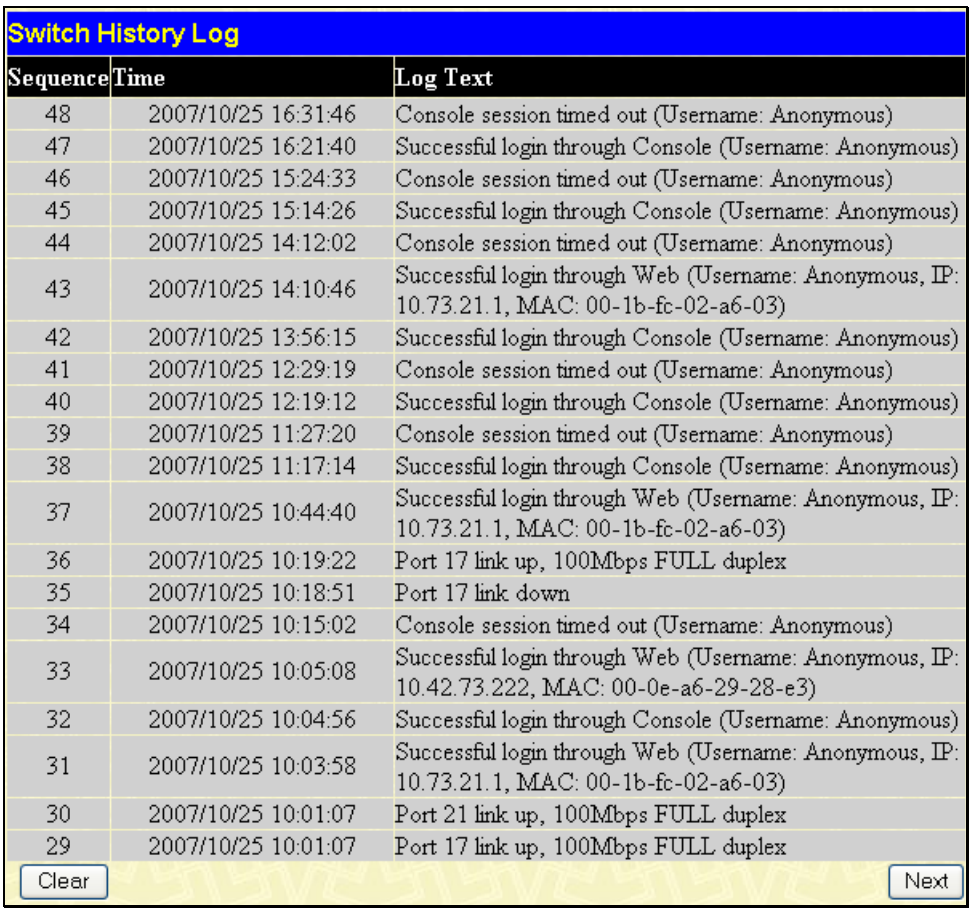
Figure 12- 39. WRED Settings window

The following parameters are displayed above

Parameter	Description
Search Port	Select a port using the pull down menu by which to display the WRED settings.
Class ID	Displays the Class IDs on the port currently being viewed.
Drop Start	Displays the Drop Start set as a percentage from 1-100.
Drop Slope	Displays the Drop Slope set as a degree between 0 and 90.
Average Time	Displays the average time the WRED mechanism checks the packet fill of the QoS queues and the rate of ingress packets.

Switch 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** > **Switch Log**.



Switch History Log

Sequence	Time	Log Text
48	2007/10/25 16:31:46	Console session timed out (Username: Anonymous)
47	2007/10/25 16:21:40	Successful login through Console (Username: Anonymous)
46	2007/10/25 15:24:33	Console session timed out (Username: Anonymous)
45	2007/10/25 15:14:26	Successful login through Console (Username: Anonymous)
44	2007/10/25 14:12:02	Console session timed out (Username: Anonymous)
43	2007/10/25 14:10:46	Successful login through Web (Username: Anonymous, IP: 10.73.21.1, MAC: 00-1b-fc-02-a6-03)
42	2007/10/25 13:56:15	Successful login through Console (Username: Anonymous)
41	2007/10/25 12:29:19	Console session timed out (Username: Anonymous)
40	2007/10/25 12:19:12	Successful login through Console (Username: Anonymous)
39	2007/10/25 11:27:20	Console session timed out (Username: Anonymous)
38	2007/10/25 11:17:14	Successful login through Console (Username: Anonymous)
37	2007/10/25 10:44:40	Successful login through Web (Username: Anonymous, IP: 10.73.21.1, MAC: 00-1b-fc-02-a6-03)
36	2007/10/25 10:19:22	Port 17 link up, 100Mbps FULL duplex
35	2007/10/25 10:18:51	Port 17 link down
34	2007/10/25 10:15:02	Console session timed out (Username: Anonymous)
33	2007/10/25 10:05:08	Successful login through Web (Username: Anonymous, IP: 10.42.73.222, MAC: 00-0e-a6-29-28-e3)
32	2007/10/25 10:04:56	Successful login through Console (Username: Anonymous)
31	2007/10/25 10:03:58	Successful login through Web (Username: Anonymous, IP: 10.73.21.1, MAC: 00-1b-fc-02-a6-03)
30	2007/10/25 10:01:07	Port 21 link up, 100Mbps FULL duplex
29	2007/10/25 10:01:07	Port 17 link up, 100Mbps FULL duplex

Clear Next

Figure 12- 40. Switch History 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 Switch History Log. Clicking **Clear** will allow the user to clear the Switch History Log.

NOTE: For detailed information regarding Log entries that will appear in this window, please refer to Appendix C at the back of this manual.

The information is described as follows:

Parameter	Description
Sequence	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Displays the time in days, hours, and minutes since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

Section 13

Switch Maintenance

Reset

Reboot System

Save Changes

Logout

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

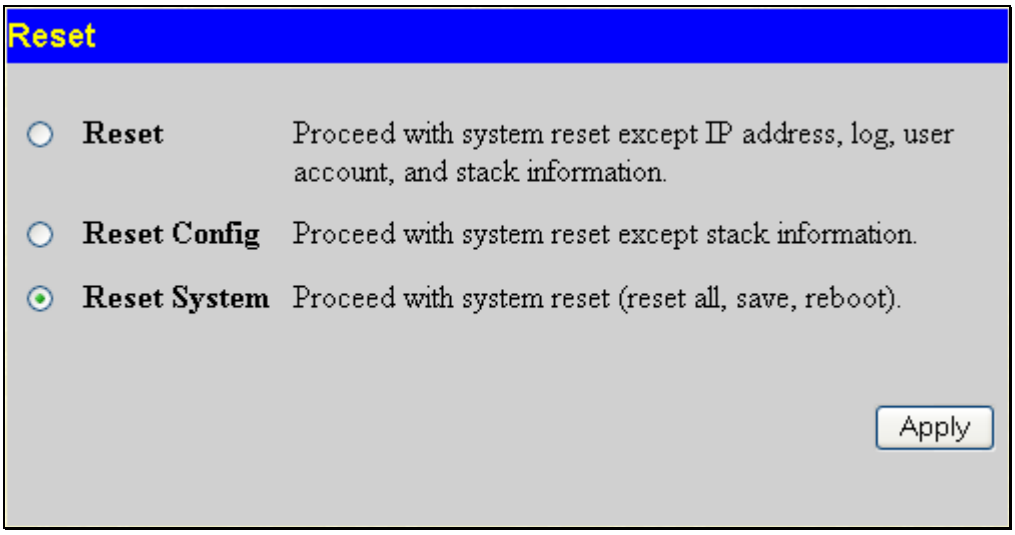


Figure 13- 1. Reset window

Reboot System

The following window is used to restart the Switch.

All of the configuration information entered from the last time **Save Changes** was executed will be lost. Click the **Reboot** button to restart the Switch.

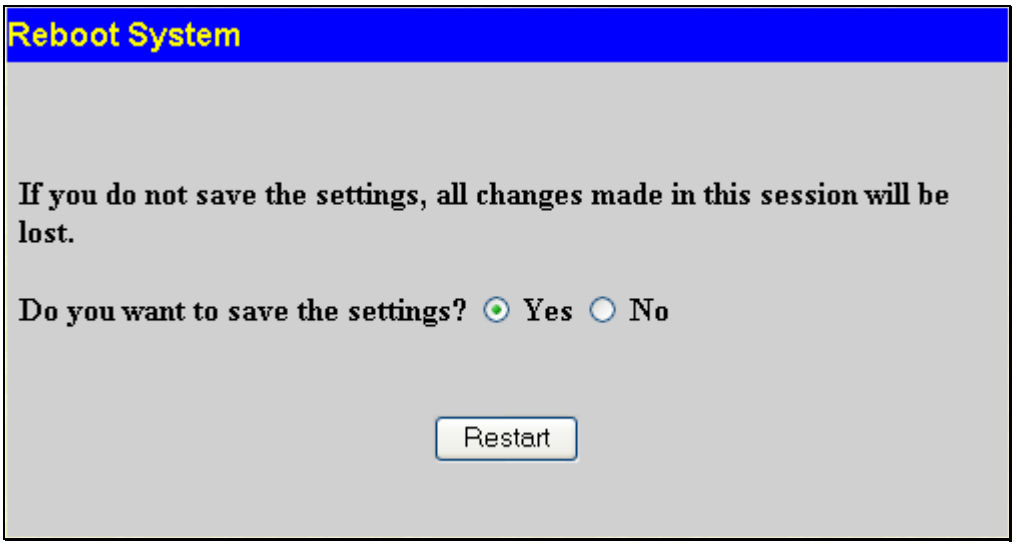


Figure 13- 2. Reboot window

Save Changes

The Switch has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by clicking the **Apply** button. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the Switch.

To retain any configuration changes permanently, click the **Save Changes** link. The following window will appear:

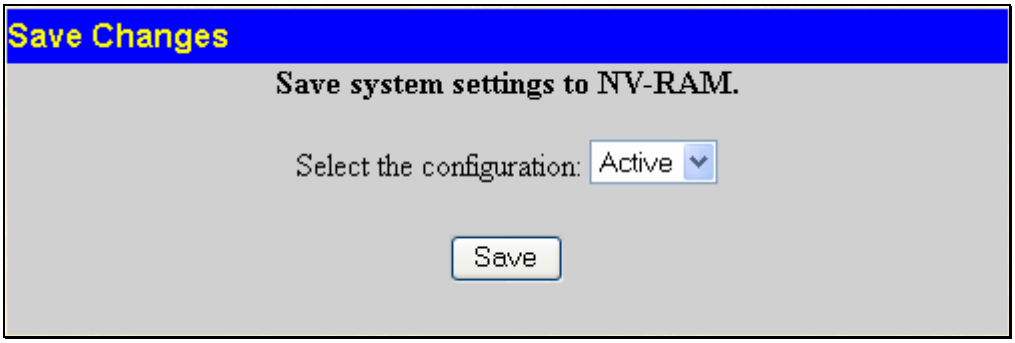


Figure 13- 3. Save Configuration window

The Switch contains two places to save configuration settings in its internal memory. Using the pull down menu, the user may select a place to put the save configurations, marked as *1* or *2*. Also, the user may select the current settings to be the current active configurations of the Switch by selecting *Active*. These settings will be used every time the Switch is rebooted. Clicking the Save button will save the configurations to the place set above. The following dialog box will confirm that the configuration has been saved:

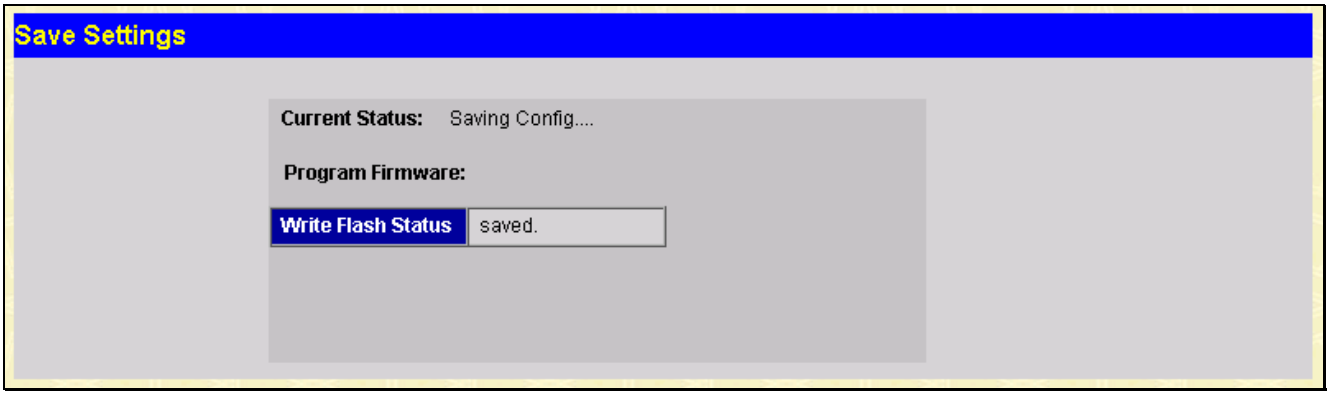


Figure 13- 4. Save Settings dialog box

Logout

Use the Logout page to logout of the Switch's Web-based management agent by clicking on the **Log Out** button.

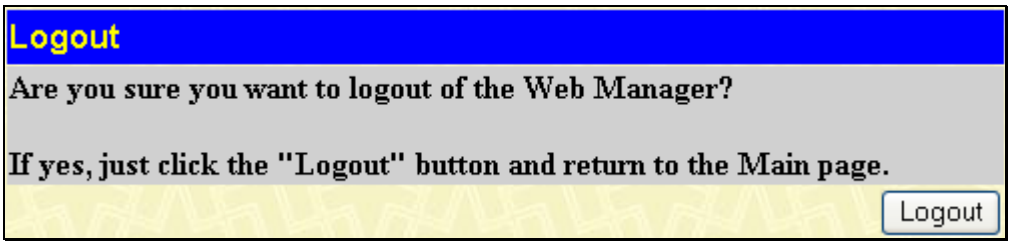


Figure 13- 5. Logout Web Setup window

Appendix A

Technical Specifications

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP "Mini GBIC") IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation IEEE 802.3af Power over Ethernet
Protocols	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)
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 10/100 Mbps ports (48 for the DES-3852) 2 combo 1000Base-T/SFP ports 2 1000Base-T copper ports

Physical and Environmental	
Internal power supply	**DES-3828 and DES-3852** Input: 100~240V, AC/1A, 50~60Hz Output: 12V, 5A (MAX), **DES-3828P** Input: 100~240V, AC/10A, 50~60Hz Output: -50V, -50Vrtn, 7.5A (MAX); 12V, 10.5A (MAX), **PoE**: Output capacity for whole system: 370W Per Port: 15.4W (Default) Per port → 1~16.8W (Customer can set up) **DES-3828DC DC** DC Power Input: 48 V,
Power Consumption	24 watts maximum for DES-3828/DES-3828DC 395.2 watts maximum for DES-3828P 47 watts maximum for the DES-3852
DC fans	one 15cm fan for DES-3828/DES-3828DC/DES-3828P/DES-3852 two 8.3cm fans for the DES-3852 one additional 27cm blower for DES-3828P
Operating Temperature	0 - 40°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	DES-3828/DES3828DC/DES-3852: 441 mm x 310 mm x 44 mm DES-3828P: 441mm x 369mm x 44mm
Weight	DES-3828/DES-3828DC: 4.24kg (9.35lbs) DES-3828P: 6.02kg (13.27lbs) DES-3852: 4.25kg (9.83lbs)
EMI	CE class A, FCC Class A, VCCI Class A, C-Tick
Safety	CSA International, CB report

Performance	
Transmission Method	Store-and-forward
Packet Buffer	32 MB per device
Packet Filtering/Forwarding Rate	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1Gbps port)
MAC Address Learning	Automatic update. Supports 16K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

Appendix B

System Log Entries

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

Cat.	Event Description	Log Content	Severity	Remark
System	Reboot by UI command	System warm start	Critical	
	Reboot by power cycle	System cold start	Critical	
	Configuration saved to flash	Configuration and log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console" and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	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	
	Fan fail	FAN <id> (1:back fan, 2:side fan) failed	Critical	DES3828 series only
	Fan recovered	FAN <id> (1:back fan, 2:side fan) is recovered	Informational	DES3828 series only
	Fan fail	FAN <id> (1:left side fan, 2:right side fan) failed	Critical	DES3852 series only
	Fan recovered	FAN <id> (1:left side fan, 2:right side fan) is recovered	Informational	DES3852 series only
upload/down-load	Firmware upgraded successfully	Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgrade was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging

	Configuration successfully downloaded	Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload was unsuccessful	Configuration uploaded by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
Interface	Port link up	Port <portNum> link up, <link state>	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	Port <portNum> link down	Informational	
Console	Successful login through Console	Successful login through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console	Login failed through Console (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Logout through Console	Logout through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.

	Console session timed out	Console session timed out (Username: <username>)	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Successful login through SSL	Successful login through Web(SSL) (Username: <string>, IP: <ip>, MAC: <mac>)	Informational	
	Logout through SSL	Logout through Web(SSL) (Username: <string>, IP: <ip>, MAC: <mac>)	Informational	
	Login failed through SSL	Login failed through Web (SSL) (Username: <string>, IP: <ip>, MAC: <mac>)	Warning	
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational	
STP	Topology changed	Topology changed	Informational	
	New Root selected	New Root selected	Informational	
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational	
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational	
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	

	SSH server is enabled	SSH server is enabled	Informational	
	SSH server is disabled	SSH server is disabled	Informational	
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational	
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational	
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational	
	Login failed through Web authenticated by AAA local method	Login failed through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning	
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational	
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning	
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational	
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning	
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Informational	
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)	Warning	
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational	

	Successful login through Web (SSL) authenticated by AAA none method	Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational	
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational	
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)	Informational	
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, 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	
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>, 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	
	Login failed through Telnet due to AAA server timeout or improper configuration	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>, 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	
	Login failed through SSH due to AAA server timeout or improper configuration	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, 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 Web (SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA local_enable method	Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>, 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 Web (SSL) authenticated by AAA none method	Successful Enable Admin through Web (SSL) 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	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	

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

	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)	Warning	
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
Port Security	Port security is exceeded to its maximum learning size and will not learn any new address	Port security violation (Port: <portNum>, MAC: <macaddr>)	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	
Dual Configuration	Record the execute error while the system in booting	Configuration had <int> syntax error and <int> execute error)	Warning	
RIP	RIP is enabled	RIP is enabled	Informational	
	RIP is disabled	RIP is disabled	Informational	
OSPF	OSPF is enabled	OSPF is enabled	Informational	
	OSPF is disabled	OSPF is disabled	Informational	
VRRP	VRRP is enabled	VRRP is enabled	Informational	
	VRRP is disabled	VRRP is disabled	Informational	
	Invalid version packet is received	VRRP receives an invalid version packet	Warning	
	Invalid virutal ID packet is received	VRRP receives an invalid virtual ID packet	Warning	
	Invalid checksum packet is received	VRRP receives an invalid checksum packet	Warning	
	Invalid TTL packet is received	Interface <string>, VRID <id> receives an invalid VRRP TTL packet	Warning	string is "interface name"
	Different advertisement interval is received	Interface <string>, VRID <id> receives a different VRRP advertisement interval packet	Warning	string is "interface name"
	Receive an authentication fail packet	Interface <string>, VRID <id> receives a VRRP authentication fail packet	Warning	string is "interface name"
	Invalid virtual ip packet is received	Interface <string>, VRID <id> receives an invalid VRRP virtual ip packet	Warning	string is "interface name"
	Receive an authentication type mismatch packet	Interface <string>, VRID <id> receives a VRRP authentication type mismatch packet	Warning	string is "interface name"

	Receive a not-support authentication type packet	Interface <string>, VRID <id> receives an invalid VRRP authentication type packet	Warning	string is "interface name"
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 is occuring	Broadcast storm is occurring (port: <id>)	Warning	
	Broadcast storm has cleared	Broadcast storm has cleared (port: <id>)	Informational	
	Multicast strom is occuring	Multicast storm is occurring (port: <id>)	Warning	
	Multicast storm has cleared	Multicast storm has cleared (port: <id>)	Informational	
	port shut down due to a storm	Port <id> is currently shut down due to a storm	Warning	
Loopback Detection	Port loop occurred	Port <[unitID:]portNum> LBD loop occurred. Port blocked.	Warning	
	Port loop detection restarted after interval time	Port <[unitID:]portNum> LBD port recovered. Loop detection restarted.	Informational	
	Port with VID loop occurred	Port <[unitID:]portNum> VID <vlanID> LBD loop occurred. Packet discard begun.	Warning	
	Port with VID Loop detection restarted after interval time	Port <[unitID:]portNum> VID <vlanID> LBD recovered. Loop detection restarted.	Informational	
DOS Attack	1. source ip is the same as the switch's ip in ARP packet 2. detect self IP packet	Possible spoofing attack from <macaddr> port <id>	Critical	

Appendix C

Cables and Connectors

When connecting the Switch to another switch, a bridge or hub, a normal cable is necessary. Please review these products for matching cable pin assignment.

The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments.

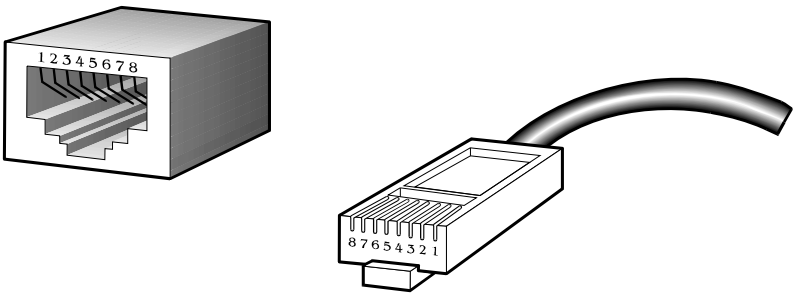


Figure B- 1. The standard RJ-45 port and connector

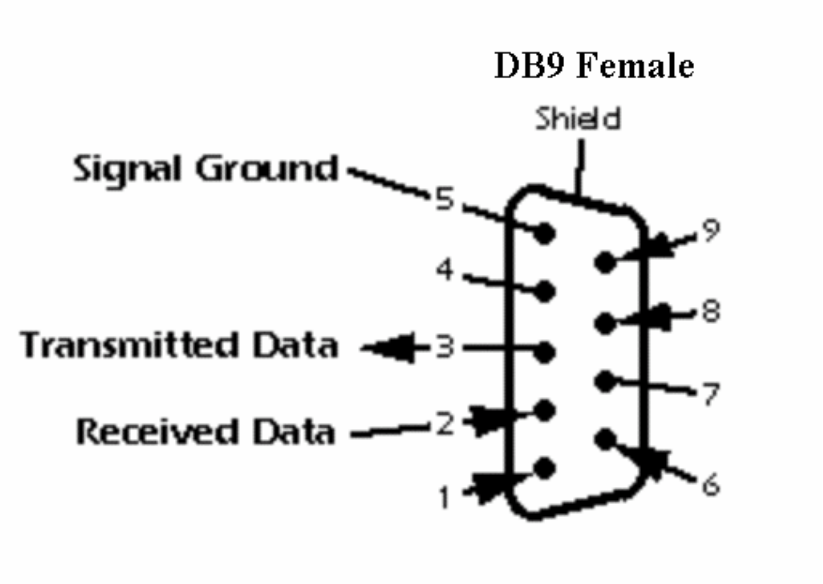
RJ-45 Pin Assignments		
Contact	MDI-X Port	MDI-II Port
1	RD+ (receive)	TD+ (transmit)
2	RD- (receive)	TD- (transmit)
3	TD+ (transmit)	RD+ (receive)
4	Not used	Not used
5	Not used	Not used
6	TD- (transmit)	RD- (receive)
7	Not used	Not used
8	Not used	Not used

Table B- 1. The standard RJ-45 pin assignments

Appendix D

Console Cable Pin Assignment

The following picture describes the pin assignment for the null modem straight-through RS-232 cable with a female DB-9 connector.



Appendix E

Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

Standard	Media Type	Maximum Distance
Mini-GBIC	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 Category 5 UTP Cable (1000 Mbps)	100m
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

Appendix F

ARP 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 that crackers can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce ARP protocol, ARP spoofing attacks, and the countermeasure devised by D-Link to put an end to ARP spoofing attacks.

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.

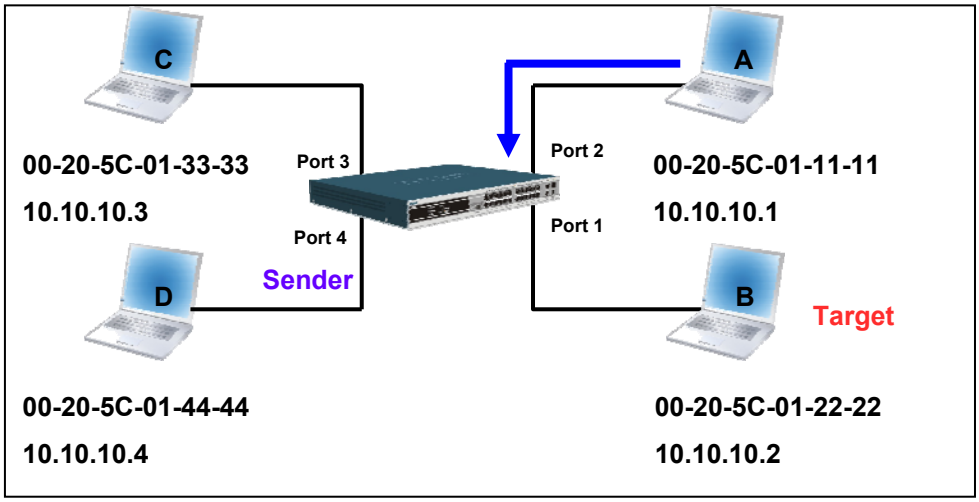


Figure-1

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 the 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 the ARP request is sent via a broadcast method, the "Destination address" is in the format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Table-2 (Ethernet frame format)

Destination address	Source address	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	***00-20-5C-01-11-11***			

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 and enter them in its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11

In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure -2).

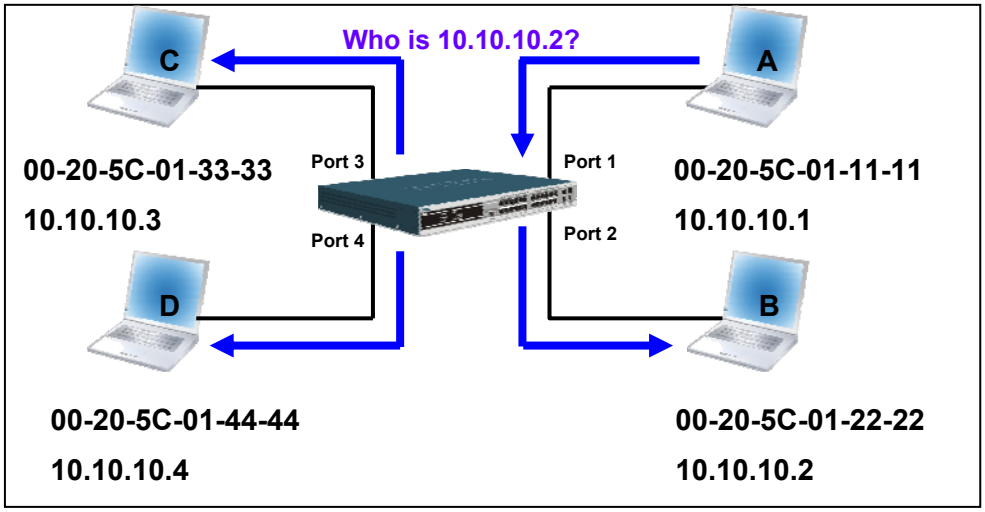


Figure - 2

When the switch floods the frame of the ARP request to the network, all PCs will receive and examine the frame but only PC B will reply to the query because the destination IP matched (see Figure-3).

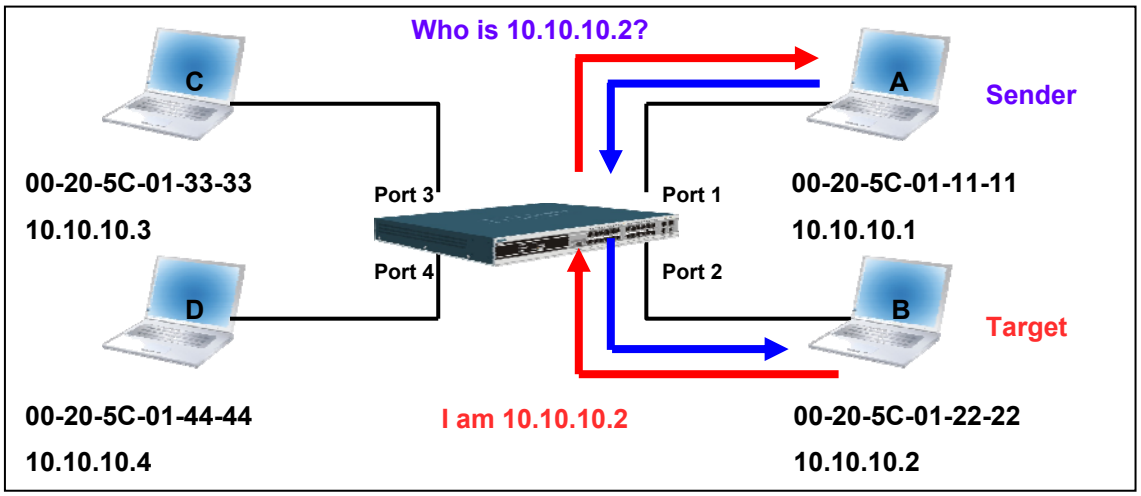


Figure-3

When PC B replies to an ARP request, its MAC address will be written into the “Target H/W Address” table 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 to the query, the "Destination Address" in the Ethernet frame will be changed to PC A's MAC address. The "Source Address" will be changed to PC B's MAC address (see 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 if it finds 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 addresses 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 attacks are caused by Gratuitous ARPs that occur 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.

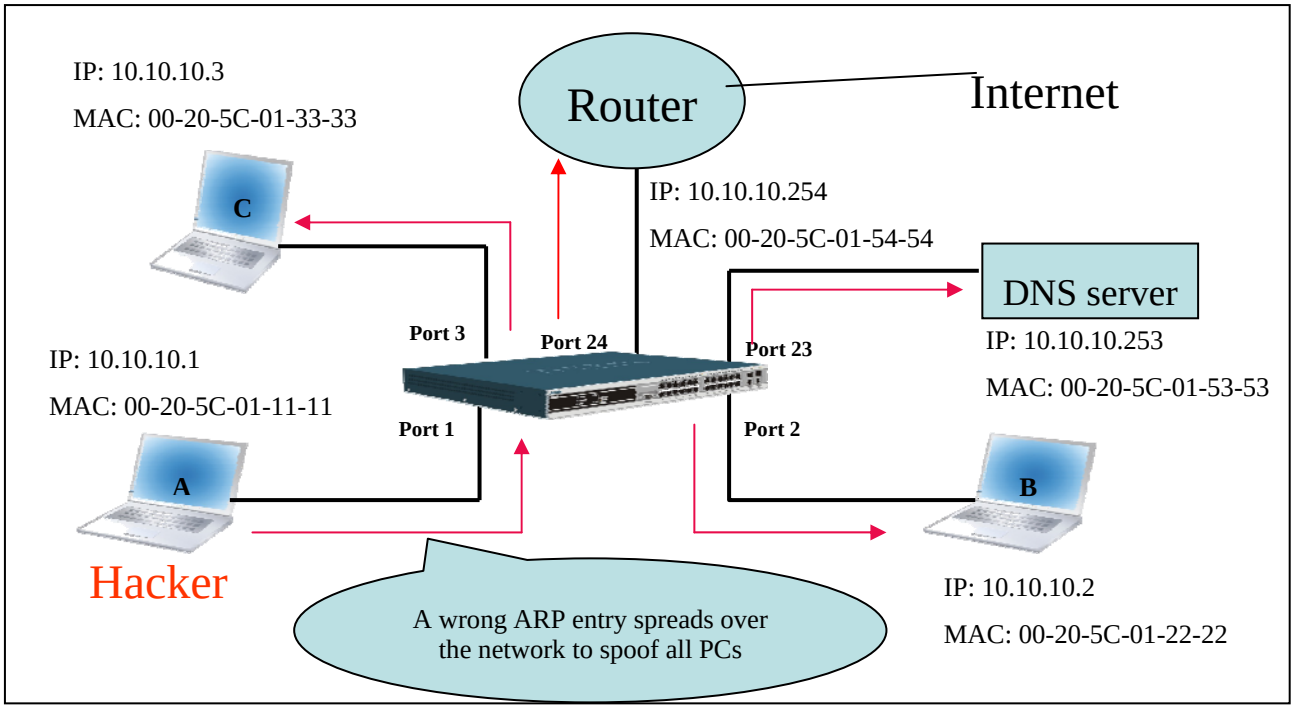


Figure-4

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. 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 any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast ONE Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets sent through 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 fools the victims PC to make it believe it is a router and fools the router to make it believe it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker without the users knowledge.

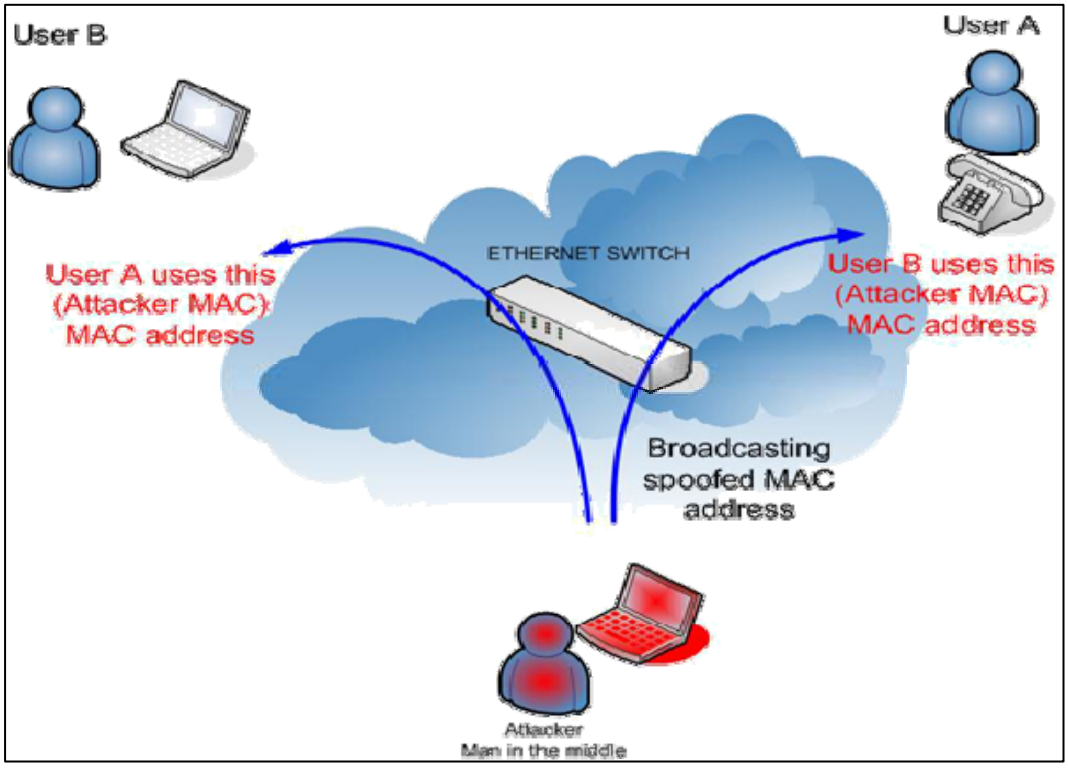
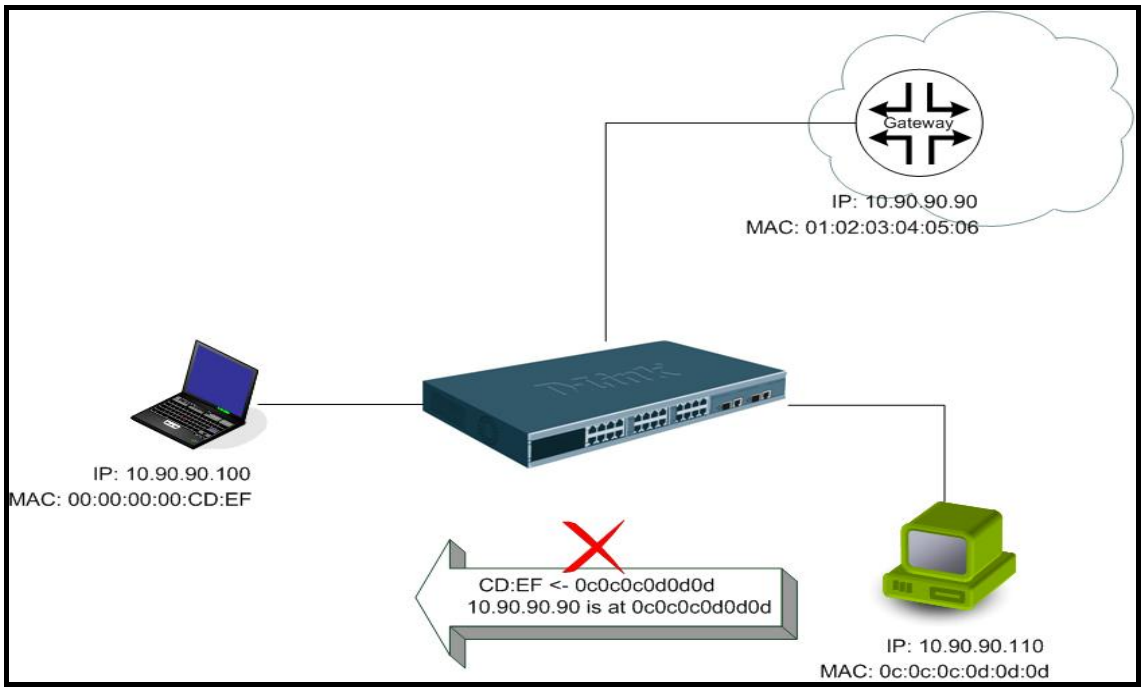


Figure-5

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 the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attacks, we will demonstrate here using the Packet Content ACL on the DES-3800 to block the invalid ARP packets which contain faked gateway's MAC and IP binding.



Example Topology

Configuration:

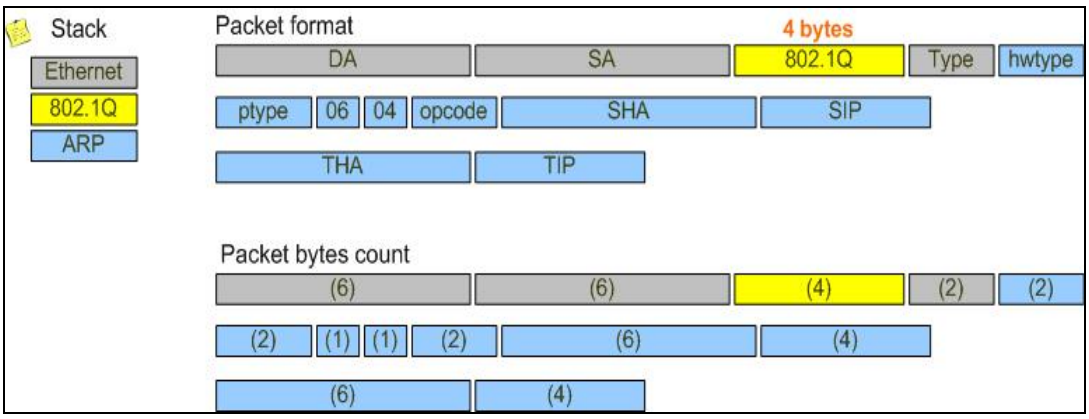
The design of the Packet Content ACL on the DES-3800 series can inspect any specified content in the first 48 bytes of an ARP packet (up to 80 bytes in total at one time). It utilizes offsets to match individual fields in the Ethernet Frame. An offset contains 16 bytes and each offset is divided into four 4-byte values in a HEX format. (refer to the configuration example below for details)

In addition, the configuration logics are:

1. Only if the ARP matches the Source MAC addresses in Ethernet, Sender's MAC address and Senders IP address in the ARP protocol can it pass through the switch. (In this example, it is gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

When calculating packet offset on DES-3800 series, remember that even though a port is an untagged port, the packet will add additional **4 bytes** of 802.1Q header (TCI) for switching internal process, shown in Figure-6.

All packets will be added additional 4 bytes to assign PVID for switching internal process.


Stack
Ethernet
802.1Q
ARP
Packet format
4 bytes
DA
SA
802.1Q
Type
hwtype
ptype
06
04
opcode
SHA
SIP
THA
TIP
Packet bytes count
(6)
(6)
(4)
(2)
(2)
(2)
(1)
(1)
(2)
(6)
(4)
(6)
(4)

	Command	Description
Step1	create access_profile packet_content_mask offset_0-15 0x0 0x0000ffff 0xffffffff 0x0 DA(6-byte) SA(6-byte) TCI(4-byte) offset_16-31 0xffff0000 0x0 0x0000ffff 0xffffffff Ethernet Type(2-byte) Operation(2-byte) Sdr MAC(6-byte) offset_32-47 0xffffffff 0x0 0x0 0x0 Sdr IP(4-byte) profile_id 1	- Create access profile 1 - offset_0-15: mask for Source MAC in Ethernet frame - offset_16-31: mask for Ethernet Type in Ethernet frame and Sender MAC in ARP packet - offset_32-47: mask for Sender IP in ARP packet
Step2	config access_profile profile_id 1 add access_id 1 packet_content_mask offset_0-15 0x0 0x00000102 0x03040506 0x0 DA(6-byte) SA(6-byte) TCI(4-byte) offset_16-31 0x08060000 0x0 0x00000102 0x03040506 Ethernet Type(2-byte) Operation(2-byte) Sdr MAC(6-byte) offset_32-47 0x0a5a5a5a 0x0 0x0 0x0 Sdr IP(4-byte): 10.90.9090 port 1-26 permit	- Configure access profile 1 - Only if the gateway's ARP packet that matches above can pass through.
Step3	create access_profile packet_content_mask offset_16-31 0xffff0000 0x0 0x0 0x0 offset_32-47 0xffffffff 0x0 0x0 0x0 profile_id 2	- Create access profile 2 - offset_16-31: mask for Ethernet Type in Ethernet frame - offset_32-47: mask for Sender IP in ARP packet
Step4	config access_profile profile_id 2 add access_id 1 packet_content_mask offset_16-31 0x08060000 0x0 0x0 0x0 offset_32-47 0x0a5a5a5a 0x0 0x0 0x0 port 1-26 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

Glossary

1000BASE-LX: A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters

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

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/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.

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。

BSMI Warning

警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,

在這種情況下使用者會被要求採取某些適當的對策

Warranty and Support (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this lifetime product warranty for hardware:

- Only for products purchased, delivered and used 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, and;
- Only with proof of purchase.

Product Warranty: D-Link warrants that the hardware portion of the D-Link product, including internal and external power supplies and fans (“Hardware”), will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product (“Warranty Period”), except as otherwise stated herein.

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the 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.

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 Warranty provided hereunder for D-Link's products will not be applied to and does not cover any products obtained through a special or unique pricing agreement, if such agreement provides for warranty terms different from those normally provided with the product or set forth herein, nor to 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 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).
- The customer must obtain a Case ID Number from D-Link Technical Support by going to https://support.dlink.com, 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. Include any manuals or accessories in the shipping package.
- 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 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 Warranty.

Disclaimer of Other Warranties: EXCEPT AS SPECIFICALLY SET FORTH ABOVE OR AS REQUIRED BY LAW, 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 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 WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING 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.

Lifetime Warranty: IF LOCAL LAW MANDATES THE USE OF A DEFINITION OF "LIFETIME WARRANTY" DIFFERENT FROM THAT PROVIDED HEREIN, THEN THE LOCAL LAW DEFINITION WILL SUPERSEDE AND TAKE PRECEDENCE, TO THE EXTENT NECESSARY TO COMPLY.

Governing Law: This 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 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.

LIMITED WARRANTY (Exclude USA, Europe, China and Taiwan)

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 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 Singapore.

Trademarks
D-Link is a registered trademark of D-Link Corporation/ D-Link International Ptd Ltd. All other trademarks belong to their respective proprietors.

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:

USA - 877-DLINK-55 (877-354-6555)

D-Link Technical Support over the Internet:

http://support.dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

877-354-6560

D-Link Technical Support over the Internet:

http://support.dlink.com

D-Link®
Building Networks for People

Technical Support

United Kingdom (Mon-Fri)

Home Wireless/Broadband 0871 873 3000 (9.00am–06.00pm, Sat 10.00am-02.00pm)

Managed, Smart, & Wireless Switches, or Firewalls 0871 873 0909 (09.00am – 05.30pm)

(BT 10ppm, other carriers may vary.)

Ireland (Mon-Fri)

All Products 1890 886 899 (09.00am-06.00pm, Sat 10.00am-02.00pm)

€ 0.05ppm peak, €0.045ppm off peak Times

Internet

http://www.dlink.co.uk

ftp://ftp.dlink.co.uk

Technische Unterstützung

Deutschland:	Web:	http://www.dlink.de
	E-Mail:	support@dlink.de
	Telefon:	+49(0)1805 2787 0,14 € pro Minute
	Zeiten:	Mo. –Fr. 09:00 – 17:30 Uhr
Österreich:	Web:	http://www.dlink.at
	E-Mail:	support@dlink.at
	Telefon:	+43(0)820 480084 0,116 € pro Minute
	Zeiten:	Mo. –Fr. 09:00 – 17:30 Uhr
Schweiz:	Web:	http://www.dlink.ch
	E-Mail:	support@dlink.ch
	Telefon:	+41(0)848 331100 0,08 CHF pro Minute
	Zeiten:	Mo. –Fr. 09:00 – 17:30 Uhr

* Gebühren aus Mobilnetzen und von anderen Providern können abweichen.

* Gebühren aus Mobilnetzen und von anderen Providern können abweichen.

Assistance technique

Assistance technique D-Link par téléphone : 0 820 0803 03
0,12 €/min la minute : Lundi – Vendredi de 9h à 13h et de 14h à 19h
Samedi 9h à 13h et de 14h à 16h
Assistance technique D-Link sur internet :
http://www.dlink.fr

Asistencia Técnica

Asistencia Técnica Telefónica de D-Link: +34 902 30 45 45
0,067 €/min
De Lunes a Viernes de 9:00 a 14:00 y de 15:00 a 18:00
http://www.dlink.es

Supporto tecnico

Supporto Tecnico dal lunedì al venerdì dalle ore 9.00 alle ore 19.00 con orario continuato
Telefono: 199400057
http://www.dlink.it/support

Technical Support

Tech Support for customers within the Netherlands:
0900 501 2007 / www.dlink.nl / €0.15ppm anytime.
Tech Support for customers within Belgium:
070 66 06 40 / www.dlink.be / €0.175ppm peak, €0.0875ppm off peak
Tech Support for customers within Luxemburg:
+32 70 66 06 40 / www.dlink.be

Pomoc techniczna

Telefoniczna pomoc techniczna firmy D-Link: 0 801 022 021
Pomoc techniczna firmy D-Link świadczona przez Internet:
URL: http://www.dlink.pl
e-mail: serwis@dlink.pl

Technická podpora

Web: http://www.dlink.cz/suppport/
E-mail: support@dlink.cz
Telefon: 225 281 553
Telefonická podpora je v provozu: PO- PÁ od 09.00 do 17.00
Land Line 1,78 CZK/min - Mobile 5.40 CZK/min

Technikai Támogatás

Tel. : 06 1 461-3001
Fax : 06 1 461-3004
Land Line 14,99 HUG/min - Mobile 49.99,HUF/min
email : support@dlink.hu
URL : http://www.dlink.hu

Teknisk Support

D-Link Teknisk telefon Support: 820 00 755

(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett: http://www.dlink.no

Teknisk Support

D-Link teknisk support over telefonen: Tlf. 7026 9040
Åbningstider: kl. 08:00 – 20:00
D-Link teknisk support på Internettet: http://www.dlink.dk

Teknistä tukea asiakkaille Suomessa:

Arkisin klo. 9 - 21
numerosta : **06001 5557**
Internetin kautta : http://www.dlink.fi

Teknisk Support

D-Link Teknisk Support via telefon: 0900-100 77 00
Vardagar 08.00-20.00
D-Link Teknisk Support via Internet: http://www.dlink.se

Assistência Técnica

Assistência Técnica da D-Link na Internet:
http://www.dlink.pt
e-mail: soporte@dlink.es

Τεχνική Υποστήριξη

D-Link Hellas Support Center
Κεφαλληνίας 64, 11251 Αθήνα,
Τηλ: 210 86 11 114 (Δευτέρα- Παρασκευή 09:00-17:00)
Φαξ: 210 8611114
http://www.dlink.gr/support

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

www.dlink.biz/hr

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

www.dlink.biz/sl

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

www.dlink.ro

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

24/7(24Hrs, 7days a week) technical support

http://www.dlink.com.au

e-mail: support@dlink.com.au

India:

Customer Support: - 1800-233-0000 (MTNL & BSNL Toll Free) or

+91-832-2885700 (GSM, CDMS & Others)

E-Mail Address: - helpdesk@dlink.co.in, techsupport@dlink.co.in

Website: - www.dlink.co.in

Indonesia, Malaysia, Singapore and Thailand:

Tel: +62-21-5731610 (Indonesia)

Tel: 1800-882-880 (Malaysia)

Tel: +65 6501 4200 (Singapore)

Tel: +66-2-719-8978/9 (Thailand)

24/7, for English Support Only

http://www.dlink.com.sg/support/

e-mail: support@dlink.com.sg

Korea:

Tel: +82-2-2028-1815

Monday to Friday 9:00am to 6:00pm

http://www.d-link.co.kr

e-mail: arthur@d-link.co.kr

New Zealand:

Tel: 0800-900-900

24/7(24Hrs, 7days a week) technical support

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

Email: support.eg@dlink-me.com

Iran:

Te: +98-21-88880918,19

Saturday to Thursday 9:00am to 5:00pm

http://support.dlink-me.com

Email : support.ir@dlink-me.com & support@dlink.ir

Israel:

Magshimim 20 St., Matalon center,

Petach Tikva, Israel 49348

Consumer support line: 03-9212886

Business support line: 03-9212608

Pakistan:

Tel: +92-21-4548158 or +92-21-4548310

Monday to Friday 10:00am to 6:00pm

http://support.dlink-me.com

E-mail: zkashif@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: +971-4-4278127 (U.A.E)

Sunday to Thursday 9.00AM to 6.00PM GMT+4

Web: http://www.dlink-me.com

E-mail: support.me@dlink-me.com

Saudi ARABIA (KSA):

Telephone : +966 01 217 0008

Facsimile : +966 01 217 0009

e-mail: Support.sa@dlink-me.com

Saturday to Wednesday 9.30AM to 6.30PM

Thursdays 9.30AM to 2.00 PM

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:
+7(495) 744-00-99

Техническая поддержка через Интернет
http://www.dlink.ru
e-mail: support@dlink.ru

D-Link®
Building Networks for People

SOPORTE TÉCNICO

Usted puede encontrar actualizaciones de softwares o firmwares y documentación para usuarios a través de nuestro sitio www.dlinkla.com

SOPORTE TÉCNICO PARA USUARIOS EN LATINO AMERICA

Soporte técnico a través de los siguientes teléfonos de D-Link

PAIS	NUMERO	HORARIO
Argentina	0800 - 12235465	Lunes a Viernes 08:00am a 21:00pm
Chile	800 - 835465 ó (02) 5941520	Lunes a Viernes 08:00am a 21:00pm
Colombia	01800 - 9525465	Lunes a Viernes 06:00am a 19:00pm
Costa Rica	0800 - 0521478	Lunes a Viernes 05:00am a 18:00pm
Ecuador	1800 - 035465	Lunes a Viernes 06:00am a 19:00pm
El Salvador	800 - 6335	Lunes a Viernes 05:00am a 18:00pm
Guatemala	1800 - 8350255	Lunes a Viernes 05:00am a 18:00pm
México	01800 - 1233201	Lunes a Viernes 06:00am a 19:00pm
Panamá	011 008000525465	Lunes a Viernes 05:00am a 18:00pm
Perú	0800 - 00968	Lunes a Viernes 06:00am a 19:00pm
República Dominicana	18887515478	Lunes a Viernes 05:00am a 18:00pm
Venezuela	0800 - 1005767	Lunes a Viernes 06:30am a 19:30pm

Soporte Técnico de D-Link a través de Internet

www.dlinkla.com

e-mail: soporte@dlinkla.com & consultas@dlinkla.com

D-Link®

Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de usuário no site da D-Link Brasil.

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9:00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

Technical Support

この度は弊社製品をお買い上げいただき、誠にありがとうございます。

下記弊社 Web サイトからユーザ登録及び新製品登録を
行っていただくと、ダウンロードサービスにて
サポート情報、ファームウェア、ユーザマニュアルを
ダウンロードすることができます。

ディーリンクジャパン Web サイト
URL:http://www.dlink-jp.com

D-Link®
Building Networks for People

技术支持

您可以在 D-Link 的官方网站找到产品的软件升级和使用手册

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