Web UI Reference Guide

Product Model: xStack® DGS-3600 Series
Layer 3 Managed Gigabit Ethernet Switch
Release 3.0

Information in this document is subject to change without notice.

November, 2012

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 their 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、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。 VCCI-A

Table of Contents

Intended Readers

The ***DGS-3600 Series Web UI Reference Guide*** contains information for setup and management of the Switch. The term, “the Switch” will be used when referring to all five 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** window 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 file names, 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.
Window Name > Window Option	**Window Name > Window Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties window option under the Port window option that is located under the Device window.

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 and service markings:

- Do not service any product except as explained in your system documentation.
- Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
- Only a trained service technician should service components inside these compartments.

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

- The power cable, extension cable, or plug is damaged.
- An object has fallen into the product.
- The product has been exposed to water.
- The product has been dropped or damaged.
- The product does not operate correctly when you follow the operating instructions.

Keep your system away from radiators and heat sources. Also, do not block cooling vents.

Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.

Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.

Use the product only with approved equipment.

Allow the product to cool before removing covers or touching internal components.

Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.

To help avoid damaging your system, be sure the voltage on the power supply is set to match the power available at your location:

- 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
- 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
- 230 V/50 Hz in most of Europe, the Middle East, and the Far East

Also, be sure that attached devices are electrically rated to operate with the power available in your location.

Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.

To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.

Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.

To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).

Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.

Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

- Install the power supply before connecting the power cable to the power supply.
- Unplug the power cable before removing the power supply.
- If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.

Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

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

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

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

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

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

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

Web-based Switch Configuration

Introduction
Login to Web manager
Web-Based User Interface
Web Pages

Introduction

All software functions of the Switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Firefox or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

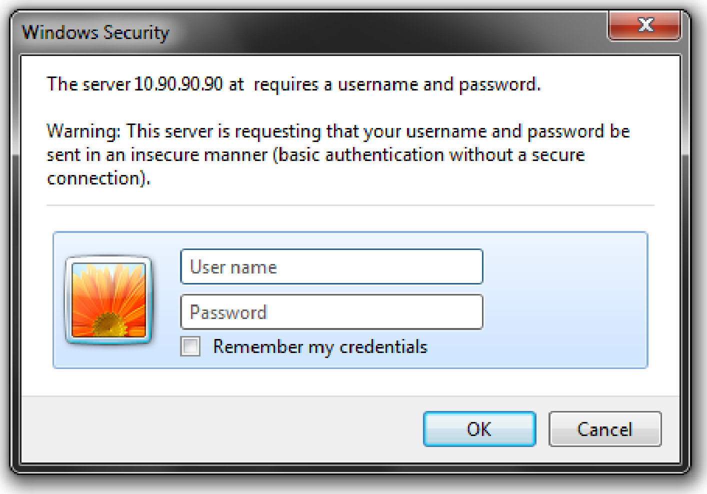
The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Login to Web Manager

To begin managing the Switch, simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

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

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



The server 10.90.90.90 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name
Password
□ Remember my credentials

Figure 1- 1. Enter Network Password window

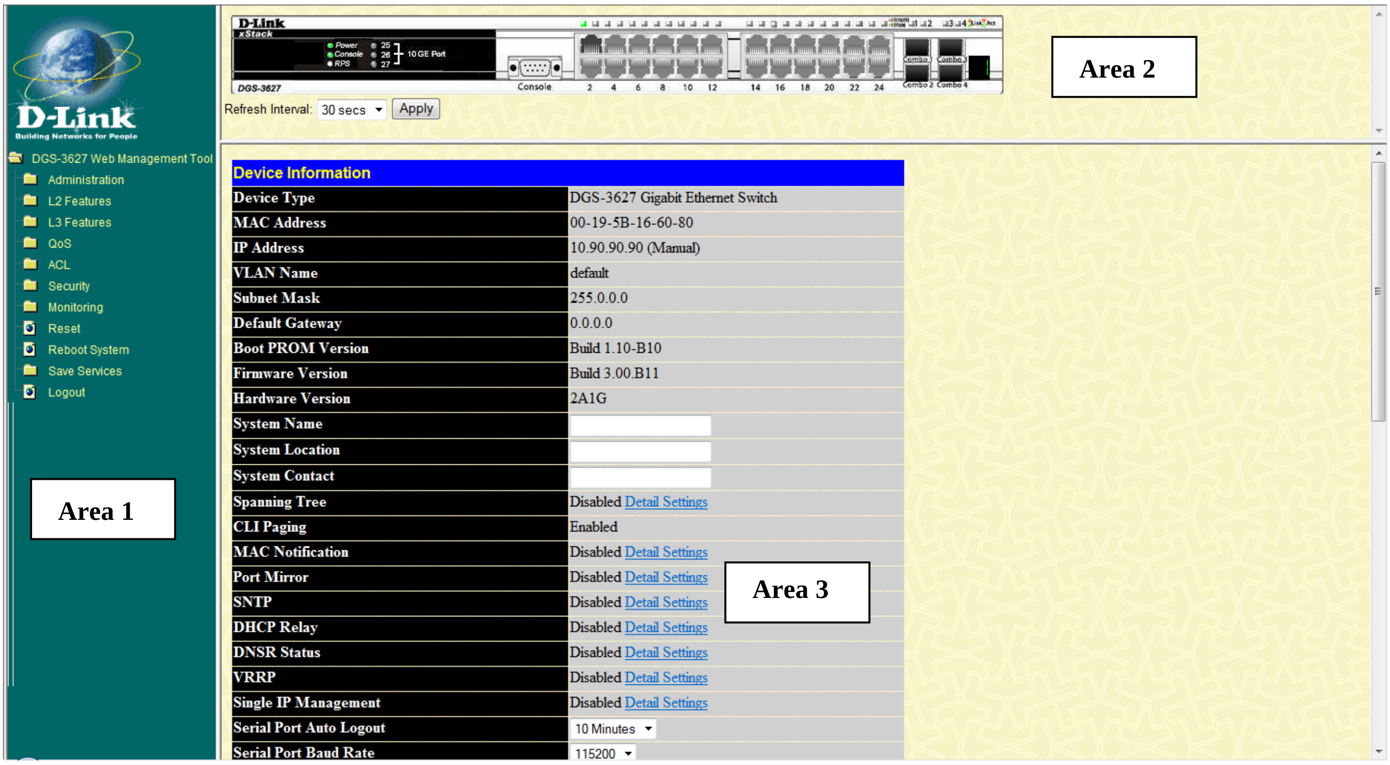
Leave both the User Name field and the **Password** field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

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



Device Information

Device Type	DGS-3627 Gigabit Ethernet Switch
MAC Address	00-19-5B-16-60-80
IP Address	10.90.90.90 (Manual)
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Boot PROM Version	Build 1.10-B10
Firmware Version	Build 3.00.B11
Hardware Version	2A1G
System Name	
System Location	
System Contact	
Spanning Tree	Disabled Detail Settings
CLI Paging	Enabled
MAC Notification	Disabled Detail Settings
Port Mirror	Disabled Detail Settings
SNTP	Disabled Detail Settings
DHCP Relay	Disabled Detail Settings
DNSR Status	Disabled Detail Settings
VRRP	Disabled Detail Settings
Single IP Management	Disabled Detail Settings
Serial Port Auto Logout	10 Minutes
Serial Port Baud Rate	115200

Figure 1- 2. Main Web Manager window

Area	Function
Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyper-linked window buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link Website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including port configuration.
Area 3	Presents switch information based on your selection and the entry of configuration data.

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

Web Pages

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

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

Administration – Contains the following folders and windows: IP Address, IP MTU Settings, Stacking, Port Configuration, User Accounts, Password Encryption, Mirror, System Log, System Severity Settings, Command Logging Settings, SNTP Settings, MAC Notification Settings, TFTP Services, File System Services, RCP, Ping Test, IPv6 Neighbor, DHCP Auto Configuration Settings, DHCP/BOOTP Relay, DHCP/BOOTP Local Relay Settings, DHCPv6 Relay, Layer 2 Protocol Tunneling Settings, RSPAN, SNMP Manager, Trap Source Interface Settings, sFlow, and Single IP Management Settings.

L2 Features – Contains the following folders and windows: VLAN, Trunking, IGMP Snooping, MLD Snooping, Loopback Detection Global Settings, Spanning Tree, Forwarding & Filtering, LLDP, Q-in-Q, ERPS, DULD Settings, and NLB Multicast FDB Settings.

L3 Features – Contains the following folders and windows: Interface Settings, MD5 Key Settings, Route Redistribution Settings, Multicast Static Route Settings, Static/Default Route Settings, Route Preference Settings, Static ARP Settings, Gratuitous ARP Settings, Policy Route Settings, ECMP Algorithm Settings, IP Tunnel Settings, RIP, OSPF, DHCP Server, Filter DHCP Server, DNS Relay, DNS Resolver, VRRP, IP Multicast Routing Protocol, BGP, and IP Route Filter.

QoS – Contains the following folders and windows: 802.1p Settings, Bandwidth Control, HOL Prevention Settings, and Schedule Settings.

ACL – Contains the following folders and windows: Time Range, Access Profile Table, ACL Flow Meter, and CPU Interface Filtering.

Security – Contains the following folders and windows: Authorization Attributes State Settings, Traffic Control, Port Security, IP-MAC-Port Binding, 802.1X, Web-based Access Control (WAC), Trust Host, BPDU Attack Protection Settings, ARP Spoofing Prevention Settings, Access Authentication Control, MAC-based Access Control, Safeguard Engine, Traffic Segmentation, SSL, SSH, Compound Authentication, and Japanese Web-based Access Control (JWAC).

Monitoring – Contains the following folders and windows: Device Status, Stacking Information, Stacking Device, Module Information, DRAM & Flash Utilization, CPU Utilization, Port Utilization, Packets, Errors, Packet Size, Browse Router Port, Browse MLD Router Port, VLAN Status, VLAN Status Port, Port Access Control, MAC Address Table, IGMP Snooping Group, MLD Snooping Group, Trace Route, IGMP Snooping Forwarding, MLD Snooping Forwarding, IP Forwarding Table, Routing Table, Browse IP Multicast Forwarding Table, Browse IP Multicast Interface Table, Browse IGMP Group Table, DVMRP Monitor, PIM Monitor, OSPF Monitor, Switch Logs, Browse ARP Table, Session Table, and MAC-based Access Control Authentication Status.

Reset, Reboot System and **Logout** links are displayed in the main directory.

Save Services – Contains the following folders and windows: Save Changes and Current Configuration Settings.

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

Section 2

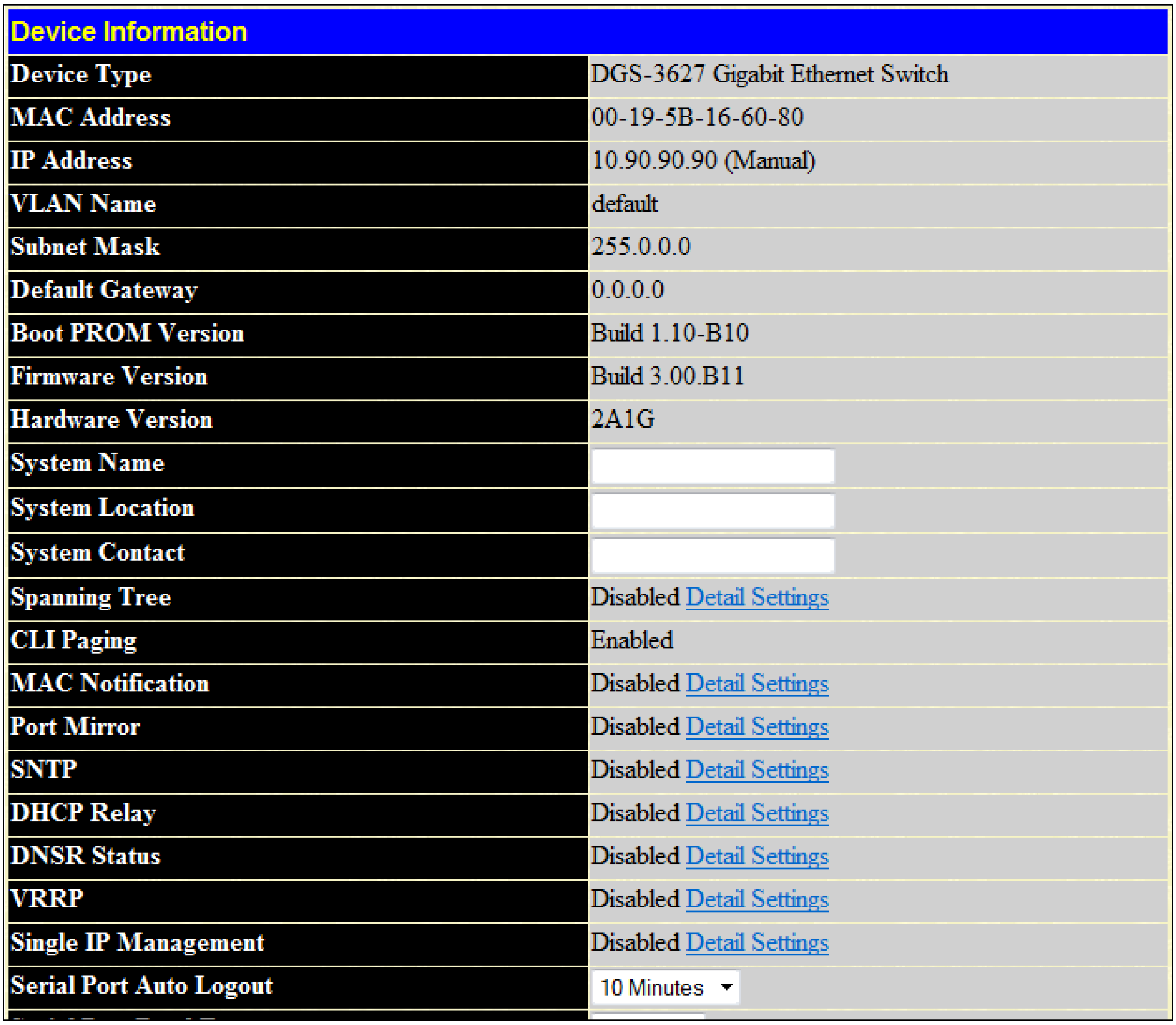
Administration

Device Information (DGS-3600 Web Management Tool)
IP Address
IP MTU Settings
Stacking
Port Configuration
DDM
User Accounts
Password Encryption
Mirror
System Log
System Severity Settings
Command Logging Settings
SNTP Settings
MAC Notification Settings
TFTP Services
File System Services
Ping Test
IPv6 Neighbor
DHCP Auto Configuration Settings
DHCP/BOOTP Relay
DHCP/BOOTP Local Relay Settings
DHCPv6 Relay
Layer 2 Protocol Tunneling Settings
RSPAN
SNMP Manager
Trap Source Interface Settings
sFlow
Single IP Management Settings

Device Information

This window contains the main settings for all major functions of the Switch and appears automatically when you log on. To return to the **Device Information** window, click the **DGS-3600 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, Hardware Version and Serial Number. 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. In addition, this window displays the status of functions on the Switch to quickly assess their current global status. Some functions are hyper-linked to their configuration window for easy access from the **Device Information** window.

NOTE: DGS-3612/DGS-3612G/ DGS-3627/DGS-3627G/DGS-3650 Switch series will display the serial number in the **Device Information** window for Firmware version Build 3.00.B11.



Device Information

Device Type	DGS-3627 Gigabit Ethernet Switch
MAC Address	00-19-5B-16-60-80
IP Address	10.90.90.90 (Manual)
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Boot PROM Version	Build 1.10-B10
Firmware Version	Build 3.00.B11
Hardware Version	2A1G
System Name	
System Location	
System Contact	
Spanning Tree	Disabled Detail Settings
CLI Paging	Enabled
MAC Notification	Disabled Detail Settings
Port Mirror	Disabled Detail Settings
SNTP	Disabled Detail Settings
DHCP Relay	Disabled Detail Settings
DNSR Status	Disabled Detail Settings
VRRP	Disabled Detail Settings
Single IP Management	Disabled Detail Settings
Serial Port Auto Logout	10 Minutes ▾

Figure 2- 1. Device Information window

The configurable fields are described below:

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

System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.
Spanning Tree	To configure Spanning Tree Protocol (STP compatible, MSTP, or RSTP) on the Switch, use the **STP Bridge Global Settings** window (**L2 Features** > **Spanning Tree** > **STP Bridge Global Settings**) or click Detail Settings.
MAC Notification	To monitor MAC addresses learned and entered into the forwarding database, enable MAC notification by using the **MAC Notification Global Settings** window (**Administration** > **MAC Notification Global Settings**) or click Detail Settings.
Port Mirror	To configure port mirroring on the Switch, use the **Port Mirror Global Settings** window (**Administration** > **Mirror** > **Port Mirror Global Settings**) or click Detail Settings.
SNTP	To configure time settings, use the **Time Settings - Current Time** window (**Administration** > **SNTP Settings** > **Time Settings**) or click Detail Settings.
DHCP Relay	To configure DHCP/BOOTP relay, use the **DHCP/BOOTP Relay Global Settings** window (**Administration** > **DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Global Settings**) or click Detail Settings.
DNSR Status	To configure DNS Relay, use the **DNS Relay Global Settings** window (**L3 Features** > **DNS Relay** > **DNS Relay Global Settings**) or click Detail Settings.
VRRP	To configure VRRP, use the **VRRP Global Settings** window (**L3 Features** > **VRRP** > **VRRP Global Settings**) or click Detail Settings.
Single IP Management	To configure Single IP Management, use the **SIM Settings** window (**Administration** > **Single IP Management Settings** > **SIM Settings**) or click Detail Settings.
Serial Port Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes* or *Never*. The default setting is *10 minutes*.
Serial Port Baud Rate	This field specifies the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, *9600*, *19200*, *38400* and *115200.* For a connection to the Switch using the CLI interface, the baud rate must be set to *115200*, which is the default setting.
MAC Address Aging Time (10-1000000)	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. To configure IGMP Snooping for individual VLANs, use the **IGMP Snooping Settings** window (**L2 Features** > **IGMP Snooping** > **IGMP Snooping Settings**) or click Detail Settings.
MLD Snooping	To enable system-wide MLD Snooping capability, select *Enabled*. MLD snooping is *Disabled* by default. To configure MLD Snooping for individual VLANs, use the **MLD Snooping Settings** window window (**L2 Features** > **MLD Snooping** > **MLD Snooping Settings**) or click Detail Settings.
GVRP Status	Use this pull-down menu to enable or disable GVRP on the Switch.
Telnet Status	Telnet configuration is *Enabled* by default. If users 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 users choose to disable this by selecting *Disabled*, they will lose the ability to configure the system through the Web interface as soon as these settings are applied.

Web TCP Port Number (1-65535)	The Web (GUI) port number. TCP ports are numbered between *1* and *65535*. The "well-known" TCP port for the Web protocol is *80*.
SNMP Status	Use this pull-down menu to enable or disable Simple Network Management Protocol (SNMP) on the Switch.
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. 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 can be configured to *Local*.
802.1X Authen Network RADIUS	Enables or disables 802.1X Authentication Network RADIUS. The default is *Enabled*.
Forward EAPOL PDU	Enables or disables Forward EAPOL PDU. The default is *Disabled*.
HOL Prevention	If this option is enabled it prevents the forwarding of data to a port that is blocked. Traffic that would normally be sent to the buffer memory of the Switch's TX queue is dropped so that memory usage is conserved and performance across all ports remains high.
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 Ethernet frame size of 1536 bytes) of up to 9216 bytes (tagged) can be transmitted by the Switch.
Syslog State	Enables or disables Syslog State. The default is *Disabled*.
Broadcast Ping Reply State	Enables or disables the Broadcast Ping Reply State. The default is *Enabled*.
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* to *65535* minutes with a default setting of *20* minutes.
DVMRP State	The user may globally enable or disable the Distance Vector Multicast Routing Protocol (DVMRP) function by using the **DVMRP Global Settings** window (**L3 Features** > **IP Multicast Routing Protocol** > **DVMRP Global Settings** or click Detail Settings).
PIM State	The user may globally enable or disable the Protocol Independent Multicast - Dense Mode (PIM-DM) function by using the **PIM Global Settings** window (**L3 Features** > **IP Multicast Routing Protocol** > **PIM** > **PIM Global Settings** or click Detail Settings).
BGP State	The user may configure Border Gateway Protocol (BGP) by using the **BGP State Settings** window (**L3 Features** > **BGP** > **BGP Global Settings** or click Detail Settings).
OSPF State	The user may globally enable or disable the Open Shortest Path First (OSPF) function by using the **OSPF Global Settings** window (**L3 Features** > **OSPF** > **OSPF Global Settings** or click Detail Settings).
OSPFv3 State	The user may globally enable or disable the Open Shortest Path First (OSPF) version 3 function by using the **OSPFv3 Global Settings** window (**L3 Features** > **OSPF** > **OSPFv3** > **OSPFv3 Global Settings** or click Detail Settings).

DNS Resolver State	The user may globally enable or disable the Domain Name Server Resolver function by using the **DNS Resolver Global Settings** window (**L3 Features** > **DNS Resolver** > **DNS Resolver Global Settings** or click Detail Settings).
RIP State	The user may globally enable or disable the Routing Information Protocol (RIP) function by using the **RIP Global Settings** window (**L3 Features** > **RIP** > **RIP Global Settings** or click Detail Settings).
RIPng State	The user may globally configure RIPng by using the **RIPng Global Settings** window (**L3 Features** > **RIP** > **RIPng** > **RIPng Global Settings** or click Detail Settings).

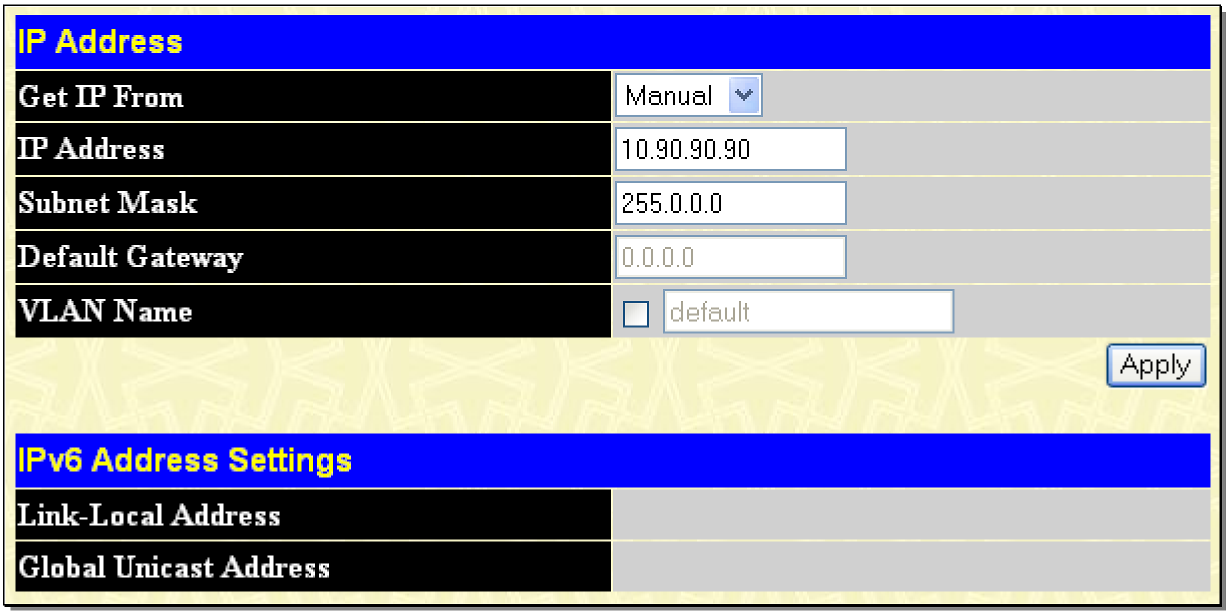
Click **Apply** to implement changes made.

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 ***DGS-3600 Series CLI Refence Guide*** or return to Section 4 of this manual for more information.

To configure the Switch's IP address:

To view the Switch's current IP settings, click **Administration > IP Address**, as shown below:



IP Address

Get IP From	Manual
IP Address	10.90.90.90
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
VLAN Name	□ default

IPv6 Address Settings

Link-Local Address	
Global Unicast Address	

Figure 2- 2. IP Address 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. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.
4. If no VLANs have been previously configured on the Switch, you can use the *default* VLAN Name. The *default* VLAN contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the VLAN Name of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.

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

To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address:

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.

The IP Address Setting 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 in 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.
IP Address	Enter an IP address. These fields should be in the form **xxx.xxx.xxx.xxx**, where each **xxx** is a number (represented in decimal form) between 0 and 255.
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** window (**Security** > **Trust Host**). 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.
Link-Local Address	This read-only field displays the current link-local address, if applicable.
Global Unicast Address	This read-only field displays the current global unicast address, if applicable.

Click **Apply** to implement changes made.

Setting the Switch's IP Address using the Console Interface

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

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

- Starting at the command line prompt, enter the commands config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy. Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.
- Alternatively, you can enter config ipif System ipaddress xxx.xxx.xxx.xxx/z. Where the x's represent the IP address to be assigned to the IP interface named System and the z represents the corresponding number of subnets in CIDR notation.

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

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

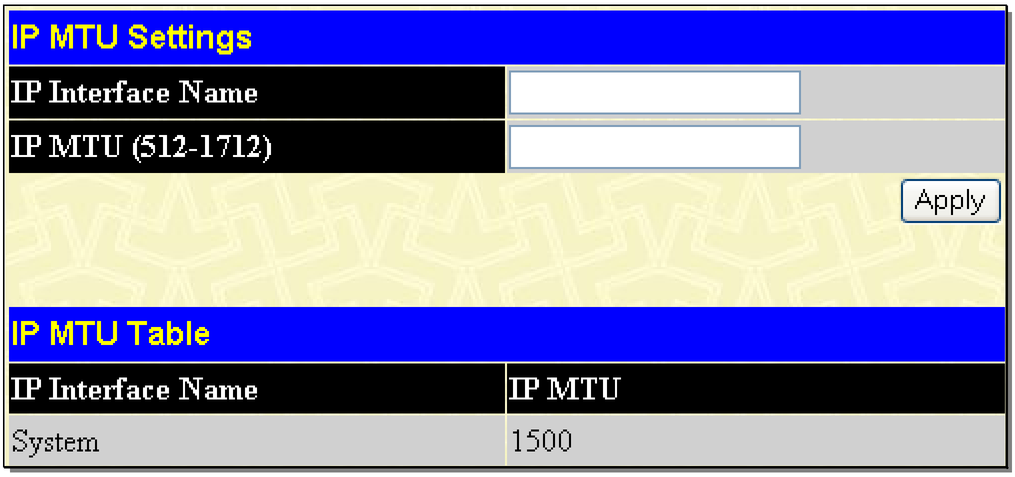
IP MTU Settings

The IP MTU Settings window is used to configure the IP layer MTU settings on the Switch. The MTU is the largest size of IP datagram which may be transferred using a specific data link connection. The MTU value is a design parameter of a LAN and is a mutually agreed value (i.e. both ends of a link agree to use the same specific value) for most WAN links. The size of MTU may vary greatly between different links. Instead of making routers fragment packets, an end system could try to find out the largest IP packet that may be sent to a specific destination.

When one IP host wants to transmit an IP datagram, it is usually preferable that the datagrams be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. The path MTU is equal to the minimum MTUs of each hop in the path.

Path MTU discovery is intended to dynamically discover the PMTU of a path. Basically a source host initially assumes that the PMTU of a path is the (known) MTU of its first hop, and sends all datagrams on that path with the DF bit set. If any of the datagrams are too large to be forwarded without fragmentation by some router along the path, that router will discard them and return ICMP Destination Unreachable messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message (we can call this message "Datagram Too Big" message), the source host reduces it’s assumed PMTU for the path. The PMTU discovery process ends when the host's estimate of the PMTU is low enough that its datagrams can be delivered without fragmentation or the host may elect to end the discovery process by ceasing to set the DF bit in the datagram headers.

To configure the Switch's current IP MTU settings, click **Administration > IP MTU Settings**, as shown below:



IP MTU Settings

IP Interface Name	
IP MTU (512-1712)	

IP MTU Table

IP Interface Name	IP MTU
System	1500

Figure 2- 3. IP MTU Settings window

The following fields can be configured:

Parameter	Description
IP Interface Name	Specifies the name of the IP Interface to be used.
IP MTU (512-1712)	The user can configure each interface’s IP MTU. If the user does not designate an MTU value when creating an interface, the default value of 1500 will be used.

Stacking

From firmware release v2.00 of this Switch, the xStack® DGS-3600 Series now supports switch stacking, where a set of twelve switches can be combined to be managed by one IP address through Telnet, the GUI interface (web), the console port or through SNMP. Each switch of this series has two stacking slots located at the rear of the device, which can be used to add 10-gigabit DEM-410CX or DEM-410X stacking modules, sold separately. After adding these stacking ports, the user may connect these ports together using copper or fiber stacking cables (also sold separately) in one of two possible topologies.

Duplex Chain – As shown in Figure 2-4, The Duplex Chain topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will obviously be affected.

Duplex Ring – As shown in Figure 2-5, the Duplex Ring stacks switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient due to the fact that if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack.

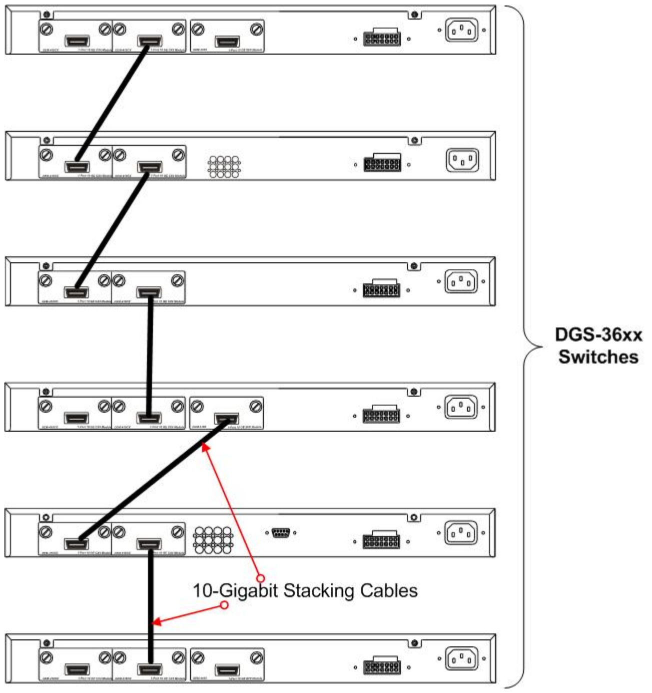


Figure 2- 4. Switches stacked in a Duplex Chain

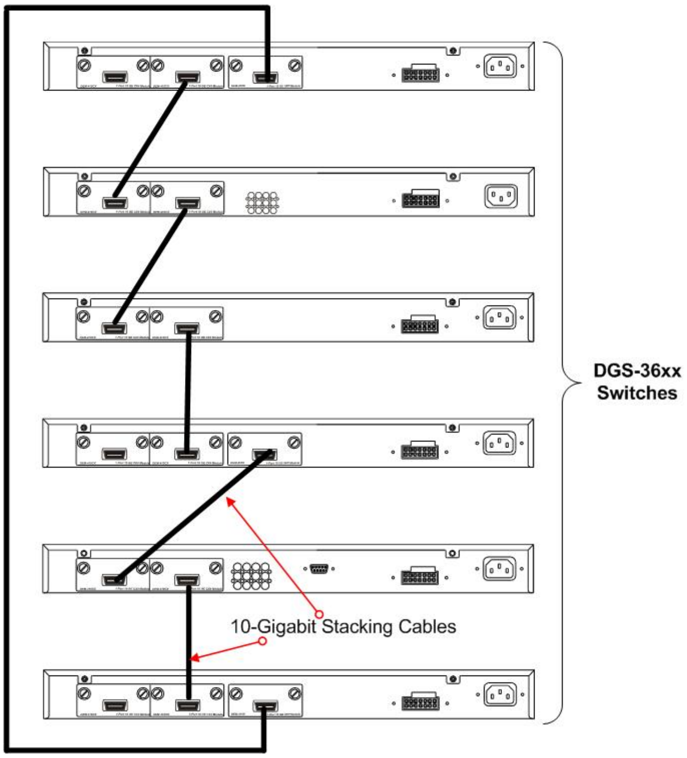


Figure 2- 5. Switches stacked in a Duplex Ring

Within each of these topologies, each switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the Switch stack. Three possible roles exist when stacking with the xStack® DGS-3600 Series.

NOTE: Only ports 26 and 27 of the DGS-3627 support stacking. Port 25 cannot be used for stacking, and is to be used only as a 10-Gigabit uplink port.

Primary Master – The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This switch will also assign Stack Unit IDs, synchronize configurations and transmit commands to remaining switches in the switch stack. The Primary Master can be manually set by assigning this Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process which determines the lowest MAC address and then will assign that switch as the Primary Master, if all priorities are the same. The Primary master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and 'H'.

Backup Master – The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority before physically assembling the stack, or it can be determined automatically by the stack through an election process which determines the second lowest MAC address and then will assign that switch as the Backup Master, if all priorities are the same.

Slave – Slave switches constitute the rest of the switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave switches perform operations requested by the master, monitor the status of neighbor switches in the stack and the stack topology and adhere to the Backup Master's commands once it becomes a Primary Master. Slave switches will do a self-check to determine if it is to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, it will determine if it is to become the Primary Master. These roles will be determined, first by priority and if the priority is the same, the lowest MAC address.

Once switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

Initialization State – This is the first state of the stack, where the runtime codes are set and initialized and the system conducts a peripheral diagnosis to determine each individual switch is functioning properly.

Master Election State – Once the codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.

Synchronization State – Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to switches in the stack, synchronize configurations for all switches and then transmit commands to the rest of the switches based on the user configurations of the Primary Master.

Once these steps have been completed, the switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the xStack® DGS-3600 supports "hot swapping" of switches in and out of the running stack. Users may remove or add switches to the stack without powering down or largely affecting the transfer of data between switches in the stack, with a few minor provisions.

When switches are "hot inserted" into the running stack, the new switch may take on the Backup Master or Slave role, depending on configurations set on the newly added switch, such as configured priority or MAC address. The new device will not be the Primary Master, if adding one switch at a time to the Stack. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master's roles for all new switches that were hot inserted. This process is done using discovery packets that circulate through the switch stack every 1.5 seconds until the discovery process has been completed.

The "hot remove" action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master or Slave, may be removed from the stack, yet different processes occur for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master's role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

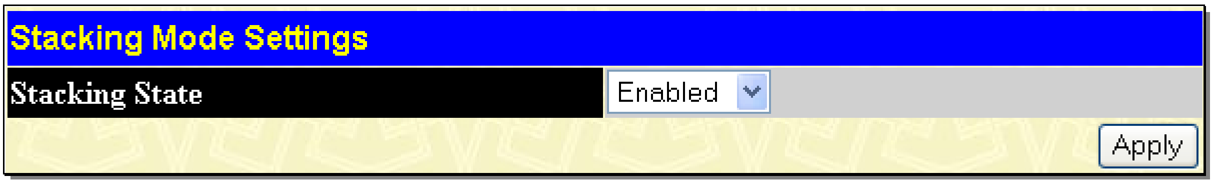
If both the Primary Master and the Backup Master are removed, the election process is immediately processed and a new Primary Master and Backup Master are determined. Switches in the stack will clear the configurations of the units removed, and dynamically learned databases, such as ARP, will be cleared as well. Static switch configurations still remain in the database of the remaining switches in the stack and those functions will not be affected.

NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack.

Mode Settings

To begin the stacking process, users must first enable this device for stacking by using the following window.

To view this window, click **Administration** > **Stacking** > **Mode Settings**, as shown below:



Stacking Mode Settings

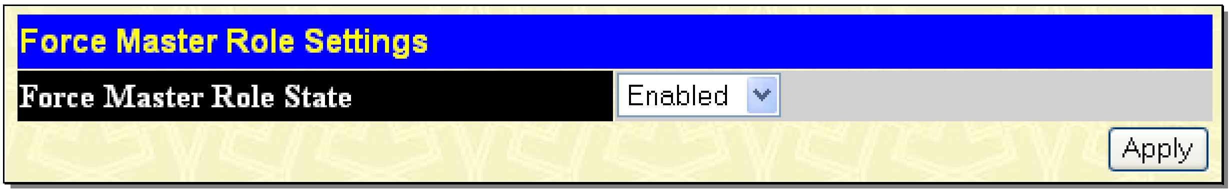
Stacking State	Enabled

Figure 2- 6. Stacking Mode Settings window

Force Master Role Settings

This window is used to ensure the master role is unchanged when adding a new device to the current stacking topology. Select *Enabled* from the drop-down menu, and the master's priority will become zero after the stacking has stabilized.

To view this window, click **Administration** > **Stacking** > **Force Master Role Settings**, as shown below:



Force Master Role Settings

Force Master Role State	Enabled

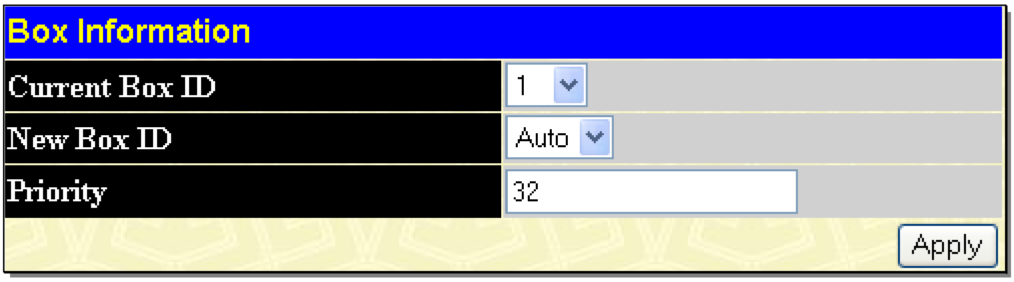
Figure 2- 7. Force Master Role Settings window

Information configured in this window is found in the **Monitoring** folder under **Stacking Information**.

Box Information

This window is used to configure stacking parameters associated with all switches in the xStack® DGS-3600 Series. The user may configure parameters such as box ID, box priority and pre-assigning model names to switches to be entered into the switch stack.

To view this window click, **Administration** > **Stacking** > **Box Information**, as shown below:



Box Information

Current Box ID	1
New Box ID	Auto
Priority	32

Figure 2- 8. Box Information window

Parameter	Description
Current Box ID	The Box ID of the switch in the stack to be configured.
New Box ID	The new box ID of the selected switch in the stack that was selected in the **Current Box ID** field. The user may choose any number between *1* and *12* to identify the switch in the switch stack. *Auto* will automatically assign a box number to the switch in the switch stack.
Priority	Displays the priority ID of the Switch. The range is *1* to *63*. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack is the Primary Master switch. The Primary Master switch will be used to configure applications of the switch stack.

Information configured in this window is found in the **Monitoring** folder under **Stack Information**.

NOTE: Configured box priority settings will not be implemented until users physically save it using the Web GUI or the CLI.

IP Interface Setup

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 2- 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 six network addresses and six 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 2- 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 **Setup IP Interface** window.

Port Configuration

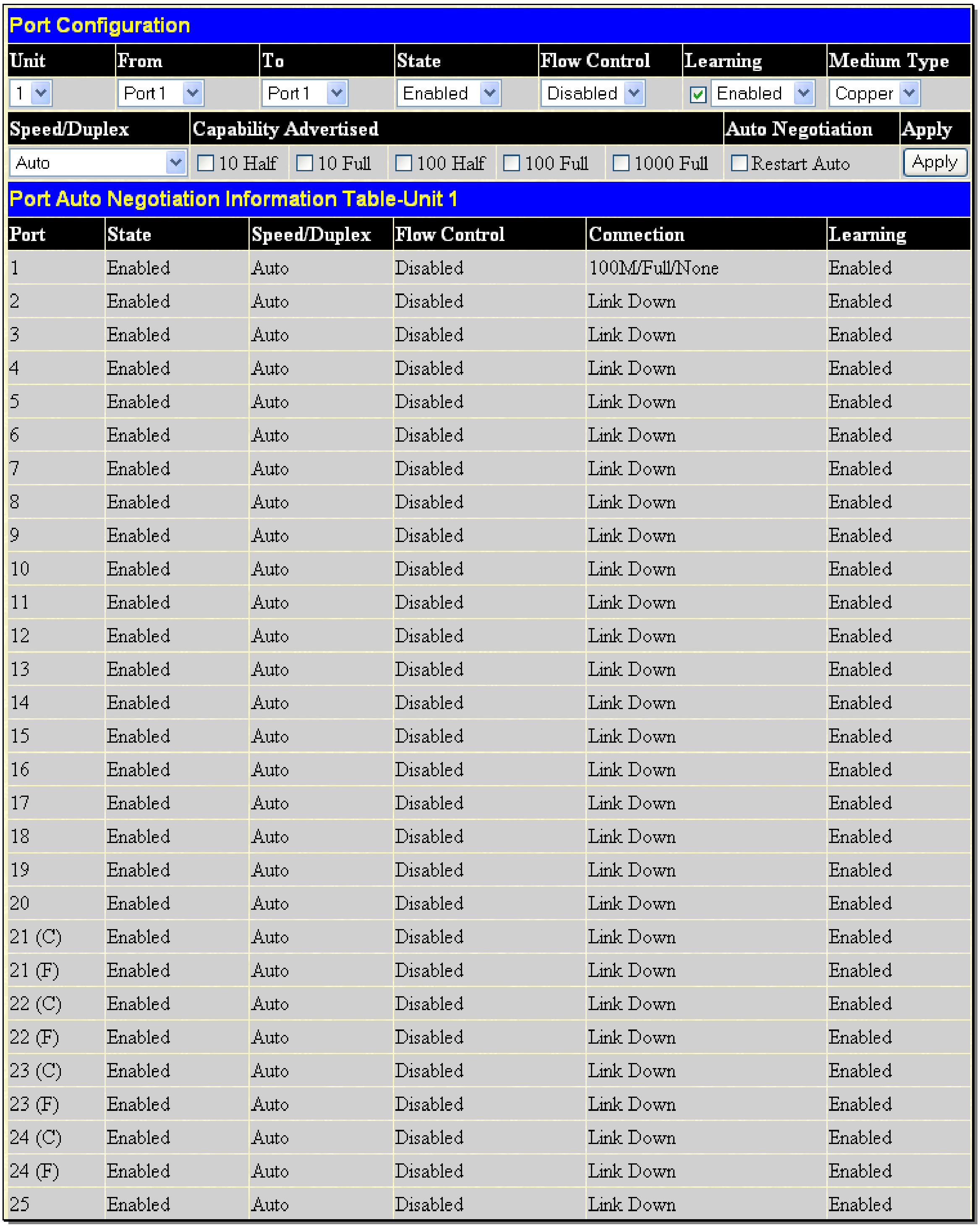
This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control.

Port Configuration

To display the following window, click **Administration** > **Port Configuration > Port Configuration**, as shown below:

To configure switch ports:

1. Choose the port or sequential range of ports using the From and To port pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:



Port Configuration

Unit	From	To	State	Flow Control	Learning	Medium Type
1	Port 1	Port 1	Enabled	Disabled	☑ Enabled	Copper

Speed/Duplex	Capability Advertised					Auto Negotiation	Apply
Auto	□ 10 Half	□ 10 Full	□ 100 Half	□ 100 Full	□ 1000 Full	□ Restart Auto	Apply

Port Auto Negotiation Information Table-Unit 1

Port	State	Speed/Duplex	Flow Control	Connection	Learning
1	Enabled	Auto	Disabled	100M/Full/None	Enabled
2	Enabled	Auto	Disabled	Link Down	Enabled
3	Enabled	Auto	Disabled	Link Down	Enabled
4	Enabled	Auto	Disabled	Link Down	Enabled
5	Enabled	Auto	Disabled	Link Down	Enabled
6	Enabled	Auto	Disabled	Link Down	Enabled
7	Enabled	Auto	Disabled	Link Down	Enabled
8	Enabled	Auto	Disabled	Link Down	Enabled
9	Enabled	Auto	Disabled	Link Down	Enabled
10	Enabled	Auto	Disabled	Link Down	Enabled
11	Enabled	Auto	Disabled	Link Down	Enabled
12	Enabled	Auto	Disabled	Link Down	Enabled
13	Enabled	Auto	Disabled	Link Down	Enabled
14	Enabled	Auto	Disabled	Link Down	Enabled
15	Enabled	Auto	Disabled	Link Down	Enabled
16	Enabled	Auto	Disabled	Link Down	Enabled
17	Enabled	Auto	Disabled	Link Down	Enabled
18	Enabled	Auto	Disabled	Link Down	Enabled
19	Enabled	Auto	Disabled	Link Down	Enabled
20	Enabled	Auto	Disabled	Link Down	Enabled
21 (C)	Enabled	Auto	Disabled	Link Down	Enabled
21 (F)	Enabled	Auto	Disabled	Link Down	Enabled
22 (C)	Enabled	Auto	Disabled	Link Down	Enabled
22 (F)	Enabled	Auto	Disabled	Link Down	Enabled
23 (C)	Enabled	Auto	Disabled	Link Down	Enabled
23 (F)	Enabled	Auto	Disabled	Link Down	Enabled
24 (C)	Enabled	Auto	Disabled	Link Down	Enabled
24 (F)	Enabled	Auto	Disabled	Link Down	Enabled
25	Enabled	Auto	Disabled	Link Down	Enabled

Figure 2- 9. Port Configuration window

The following parameters can be configured:

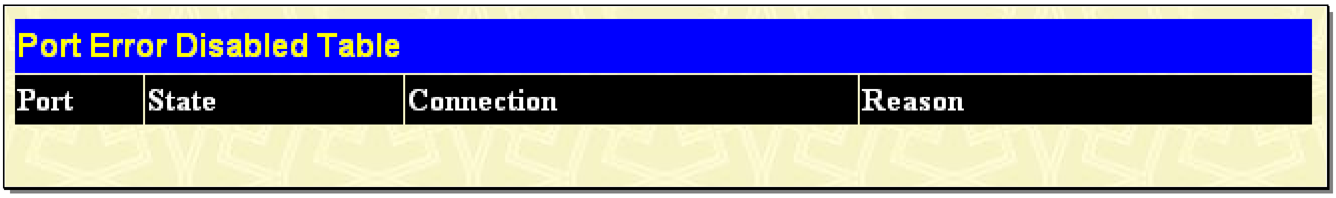
Parameter	Description
Unit	Use the pull-down menu to select switch unit to configure.
From/To	Use the pull-down menus to select the port or range of ports to be configured.
State	Toggle this field to either enable or disable a given port or group of ports.
Flow Control	Displays the flow control scheme 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*, 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 *Enabled*.
Medium Type	This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be set at *Fiber* and the Combo 1000BASE-T ports should be set at *Copper*.
Speed/Duplex	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. Auto denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are Auto, 10M/Half, 10M/Full, 100M/Half and 100M/Full, 1000M/Full_M and 1000M/Full_S. There is no automatic adjustment of port settings with any option other than Auto. The Switch allows the user to configure two types of gigabit connections; 1000M/Full_M and 1000M/Full_S. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The 1000M/Full_M (master) and 1000M/Full_S (slave) parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (1000M/Full_M) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M/Full_S) uses loop timing, where the timing comes form a data stream received from the master. If one connection is set for 1000M/Full_M, the other side of the connection must be set for 1000M/Full_S. Any other configuration will result in a link down status for both ports.

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

Port Error Disabled

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

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



Port Error Disabled Table

Port	State	Connection	Reason

Figure 2- 10. Port Error Disabled Table window

The following parameters are displayed:

Parameter	Description
Port	Displays the port that has been error disabled.
State	Describes the current running state of the port, whether enabled or disabled.

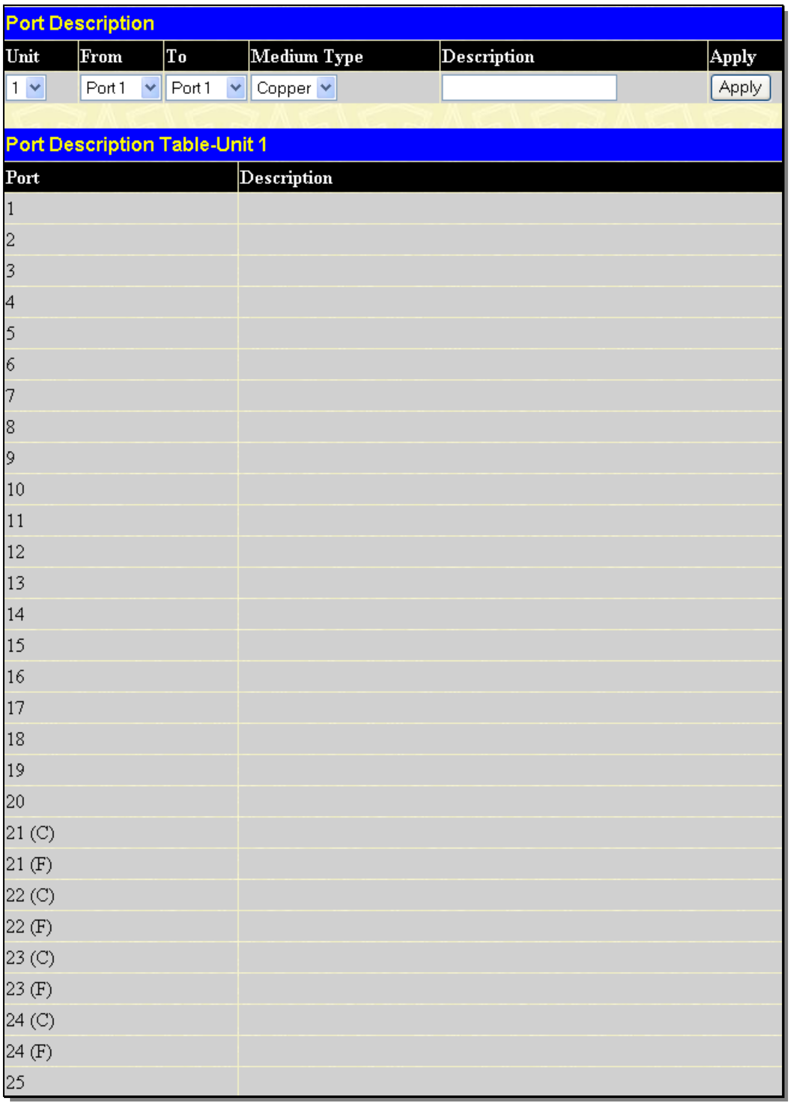
Connection	This field will read the uplink status of the individual ports, whether enabled or disabled.
Reason	Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

Port Description

The Switch supports a port description feature where the user may name various ports on the Switch. Use the From and To pull-down menu to choose a port or range of ports to describe, and then enter a description of the port(s). Click **Apply** to set the descriptions in the Port Description Table.

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

To assign names to various ports, click **Administration** > **Port Configuration** > **Port Description**, as shown.



Port Description

Unit	From	To	Medium Type	Description	Apply
1	Port 1	Port 1	Copper		Apply

Port Description Table-Unit 1

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21 (C)	
21 (F)	
22 (C)	
22 (F)	
23 (C)	
23 (F)	
24 (C)	
24 (F)	
25	

Figure 2- 11. Port Description window

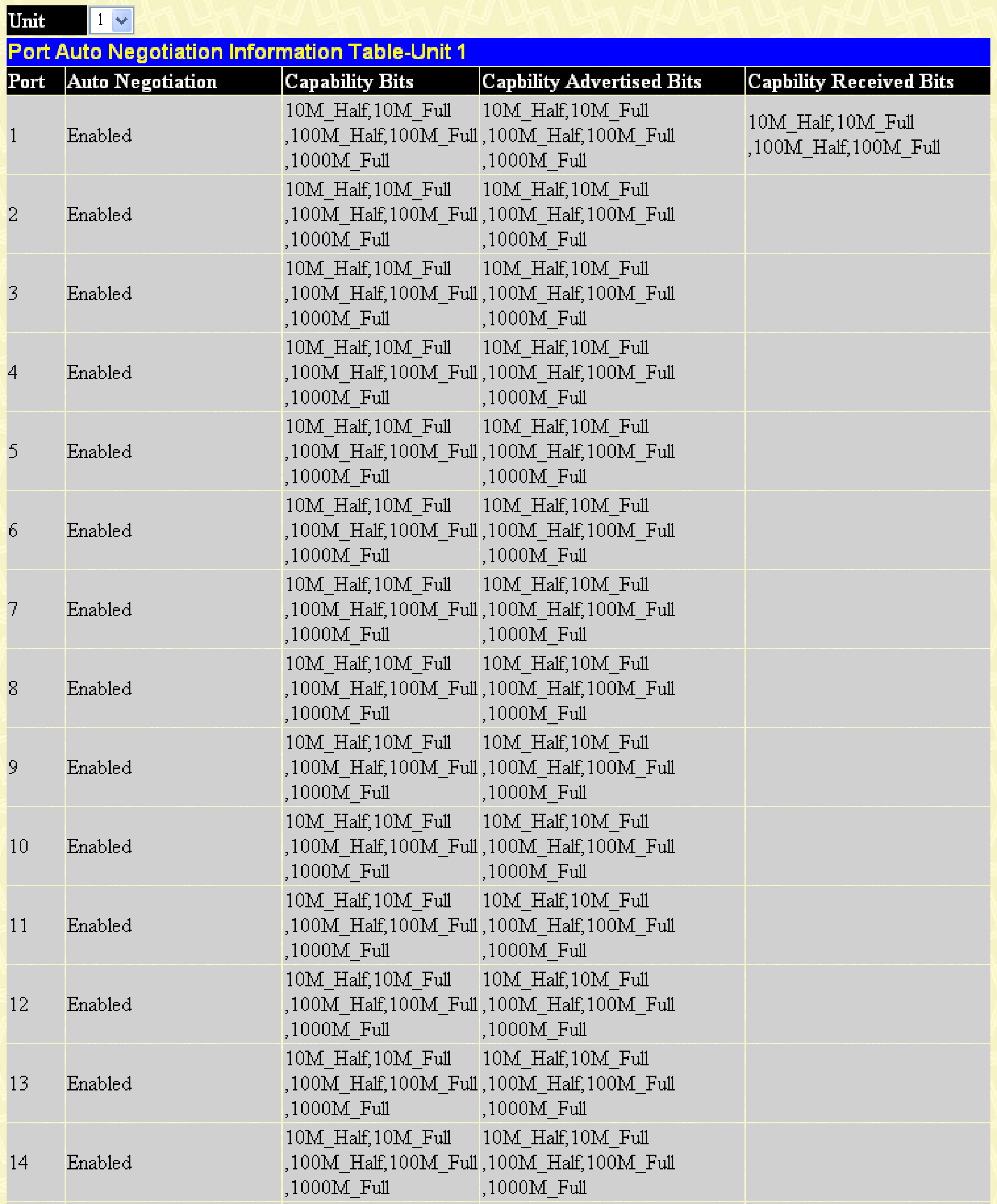
The following parameters are displayed:

Parameter	Description
Unit	Use the pull-down menu to select switch unit to configure.
From/To	Use the pull-down menus to select the port or range of ports to be configured.
Medium Type	The Medium Type applies only to the Combo ports. If configuring the Combo ports, this defines the type of transport medium used. SFP ports should be nominated *Fiber* and the Combo 1000BASE-T ports should be nominated *Copper*. The result will be displayed in the appropriate switch port number slot (C for copper ports and F for fiber ports).
Description	Enter a name for the specified port or ports on the Switch.

Port Auto Negotiation Information

The Port Auto Negotiation Information window displays the current configurations of a range of ports. Use the drop-down menu to select the unit you wish to view and the relevant port information will be displayed in the table below.

To view this window, click **Administration** > **Port Configuration** > **Port Auto Negotiation Information**, as shown below:



Unit: 1

Port Auto Negotiation Information Table-Unit 1

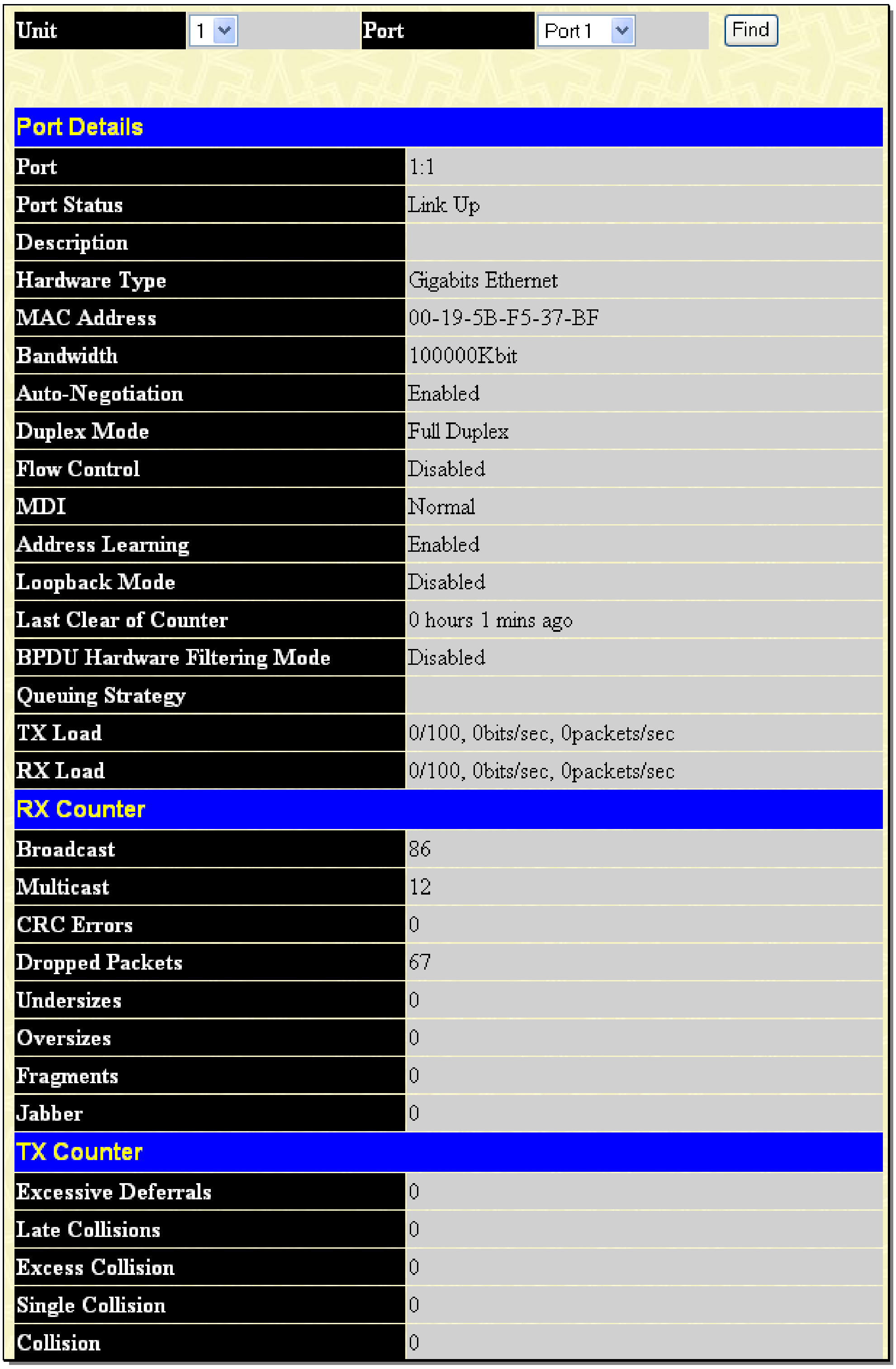
Port	Auto Negotiation	Capability Bits	Capbility Advertised Bits	Capbility Received Bits
1	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full
2	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
3	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
4	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
5	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
6	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
7	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
8	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
9	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
10	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
11	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
12	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
13	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
14	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	

Figure 2- 12. Port Auto Negotiation Information window

Port Details

This window is used to view detailed port information for individual ports on a particular unit. Use the drop-down menus to select the specific port of the unit you wish to view and click **Find**.

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



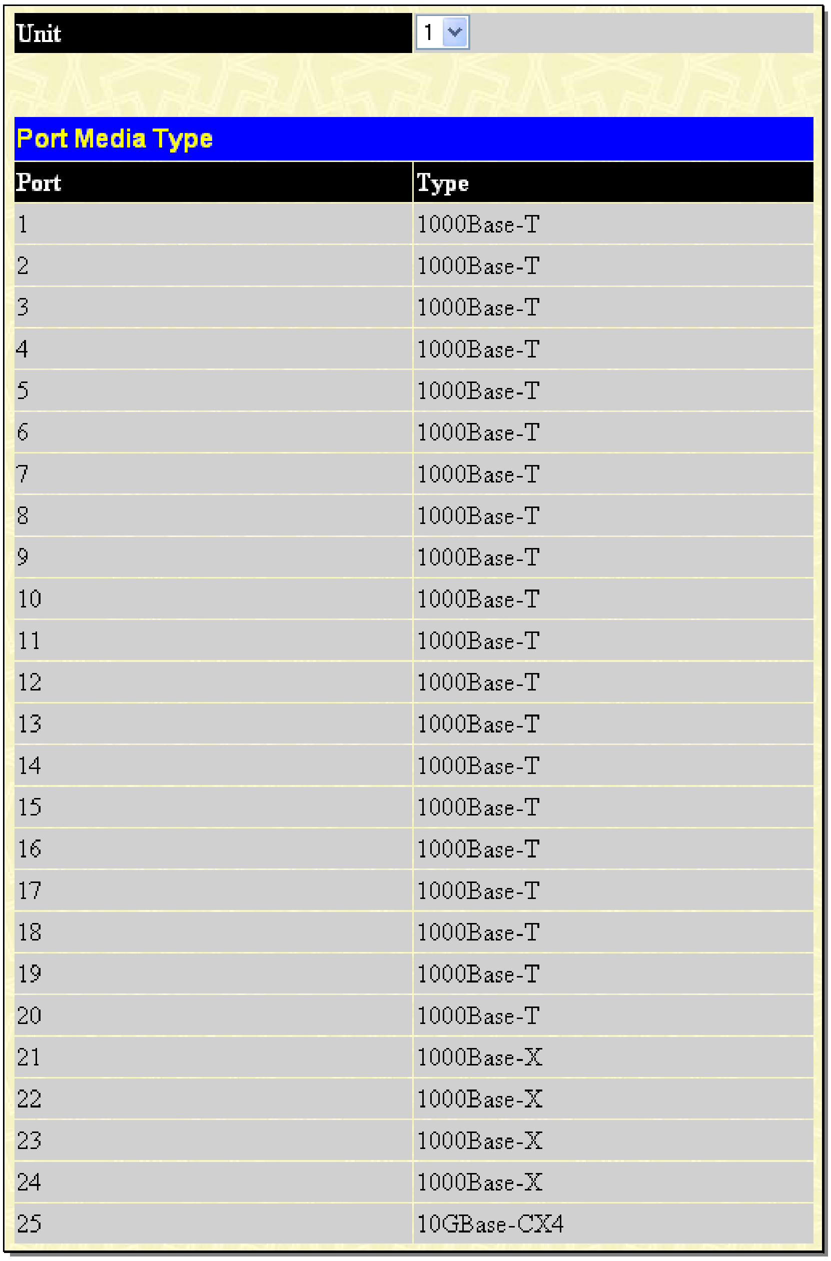
Port Details	
Port	1:1
Port Status	Link Up
Description	
Hardware Type	Gigabits Ethernet
MAC Address	00-19-5B-F5-37-BF
Bandwidth	100000Kbit
Auto-Negotiation	Enabled
Duplex Mode	Full Duplex
Flow Control	Disabled
MDI	Normal
Address Learning	Enabled
Loopback Mode	Disabled
Last Clear of Counter	0 hours 1 mins ago
BPDU Hardware Filtering Mode	Disabled
Queuing Strategy	
TX Load	0/100, 0bits/sec, 0packets/sec
RX Load	0/100, 0bits/sec, 0packets/sec
RX Counter	
Broadcast	86
Multicast	12
CRC Errors	0
Dropped Packets	67
Undersizes	0
Oversizes	0
Fragments	0
Jabber	0
TX Counter	
Excessive Deferrals	0
Late Collisions	0
Excess Collision	0
Single Collision	0
Collision	0

Figure 2- 13. Port Details window

Port Media Type

This window is used to display the port media type available on each unit. To view a particular switch in the stack use the drop-down menu to select the unit.

To view this window, click **Administration** > **Port Configuration** > **Port Media Type**, as shown below:



Unit: 1

Port Media Type

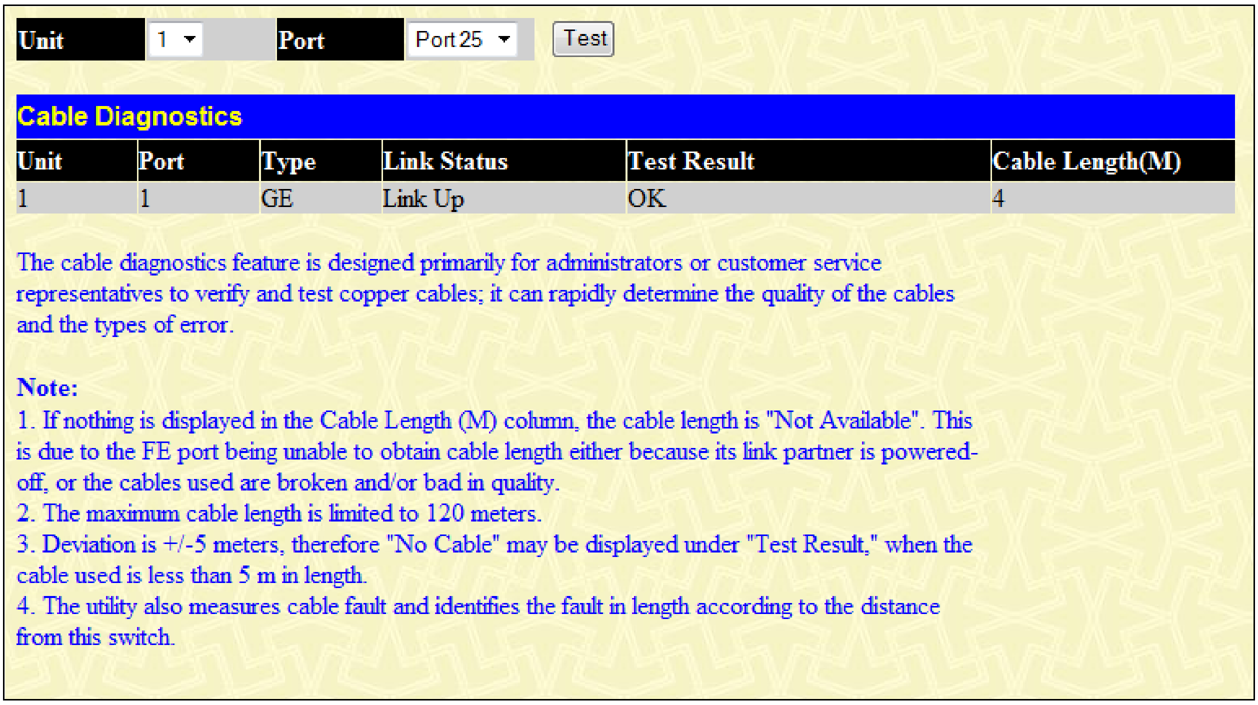
Port	Type
1	1000Base-T
2	1000Base-T
3	1000Base-T
4	1000Base-T
5	1000Base-T
6	1000Base-T
7	1000Base-T
8	1000Base-T
9	1000Base-T
10	1000Base-T
11	1000Base-T
12	1000Base-T
13	1000Base-T
14	1000Base-T
15	1000Base-T
16	1000Base-T
17	1000Base-T
18	1000Base-T
19	1000Base-T
20	1000Base-T
21	1000Base-X
22	1000Base-X
23	1000Base-X
24	1000Base-X
25	10GBase-CX4

Figure 2- 14. Port Media Type window

Cable Diagnostics

This window is used to control the cable diagnostics and determine where and what kind of errors have occurred on the cable. This function is primarily used for administrators to view tests on copper cables.

To view this window, click **Administration > Port Configuration > Cable Diagnostics**, as shown below:



Cable Diagnostics

Unit	Port	Type	Link Status	Test Result	Cable Length(M)
1	1	GE	Link Up	OK	4

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

Note:
1. If nothing is displayed in the Cable Length (M) column, the cable length is "Not Available". This is due to the FE port being unable to obtain cable length either because its link partner is powered-off, or the cables used are broken and/or bad in quality.
2. The maximum cable length is limited to 120 meters.
3. Deviation is +/-5 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 5 m in length.
4. The utility also measures cable fault and identifies the fault in length according to the distance from this switch.

Figure 2- 15. Cable Diagnostics window

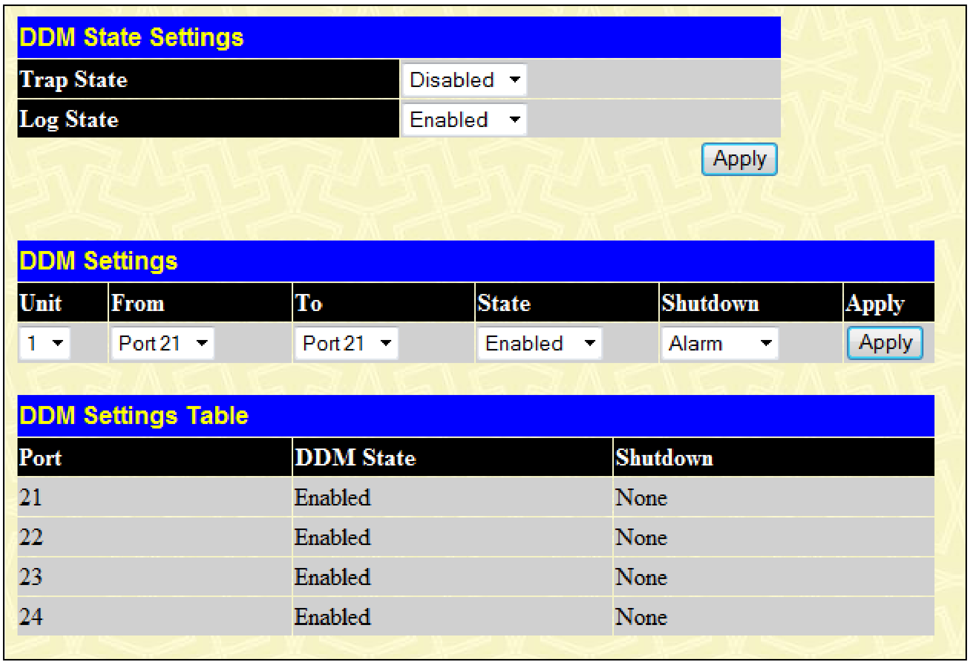
DDM

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

DDM Settings

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

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM Settings**, as show below:



DDM State Settings

Trap State	Disabled
Log State	Enabled

DDM Settings

Unit	From	To	State	Shutdown	Apply
1	Port 21	Port 21	Enabled	Alarm	Apply

DDM Settings Table

Port	DDM State	Shutdown
21	Enabled	None
22	Enabled	None
23	Enabled	None
24	Enabled	None

Figure 2- 16. DDM State Settings window

The following parameters can be configured:

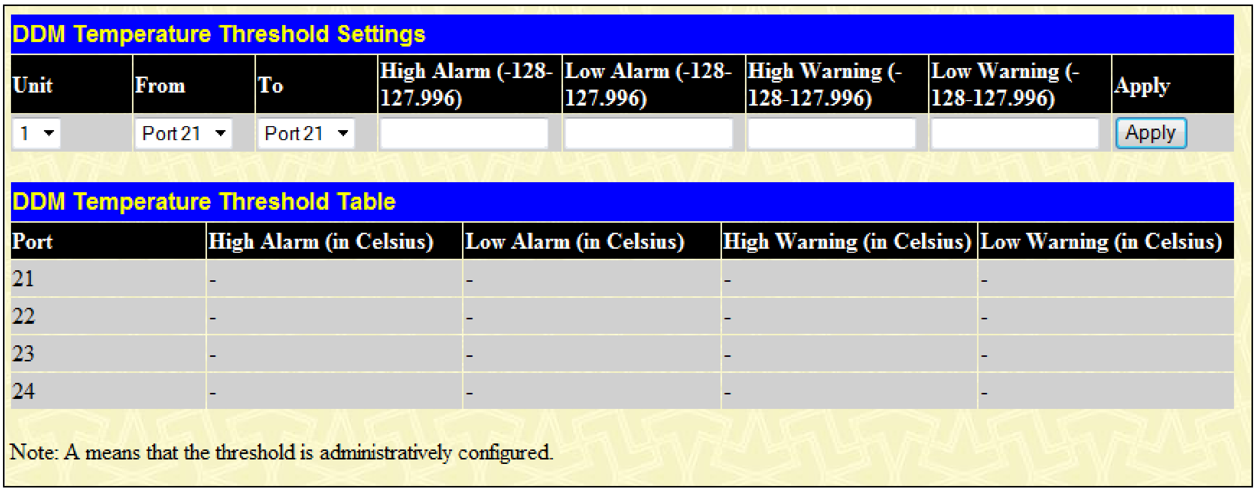
Parameter	Description
Trap State	Specify whether to send the trap, when the operating parameter exceeds the alarm or warning threshold.
Log State	Specify whether to send the log, when the operating parameter exceeds the alarm or warning threshold.
Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shutdown the port, when the operating parameter exceeds the Alarm or Warning threshold. *Alarm* - Shutdown the port when the configured alarm threshold range is exceeded. *Warning* - Shutdown the port when the configured warning threshold range is exceeded. *None* - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

Click **Apply** to implement the changes.

DDM Temperature Threshold Settings

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

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM Temperature Threshold Settings**, as show below:



DDM Temperature Threshold Settings

Unit	From	To	High Alarm (-128-127.996)	Low Alarm (-128-127.996)	High Warning (-128-127.996)	Low Warning (-128-127.996)	Apply
1	Port 21	Port 21					Apply

DDM Temperature Threshold Table

Port	High Alarm (in Celsius)	Low Alarm (in Celsius)	High Warning (in Celsius)	Low Warning (in Celsius)
21	-	-	-	-
22	-	-	-	-
23	-	-	-	-
24	-	-	-	-

Note: A means that the threshold is administratively configured.

Figure 2- 17. DDM Temperature Threshold Settings window

The following parameters can be configured:

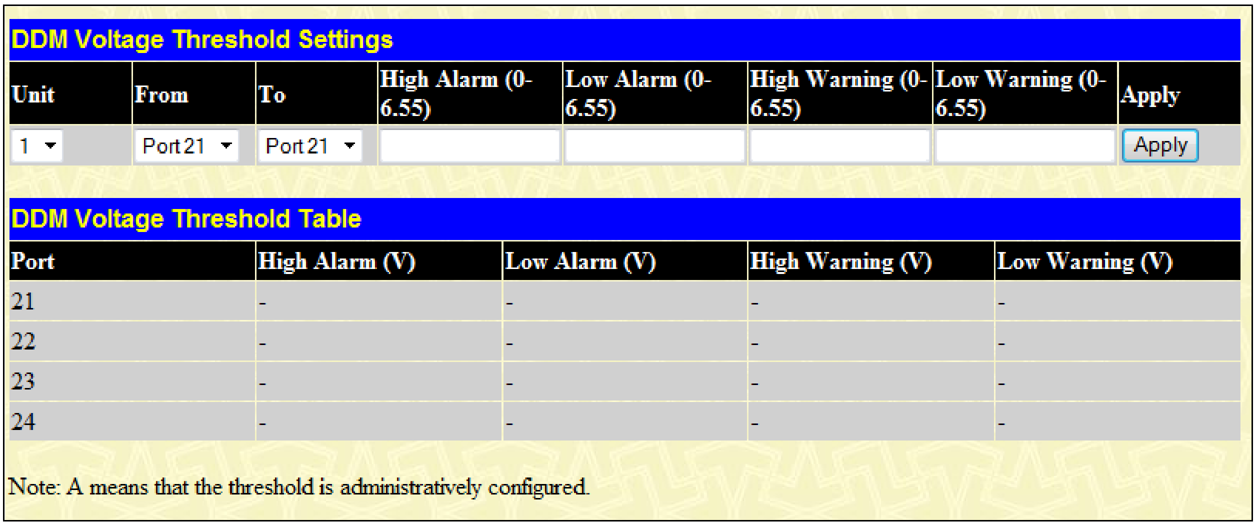
Parameter	Description
Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
High Alarm	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

Click **Apply** to implement the changes.

DDM Voltage Threshold Settings

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

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM Voltage Threshold Settings**, as show below:



DDM Voltage Threshold Settings

Unit	From	To	High Alarm (0-6.55)	Low Alarm (0-6.55)	High Warning (0-6.55)	Low Warning (0-6.55)	Apply
1	Port 21	Port 21					Apply

DDM Voltage Threshold Table

Port	High Alarm (V)	Low Alarm (V)	High Warning (V)	Low Warning (V)
21	-	-	-	-
22	-	-	-	-
23	-	-	-	-
24	-	-	-	-

Note: A means that the threshold is administratively configured.

Figure 2- 18. DDM Voltage Threshold Settings window

The following parameters can be configured:

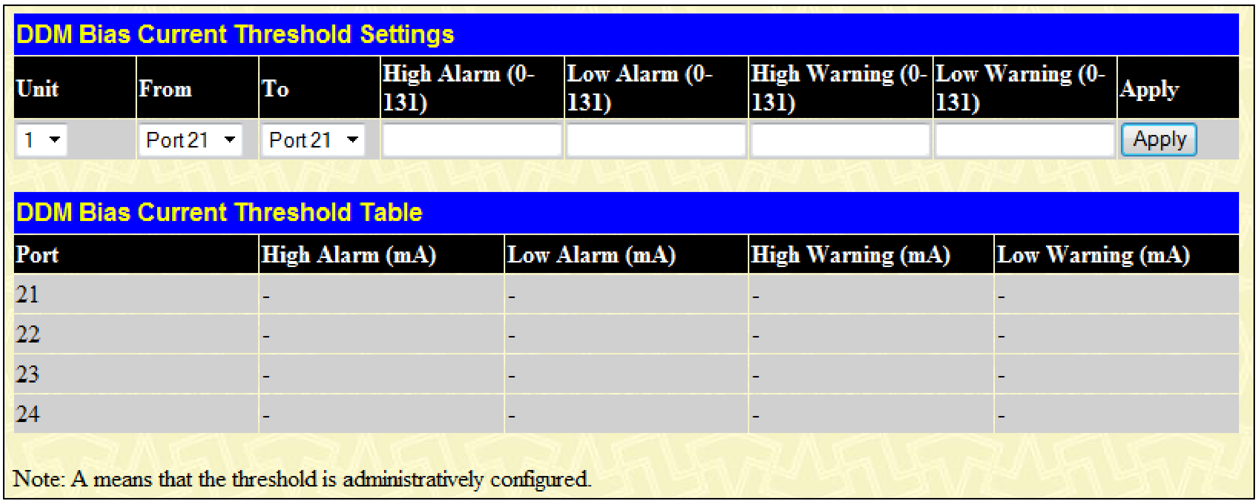
Parameter	Description
Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
High Alarm	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

Click **Apply** to implement the changes.

DDM Bias Current Threshold Settings

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

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM Bias Current Threshold Settings**, as show below:



DDM Bias Current Threshold Settings

Unit	From	To	High Alarm (0-131)	Low Alarm (0-131)	High Warning (0-131)	Low Warning (0-131)	Apply
1	Port21	Port21					Apply

DDM Bias Current Threshold Table

Port	High Alarm (mA)	Low Alarm (mA)	High Warning (mA)	Low Warning (mA)
21	-	-	-	-
22	-	-	-	-
23	-	-	-	-
24	-	-	-	-

Note: A means that the threshold is administratively configured.

Figure 2- 19. DDM Bias Current Threshold Settings window

The following parameters can be configured:

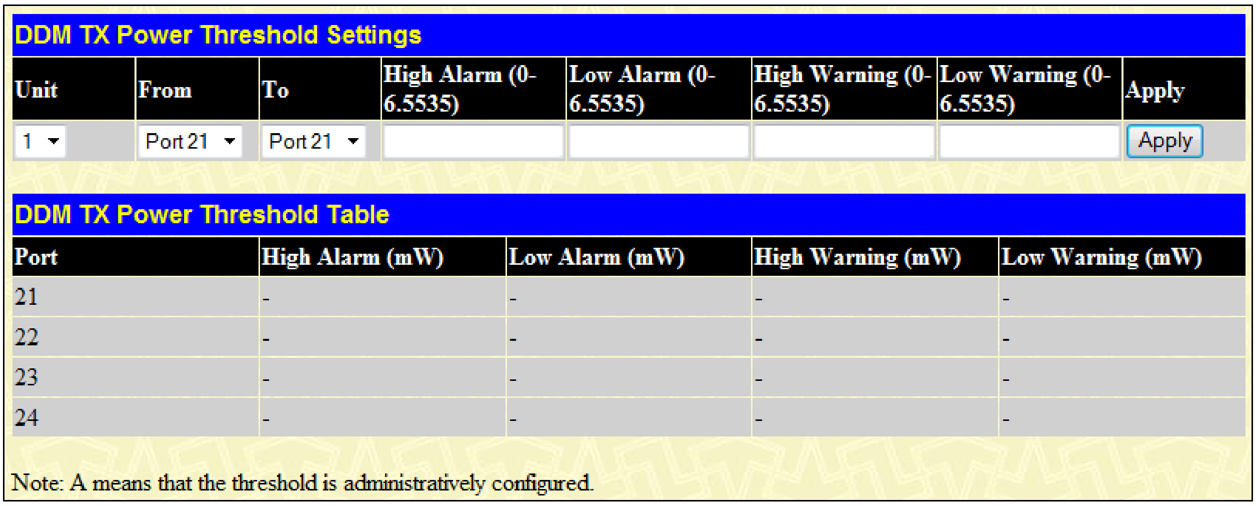
Parameter	Description
Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
High Alarm	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

Click **Apply** to implement the changes.

DDM TX Power Threshold Settings

This window is used to configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM TX Power Threshold Settings**, as show below:



DDM TX Power Threshold Settings

Unit	From	To	High Alarm (0-6.5535)	Low Alarm (0-6.5535)	High Warning (0-6.5535)	Low Warning (0-6.5535)	Apply
1	Port 21	Port 21					Apply

DDM TX Power Threshold Table

Port	High Alarm (mW)	Low Alarm (mW)	High Warning (mW)	Low Warning (mW)
21	-	-	-	-
22	-	-	-	-
23	-	-	-	-
24	-	-	-	-

Note: A means that the threshold is administratively configured.

Figure 2- 20. DDM TX Power Threshold Settings window

The following parameters can be configured:

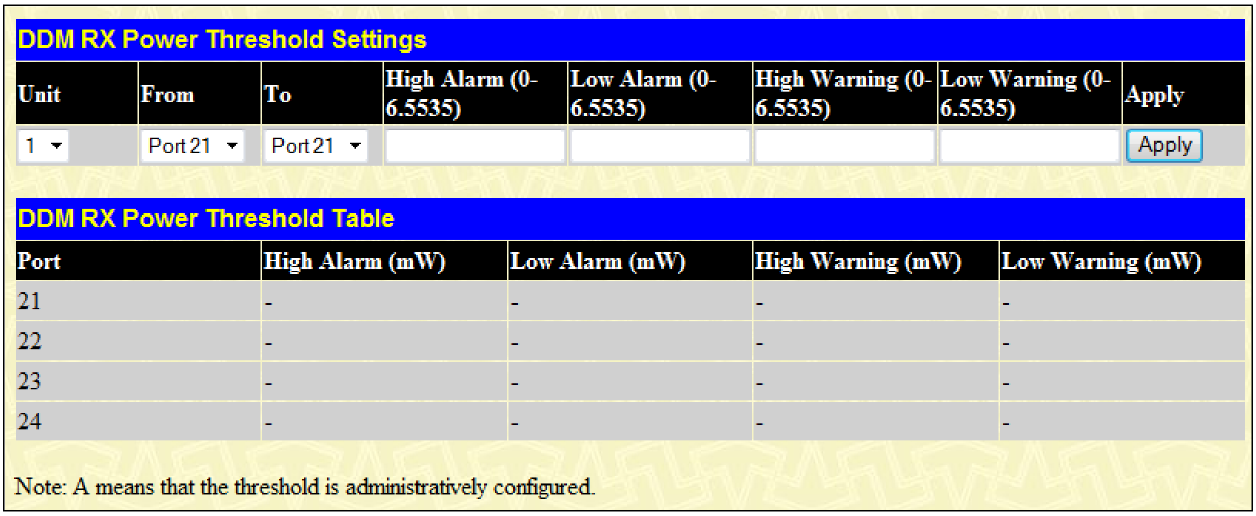
Parameter	Description
Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
High Alarm	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

Click **Apply** to implement the changes.

DDM RX Power Threshold Settings

This window is used to configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM RX Power Threshold Settings**, as show below:



DDM RX Power Threshold Settings

Unit	From	To	High Alarm (0-6.5535)	Low Alarm (0-6.5535)	High Warning (0-6.5535)	Low Warning (0-6.5535)	Apply
1	Port 21	Port 21					Apply

DDM RX Power Threshold Table

Port	High Alarm (mW)	Low Alarm (mW)	High Warning (mW)	Low Warning (mW)
21	-	-	-	-
22	-	-	-	-
23	-	-	-	-
24	-	-	-	-

Note: A means that the threshold is administratively configured.

Figure 2- 21. DDM RX Power Threshold Settings window

The following parameters can be configured:

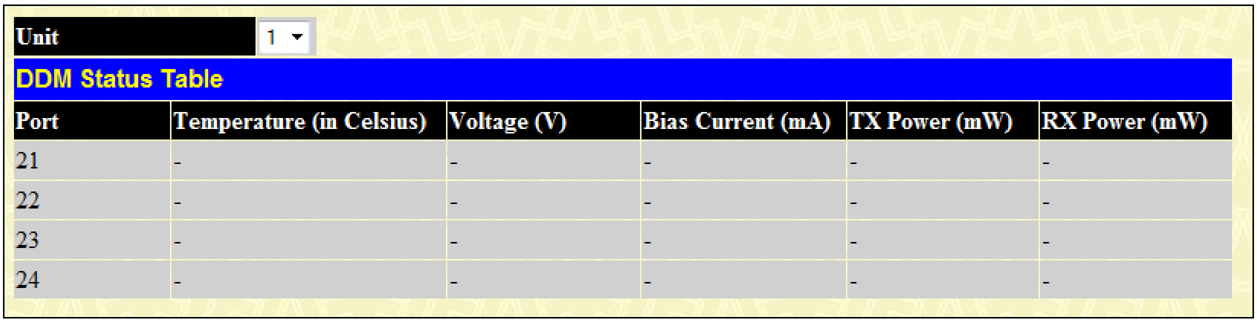
Parameter	Description
Unit	Specify the unit of the DDM TX and RX power.
From Port / To Port	Select a range of ports to be configured.
High Alarm	This is the highest threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken.
Low Alarm	This is the lowest threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken.
High Warning	This is the highest threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken.
Low Warning	This is the lowest threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken.

Click **Apply** to implement the changes.

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **Administration** > **Port Configuration** > **DDM** > **DDM Status Table**, as show below:



Unit 1

DDM Status Table

Port	Temperature (in Celsius)	Voltage (V)	Bias Current (mA)	TX Power (mW)	RX Power (mW)
21	-	-	-	-	-
22	-	-	-	-	-
23	-	-	-	-	-
24	-	-	-	-	-

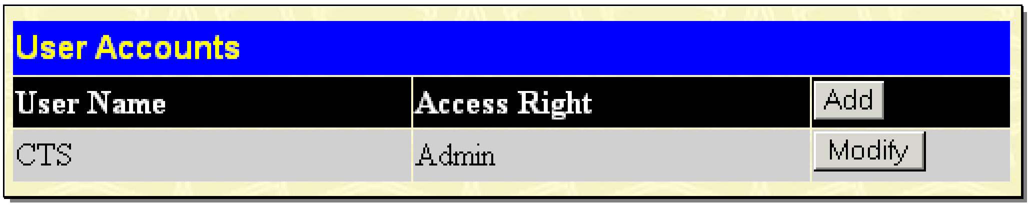
The following parameters can be configured:

Parameter	Description
Unit	Specify the unit of the DDM TX and RX power.

User Accounts

Use the **User Account Management** window to control user privileges. Any existing User Accounts will be displayed in the table below.

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

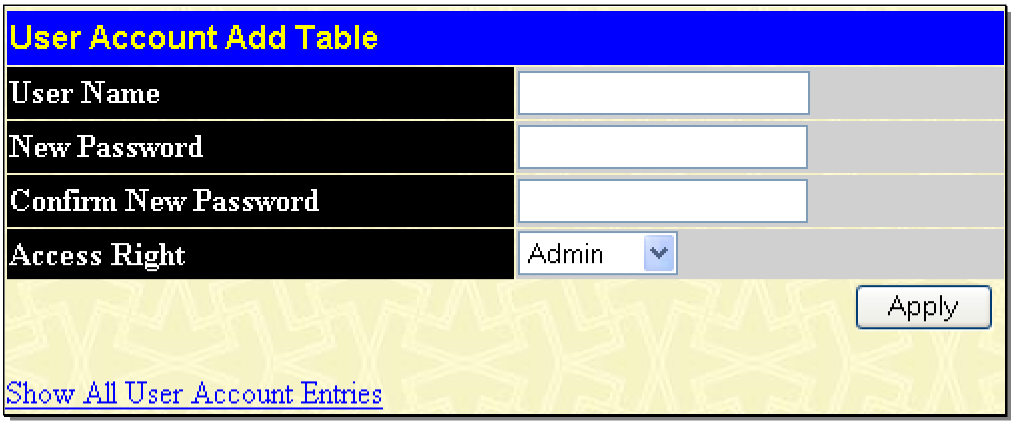


User Accounts

User Name	Access Right	Add
CTS	Admin	Modify

Figure 2- 22. 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.

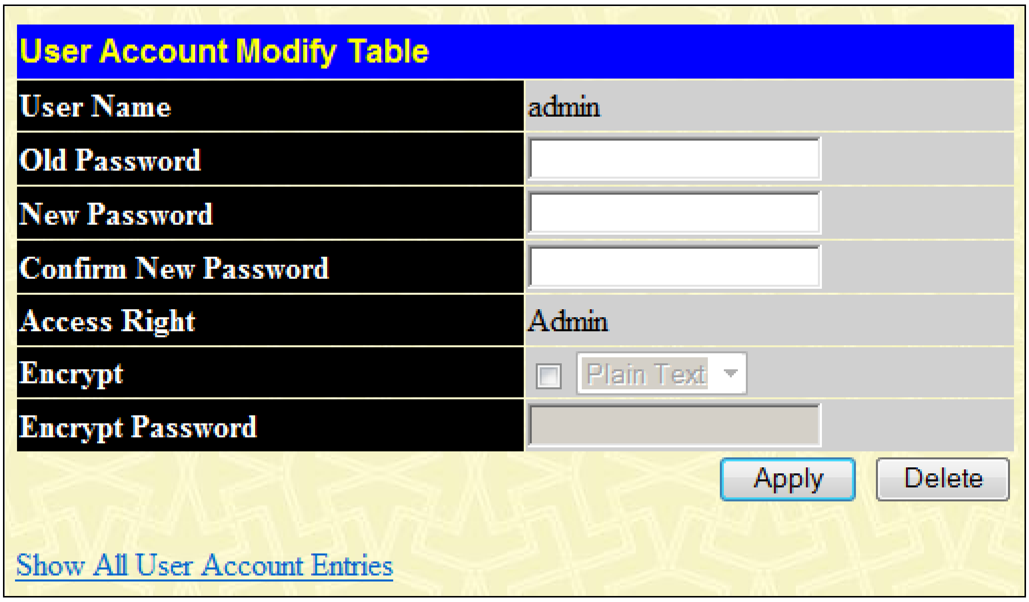


User Account Add Table

User Name	
New Password	
Confirm New Password	
Access Right	Admin

Figure 2- 23. User Account Add Table window

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



User Account Modify Table

User Name	admin
Old Password	
New Password	
Confirm New Password	
Access Right	Admin
Encrypt	□ Plain Text
Encrypt Password	

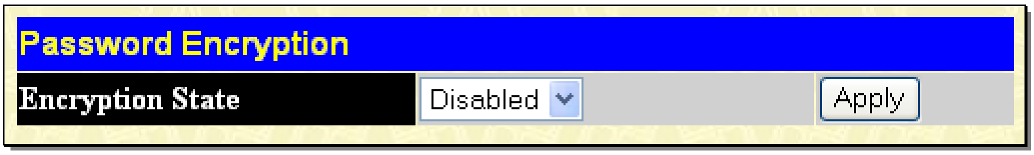
Figure 2- 24. User Account Modify Table window

Modify or delete an existing user account in the **User Account Modify Table** window. 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. To encrypt this user account information, tick the Encrypt checkbox, toggle between *Plain Text* and *SHA_1*, and enter the encryption password in the last field. Click **Apply** to implement changes.

Password Encryption

This window is used to set the password encryption state.

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



Password Encryption

Encryption State: Disabled

Figure 2- 25. Password Encryption window

The following parameters can be configured:

Parameter	Description
Encryption State	Use the pull-down menu to enable or disable the password encryption. Select *Enabled* to change the password into encrypted form. When password encryption is *Disabled*, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last **enable password encryption** command in the CLI, the password will still be in encrypted form and cannot be reverted back to plaintext form.

Click **Apply** to implement the changes.

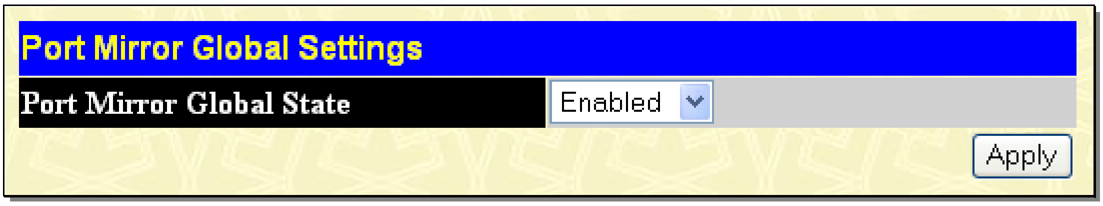
Mirror

This section contains information for mirroring port configurations, including Port Mirror Global Settings and Port Mirror Settings.

Port Mirror Global Settings

This window is used to set the port mirror global state.

To view the **Port Mirror Global Settings** window, click **Administration** > **Mirror** > **Port Mirror Global Settings**, as shown below:



Port Mirror Global Settings

Port Mirror Global State: Enabled

Figure 2- 26. Port Mirror Global Settings window

The following parameters can be configured:

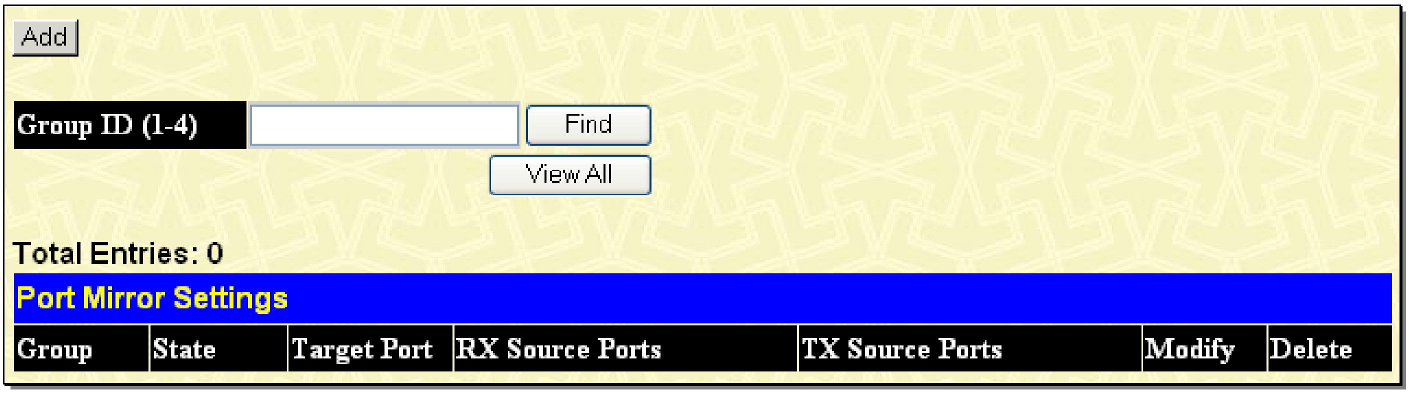
Parameter	Description
Porting Mirror Global State	Use the pull-down menu to enable or disable the port mirror status.

Click **Apply** to implement the changes.

Port Mirror Settings

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

To view the **Port Mirror Settings** window, click **Administration** > **Mirror** > **Port Mirror Settings**, as shown below:



Total Entries: 0

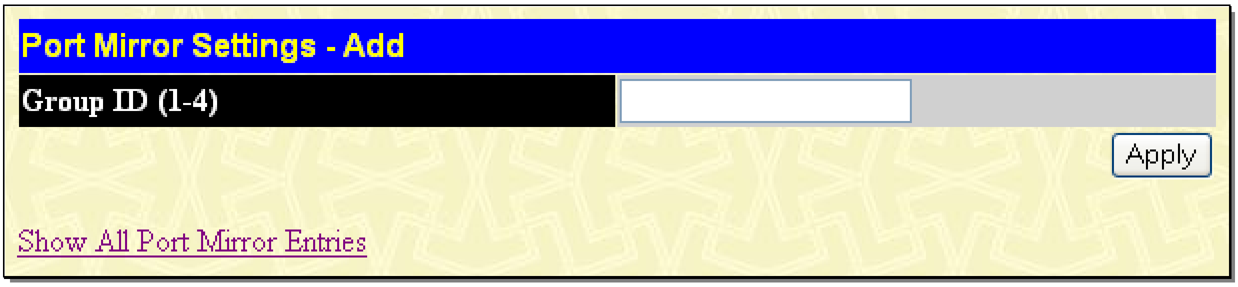
Port Mirror Settings

Group	State	Target Port	RX Source Ports	TX Source Ports	Modify	Delete

Figure 2- 27. Port Mirror Settings window

Enter an ID in the Group ID (1-4) field and click **Find** to see all the entries that belong to the group in the lower half of the window. Click **View All** to see all the entries. Click ☒ to remove the corresponding entry.

To add a new mirror port, click the **Add** button, and the window below appears:

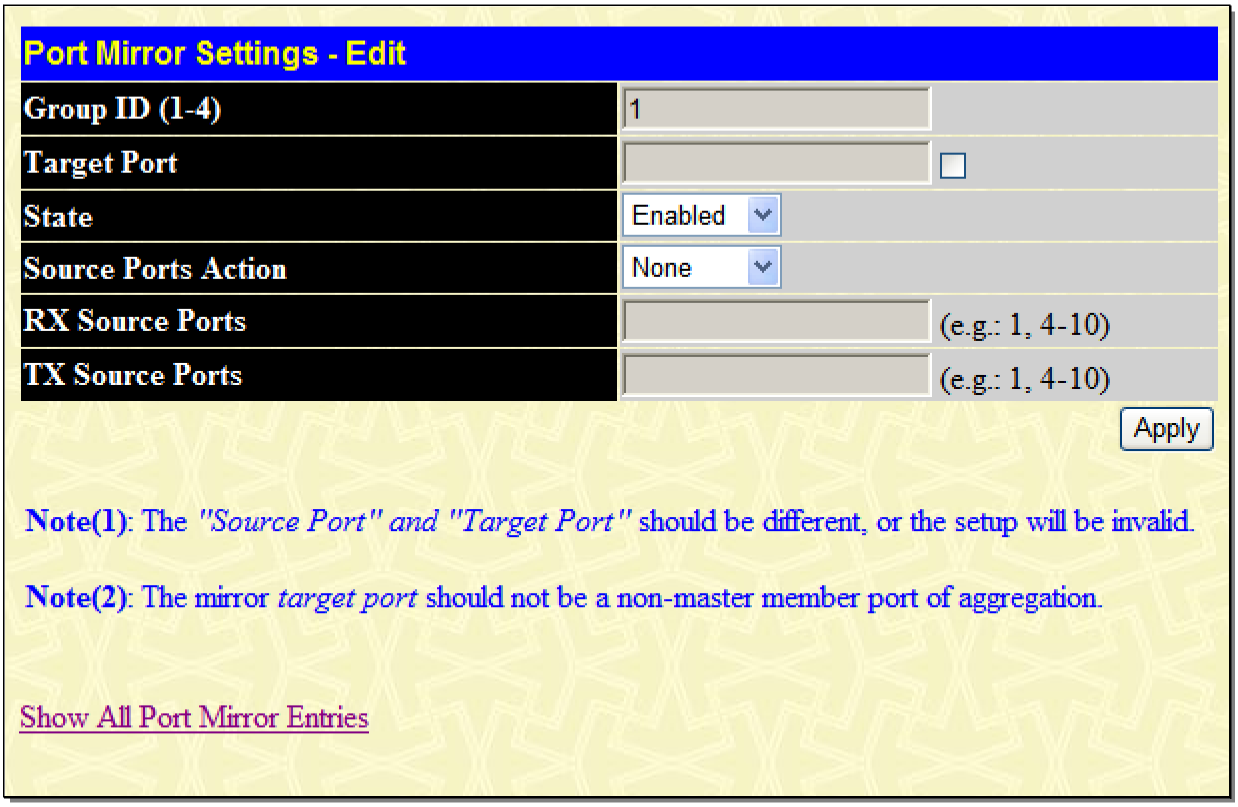


Port Mirror Settings - Add

Group ID (1-4):

Figure 2- 28. Port Mirror Settings - Add window

To modify an existing mirror port, click the **Modify** button of the corresponding entry, and the window below appears:



Port Mirror Settings - Edit

Group ID (1-4)	1	
Target Port		□
State	Enabled	
Source Ports Action	None	
RX Source Ports		(e.g.: 1, 4-10)
TX Source Ports		(e.g.: 1, 4-10)

Note(1): The *"Source Port" and "Target Port"* should be different, or the setup will be invalid.

Note(2): The mirror *target port* should not be a non-master member port of aggregation.

Show All Port Mirror Entries

Figure 2- 29. Port Mirror Settings - Edit window

The following parameters are displayed or can be configured:

Parameter	Description
Group ID (1-4)	Enter or display the group ID this entry belongs to.
Target Port	Tick the check box and enter the port which received the copies from the source port.
State	Use the pull-down menu to enable or disable the mirror group function.
Source Ports Action	User the pull-down menu to add or delete the source port.
RX Source Ports	Only the received packets on the mirror group source ports will be mirrored to the mirror group target port.
TX Source Ports	Only the sent packets on the mirror group source ports will be mirrored to the mirror group target port.

Click the Show All Port Mirror Entries link to return to the Port Mirror Settings window. Click **Apply** to implement the changes.

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

NOTE: When the device with the source port has been removed from a stack, the configuration will be disabled temporarily until another device has been installed in its place. If configurations are saved to NVR RAM during this period the configuration will be removed forever.

Mirroring within the Switch Stack

Users may configure mirroring between switches in the switch stack but certain conditions and restrictions apply.

1. When mirroring is configured in the stack, the primary master and the backup master will save and synchronize these mirroring configurations in their respective databases. Therefore, if the primary master is removed, the backup master will still hold the mirroring configurations set.
2. If the device hot-removed from the stack holds the target port for the mirroring function, the primary master will disable the mirroring function for the whole stack.
3. Stacking ports cannot be source ports or target mirror ports.

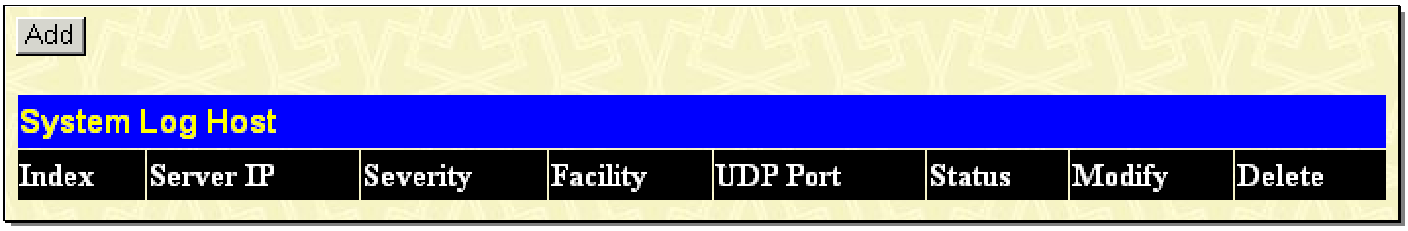
System Log

The System log on 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. The **System Log** folder contains two main windows **System Log Host** and **System Log Save Mode Settings**.

System Log Host

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

To view this window, click **Administration** > **System Log > System Log Host**, as shown below:

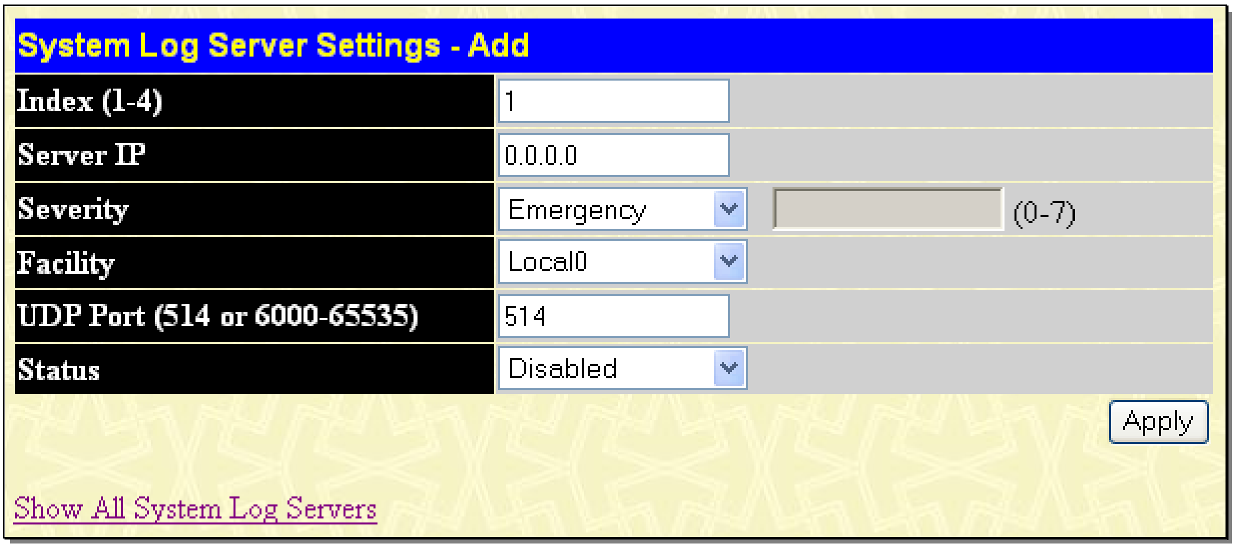


System Log Host

Index	Server IP	Severity	Facility	UDP Port	Status	Modify	Delete

Figure 2- 30. 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.



System Log Server Settings - Add

Index (1-4)	1
Server IP	0.0.0.0
Severity	Emergency (0-7)
Facility	Local0
UDP Port (514 or 6000-65535)	514
Status	Disabled

Figure 2- 31. System Log Server Settings – Add window

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.

The following parameters can be set:

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td><b>Index (1-4)</b></td><td colspan="2">Syslog server settings index (<i>1</i> to <i>4</i>).</td></tr>
<tr><td><b>Server IP</b></td><td colspan="2">The IP address of the Syslog server.</td></tr>
<tr><td><b>Severity</b></td><td colspan="2">This drop-down menu allows you to select the level of messages that will be sent. The options are <i>Emergency</i>, <i>Alert</i>, <i>Critical</i>, <i>Error</i>, <i>Warning</i>, <i>Notice</i>, <i>Informational</i>, <i>Debug</i>, <i>All,</i> and <i>Level</i>.</td></tr>
<tr><td rowspan="25"><b>Facility</b></td><td colspan="2">Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: <b>Bold</b> font indicates the facility values that the Switch is currently employing.</td></tr>
<tr><td><b>Numerical Code</b></td><td><b>Facility</b></td></tr>
<tr><td>0</td><td>kernel messages</td></tr>
<tr><td>1</td><td>user-level messages</td></tr>
<tr><td>2</td><td>mail system</td></tr>
<tr><td>3</td><td>system daemons</td></tr>
<tr><td>4</td><td>security/authorization messages</td></tr>
<tr><td>5</td><td>messages generated internally by syslog line printer subsystem</td></tr>
<tr><td>6</td><td>network news subsystem</td></tr>
<tr><td>7</td><td>UUCP subsystem</td></tr>
<tr><td>8</td><td>clock daemon</td></tr>
<tr><td>9</td><td>security/authorization messages</td></tr>
<tr><td>10</td><td>FTP daemon</td></tr>
<tr><td>11</td><td>NTP subsystem</td></tr>
<tr><td>12</td><td>log audit</td></tr>
<tr><td>13</td><td>log alert</td></tr>
<tr><td>14</td><td>clock daemon</td></tr>
<tr><td>15</td><td><b>local use 0 (local0)</b></td></tr>
<tr><td><b>16</b></td><td><b>local use 1 (local1)</b></td></tr>
<tr><td><b>17</b></td><td><b>local use 2 (local2)</b></td></tr>
<tr><td><b>18</b></td><td><b>local use 3 (local3)</b></td></tr>
<tr><td><b>19</b></td><td><b>local use 4 (local4)</b></td></tr>
<tr><td><b>20</b></td><td><b>local use 5 (local5)</b></td></tr>
<tr><td><b>21</b></td><td><b>local use 6 (local6)</b></td></tr>
<tr><td><b>22</b></td><td><b>local use 7 (local7)</b></td></tr>
<tr><td><b>UDP Port (514 or 6000-65535)</b></td><td colspan="2">Type the UDP port number used for sending Syslog messages. The default is <i>514</i>.</td></tr>
<tr><td><b>Status</b></td><td colspan="2">Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate.</td></tr>
</table>

System Log Save Mode Settings

This window may be used to choose a method for which to save the switch log to the flash memory of the Switch.

To view this window, click **Administration** > **System Log** > **System Log Save Mode Settings**, as shown below:

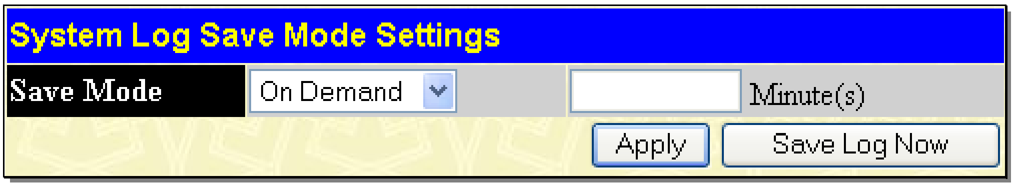


Figure 2- 32. System Log Save Mode Settings window

The following parameters can be configured:

Parameter	Description
Save Mode	Use the pull-down menu to choose the method for saving the switch log to the Flash memory. There are three options: *Time Interval* – Configure a time interval by which the switch will save the log files. *On Demand* – Only save log files when manually telling the Switch to do so. Go to **Save Services** > **Save Changes** to manually save log. *On Trigger* – Save log files to the Switch every time when a log event occurs on the Switch.
Minute(s)	When *Time Interval* is selected in **Save Mode**, set a time between *1* and *65535* minutes in the field. The default value is *1* minute.

Click **Apply** to implement the changes. Click **Save Log Now** to immediately save log files currently on the Switch.

System Log Source Interface Settings

This window is used to configure syslog source interface settings.

To view this window, click **Administration** > **System Log** > **System Log Source Interface Settings**, as shown below:

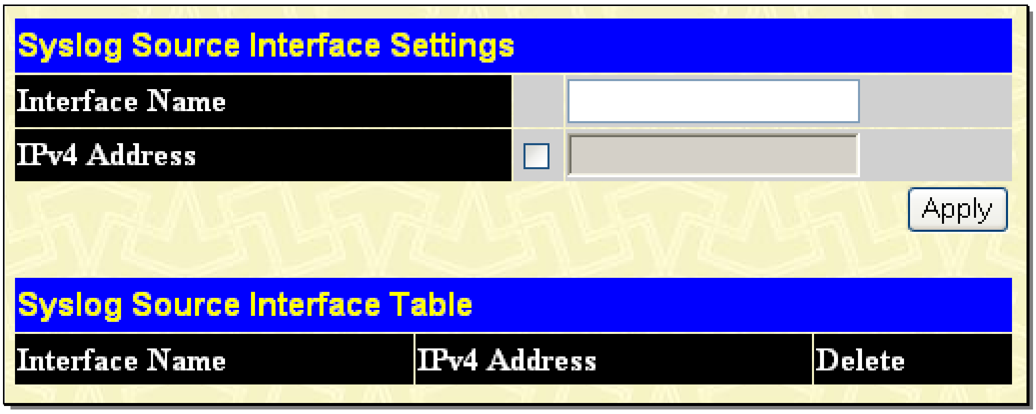
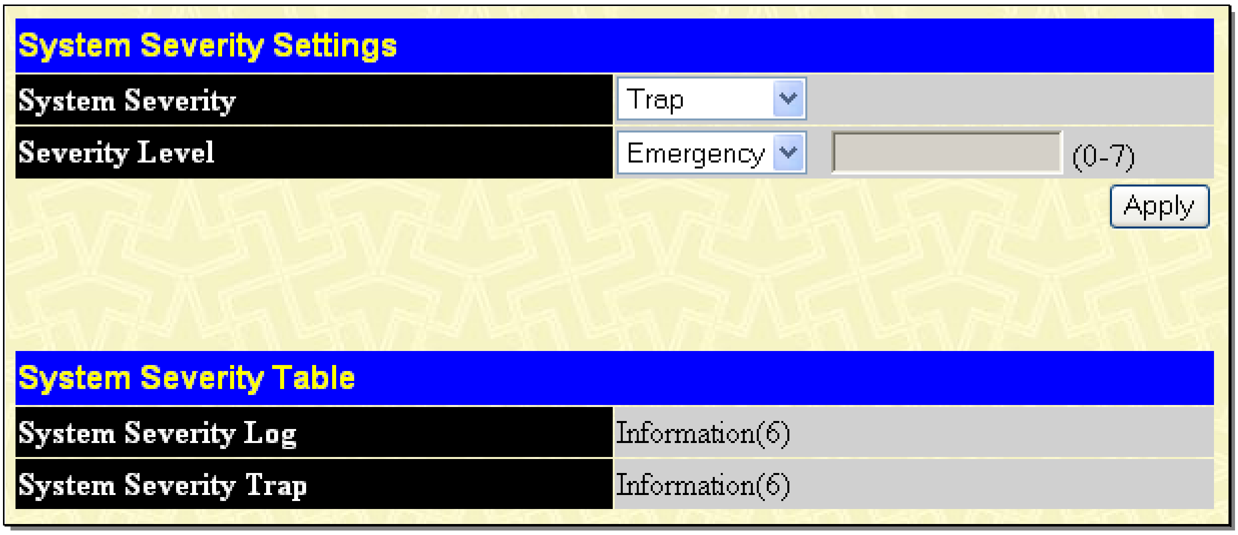


Figure 2- 33. Syslog Source Interface Settings window

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** window to set the criteria for alerts. The current settings are displayed in the lower half of the window.

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



System Severity Settings

System Severity	Trap
Severity Level	Emergency (0-7)

System Severity Table

System Severity Log	Information(6)
System Severity Trap	Information(6)

Figure 2- 34. System Severity Settings window

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

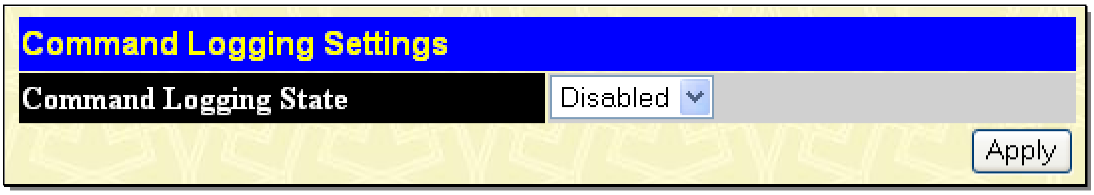
Parameter	Description
System Severity	Choose how the alerts are used from the drop-down menu. Select *Log* to send the alert of the Severity Type configured to the Switch's log for analysis. Choose *Trap* to send it to an SNMP agent for analysis. Select *All* to send the chosen alert type to an SNMP 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 *Emergency* to send only Emergency events to the Switch's log or SNMP agent. Select *Alert* to send Emergency and alert events to the Switch's log or SNMP agent. Select *Critical* to send emergency, alert and critical events to the Switch's log or SNMP agent. Select *Error* to send error, critical, alert and emergency events to the Switch's log or SNMP agent. Select *Warning* to send warning, error, critical, alert and emergency events to the Switch's log or SNMP agent. Select *Notice* to send notice, warning, error, critical, alert and emergency events to the Switch's log or SNMP agent. Select *Information* to send information, notice, warning, error, critical, alert and emergency events to the Switch's log or SNMP agent. Select *Debug* to send debug, information, notice, warning, error, critical, alert and emergency events to the Switch's log or SNMP agent.

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

Command Logging Settings

This window is used to enable or disable command logging settings.

To view this window, click **Administration** > **Command Logging Settings**, as shown below:



Command Logging Settings

Command Logging State: Disabled

Figure 2- 35. Command Logging Settings window

The following parameters are displayed or can be configured:

Parameter	Description
Command Logging State	Enable or disable command logging settings. The default is *Disabled*.

Click **Apply** to implement the changes.

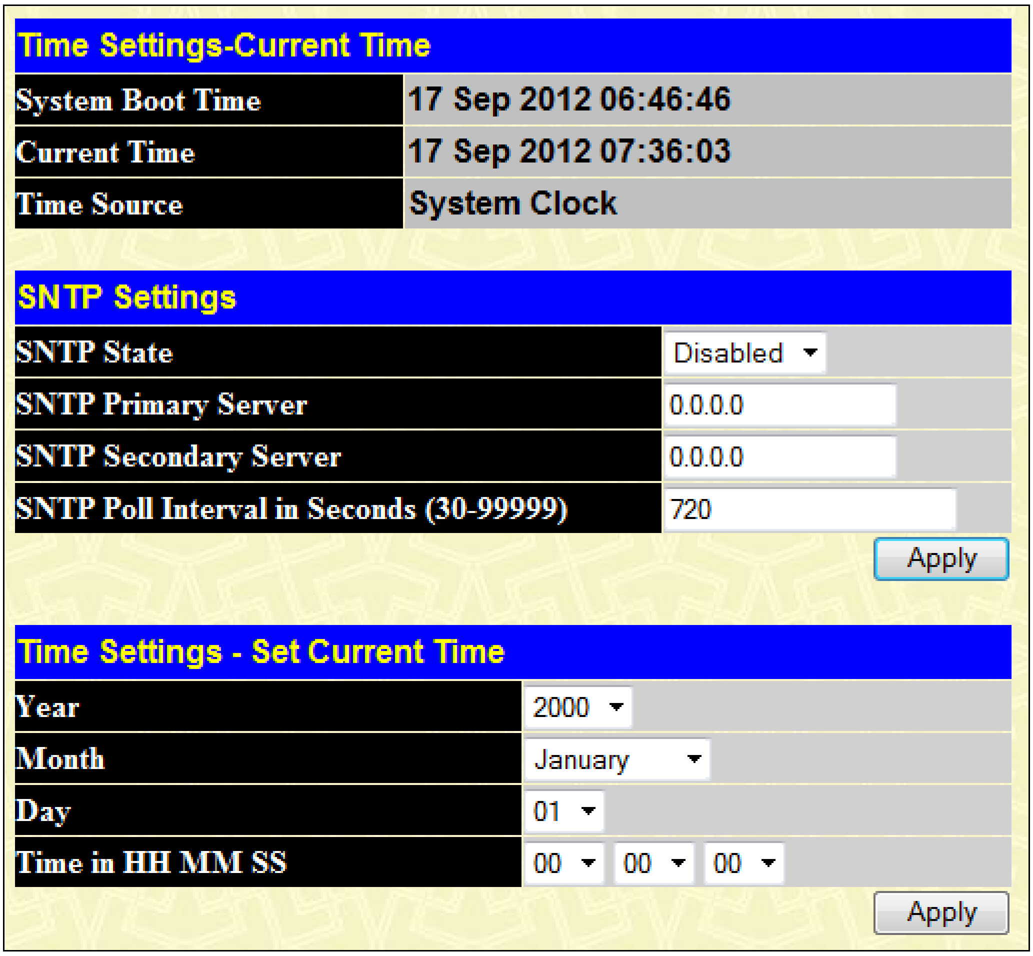
NOTE: When the Switch is undergoing the booting procedure, all configuration commands will not be logged. When the user uses AAA authentication to log in, the user name should not be changed if the user has used the Enable Admin function to replace its privilege.

SNTP Settings

Time Settings

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

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



Time Settings-Current Time

System Boot Time	17 Sep 2012 06:46:46
Current Time	17 Sep 2012 07:36:03
Time Source	System Clock

SNTP Settings

SNTP State	Disabled
SNTP Primary Server	0.0.0.0
SNTP Secondary Server	0.0.0.0
SNTP Poll Interval in Seconds (30-99999)	720

Time Settings - Set Current Time

Year	2000
Month	January
Day	01
Time in HH MM SS	00 00 00

Figure 2- 36. Time Settings window

The following parameters can be set or are displayed:

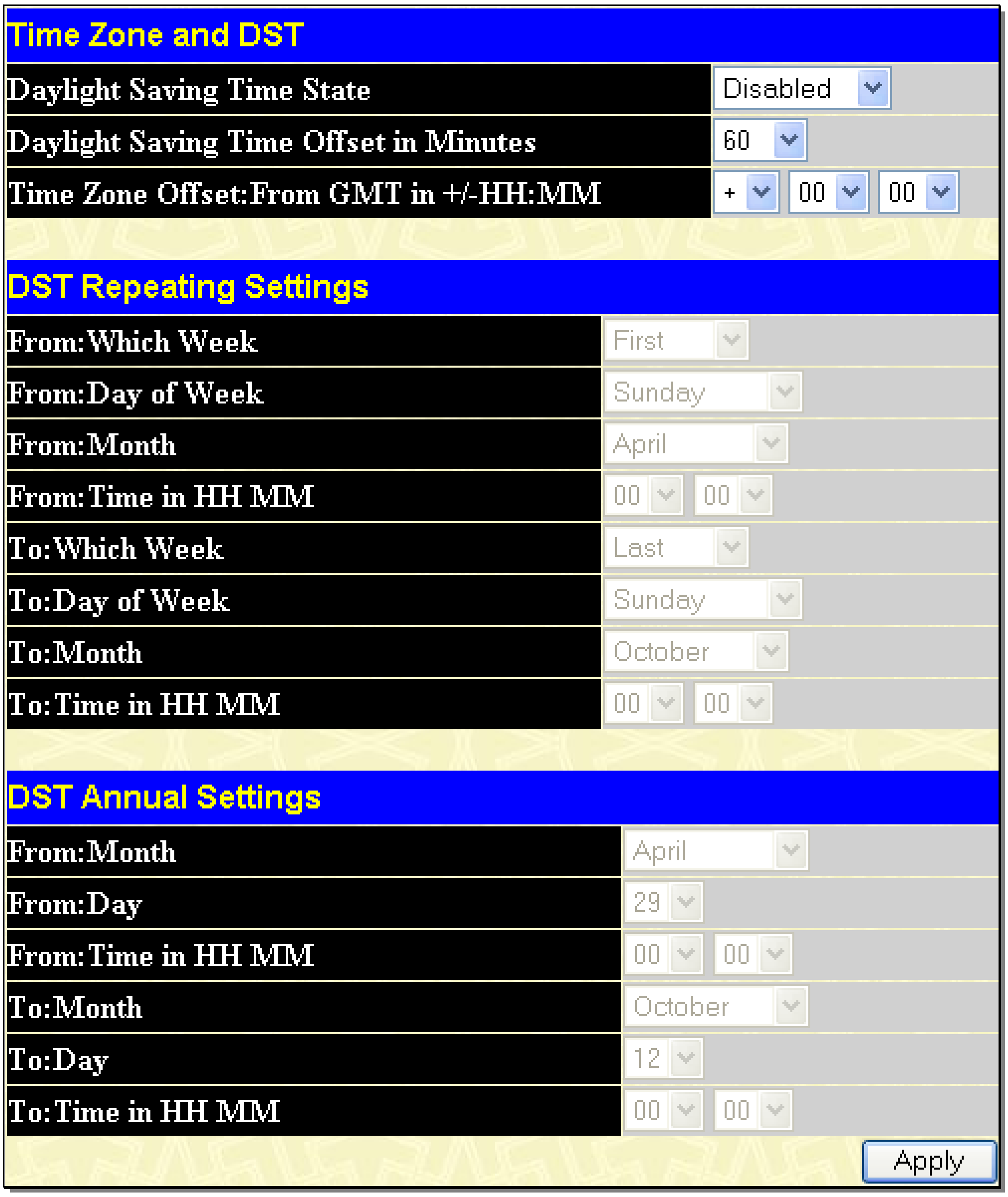
Parameter	Description
Current Time	
System Boot Time	Displays the time when the Switch was initially started for this session.
Current Time	Displays the Current Time set on the Switch.
Time Source	Displays the time source for the system.
SNTP Settings	
SNTP State	Use this pull-down menu to *Enabled* 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 to update the system clock.
Month	Enter the current month to update the system clock.
Day	Enter the current day to update the system clock.
Time in HH MM SS	Enter the current time in hours, minutes, and seconds.

Click **Apply** to implement changes made.

Time Zone and DST

The following are windows used to configure time zones and Daylight Savings time settings for SNTP.

To view this window, click **Administration** > **SNTP Settings** > **Time Zone and DST**, as shown below:



Time Zone and DST

Daylight Saving Time State: Disabled
Daylight Saving Time Offset in Minutes: 60
Time Zone Offset:From GMT in +/-HH:MM: + 00 00

DST Repeating Settings

From:Which Week: First
From:Day of Week: Sunday
From:Month: April
From:Time in HH MM: 00 00
To:Which Week: Last
To:Day of Week: Sunday
To:Month: October
To:Time in HH MM: 00 00

DST Annual Settings

From:Month: April
From:Day: 29
From:Time in HH MM: 00 00
To:Month: October
To:Day: 12
To:Time in HH MM: 00 00

Figure 2- 37. Time Zone and DST window

The following parameters can be set:

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

From: Day of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month that DST will start on.
From: Time in HH MM	Enter the time of day that DST will start on.
To: Which Week	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 of day that 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, click **Admininstration** > **MAC Notification Settings**, as shown.

Global Settings

The following parameters may be viewed and modified:

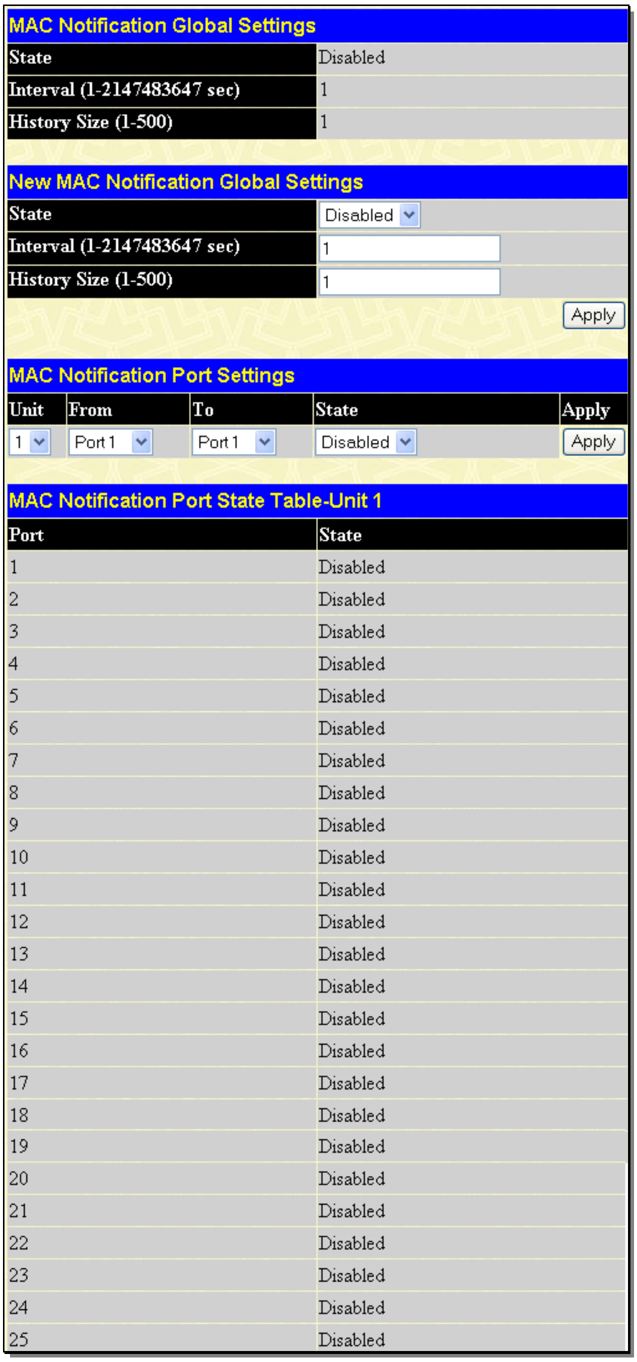
Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval (1-2147483647 sec)	The time in seconds between notifications.
History Size (1-500)	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

Port Settings

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

Parameter	Description
Unit	Select the unit to configure.
From/To	Select a port or group of ports to enable for MAC notification using the pull-down menus.
State	Enable or disable MAC Notification.

Click **Apply** to implement changes made.



MAC Notification Global Settings

State	Disabled
Interval (1-2147483647 sec)	1
History Size (1-500)	1

New MAC Notification Global Settings

State	Disabled
Interval (1-2147483647 sec)	1
History Size (1-500)	1

MAC Notification Port Settings

Unit	From	To	State	Apply
1	Port 1	Port 1	Disabled	Apply

MAC Notification Port State Table-Unit 1

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

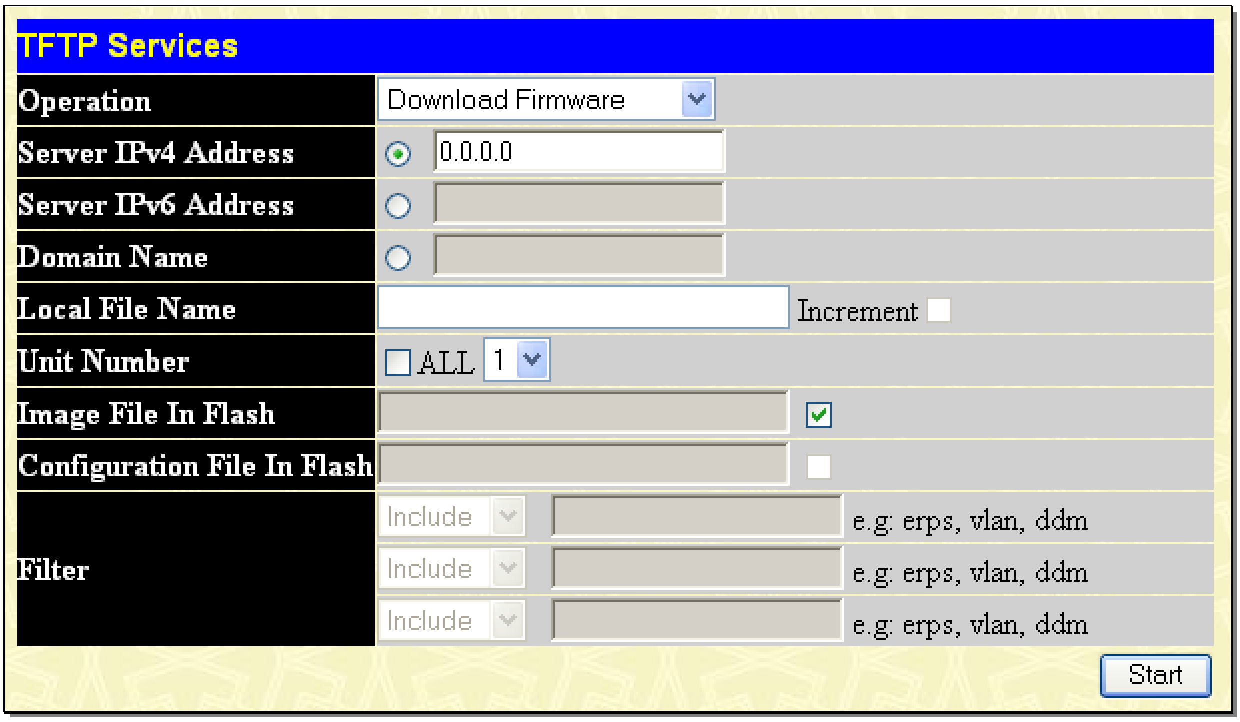
Figure 2- 38. MAC Notification Global Settings window

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.

The user also has the option of transferring firmware and configuration files to and from the internal Flash drive, located on the Switch. Using this window, the user can receive a configuration or firmware file from a TFTP server, or transfer that firmware or configuration file to a TFTP server. More about configuring the internal Flash drive can be found in the next section entitled Flash File Services. 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**, as shown below:



TFTP Services

Operation	Download Firmware ▾	
Server IPv4 Address	● 0.0.0.0	
Server IPv6 Address	○	
Domain Name	○	
Local File Name		Increment □
Unit Number	□ ALL 1 ▾	
Image File In Flash		☑
Configuration File In Flash		□
Filter	Include ▾	e.g: erps, vlan, ddm
	Include ▾	e.g: erps, vlan, ddm
	Include ▾	e.g: erps, vlan, ddm

Figure 2- 39. TFTP Services window

The following parameters can be configured:

Parameter	Description
Operation	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. *Upload Attack Log* - Enter the IP address of the TFTP server and the path and filename for the attack log on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. *Upload Firmware* - Enter the IP address of the TFTP server and the path and filename for the place to put this firmware on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Server IPv4 Address	Enter the IPv4 address of the server from which to upload or download firmware and configuration and upload log.
Server IPv6 Address	Enter the IPv6 address of the server from which to upload or download firmware and configuration and upload log.
Domain Name	Enter the domain name of the TFTP server.
Local File Name	Enter the path and filename of the firmware or configuration file to upload or download, located on the TFTP server.
Unit Number	Select the unit to configure, or tick the ALL check box to select all available units.
Image File in Flash	To select a firmware file from the internal Flash drive to be transferred, or to load a firmware file on to the Flash drive, enter the path and filename here and tick the corresponding check box. Remember, the only path that can be used on the flash is named C:\ (ex. C:\runtime.had)
Configuration File in Flash	To select a configuration file from the internal Flash drive to be transferred, or to load a configuration file on to the Flash drive, enter the path and filename here and tick the corresponding check box. Remember, the only path that can be used on the flash is named C:\ (ex. C:\configuration.had)
Filter	This is used to filter the configuration data that relates to upload configuration.

Click **Start** to initiate the file transfer.

File System Services

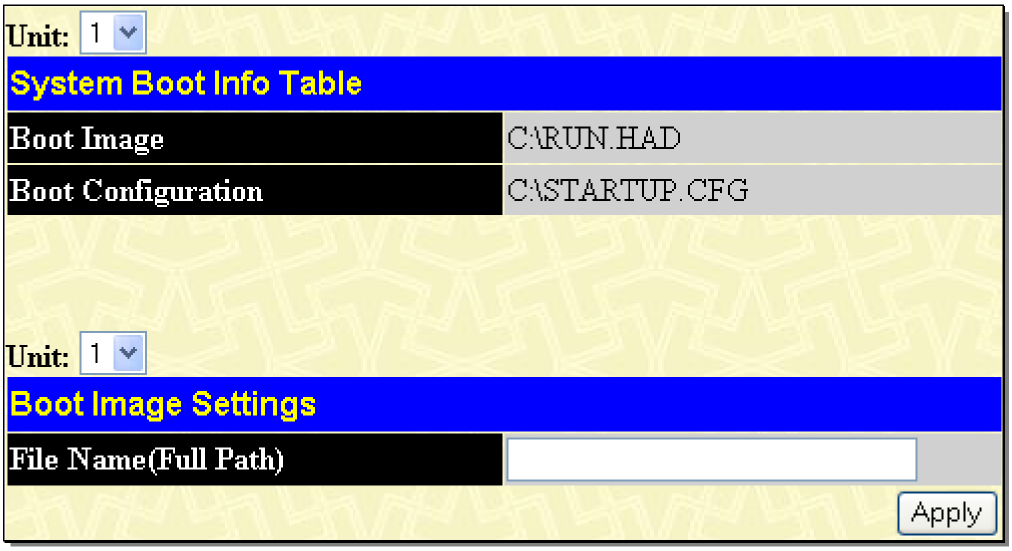
The Switch contains a 15-megabyte Flash memory where the user may store files for further use on the Switch. The user may place over 200 re-nameable files on the FAT 16 mode Flash memory, of which the user has the option of setting firmware images and configuration files as boot up files, upon the next reboot of the Switch.

The Switch automatically assigns default names to the default boot up files located in the flash memory. The default firmware files are named RUN.HAD while the default boot up configuration file is named STARTUP.CFG. After the system has powered up or has been reset, the Switch will check the Flash memory for these files. If no corruption or other problems exist on the Flash, the Switch will use the files set as the boot up files and load them into the Switch. If a problem occurs, the Switch will use the PROM (programmable read-only memory) will provide the FAT 16 re-building function, which will format the Flash as FAT 16 and enter the Z-modem download mode where the user will download firmware, saved as RUN.HAD and then boot from this firmware image. To configure the files located on the Flash memory, use the following windows to guide you.

System Boot Information

This window is used to view and configure boot up firmware images and configuration files. To set a file as a boot up file, enter the file name and path into the File Name field under the Boot Image Settings heading and click **Apply**. The Switch will recognize .HAD files as firmware images and .CFG files as configuration files when being set as the boot up file. Newly configured boot up files will be displayed in the System Boot Info Table.

To view this table, click **Administration > File System Services > System Boot Information**, as shown below:



Unit: 1

System Boot Info Table

Boot Image	C:\RUN.HAD
Boot Configuration	C:\STARTUP.CFG

Unit: 1

Boot Image Settings

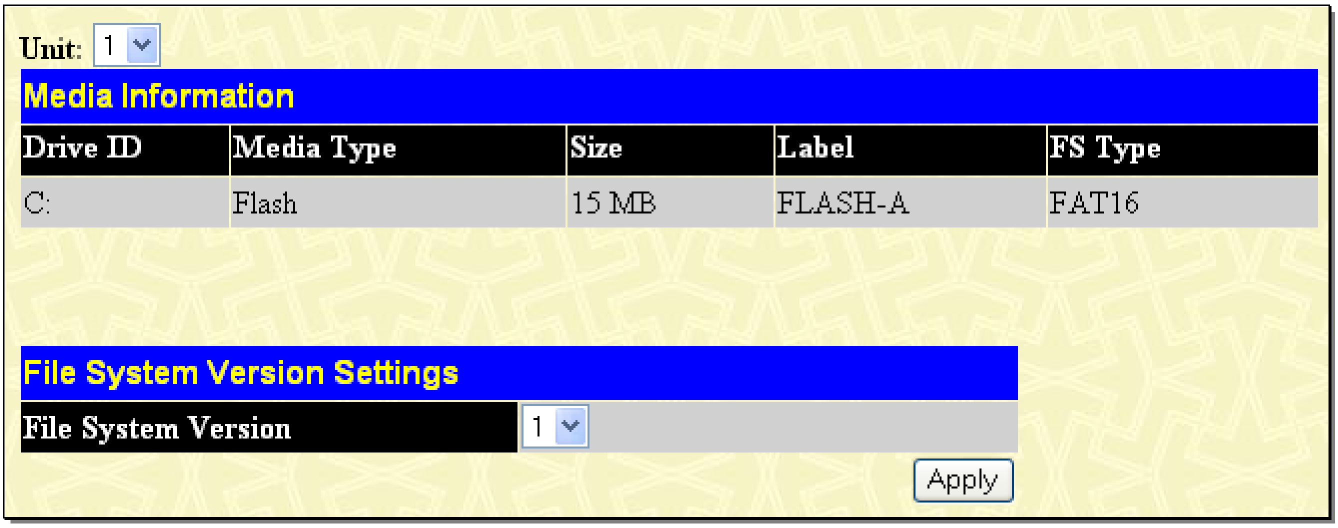
File Name(Full Path):

Figure 2- 40. System Boot Info Table window

FS Information

This window allows users to view the settings of the Flash Drive in the Switch. This information is read-only and is just a description of the internal Flash memory.

To view this window, click **Administration** > **File System Services** > **FS Information**, as shown below:



Unit: 1

Media Information

Drive ID	Media Type	Size	Label	FS Type
C:	Flash	15 MB	FLASH-A	FAT16

File System Version Settings

File System Version: 1

Figure 2- 41. Media Information window

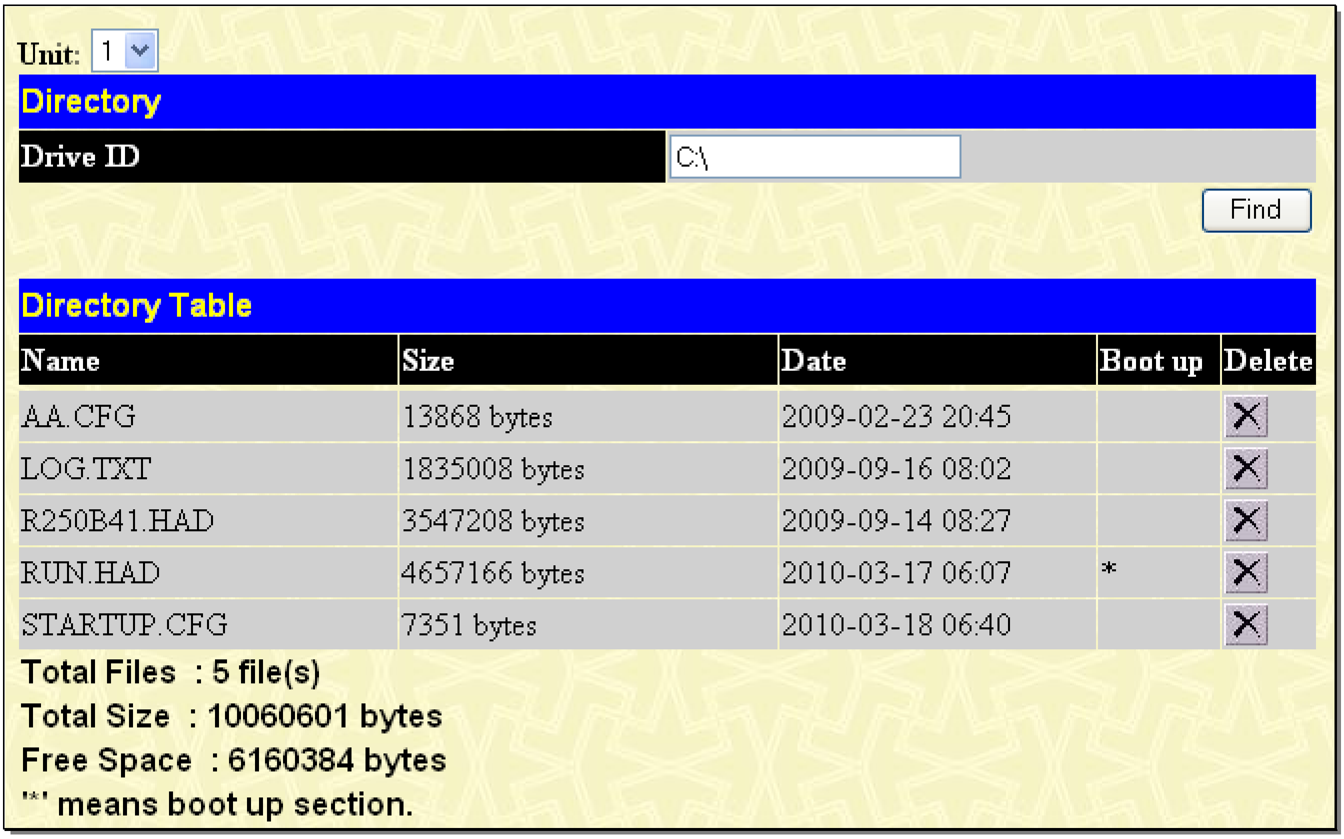
This window offers the following information about the internal Flash drive.

Parameter	Description
Drive ID	The name of the drive of the memory. There is only one drive in the Flash and it is named C:.
Media Type	The type of storage media present in this Switch, which is a Flash memory system.
Size	Denotes the size of the flash memory, which is 15 megabytes.
Label	The label that has been factory set for this Flash memory.
FS Type	The type of File System present in the Switch. For this release, only a FAT16 file system is used in the Switch.
File System Version	Use the drop- down menu to select the File System version to use on the Switch.

Directory

This window allows users to view files stored in the flash memory of the Switch. In future releases, more than one drive may be located in the Flash drive, but for this release, the only drive located on the Flash memory of the Switch is C:. Therefore, to view files located on C:, the user should enter *C:* into the Drive ID field and click **Find**. Saved files will appear in the Directory table. This window will also display the total number of files (Total Files), the amount of free bytes left (Total free size), and the amount of memory space used for normal running of the Switch (System reserved flash size).

To view this window, click **Administration** > **File System Services** > **Directory**, as shown below:



Unit: 1

Directory

Drive ID: C:\

Directory Table

Name	Size	Date	Boot up	Delete
AA.CFG	13868 bytes	2009-02-23 20:45		☒
LOG.TXT	1835008 bytes	2009-09-16 08:02		☒
R250B41.HAD	3547208 bytes	2009-09-14 08:27		☒
RUN.HAD	4657166 bytes	2010-03-17 06:07	*	☒
STARTUP.CFG	7351 bytes	2010-03-18 06:40		☒

Total Files : 5 file(s)
Total Size : 10060601 bytes
Free Space : 6160384 bytes
'*' means boot up section.

Figure 2- 42. Directory window

The previous window contains the following information:

Parameter	Description
Unit	Use the drop down menu to select the unit you wish to configure.
Drive ID	Enter the name of the drive located on the Flash memory. There is only one drive in the Flash and it is named *C:\*.
Name	Denotes the name of the file located on the Switch's Flash memory. The default firmware image is called RUN.HAD, while the default configuration file is specified as STARTUP.CFG.
Size	Denotes the size of the save file, in bytes.
Date	Displays the date that the file was loaded onto the Switch.
Boot up	An '*' in this field denotes that the corresponding file is a boot up configuration file or firmware image.
Delete	Click the ☒ in this field corresponding to the file to be deleted from the Flash memory. Remember, once deleted, it cannot be restored by the switch unless downloaded again from an outside source.

Rename

The following window is used to rename files that are presently located in the Flash memory of the Switch. To rename a file, simply type the path and name of the current file (ex. c:/triton) into the Old File Name field, and then the new file and path into the New File Name field and click **Apply**. Remember, the path must be included in both fields, which is c:/ on this Switch. Users may return to the **Directory** window to view changes made in the file names.

To view this window, click **Administration** > **File System Services** > **Rename**, as shown below:

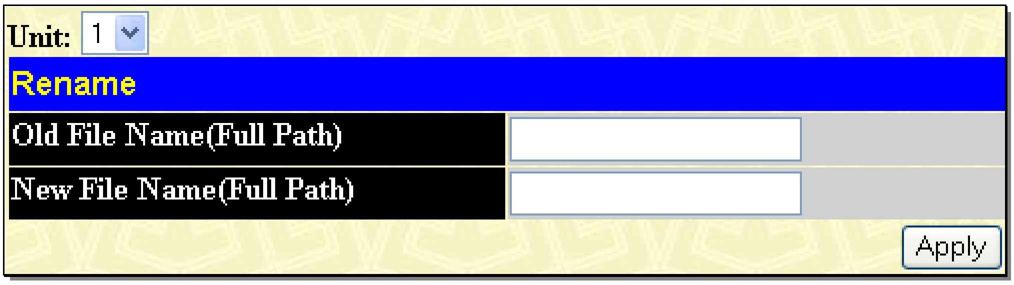


Figure 2- 43. Rename window

Copy

This window is used to copy a directory located within the Flash memory of the switch.

To view this window, click **Administration** > **File System Services** > **Copy**, as shown below:

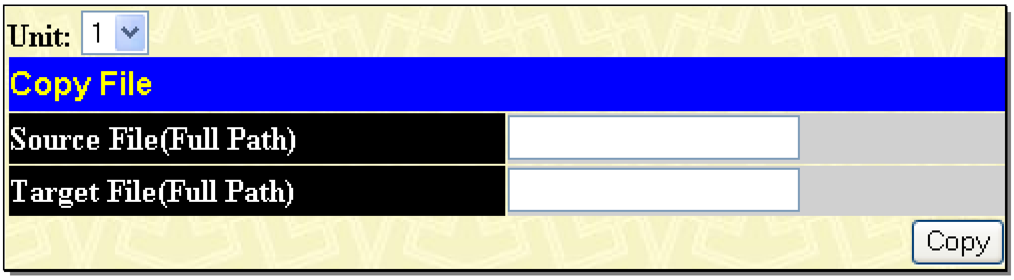


Figure 2- 44. Copy File window

This window offers the following fields to aid the user in copying files located in the Flash memory of the Switch.

Parameter	Description
Unit	Use the drop down menu to select the unit you wish to configure.
Source File (Full Path)	Enter the full path and file name of the directory to be copied. This entry cannot exceed 64 characters in length.
Target File (Full Path)	Enter the file name of the directory and the path to place the copy. This entry cannot exceed 64 characters in length.

Click **Copy** to initiate copying the file.

RCP

RCP (Remote Copy Protocol) is a UNIX Remote Shell service which allows files to be copied between a server and client. RCP is an application that operates above the TCP protocols, and uses port number 514 as the TCP destination port.

The RCP application uses client server architecture and the client can be any machine running the RCP client application.

A Switch that supports the RCP client allows users to copy firmware images, configurations and log files between the Switch and RCP Server.

Switches that do not support a file system should still be able to run an RCP client to copy firmware images, configurations and logs between the switch and RCP server.

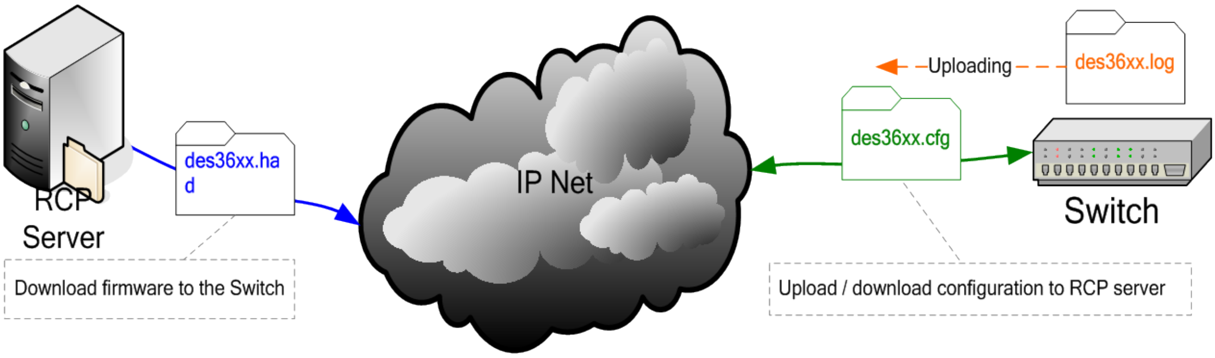

RCP Server
des36xx.had
Download firmware to the Switch
IP Net
Uploading
des36xx.log
des36xx.cfg
Switch
Upload / download configuration to RCP server

Figure 2- 45. Remote Copy Protocol between an RCP server and an Ethernet Switch

As illustrated in Figure 2 - 49, a user can:

a) Upload a configuration file from the Switch to the RCP Server.

b) Download a firmware file from the RCP Server to the Switch.

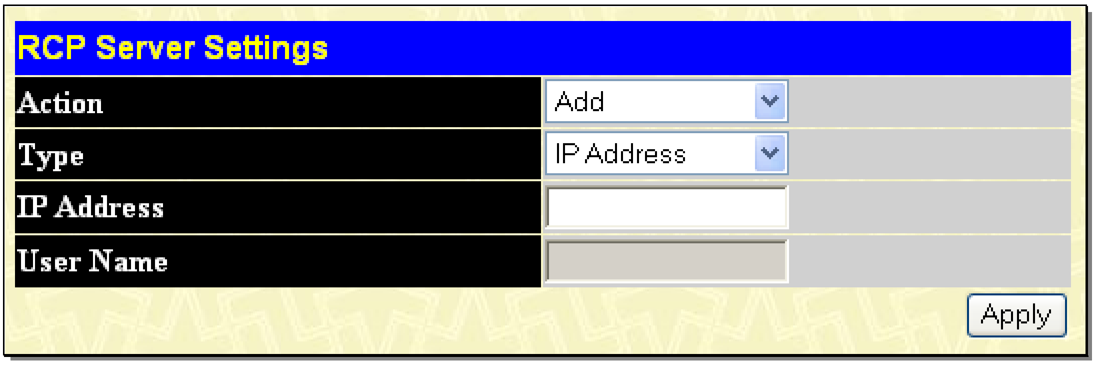
c) Upload the Log file from the Switch to the RCP Server.

d) Download the configuration file from the RCP Server to the Switch.

RCP Server Settings

This window is used to configure global RCP server information. This global RCP server setting can be used when the server or remote user name is not specified. Only one RCP server can be configured for each system.

To view this window, click **Administration** > **RCP > RCP Server Settings**, as shown below:



RCP Server Settings

Action	Add
Type	IP Address
IP Address	
User Name	

Figure 2- 46. RCP Server Settings window

The following parameters can be configured:

Parameter	Description
Action	Toggle the action between *Add* and *Clear*.

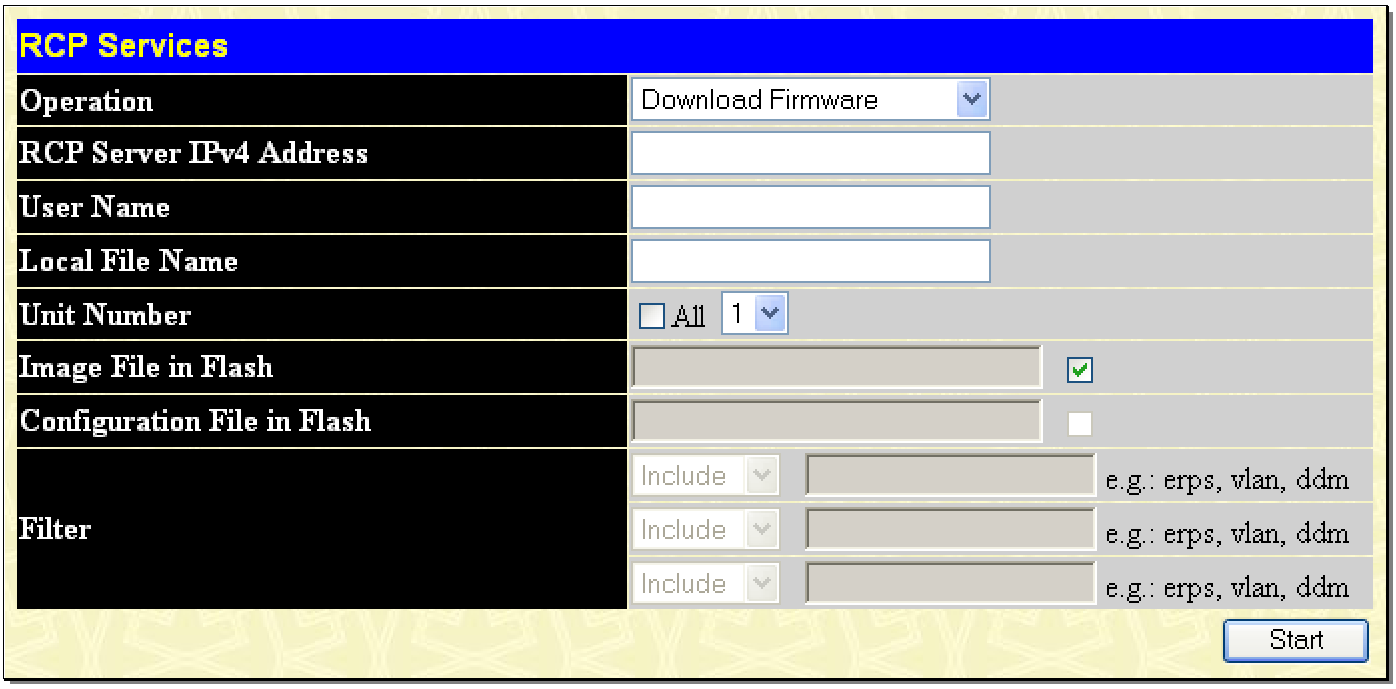
Type	Select to enter the information in IP Address and/or User Name fields. Available options are *IP Address*, *User Name* and *Both*.
IP Address	Enter the IP address of the global RCP server.
User Name	Enter the remote user name.

Click **Apply** to implement the changes.

RCP Services

This window is use to configure the services that provided by the RCP server.

To view this window, click **Administration** > **RCP > RCP Services**, as shown below:



RCP Services

Operation	Download Firmware	
RCP Server IPv4 Address		
User Name		
Local File Name		
Unit Number	□ All 1	
Image File in Flash		☑
Configuration File in Flash		□
Filter	Include	e.g.: erps, vlan, ddm
	Include	e.g.: erps, vlan, ddm
	Include	e.g.: erps, vlan, ddm

Figure 2- 47. RCP Services window

The following parameters can be configured:

Parameter	Description
Operation	Use the pull-down menu to select the method for copying files. Options are *Download Firmware*, *Download Configuration*, *Upload Configuration*, *Upload Log*, *Upload Attack Log* and *Upload Firmware*.
RCP Server IPv4 Address	Enter the IP address of the RCP Server.
User Name	Enter the remote user name on the RCP server.
Local File Name	Enter the file name in the field. Tick the Increment, and the existing configuration will not be cleared before applying the new configuration.
Unit Number	Select the switch in the switch stack from which, or to which to upload or download files. Tick the ALL check box to denote all switches in the switch stack.
Image ID	Use the pull-down menu to select the Image file ID.
Configuration ID	Use the pull-down menu to select the configuration file ID.
Filter	Use to filter configuration data.related to upload configuration.

Click **Apply** to implement the changes.

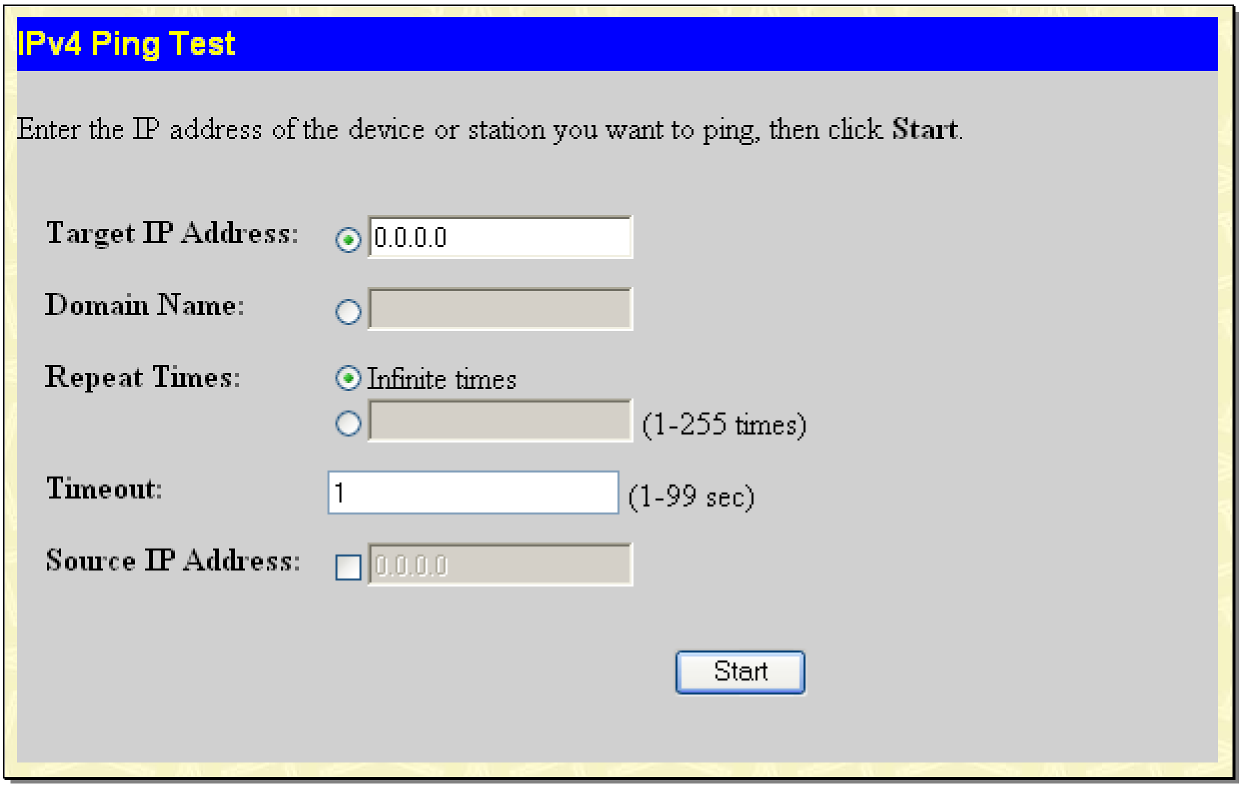
Ping Test

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.

IPv4 Ping Test

The following window is used to Ping an IPv4 address.

To view this window, click **Administration** > **Ping Test** > **IPv4 Ping Test**, as shown below:



IPv4 Ping Test

Enter the IP address of the device or station you want to ping, then click **Start**.

Target IP Address: ● 0.0.0.0

Domain Name: ○

Repeat Times: ● Infinite times ○ (1-255 times)

Timeout: 1 (1-99 sec)

Source IP Address: □ 0.0.0.0

Figure 2- 48. IPv4 Ping Test window

This window allows the following parameters to be configured to ping an IPv4 address.

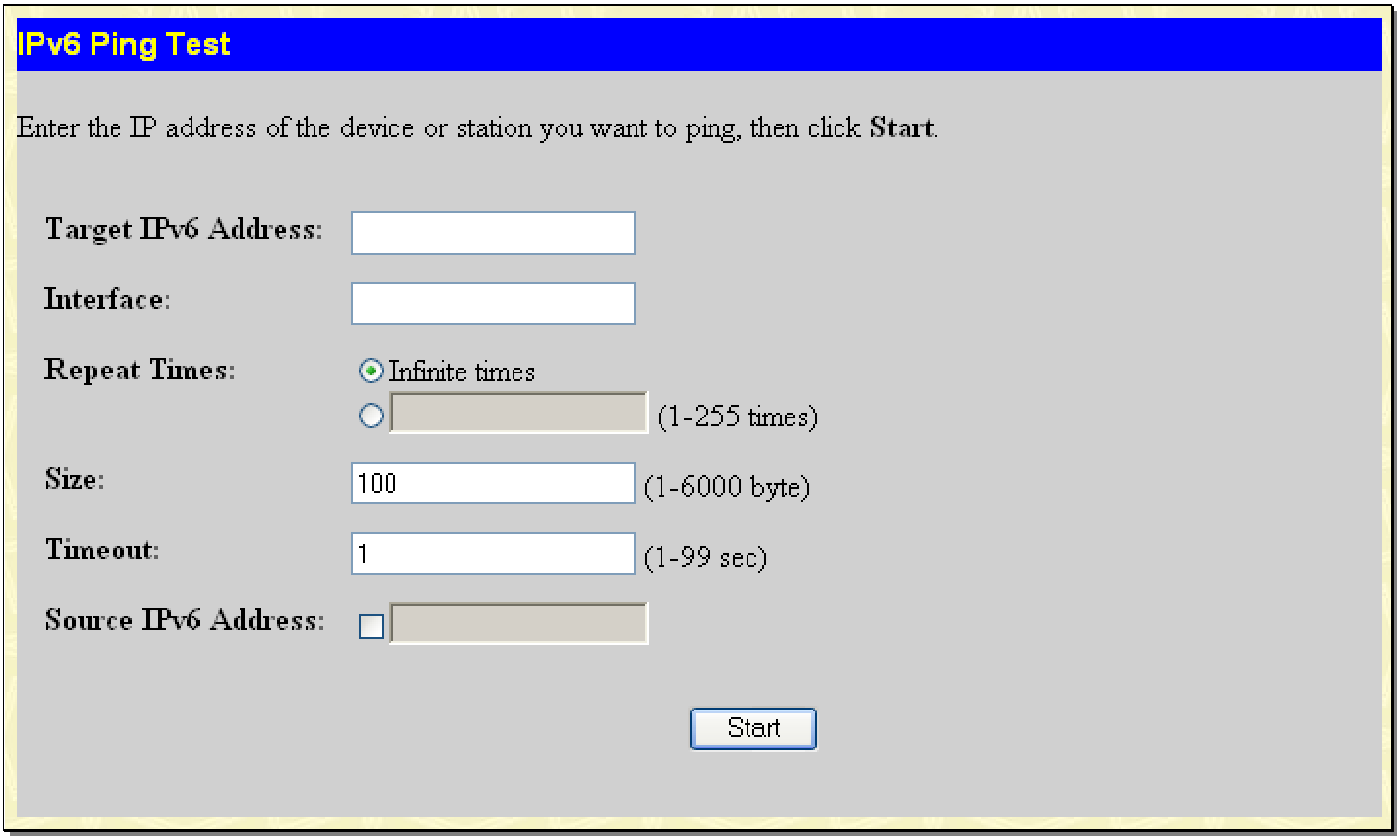
Parameter	Description
Target IP Address	Enter an IPv4 address to be pinged.
Domain Name	Enter the domain name of the host.
Repeat Times	Either click the Infinite times radio button or enter the number of times to attempt to ping the IPv4 address configured in this window. Users may enter a number between *1* and *255*.
Timeout	Select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. If the packet fails to find the IPv4 address in this specified time, the Ping packet will be dropped.
Source IP Address	Tick the check box and enter the source IP address of the ping packets. If specified, this IP address will be used as the packets' source IP address that ping sends to the remote host.

Click **Start** to initialize the Ping program.

IPv6 Ping Test

The following window is used to Ping an IPv6 address.

To view this window, click **Administration** > **Ping Test** > **IPv6 Ping Test**, as shown below:



IPv6 Ping Test

Enter the IP address of the device or station you want to ping, then click **Start**.

Target IPv6 Address:

Interface:

Repeat Times: ● Infinite times ○ (1-255 times)

Size: 100 (1-6000 byte)

Timeout: 1 (1-99 sec)

Source IPv6 Address: □

Figure 2- 49. IPv6 Ping Test window

This window allows the following parameters to be configured to ping an IPv6 address.

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Interface	The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For global IPv6 addresses, this field may be omitted.
Repeat Times	Enter the number of times desired to attempt to ping the IPv6 address configured in this window. Users may enter a number of times between *1*and *255*.
Size	Use this field to set the datagram size of the packet, or in essence, the number of bytes in each ping packet. Users may set a size between *1* and *6000* bytes. The default setting is *100* bytes.
Timeout	Select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
Source IPv6 Address	Tick the check box and enter the source IPv6 address of the ping packets. If specified, the IPv6 address will be used as the packets' source IPv6 address that ping6 sends to the remote host.

Click **Start** to initialize the Ping program.

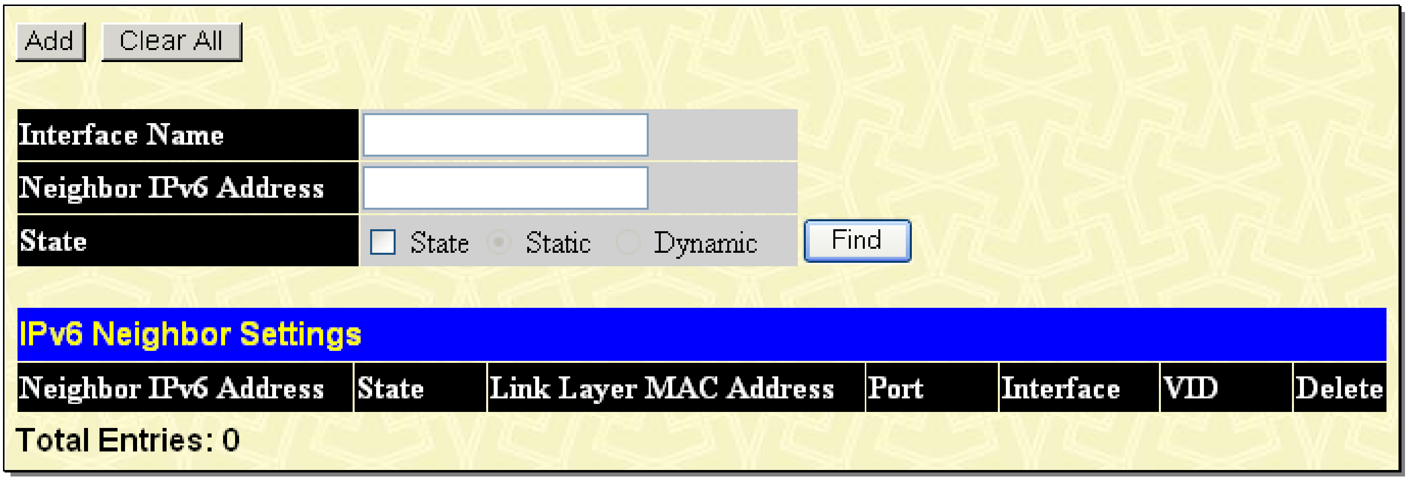
IPv6 Neighbor

IPv6 neighbors are devices on the link-local network that have been detected as being IPv6 devices. These devices can forward packets and keep track of the reachability of routers, as well as if changes occur within link-layer addresses of nodes on the network or if identical unicast addresses are present on the local link. The following two windows are used to view IPv6 neighbors, and add or delete them from the Neighbor cache.

IPv6 Neighbor Settings

The following window is used to view and configure current IPv6 neighbors of the Switch.

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



Interface Name	
Neighbor IPv6 Address	
State	□ State ● Static ○ Dynamic

IPv6 Neighbor Settings

Neighbor IPv6 Address	State	Link Layer MAC Address	Port	Interface	VID	Delete

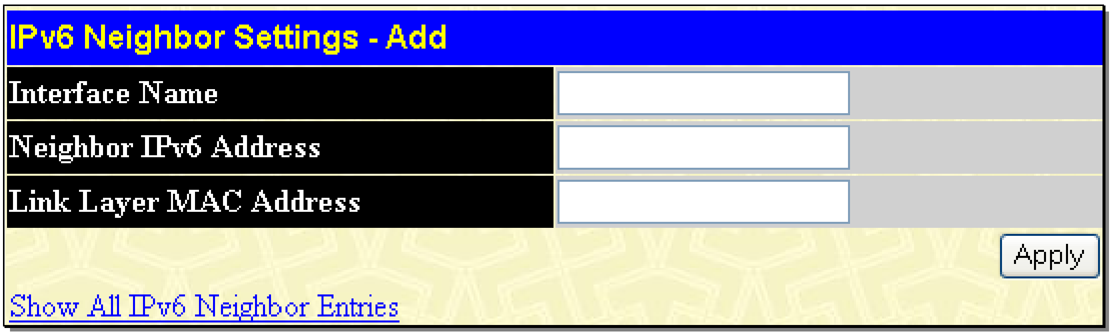
Total Entries: 0

Figure 2- 50. IPv6 Neighbor Settings window

The following fields can be viewed or configured:

Parameter	Description
Interface Name	Enter the Interface Name of the device for which to search IPv6 neighbors. Click **Find** to begin the search.
Neighbor IPv6 Address	Enter the IPv6 address of the neighbor of the IPv6 device to be searched. Click **Find** to begin the search.
State	Users may also search by running state of the IPv6 neighbor. Tick the State check box and choose to search for Static IPv6 neighbors or Dynamic IPv6 neighbors. Click **Find** to begin the search.
Neighbor IPv6 Address	Displays the IPv6 address of the neighbor device.
State	Displays the running state of the corresponding IPv6 neighbor. The user may see six possible entries in this field, which are Incomplete, Stale, Probe, Reachable, Delay, or Static.
Link Layer MAC Address	Displays the MAC address of the corresponding IPv6 device.
Port	Displays which port learned the IPv6 address of the neighbor device.
Interface	Displays the interface name associated with this IPv6 address.
VID	Displays which VLAN learned the IPv6 address of the neighbor device.

To remove any entry, click the corresponding ☒ button in the Delete column. To completely clear the IPv6 Neighbor Settings, click the **Clear All** button. To add a new entry, click the **Add** button, revealing the following window to configure:


IPv6 Neighbor Settings - Add

Interface Name	
Neighbor IPv6 Address	
Link Layer MAC Address	

Figure 2- 51. IPv6 Neighbor Settings – Add window

The following fields can be set or viewed:

Parameter	Description
Interface Name	Enter the name of the Interface associated with this entry, if any.

Neighbor IPv6 Address	The IPv6 address of the neighbor entry. Specify the address using the hexadecimal IPv6 Address (IPv6 Address is hexadecimal number, for example 1234::5D7F).
Link Layer MAC Address	The MAC address of the IPv6 neighbor entry.

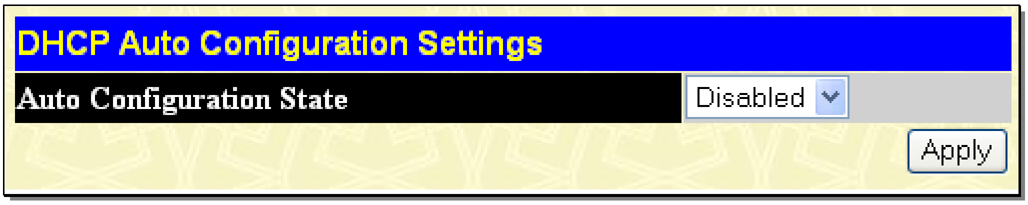
After entering the IPv6 Address and MAC Address of the Static IPv6 Neighbor entry, click **Apply** to implement the new entry. To return to the **IPv6 Neighbor Settings** window, click the Show All IPv6 Neighbor Entries link.

DHCP Auto Configuration Settings

This window is used to enable the DHCP Autoconfiguration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot up. To employ this method, 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 up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the Upload screen description located in the Maintenance section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.

To view this window, click **Administration > DHCP Auto Configuration Settings**, as shown below:


DHCP Auto Configuration Settings

Auto Configuration State: Disabled

Figure 2- 52. DHCP Auto Configuration Settings window

To enable the **DHCP Auto Configuration State**, use the pull-down menu to choose Enabled and click the **Apply** button.

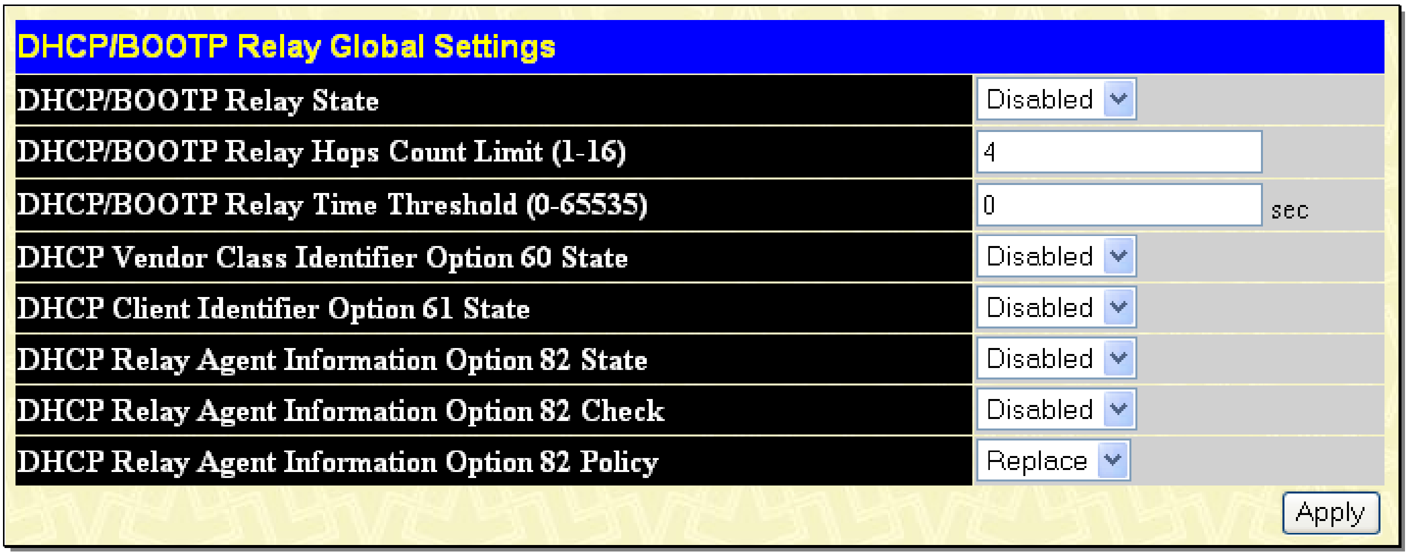
DHCP/BOOTP Relay

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

DHCP / BOOTP Relay Global Settings

This table is used to enable and configure DHCP/BOOTP Relay global settings on the Switch.

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



DHCP/BOOTP Relay Global Settings

DHCP/BOOTP Relay State	Disabled
DHCP/BOOTP Relay Hops Count Limit (1-16)	4
DHCP/BOOTP Relay Time Threshold (0-65535)	0 sec
DHCP Vendor Class Identifier Option 60 State	Disabled
DHCP Client Identifier Option 61 State	Disabled
DHCP Relay Agent Information Option 82 State	Disabled
DHCP Relay Agent Information Option 82 Check	Disabled
DHCP Relay Agent Information Option 82 Policy	Replace

Figure 2- 53. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
DHCP/BOOTP Relay State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is *Disabled*
DHCP/BOOTP Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is *4*.
DHCP/BOOTP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP/BOOTP packet. If a value of 0 is entered, the Switch will not process the value in the seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.
DHCP Vendor Class Identifier Option 60 State	This function can enable or disable the DHCP Vendor class identifier option 60 state. When option 60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 60 or per IPIF configured servers. If the relay servers are determined based on option 60, then the IPIF configured servers will be ignored. If the relay servers are not determined by option 60 then the IPIF configured servers will be used to determine the relay servers.
DHCP Client Identifier Option 61 State	This function can enable or disable the DHCP Client identifier option 61 state. When option 61 State is *Enabled*, if the packet does not have option 61, then the relay servers cannot be determined based on option 61. The relay servers will be determined based on option 61

	and the IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then IPIF configured servers will be used to determine the relay servers.
DHCP Relay Agent Information Option 82 State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is *Disabled.* *Enabled* – When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *Disabled*- If the field is toggled to *Disabled* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field. *Enabled* – When the field is toggled to *Enable*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *Disabled*- When the field is toggled to *Disabled*, the relay agent will not check the validity of the packet's option 82 field.
DHCP Relay Agent Information Option 82 Policy	This field can be toggled between *Replace, Drop,* and *Keep* by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Agent Information Option 82 Check is set to *Disabled*. The default is *Replace.* *Replace* - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* - The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.

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

NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, it is possible to 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 can configure the action that the Switch takes when it receives a packet with existing option-82 information by configuring the DHCP Agent Information Option 82 Policy.

The Implementation of DHCP Information Option 82

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

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

Circuit ID sub-option format:

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

a. Sub-option type

b. Length

c. Circuit ID type

d. Length

e. VLAN: the incoming VLAN ID of DHCP client packet.

f. Module: For a standalone switch, the Module is always 0; For a stackable switch, the Module is the Unit ID.

g. Port: The incoming port number of DHCP client packet, port number starts from 1.

Remote ID sub-option format:

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

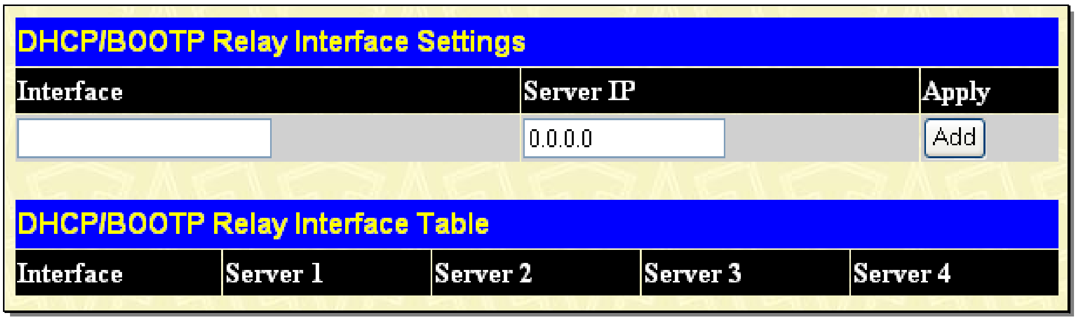
1. Sub-option type
2. Length
3. Remote ID type
4. Length
5. MAC address: The Switch’s system MAC address.

Figure 2- 54. Circuit ID and Remote ID Sub-option Format

DHCP/BOOTP Relay Interface Settings

This window allows the user to set up a server, by IP address, for relaying DHCP/ BOOTP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP client using the following window. Properly configured settings will be displayed in the 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.

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



DHCP/BOOTP Relay Interface Settings

Interface	Server IP	Apply
	0.0.0.0	Add

DHCP/BOOTP Relay Interface Table

Interface	Server 1	Server 2	Server 3	Server 4

Figure 2- 55. DHCP/BOOTP Relay Interface Settings window

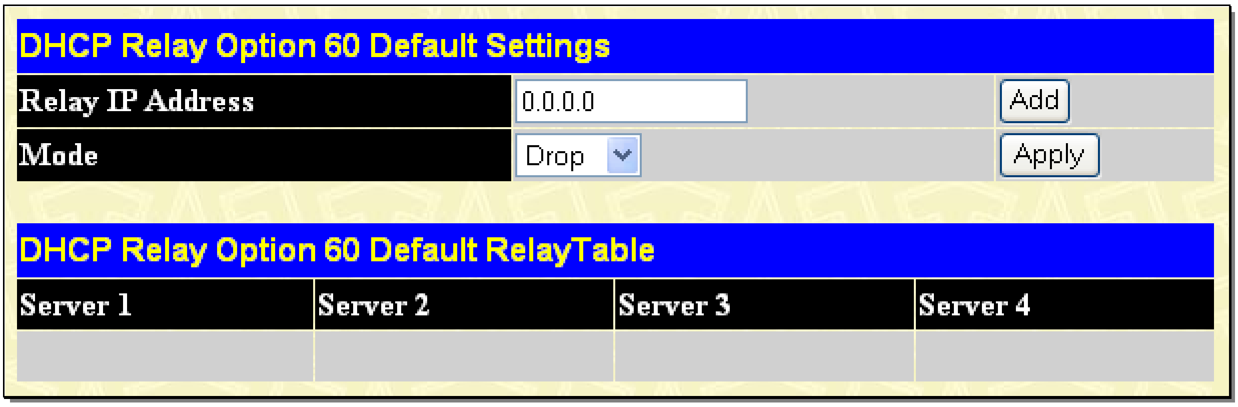
The following parameters may be configured or viewed.

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

DHCP Relay Option 60 Default Settings

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

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



DHCP Relay Option 60 Default Settings

Relay IP Address: 0.0.0.0

Mode: Drop

DHCP Relay Option 60 Default RelayTable

Server 1	Server 2	Server 3	Server 4

Figure 2- 56. DHCP Relay Option 60 Default Settings window

The following parameters can be configured:

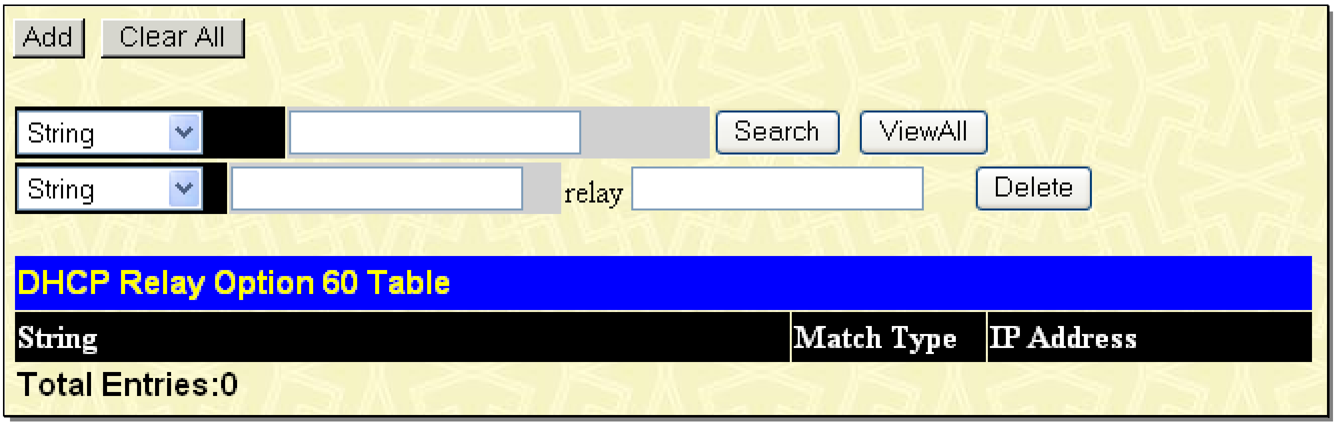
Parameter	Description
Relay IP Address	Enter the specified IP address for the DHCP relay forward.
Mode	Use the pull-down menu to choose either *Relay* or *Drop*. When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet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

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

DHCP Relay Option 60 Settings

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

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



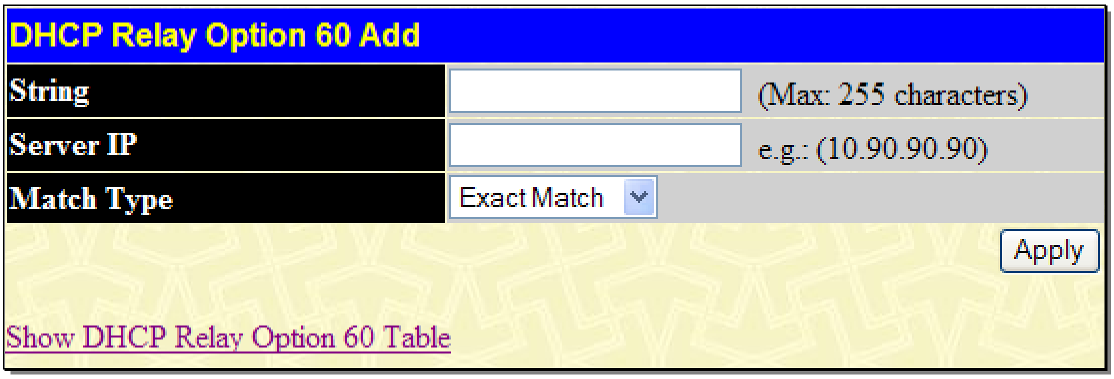
DHCP Relay Option 60 Table

String	Match Type	IP Address

Total Entries:0

Figure 2- 57. DHCP Relay Option 60 Settings window

To find a particular entry, enter the correct IP Address or String and click **Search**. Click the **View All** button to see all the entries in the table at the bottom half of the window. To delete an entry, select it and click **Delete**. To delete all the entries, click **Clear All**. To add a new entry click **Add** the following window will appear:



DHCP Relay Option 60 Add

String		(Max: 255 characters)
Server IP		e.g.: (10.90.90.90)
Match Type	Exact Match	

Show DHCP Relay Option 60 Table

Figure 2- 58. DHCP Relay Option 60 Add window

The following parameters may be configured:

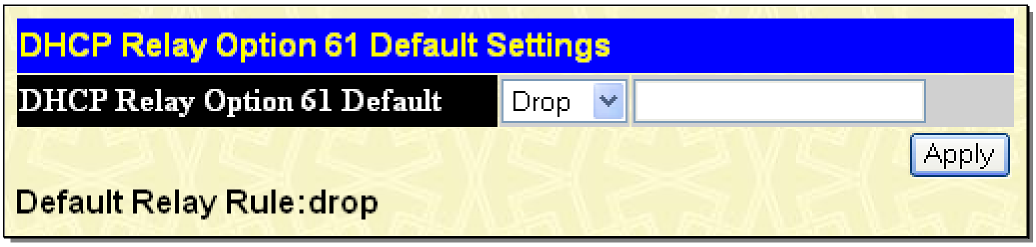
Parameter	Description
String	Enter the specified string, up to a maximum of 255 alphanumeric characters.
Server IP	Enter the relay server IP address.
Match Type	Use the drop-down menu to select either *Exact Match* or *Partial Match*. *Exact Match* – The option 60 string in the packet must fully match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

Click **Apply** to implement the changes. To return to the DHCP Relay Option 60 Table window, click the Show DHCP Relay Option 60 Table link.

DHCP Relay Option 61 Default Settings

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

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



DHCP Relay Option 61 Default Settings

DHCP Relay Option 61 Default: Drop

Default Relay Rule:drop

Figure 2- 59. DHCP Relay Option 61 Default Settings window

The following parameters can be configured:

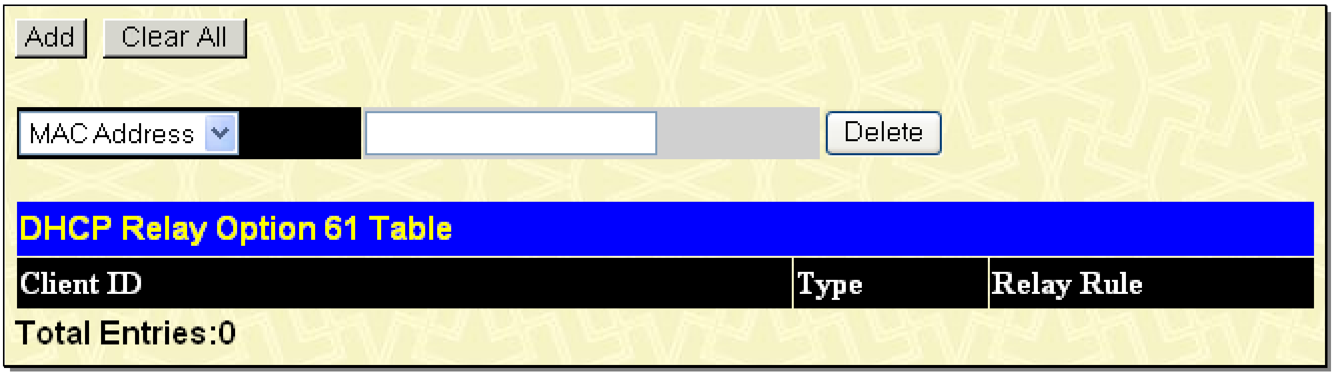
Parameter	Description
DHCP Relay Option 61 Default	Use the pull-down menu to choose either *Relay* or *Drop*. When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules. Enter the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

Click **Apply** to implement the changes.

DHCP Relay Option 61 Settings

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

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



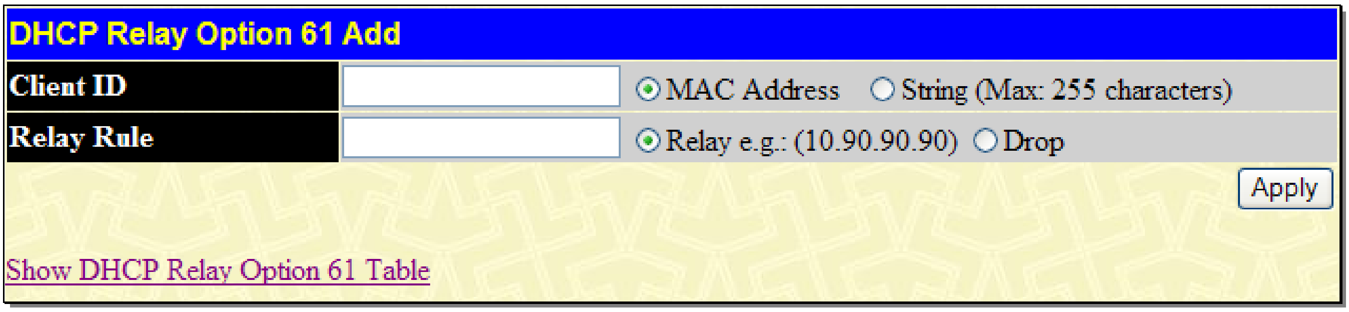
DHCP Relay Option 61 Table

Client ID	Type	Relay Rule

Total Entries:0

Figure 2- 60. DHCP Relay Option 61 Settings window

To remove an entry, enter the appropriate *MAC Address* or *String* information and click **Delete**. To delete all entries click **Clear All**. To add a new entry click **Add** the following window will appear.



DHCP Relay Option 61 Add

Client ID		● MAC Address ○ String (Max: 255 characters)
Relay Rule		● Relay e.g.: (10.90.90.90) ○ Drop

Figure 2- 61. DHCP Relay Option 61 Add window

The following parameters can be configured:

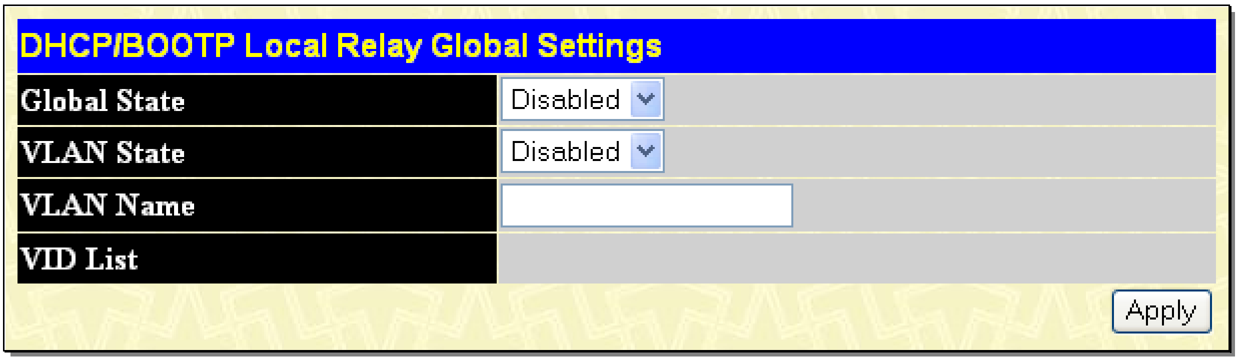
Parameter	Description
Client ID	Use the radio button to select the method of identification for the Client ID either MAC Address or String. The MAC Address will specify the hardware address of the client and the String will specify the client ID. Choose a method and enter the appropriate information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

Click **Apply** to implement the changes.

DHCP/BOOTP Local Relay Settings

This window is used to configure the global settings of DHCP/BOOTP local relay.

To view this window, click **Administration** > **DHCP/BOOTP Local Relay Settings**, as shown below:



DHCP/BOOTP Local Relay Global Settings

Global State	Disabled
VLAN State	Disabled
VLAN Name	
VID List	

Figure 2- 62. DHCP/BOOTP Local Relay Global Settings window

The following parameters are displayed or can be configured:

Parameter	Description
Global State	Use the pull-down menu to enable or disable the status.
VLAN State	Use the pull-down menu to enable or disable the VLAN status.
VLAN Name	Enter the name of VLAN.
VID List	Display the VLAN list.

Click **Apply** to implement the changes.

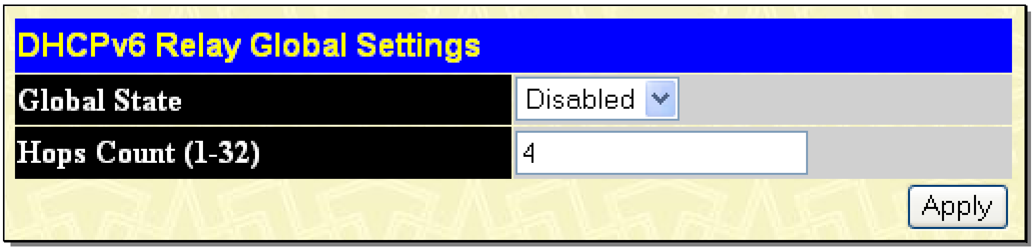
DHCPv6 Relay

This section contains information for configuring DHCPv6 relay, including DHCP v6 Relay Global Settings and DHCPv6 Relay Interface Settings.

DHCPv6 Relay Global Settings

This window is used to set up the DHCPv6 relay global status.

To view this window, click **Administration** > **DHCPv6 Relay** > **DHCPv6 Relay Global Settings**, as shown below:



DHCPv6 Relay Global Settings

Global State	Disabled
Hops Count (1-32)	4

Figure 2- 63. DHCPv6 Relay Global Settings window

The following fields can be configured:

Parameter	Description
Global State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCPv6 Relay service on the Switch. The default is *Disabled*.

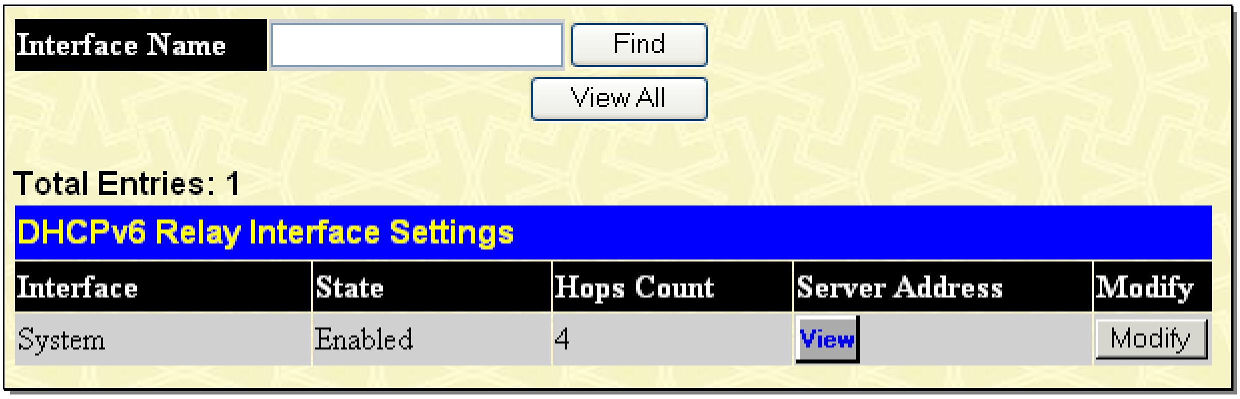
Hops Count (1-32)	This field allows an entry between *1* and *32* to define the maximum number of router hops DHCPv6 messages can be forwarded across. The default hop count is *4*.

Click **Apply** to implement the changes.

DHCPv6 Relay Interface Settings

This window displays the current DHCPv6 relay configurations.

To view this window, click **Administration > DHCPv6 Relay** > **DHCPv6 Relay Interface Settings**, as shown below:



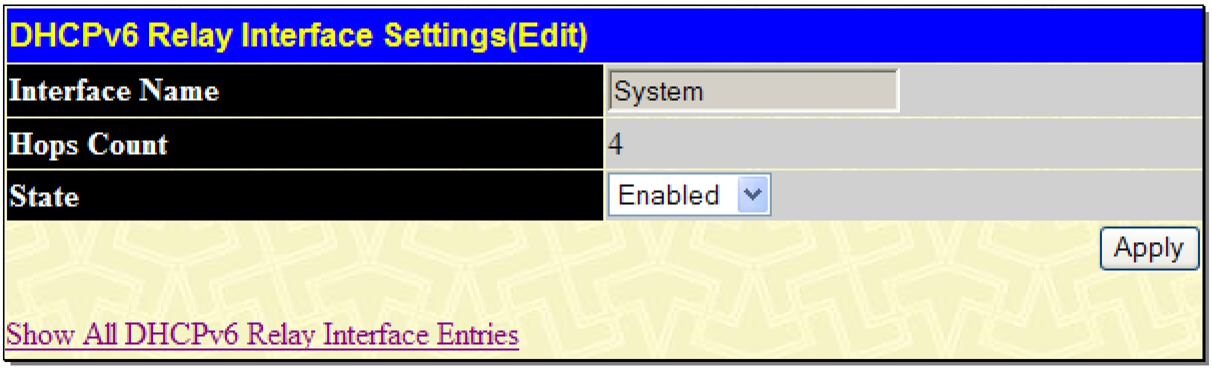
Total Entries: 1

DHCPv6 Relay Interface Settings

Interface	State	Hops Count	Server Address	Modify
System	Enabled	4	View	Modify

Figure 2- 64. DHCPv6 Relay Interface Settings window

To search for an entry, enter the Interface Name and click **Find**. To display all current entries on the Switch click **View All**. To change a current entry, click the corresponding **Modify** button of the entry, revealing the following window to configure:



DHCPv6 Relay Interface Settings(Edit)

Interface Name	System
Hops Count	4
State	Enabled

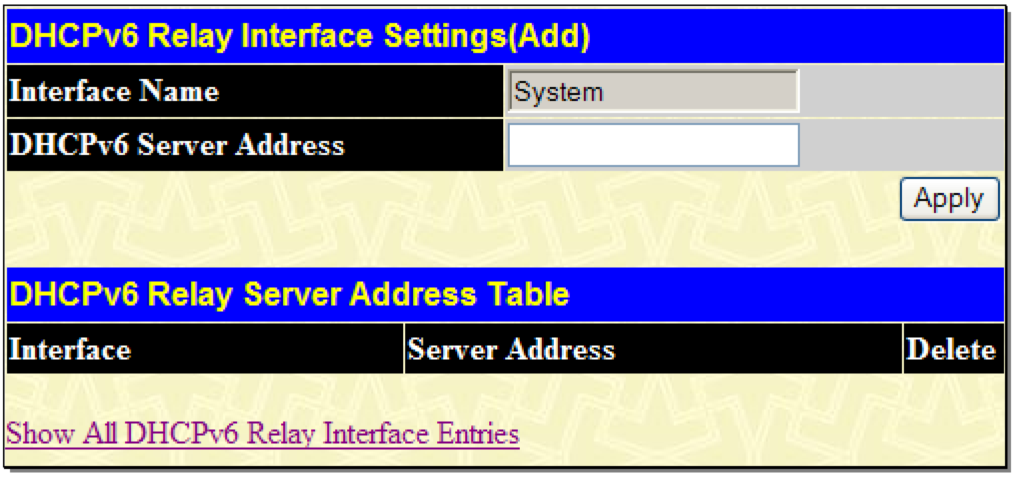
Figure 2- 65. DHCPv6 Relay Interface Settings (Edit) window

The following fields are displayed or can be configured:

Parameter	Description
Interface Name	Display the IPv6 relay interface name.
Hops Count (1-32)	This field allows an entry between *1* and *32* to define the maximum number of router hops DHCPv6 messages can be forwarded across. The default hop count is *4*.
State	Use the pull-down menu to enable or disable the DHCPv6 relay on the interface.

Click **Apply** to implement the changes. To return to the **DHCPv6 Relay Interface Settings** window, click the Show All DHCPv6 Relay Interface Entries link.

To see server addresses of an interface, click the corresponding **View** button:



DHCPv6 Relay Interface Settings(Add)

Interface Name	System
DHCPv6 Server Address	

DHCPv6 Relay Server Address Table

Interface	Server Address	Delete

Figure 2- 66. DHCPv6 Relay Interface Settings (Add) window

The following fields are displayed or can be configured:

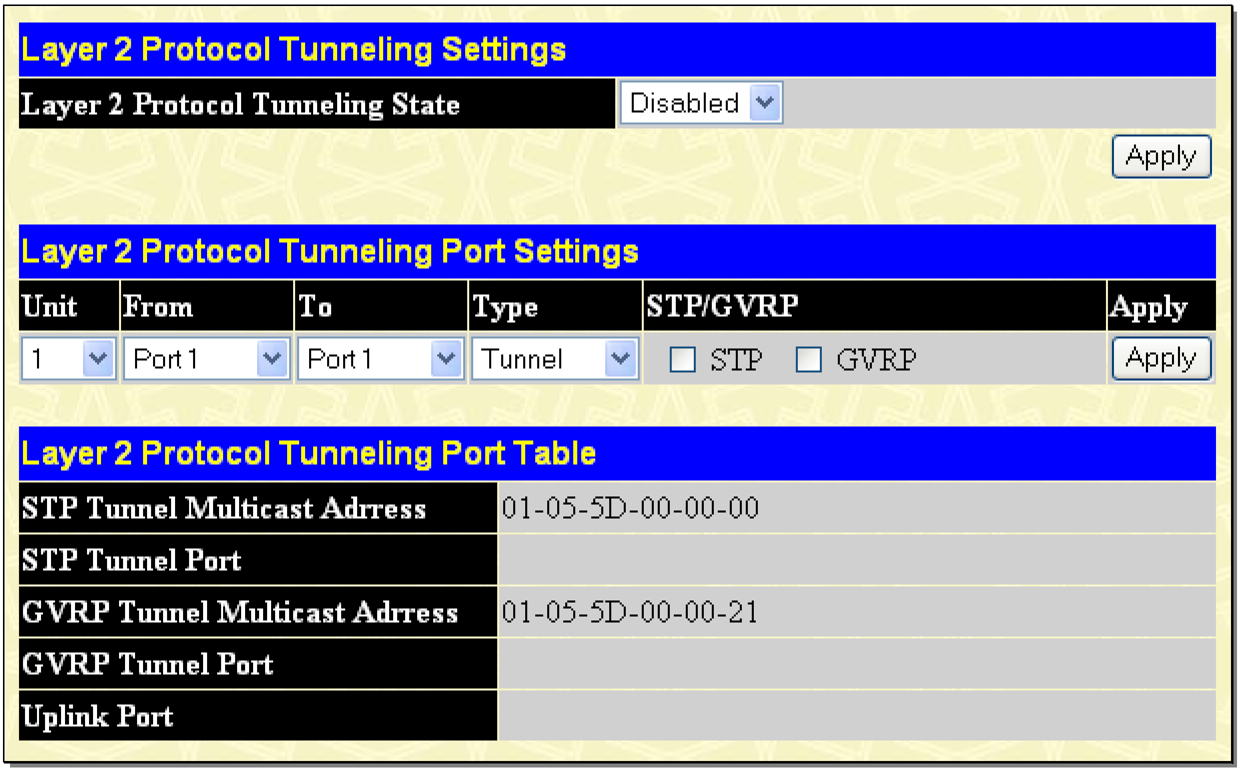
Parameter	Description
Interface Name	Display the IPv6 relay interface name.
DHCPv6 Server Address	Enter the IPv6 destination address to forward DHCPv6 packets.

Click **Apply** to implement the changes. To remove any entry, click the corresponding ☒ button. To return to the **DHCPv6 Relay Interface Settings** window, click the Show All DHCPv6 Relay Interface Entries link.

Layer 2 Protocol Tunneling Settings

The Layer 2 Protocol Tunneling function supports traffic of multiple customers across service provider networks. BPDU Tunneling enables the BPDU's of the same customer's network to be multicast over specific VLANs in the service provider's network, which in turn will ensure the same geographically dispersed customer network can implement consistent spanning tree calculations across the service provider network.

To view this window, click **Administration > Layer 2 Protocol Tunneling Settings**, as shown below:



Layer 2 Protocol Tunneling Settings

Layer 2 Protocol Tunneling State	Disabled

Apply

Layer 2 Protocol Tunneling Port Settings

Unit	From	To	Type	STP/GVRP	Apply
1	Port 1	Port 1	Tunnel	□ STP □ GVRP	Apply

Layer 2 Protocol Tunneling Port Table

STP Tunnel Multicast Adrress	01-05-5D-00-00-00
STP Tunnel Port	
GVRP Tunnel Multicast Adrress	01-05-5D-00-00-21
GVRP Tunnel Port	
Uplink Port	

Figure 2- 67. Layer 2 Protocol Tunneling Settings window

The following fields can be configured:

Parameter	Description
Layer 2 Protocol Tunneling State	Use the drop-down menu to *Enable* or *Disable* the Layer 2 Protocol Tunneling state.
Unit	Select the unit to configure.
From/To	Specify the ports on which the Layer 2 Protocol Tunneling will be enabled of disabled.
Type	Use the drop-down menu to select the configuration type. *Tunnel* – Specifies that the BPDU is received from a tunnel port, this packets DA will be replaced by a reserved multicast address and then sent out to a providers network through the uplink port. *Uplink* – Specifies that the port is a normal switch port which connects to the network provider. The encapsulated PDU received on the uplink port shall be terminated and the DA is replaced with the STP/GVRP MAC address, the packet is then sent to the tunnel port in the same VLAN. *None* – When selected an encapsulated PDU is received on a port and the forwarding behavior follows the forwarding of general multicast addresses. *None* is the default.
STP/GVRP	Select the type of tunnel multicast address to be applied to the ports either *STP* or *GVRP*. An STP enabled port can not be configured as an STP tunnel port. A GVRP enabled port can not be configured as a GVRP tunnel port.

Click **Apply** to implement changes made.

RSPAN

RSPAN (Remote Switched Port Analyzer) is a feature used to monitor and analyze the traffic passing through ports. The character 'R' is short for 'Remote' which means that the mirror source ports and the destination port are not on the same Switch. So a remote mirror session consists of at least two switches. To achieve the remote mirroring function, the mirrored traffic is tagged with a reserved VLAN which is called an RSPAN VLAN, the RSPAN VLAN is reserved in such a way that traffic tagged with RSPAN will be mirrored toward the associated destination port.

There are three roles for switches in RSPAN.

Source switch – The switch which has the monitored ports or VLANs on it is the source switch. All packets on the source ports or VLANs are copied and sent to the destination switch. When the mirrored packets are sent out from the source switch, an RSPAN VLAN tag is added to every packet. The incoming port on the source switch for the mirrored packets is referred to as the **source port**.

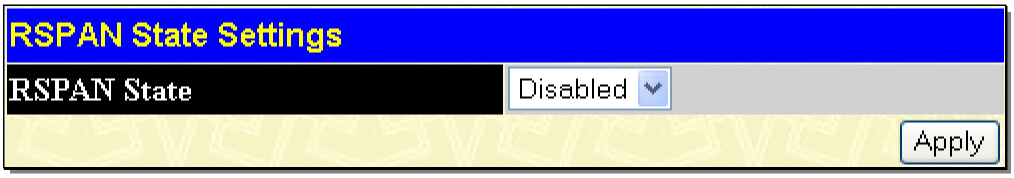
Intermediate switch The function of the intermediate switch is to mirror traffic flowing in the RSPAN VLAN toward the RSAPN destination. A switch can be have the role of an RSAPN VLAN intermediate switch as well as the role of source switch for another RSPAN VLAN.

Destination Switch The port which is directly connected to a network analyzer, other monitoring, or security device is called the **destination port**. The switch which has a destination port is called the **destination switch**. The destination switch removes the RSPAN VLAN tags from the mirrored packets when the destination port is an untagged port in the RSPAN VLAN. If the destination port is a tagged port, the tags will be reserved.

RSPAN State Settings

This window allows the user to enable or disable the RSPAN settings on the Switch. The purpose of the RSPAN function is to mirror the packets to the remote switch. The packet travels from the switch where the monitored packet is received, through the intermediate switch, then to the switch where the sniffer is attached. The first switch is also named the source switch.

To view this window, click **Administration** > **RSPAN** > **RSPAN State Settings**, as shown below:



RSPAN State Settings

RSPAN State: Disabled

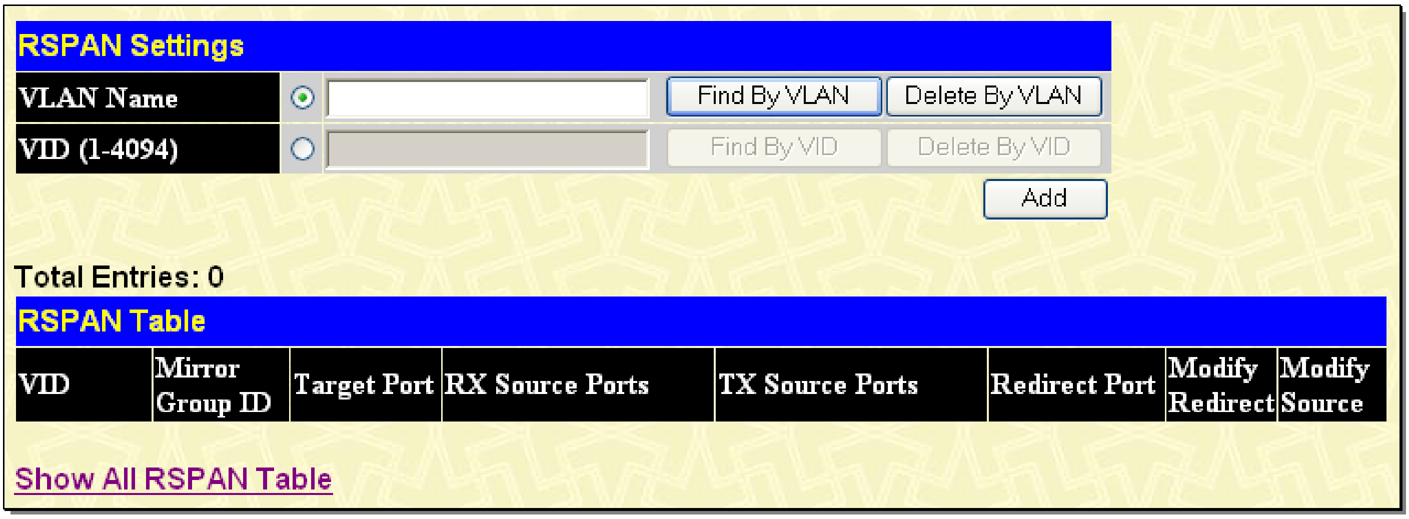
Figure 2- 68. RSPAN State Settings window

Use the drop-down menu to enable or disable the RSPAN State on the Switch and click **Apply** to implement the changes made.

RSPAN Settings

This window allows the user to search for a previously created VLAN and to view the RSPAN settings for it.

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



RSPAN Settings

VLAN Name ●

VID (1-4094) ○

Total Entries: 0

RSPAN Table

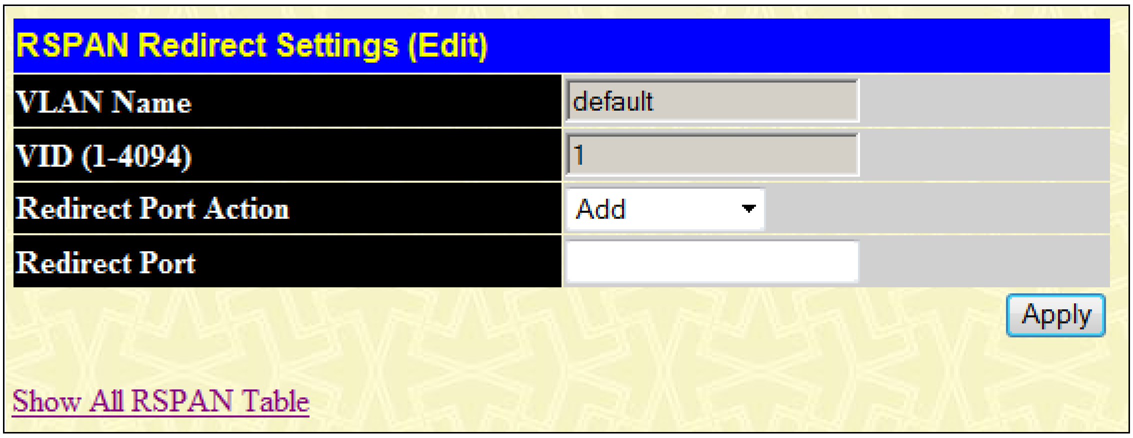
VID	Mirror Group ID	Target Port	RX Source Ports	TX Source Ports	Redirect Port	Modify Redirect	Modify Source

Figure 2- 69. RSPAN Settings window

The following fields can be configured:

Parameter	Description
VLAN Name	Enter the name of the VLAN to Add, Find or Delete.
VID (1-4094)	Enter the VLAN ID of the VLAN to Add, Find or Delete.
Mirror Group ID	The mirror group identify that specifies which mirror session is used for the RSPAN source function. If the mirror group is not specified when configuring the mirror ports, the mirror group 1 will be the default group.
Target Port	The mirror group target port which the mirror session used for the RSPAN source function.
RX Source Ports	The goal of Rx source ports is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that RSPAN session.
TX Source Ports	The goal of Tx source ports is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch.
Redirect Port	RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.
Modify Redirect	Click on the corresponding **Modify** button to edit the entries.
Modify Source	Click on the corresponding **Modify** button to edit the source setting for the RSPAN VLAN on the source switch.

To remove an entry, click the corresponding **Delete by VLAN** icon. To search for an entry enter the appropriate information and click the **Find by VLAN** button. To modify an existing entry, click the corresponding **Modify** button in the **Modify Redirect** column, revealing the following window to configure:



RSPAN Redirect Settings (Edit)

VLAN Name	default
VID (1-4094)	1
Redirect Port Action	Add
Redirect Port	

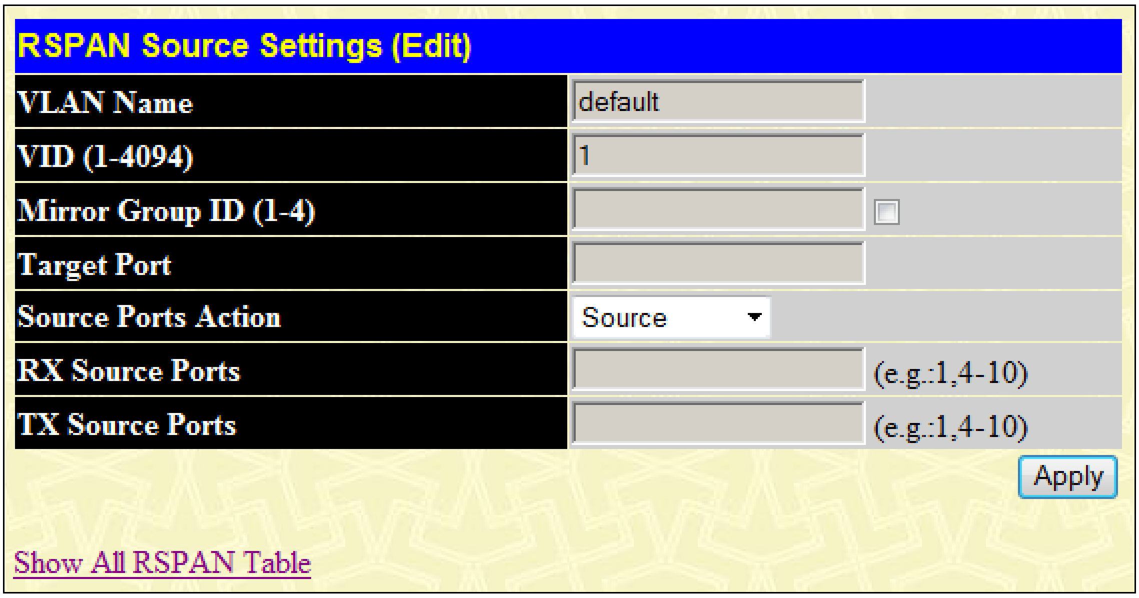
Figure 2- 70. RSPAN Redirect Settings (Edit) window

The following fields can be configured:

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN which will modify the RSPAN Entries.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN which will to modify the RSPAN Entries.
Redirect Port Action	Use the drop-down menu to select the configuration Redirect Ports Action. *Add* – Add Redirect ports. *Delete* – Delete Redirect ports.
Redirect Port	RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

Click **Apply** to implement the changes. To return to the RSPAN Settings window, click the Show All RSPAN Table link.

To modify an existing entry of its source settings, click the corresponding **Modify** button in **Modify Source** column, revealing the following window to configure:



RSPAN Source Settings (Edit)

VLAN Name	default	
VID (1-4094)	1	
Mirror Group ID (1-4)		□
Target Port		
Source Ports Action	Source	
RX Source Ports		(e.g.:1,4-10)
TX Source Ports		(e.g.:1,4-10)

Figure 2- 71. RSPAN Source Settings (Edit) window

The following fields can be configured:

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN which will modify the RSPAN entries.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN which will to modify the RSPAN entries.
Mirror Group ID (1-4)	Tick the check box and enter a group ID which mirror session is used for RSPAN source function.
Target Port	The mirror group Target Port which the mirror session used for the RSPAN source function.
Source Ports Action	Use the pull-down menu to display the source port only.
Rx Source Ports	The goal of Rx source ports is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that RSPAN session.
Tx Source Ports	The goal of Tx source ports is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch.

Click **Apply** to implement the changes.

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

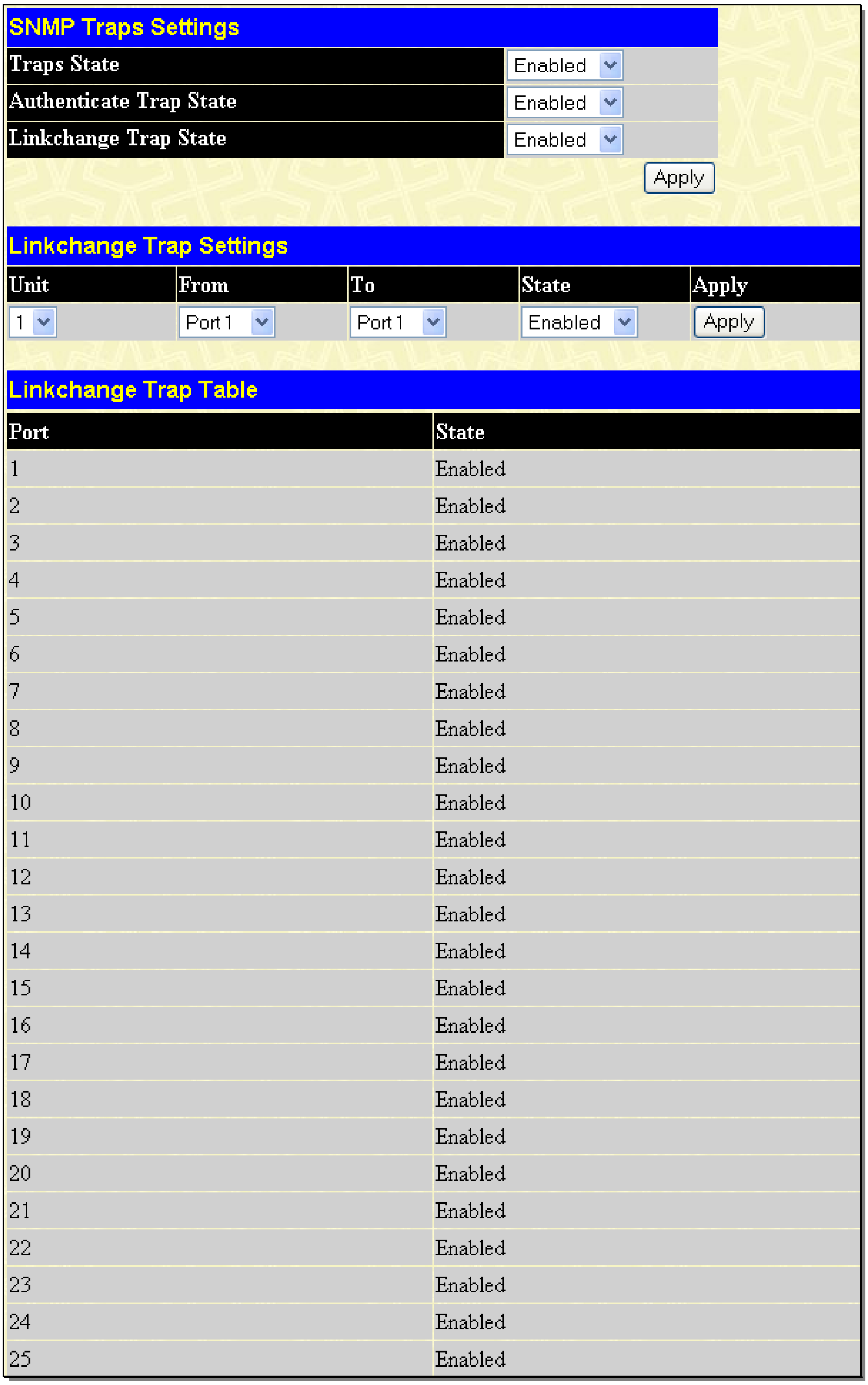
The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP 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 Trap Settings

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

To view this window for configuration, click **Administration > SNMP Manager > SNMP Trap Settings**, as shown below:



SNMP Traps Settings

Traps State	Enabled
Authenticate Trap State	Enabled
Linkchange Trap State	Enabled

Linkchange Trap Settings

Unit	From	To	State	Apply
1	Port 1	Port 1	Enabled	Apply

Linkchange Trap Table

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

Figure 2- 72. SNMP Trap Settings window

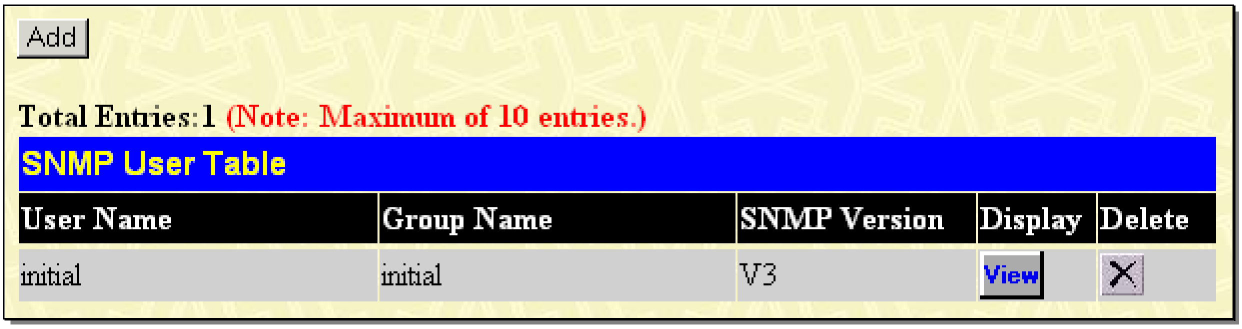
To enable or disable the Traps State, Authenticate Trap State, and/or Linkchange Trap State use the corresponding pull-down menu to change and click **Apply**.

To enable or disable linkchange trap settings for individual ports, select the ports using the From and To drop-down menus, enable State using the drop-down menu, and then click **Apply**.

SNMP User Table

This window displays all of the SNMP users currently configured on the Switch.

To view this window, click **Administration** > **SNMP Manager** > **SNMP User Table**, as shown below:



Total Entries:1 (Note: Maximum of 10 entries.)

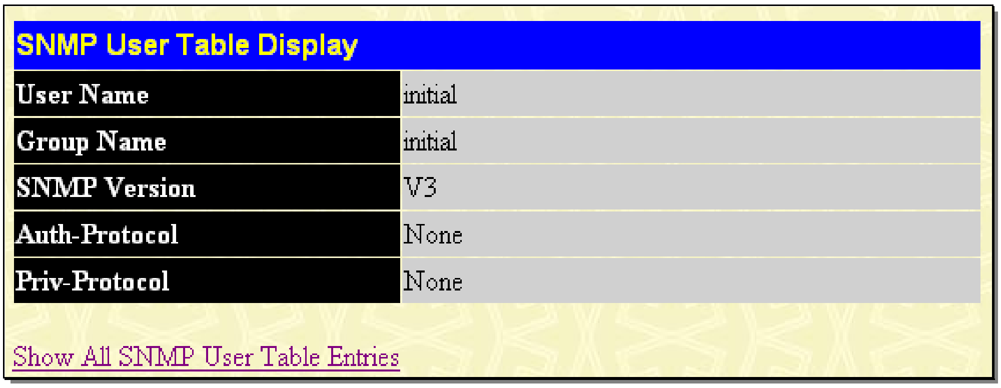
SNMP User Table

User Name	Group Name	SNMP Version	Display	Delete
initial	initial	V3	View	☒

Figure 2- 73. 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 the **View** button under the Display heading. This will open the **SNMP User Table Display** window, as shown below:



SNMP User Table Display

User Name	initial
Group Name	initial
SNMP Version	V3
Auth-Protocol	None
Priv-Protocol	None

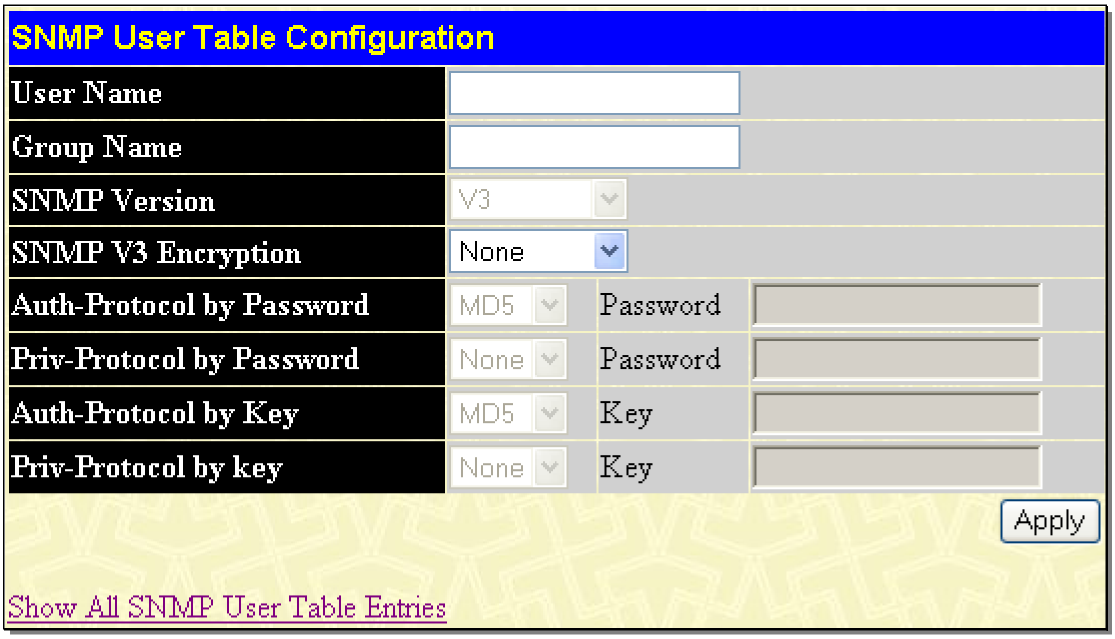
Show All SNMP User Table Entries

Figure 2- 74. 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	*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, click the **Add** button on the **SNMP User Table** window. This will open the **SNMP User Table Configuration** window, as shown below:



SNMP User Table Configuration

User Name			
Group Name			
SNMP Version	V3		
SNMP V3 Encryption	None		
Auth-Protocol by Password	MD5	Password	
Priv-Protocol by Password	None	Password	
Auth-Protocol by Key	MD5	Key	
Priv-Protocol by key	None	Key	

Figure 2- 75. SNMP User Table Configuration window

The following parameters can set:

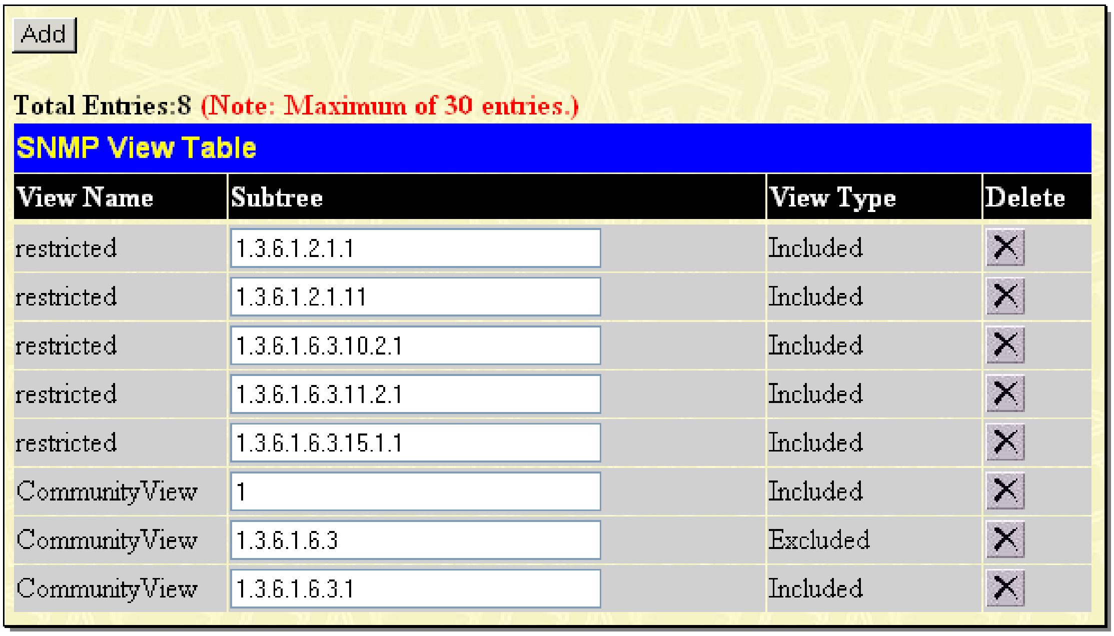
Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V3* - Specifies that SNMP version 3 will be used.
SNMP V3 Encryption	SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. Use the drop down menu to select the type of SNMP V3 encryption to be applied. The user can choose between *None*, *Password* or *Key*.
Auth-Protocol by Password / Key	*MD5* - Specifies that the HMAC-MD5-96 authentication level will be used. This is only operable when *V3* is selected in the SNMP Version field and the Encrypted check box has been ticked. This field will require the user to enter a password. *SHA* - Specifies that the HMAC-SHA authentication protocol will be used. This is only operable when *V3* is selected in the SNMP Version field and the Encrypted check box has been ticked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.
Priv-Protocol by Password / Key	*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 check box has been ticked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.

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

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

To view this window, click **Administration** > **SNMP Manager** > **SNMP View Table**, as shown below:



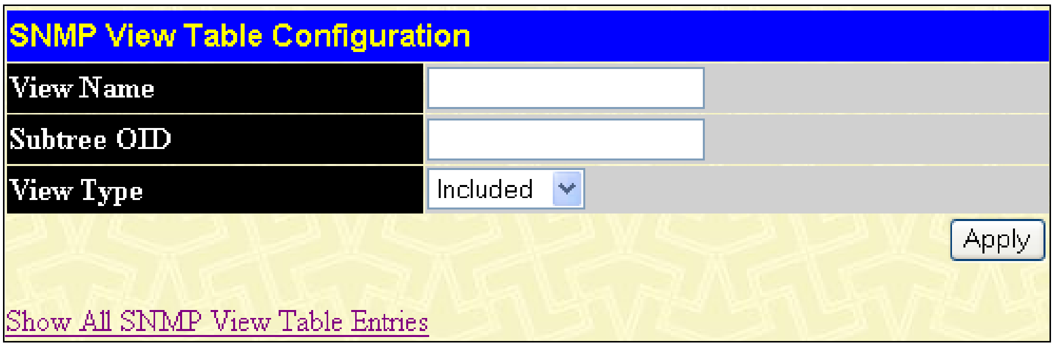
Total Entries:8 (Note: Maximum of 30 entries.)

SNMP View Table

View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	☒
restricted	1.3.6.1.2.1.11	Included	☒
restricted	1.3.6.1.6.3.10.2.1	Included	☒
restricted	1.3.6.1.6.3.11.2.1	Included	☒
restricted	1.3.6.1.6.3.15.1.1	Included	☒
CommunityView	1	Included	☒
CommunityView	1.3.6.1.6.3	Excluded	☒
CommunityView	1.3.6.1.6.3.1	Included	☒

Figure 2- 76. SNMP View Table window

To delete an existing SNMP View Table entry, click the corresponding ☒ button in the Delete column. To create a new entry, click the **Add** button which will reveal a new window.


SNMP View Table Configuration

View Name	
Subtree OID	
View Type	Included

Figure 2- 77. SNMP View Table Configuration window

The SNMP View 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:

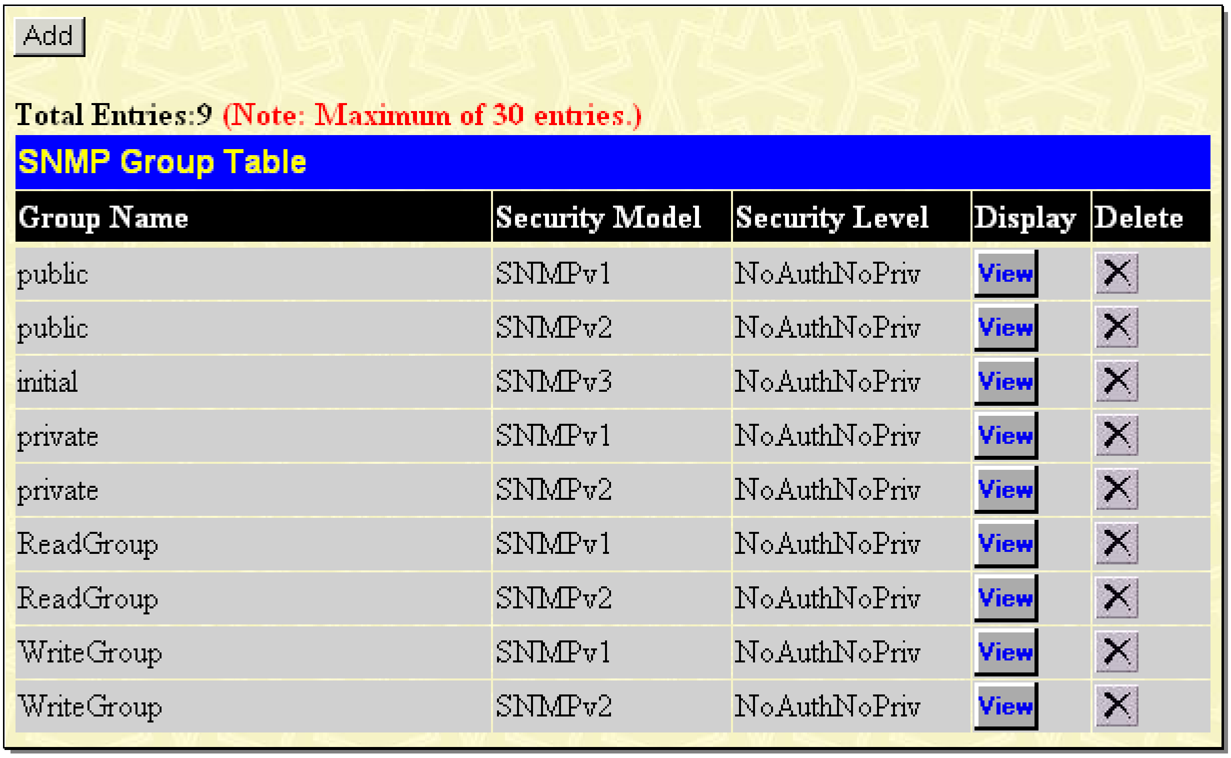
Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select *Included* to ensure this object is included 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** window, 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**, as shown below:



Add

Total Entries:9 (Note: Maximum of 30 entries.)

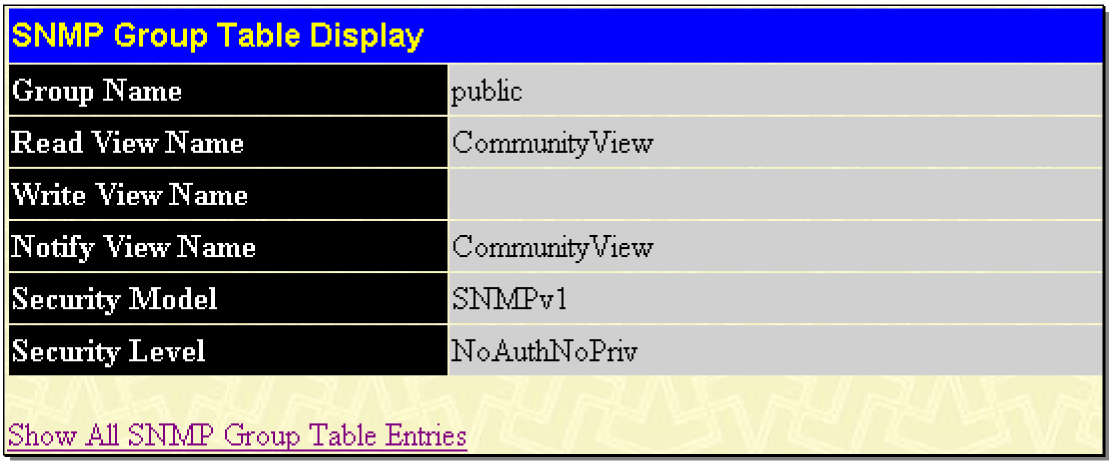
SNMP Group Table

Group Name	Security Model	Security Level	Display	Delete
public	SNMPv1	NoAuthNoPriv	View	☒
public	SNMPv2	NoAuthNoPriv	View	☒
initial	SNMPv3	NoAuthNoPriv	View	☒
private	SNMPv1	NoAuthNoPriv	View	☒
private	SNMPv2	NoAuthNoPriv	View	☒
ReadGroup	SNMPv1	NoAuthNoPriv	View	☒
ReadGroup	SNMPv2	NoAuthNoPriv	View	☒
WriteGroup	SNMPv1	NoAuthNoPriv	View	☒
WriteGroup	SNMPv2	NoAuthNoPriv	View	☒

Figure 2- 78. 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 **View** button located under the Display heading, which will show the following window.



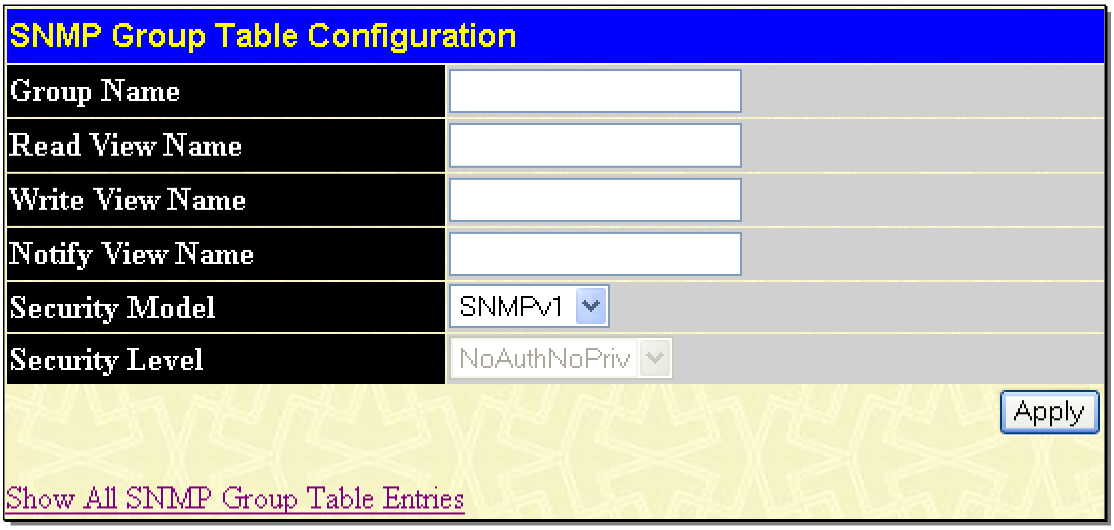
SNMP Group Table Display

Group Name	public
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv

Show All SNMP Group Table Entries

Figure 2- 79. 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:



SNMP Group Table Configuration

Group Name	
Read View Name	
Write View Name	
Notify View Name	
Security Model	SNMPv1
Security Level	NoAuthNoPriv

Figure 2- 80. SNMP Group Table Configuration window

The following parameters can set:

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

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

SNMP Community Table

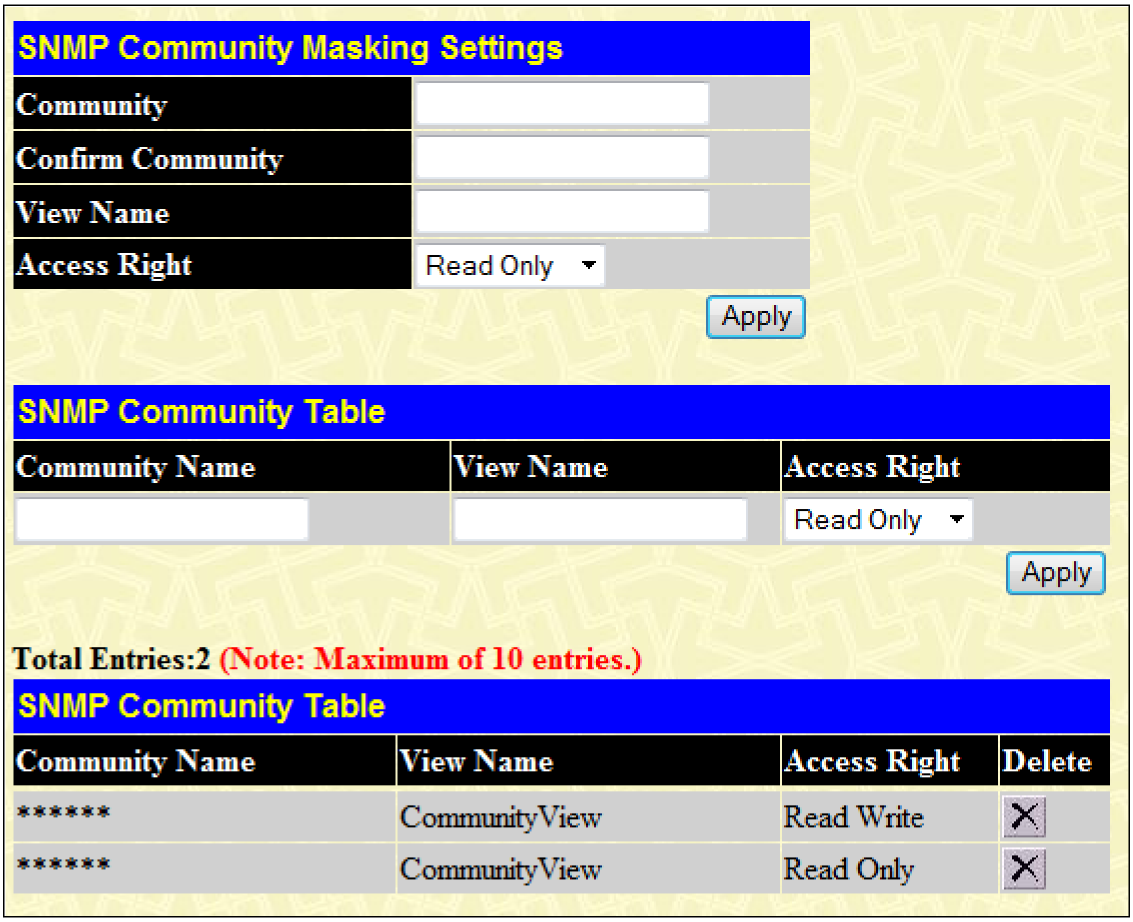
Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

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 view this window, click **Administration** > **SNMP Manager** > **SNMP Community Table**, as shown below:



SNMP Community Masking Settings

Community	
Confirm Community	
View Name	
Access Right	Read Only ▾

SNMP Community Table

Community Name	View Name	Access Right
		Read Only ▾

Total Entries:2 (Note: Maximum of 10 entries.)

SNMP Community Table

Community Name	View Name	Access Right	Delete
******	CommunityView	Read Write	☒
******	CommunityView	Read Only	☒

Figure 2- 81. SNMP Community Table window

The following parameters can set:

Parameter	Description
Community	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.
Confirm Community	Type the **Community** string again.
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.
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers

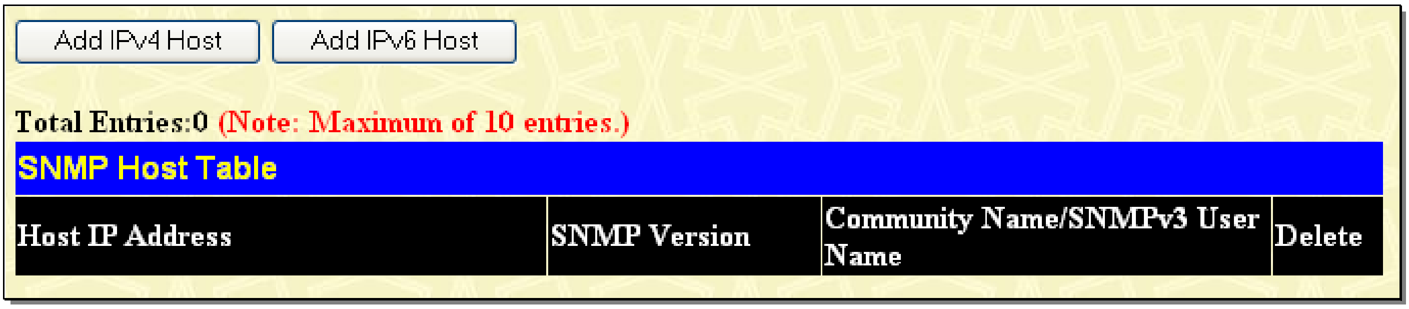
	access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	*Read Only* - Specifies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

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

SNMP Host Table

Use this window to set up SNMP trap recipients. To delete an existing SNMP Host Table entry, click the corresponding ☒ button under the Delete heading.

To view this window, click **Administration** > **SNMP Manager** > **SNMP Host Table**, as shown below:



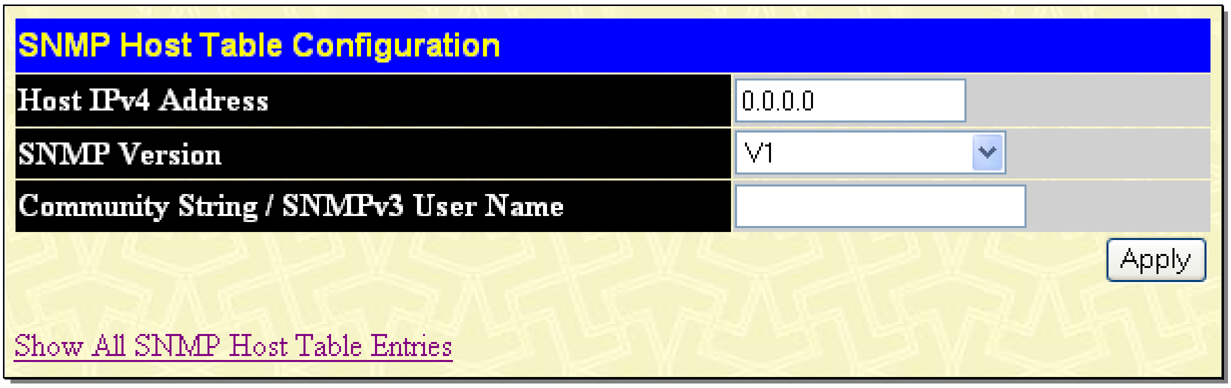
Total Entries:0 (Note: Maximum of 10 entries.)

SNMP Host Table

Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete

Figure 2- 82. SNMP Host Table window

Users now have the choice of adding an IPv4 or an IPv6 host to the SNMP host table. To add a new IPv4 entry to the Switch's SNMP Host Table, click the **Add IPv4 Host** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below:


SNMP Host Table Configuration

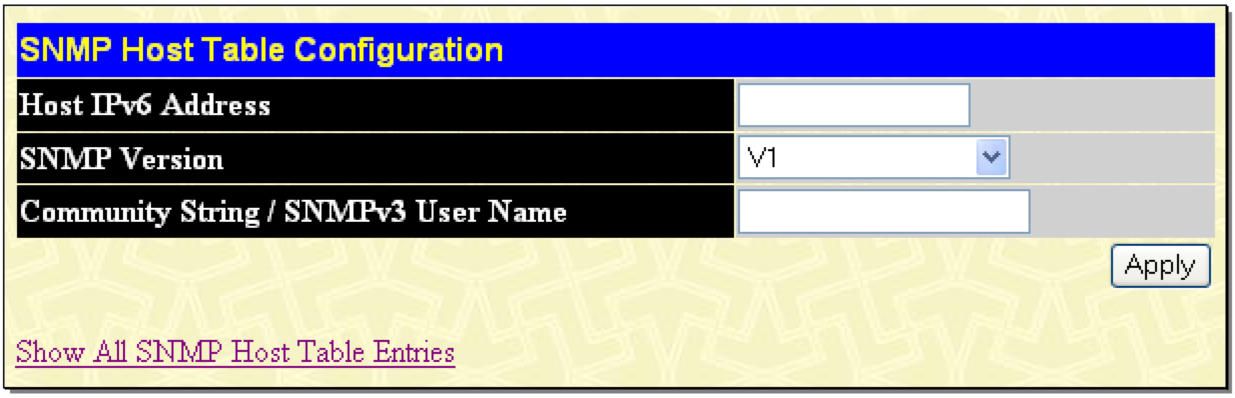
Host IPv4 Address	0.0.0.0
SNMP Version	V1
Community String / SNMPv3 User Name	

Figure 2- 83. SNMP Host Table Configuration window for IPv4

The following parameters can set:

Parameter	Description
Host IPv4 Address	Type the IPv4 address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	*V1* - This specifies that SNMP version 1 will be used. *V2* - To specify that SNMP version 2 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 or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To add a new IPv6 entry to the Switch's SNMP Host Table, click the **Add IPv6 Host** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below:



SNMP Host Table Configuration

Host IPv6 Address	
SNMP Version	V1
Community String / SNMPv3 User Name	

Figure 2- 84. SNMP Host Table Configuration window for IPv6

The following parameters can set:

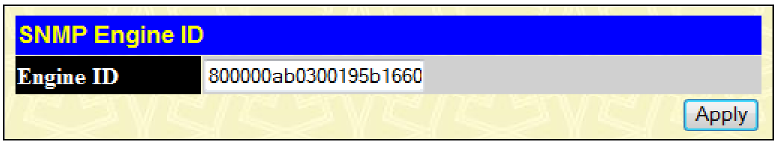
Parameter	Description
Host IPv6 Address	Type the IPv6 address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	*V1* - To specifies that SNMP version 1 will be used. *V2* - To specify that SNMP version 2 will be used. *V3-NoAuth-NoPriv* - To specify that the 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 or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To implement your new settings, click **Apply.** To return to the **SNMP Host Table** window, 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 Manager** > **SNMP Engine ID**, as shown.



SNMP Engine ID

Engine ID	800000ab0300195b1660

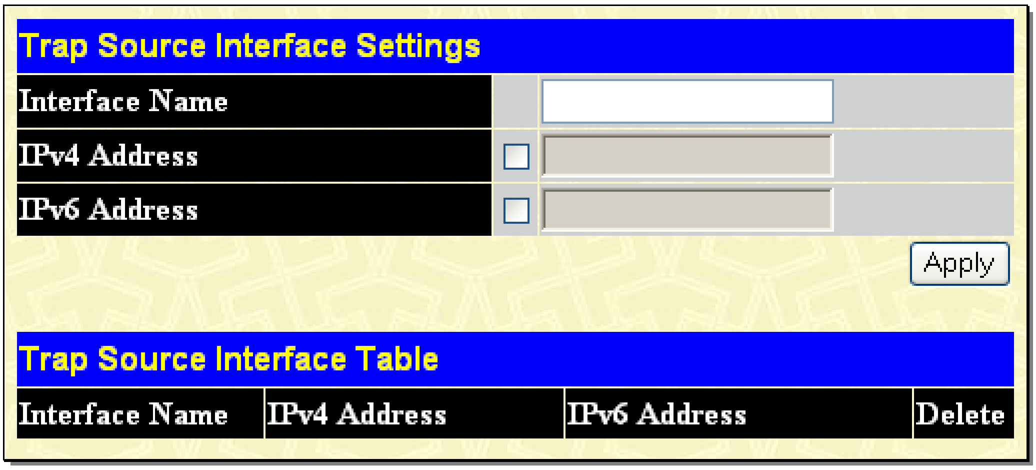
Figure 2- 85. SNMP Engine ID window

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

Trap Source Interface Settings

This window is used to configure the trap source interface settings.

To view this window, click **Administration** > **Trap Source Interface Settings**, as shown below:



Trap Source Interface Settings

Interface Name		
IPv4 Address	□	
IPv6 Address	□	

Apply

Trap Source Interface Table

Interface Name	IPv4 Address	IPv6 Address	Delete

Figure 2- 86. Trap Source Interface Settings window

The following parameters can be configured:

Parameter	Description
Interface Name	Enter a name of the interface.
IPv4 Address	Tick the check box and enter an IPv4 address.
IPv6 Address	Tick the check box and enter an IPv6 address.

Click **Apply** to implement the changes. To remove an entry, click the corresponding ☒ button.

sFlow

sFlow is a feature on the Switch that allows users to monitor network traffic running through the switch to identify network problems through packet sampling and packet counter information of the Switch. The Switch itself is the sFlow agent where packet data is retrieved and sent to an sFlow Analyzer where it can be scrutinized and utilized to resolve the problem.

The Switch can configure the settings for the sFlow Analyzer but the remote sFlow Analyzer device must have an sFlow utility running on it to retrieve and analyze the data it receives from the sFlow agent.

The Switch itself will collect three types of packet data:

1. It will take sample packets from the normal running traffic of the Switch based on a sampling interval configured by the user.
2. The Switch will take a poll of the IF counters located on the switch.
3. The Switch will also take a part of the packet header. The length of the packet header can also be determined by the user.

Once this information has been gathered by the switch, it is packaged into a packet called an sFlow datagram, which is then sent to the sFlow Analyzer for analysis.

For a better understanding of the sFlow feature of this Switch, refer to the adjacent diagram.

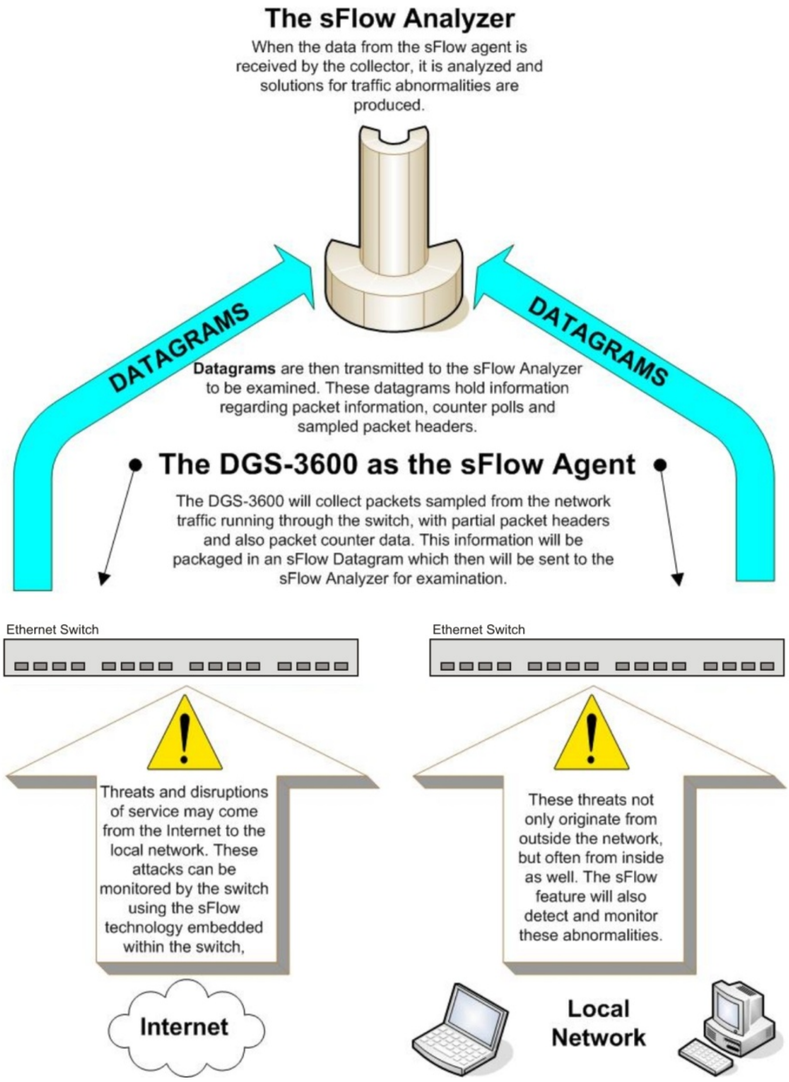
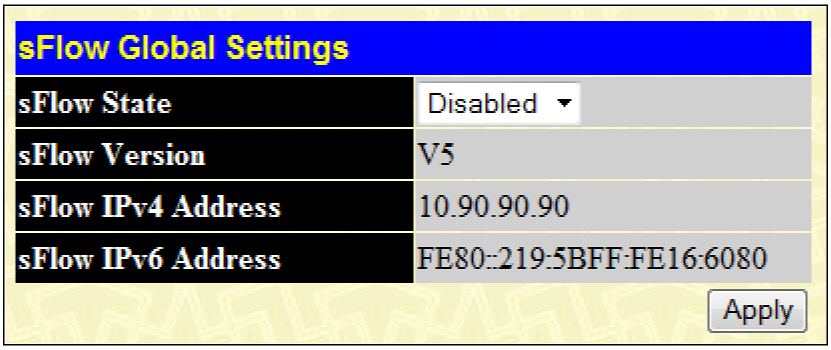

The sFlow Analyzer
When the data from the sFlow agent is received by the collector, it is analyzed and solutions for traffic abnormalities are produced.
DATAGRAMS
DATAGRAMS
Datagrams are then transmitted to the sFlow Analyzer to be examined. These datagrams hold information regarding packet information, counter polls and sampled packet headers.
The DGS-3600 as the sFlow Agent
The DGS-3600 will collect packets sampled from the network traffic running through the switch, with partial packet headers and also packet counter data. This information will be packaged in an sFlow Datagram which then will be sent to the sFlow Analyzer for examination.
Ethernet Switch
Ethernet Switch
Threats and disruptions of service may come from the Internet to the local network. These attacks can be monitored by the switch using the sFlow technology embedded within the switch.
These threats not only originate from outside the network, but often from inside as well. The sFlow feature will also detect and monitor these abnormalities.
Internet
Local Network

Figure 2- 87. sFlow Basic Setup

sFlow Global Settings

The following window is used to globally enable the sFlow feature for the Switch. Simply use the pull-down menu and click **Apply** to enable or disable sFlow. This window will also display the sFlow version currently being utilized by the Switch, along with the sFlow Address that is the Switch's IP address.

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



sFlow Global Settings

sFlow State	Disabled ▾
sFlow Version	V5
sFlow IPv4 Address	10.90.90.90
sFlow IPv6 Address	FE80::219:5BFF:FE16:6080

Figure 2- 88. sFlow Global Settings window

The following fields are displayed:

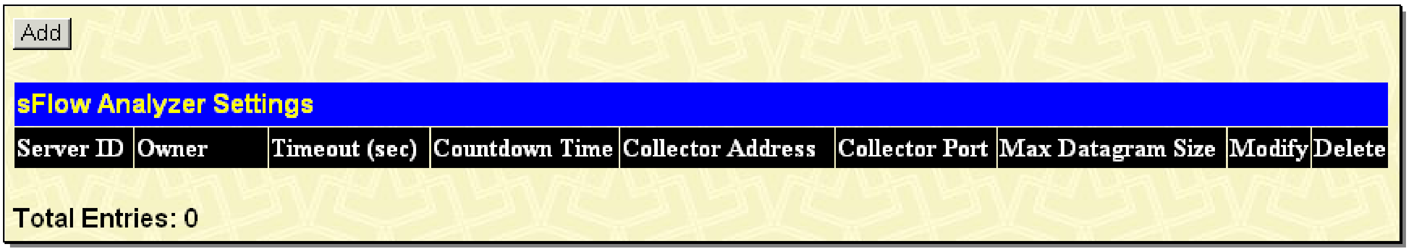
Parameter	Description

sFlow State	This field allows you to globally enable or disable sFlow.
sFlow Version	This displays the current sFlow version.
sFlow IPv4 Address	This displays the sFlow IPv4 address.
sFlow IPv6 Address	This displays the sFlow IPv6 address.

sFlow Analyzer Settings

The following windows are used to configure the parameters for the remote sFlow Analyzer (collector) that will be used to gather and analyze sFlow Datagrams that originate from the Switch. Users must have the proper sFlow software set on the Analyzer in order to receive datagrams from the switch to be analyzed, and to analyze these datagrams. Users may specify up to four unique analyzers to receive datagrams, yet the virtual port used must be unique to each entry.

To configure the settings for the sFlow analyzer, click **Administration** > **sFlow** > **sFlow Analyzer Settings**, as shown below:



sFlow Analyzer Settings

Server ID	Owner	Timeout (sec)	Countdown Time	Collector Address	Collector Port	Max Datagram Size	Modify	Delete

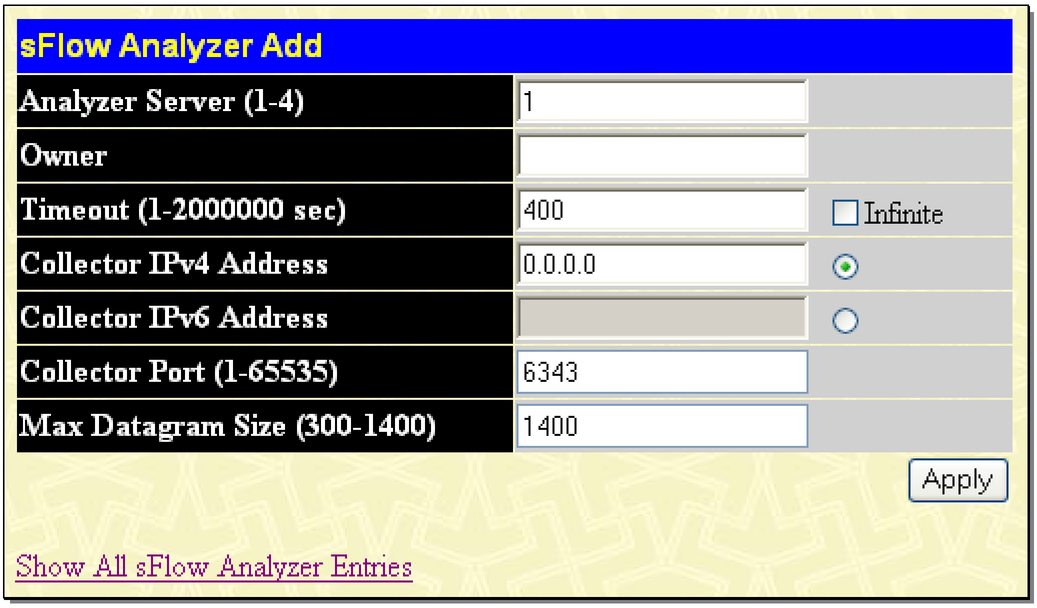
Total Entries: 0

Figure 2- 89. sFlow Analyzer Settings window

The following fields are displayed:

Parameter	Description
Server ID	This field denotes the ID of the Analyzer Server that has been added to the sFlow settings. Up to four entries can be added with the same UDP port.
Owner	Displays the owner of the entry made here. The user that added this sFlow analyzer configured this name.
Timeout (sec)	Displays the configured time, in seconds, after which the Analyzer server will time out. When the server times out, all sFlow samples and counter polls associated with this server will be deleted.
Countdown Time	Displays the current time remaining before this Analyzer server times out. When the server times out, all sFlow samples and counter polls associated with this server will be deleted.
Collector Address	Displays the IP address of the sFlow Analyzer Server. This IP address is where sFlow datagrams will be sent for analysis.
Collector Port	Displays the previously configured UDP port where sFlow datagrams will be sent for analysis.
Max Datagram Size	This field displays the maximum number of data bytes in a single sFlow datagram that will be sent to this sFlow Analyzer Server.
Modify	Click the **Modify** button to display the **sFlow Counter Analyzer Edit** window, so that users may edit the settings for this server.
Delete	Click the corresponding ☒ button of the entry to be deleted.

To add a new sFlow Analyzer, click the **Add** button in the previous window that will display the following window to be configured:



sFlow Analyzer Add

Analyzer Server (1-4)	1	
Owner		
Timeout (1-2000000 sec)	400	□ Infinite
Collector IPv4 Address	0.0.0.0	●
Collector IPv6 Address		○
Collector Port (1-65535)	6343	
Max Datagram Size (300-1400)	1400	

Figure 2- 90. sFlow Analyzer Add window

The following fields can be set or modified:

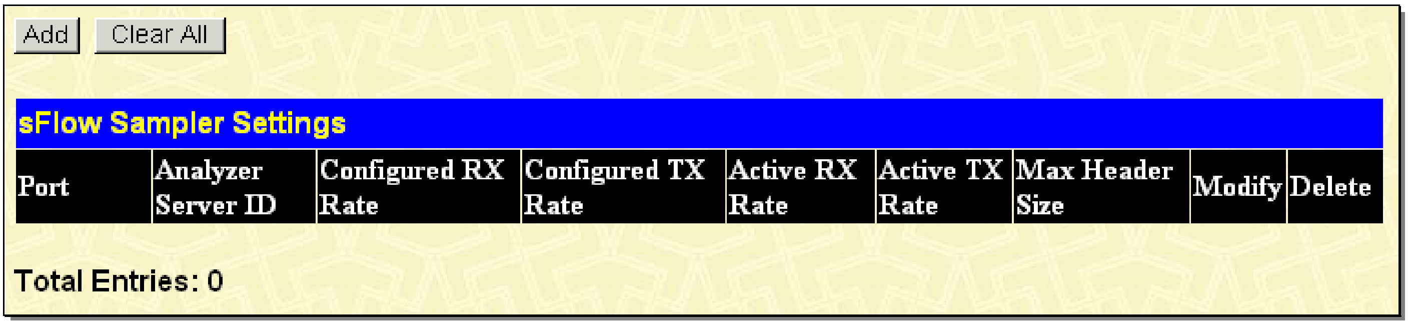
Parameter	Description
Analyzer Server (1-4)	Enter an integer from *1* to *4* to denote the sFlow Analyzer to be added. Up to four entries can be added.
Owner	Users may enter an alphanumeric string of up to 16 characters to define the owner of this entry. Users are encouraged to give this field a name that will help them identify this entry. When an entry is made in this field, the following Timeout field is automatically set to *400* seconds, unless the user alters the Timeout field.
Timeout (1-2000000 sec)	This field is used to specify the timeout for the Analyzer server. When the server times out, all sFlow samples and counter polls associated with this server will be deleted. The user may set a time between *1* and *2000000* seconds with a default setting of *400* seconds. *Infinite* can be selected to ensure that it never times out.
Collector IPv4 Address	The IPv4 address of the sFlow Analyzer Server. If this field is not specified, the entry will become 0.0.0.0 and therefore the entry will be inactive. Users must set this field when it is selected.
Collector IPv6 Address	The IPv6 address of the sFlow Analyzer Server. If this field is not specified, the entry will become 0 and therefore the entry will be inactive. Users must set this field when it is selected.
Collector Port (1-65535)	The destination UDP port where sFlow datagrams will be sent. The default setting for this field is *6343*.
Max Datagram Size (300-1400)	This field will specify the maximum number of data bytes that can be packaged into a single sFlow datagram. Users may select a value between *300* and *1400* bytes with a default setting of *1400* bytes.

Click **Apply** to save changes made.

sFlow Sampler Settings

This window will allow users to configure the Switch’s settings for taking sample packets from the network, including the sampling rate and the amount of the packet header to be extracted.

To configure the settings for the sFlow Sampler, click **Administration** > **sFlow > sFlow Sampler Settings**, as shown below:



sFlow Sampler Settings

Port	Analyzer Server ID	Configured RX Rate	Configured TX Rate	Active RX Rate	Active TX Rate	Max Header Size	Modify	Delete

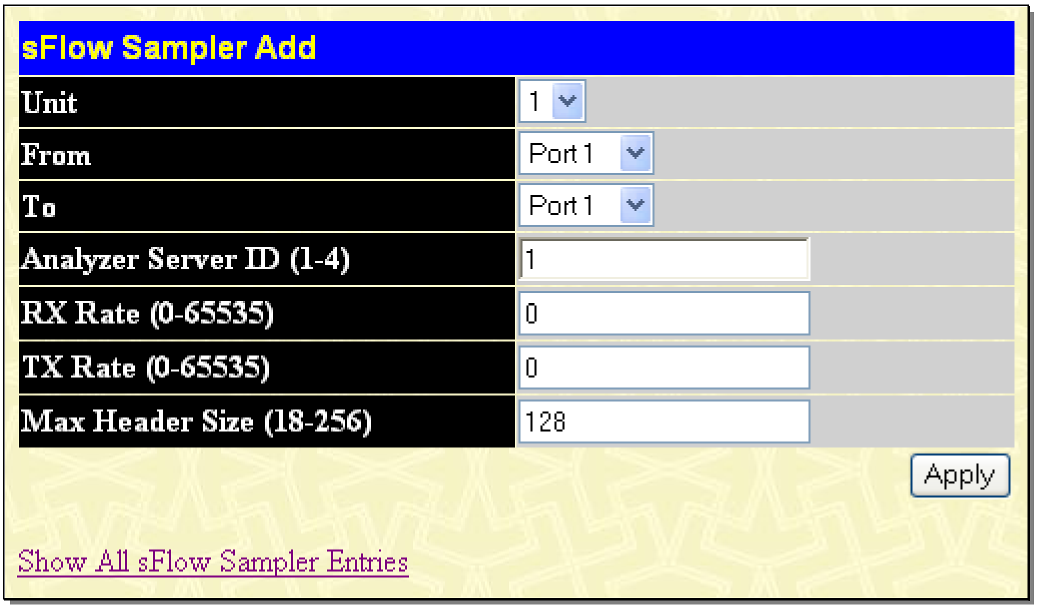
Total Entries: 0

Figure 2- 91. sFlow Sampler Settings window

The following fields are displayed:

Parameter	Description
Port	Displays the port from which packet samples are being extracted.
Analyzer Server ID	Displays the ID of the Analyzer Server where datagrams, containing the packet sampling information taken using this sampling mechanism, will be sent.
Configured RX Rate	Displays the configured rate of packet sampling for this port based on a multiple of 256. For example, if a figure of 20 is in this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port.
Configured TX Rate	Displays the configured rate of packet sampling for this port based on a multiple of 256. For example, if a figure of 20 is in this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port.
Active RX Rate	Displays the current rate op packet sampling being performed by the Switch for this port, based on a multiple of 256. For example, if a figure of 20 is in this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port.
Active TX Rate	Displays the current rate op packet sampling being performed by the Switch for this port, based on a multiple of 256. For example, if a figure of 20 is in this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port.
Max Header Size	Displays the number of leading bytes of the sampled packet header. This sampled header will be encapsulated with the datagram to be forwarded to the Analyzer Server.
Modify	Click this button to modify the settings for this entry. The **sFlow Sampler Edit** window will be produced for the user to configure.
Delete	Click the ☒ of the corresponding entry to be deleted.
Clear All	Click this button to reset the information in this window.

To add a new sFlow Sampler entry, click the **Add** button which will display the following window to be configured:



sFlow Sampler Add

Unit	1
From	Port 1
To	Port 1
Analyzer Server ID (1-4)	1
RX Rate (0-65535)	0
TX Rate (0-65535)	0
Max Header Size (18-256)	128

Figure 2- 92. sFlow Sampler Add window

The following fields may be set:

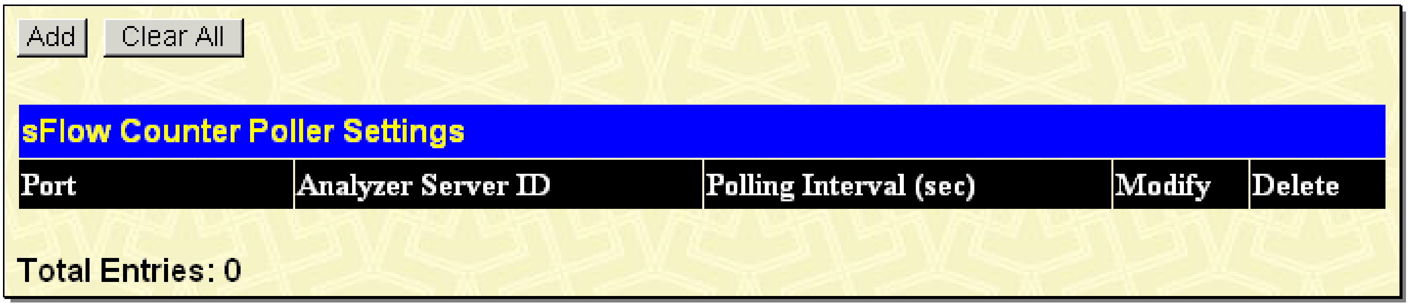
Parameter	Description
Unit	Select the unit to configure.
From/To	Choose the beginning and ending range of ports to be configured for packet sampling.
Analyzer Server ID (1-4)	Enter the previously configured Analyzer Server ID to state the device that will be receiving datagrams from the Switch. These datagrams will include the sample packet information taken using the sampling mechanism configured here.
RX Rate (0-65535)	Users can set the rate of packet sampling here. The value entered here is to be multiplied by 256 to get the percentage of packets sampled. For example, if the user enters a figure of 20 into this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port. Users may enter a value between *1* and *65535*. An entry of *0* disables the packet sampling. Since this is the default setting, users are reminded to configure a rate here. Otherwise, this function will not work.
TX Rate (0-65535)	Users can set the rate of packet sampling here. The value entered here is to be multiplied by 256 to get the percentage of packets sampled. For example, if the user enters a figure of 20 into this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port. Users may enter a value between *1* and *65535*. An entry of *0* disables the packet sampling. Since this is the default setting, users are reminded to configure a rate here. Otherwise, this function will not work.
Max Header Size (18-256)	This field will set the number of leading bytes of the sampled packet header. This sampled header will be encapsulated with the datagram to be forwarded to the Analyzer Server. The user may set a value between *18* and *256* bytes. The default setting is *128* bytes.

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

sFlow Poller Settings

The following windows will allow the user to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and then package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.

To configure the settings for the sFlow Counter Poller, click **Administration** > **sFlow** > **sFlow Poller Settings**, as shown below:



sFlow Counter Poller Settings

Port	Analyzer Server ID	Polling Interval (sec)	Modify	Delete

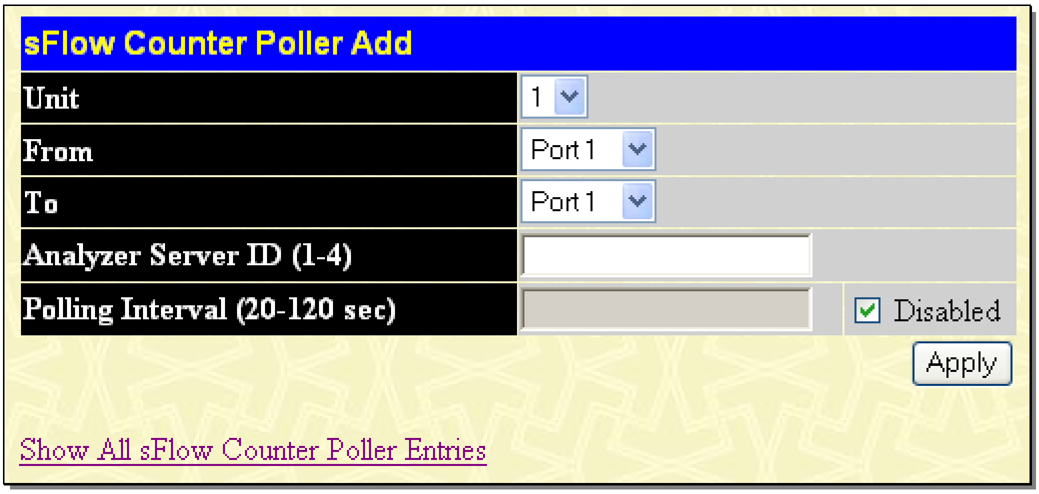
Total Entries: 0

Figure 2- 93. sFlow Counter Poller Settings window

The following fields are displayed:

Parameter	Description
Port	Displays the port from which packet counter samples are being taken.
Analyzer Server ID	Displays the ID of the Analyzer Server where datagrams, containing the packet counter polling information taken using this polling mechanism, will be sent.
Polling Interval (sec)	The Polling Interval displayed here, is measured in seconds and will take a poll of the IF counters for the corresponding port, every time the interval reaches 0 seconds.
Modify	Click this button to modify the settings for this entry. The **sFlow Counter Poller Edit** window will be produced for the user to configure.
Delete	Click the corresponding ☒ button of the entry to be deleted.

To delete all the entries in the table, click the **Clear All** button. To add a new sFlow Counter Poller setting, click the **Add** button, which will display the following window to be configured.



sFlow Counter Poller Add

Unit	1	
From	Port 1	
To	Port 1	
Analyzer Server ID (1-4)		
Polling Interval (20-120 sec)		☑ Disabled

Figure 2- 94. sFlow Counter Poller Add window

The following fields may be set:

Parameter	Description
Unit	Select the unit to configure.

From/To	Choose the beginning and ending range of ports to be configured for counter polling.
Analyzer Server ID (1-4)	Enter the previously configured Analyzer Server ID to state the device that will be receiving datagrams from the Switch. These datagrams will include the counter poller information taken using the polling mechanism configured here.
Polling Interval (20-120 sec)	Users may configure the Polling Interval here. The switch will take a poll of the IF counters every time this interval reaches 0, and this information will be included in the sFlow datagrams that will be sent to the sFlow Analyzer for examination. Ticking the Disabled check box will disable the counter polling for this entry.

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

Single IP Management Settings

Single IP Management (SIM) Overview

D-Link Single IP Management is a concept that stacks 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 1-32), 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 management 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 CaS 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.

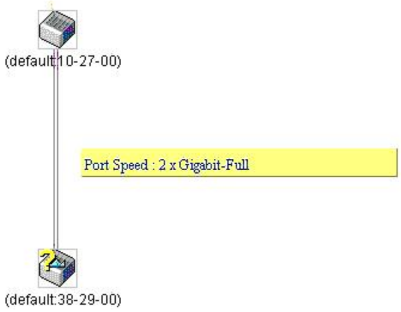
The Upgrade to v1.61

To better improve SIM management, the Switch has been upgraded to version 1.61 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.



NOTE: For more details regarding improvements made in SIMv1.61, please refer to the ***D-Link Single IP Management*** White Paper located on the D-Link website.

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

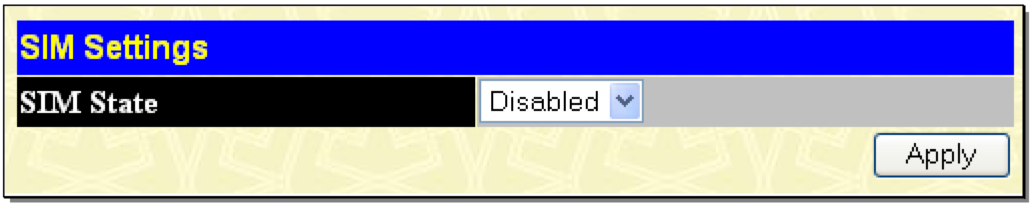
- Firmware – The switch now supports MS firmware downloads from a TFTP server.
- Configuration Files – This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS’s, using a TFTP server.
- Log – The switch now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

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

SIM Settings

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

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

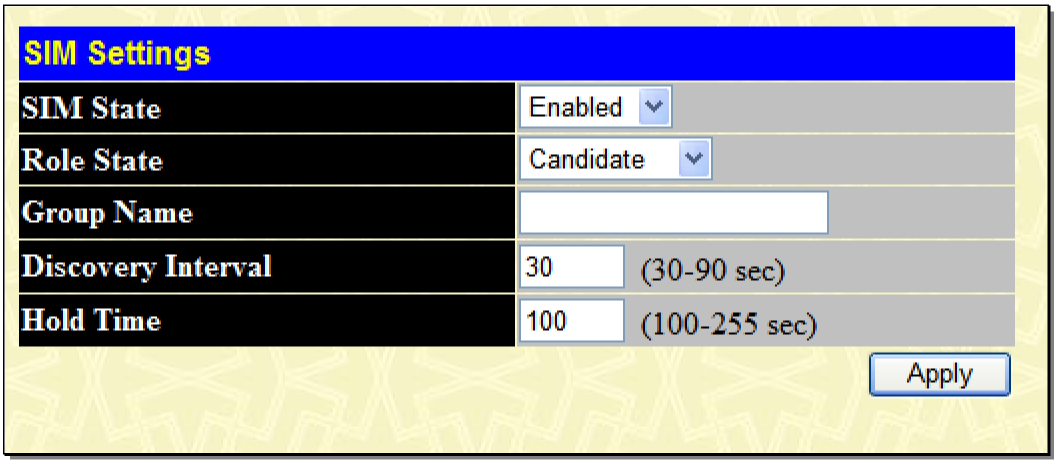


SIM Settings

SIM State: Disabled

Figure 2- 95. SIM Settings window (Disabled)

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



SIM Settings

SIM State	Enabled
Role State	Candidate
Group Name	
Discovery Interval	30 (30-90 sec)
Hold Time	100 (100-255 sec)

Figure 2- 96. 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 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.
Group Name	Enter a group name in this field.
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 the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from *100* to *255* seconds.

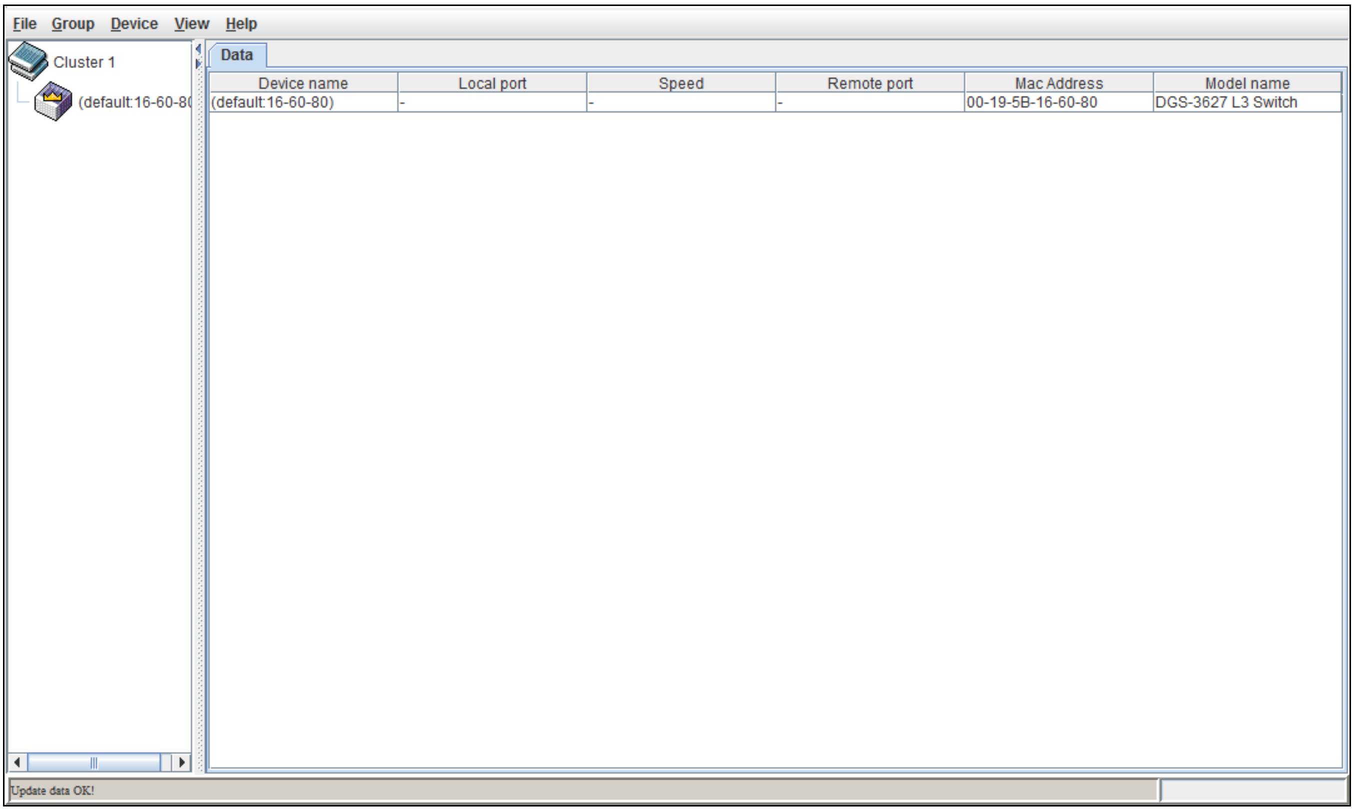
Click **Apply** to implement the settings changed.

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

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.



Device name	Local port	Speed	Remote port	Mac Address	Model name
(default:16-60-80)	-	-	-	00-19-5B-16-60-80	DGS-3627 L3 Switch

Figure 2- 97. Topology window

This window holds the following information under the **Data** tab:

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

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

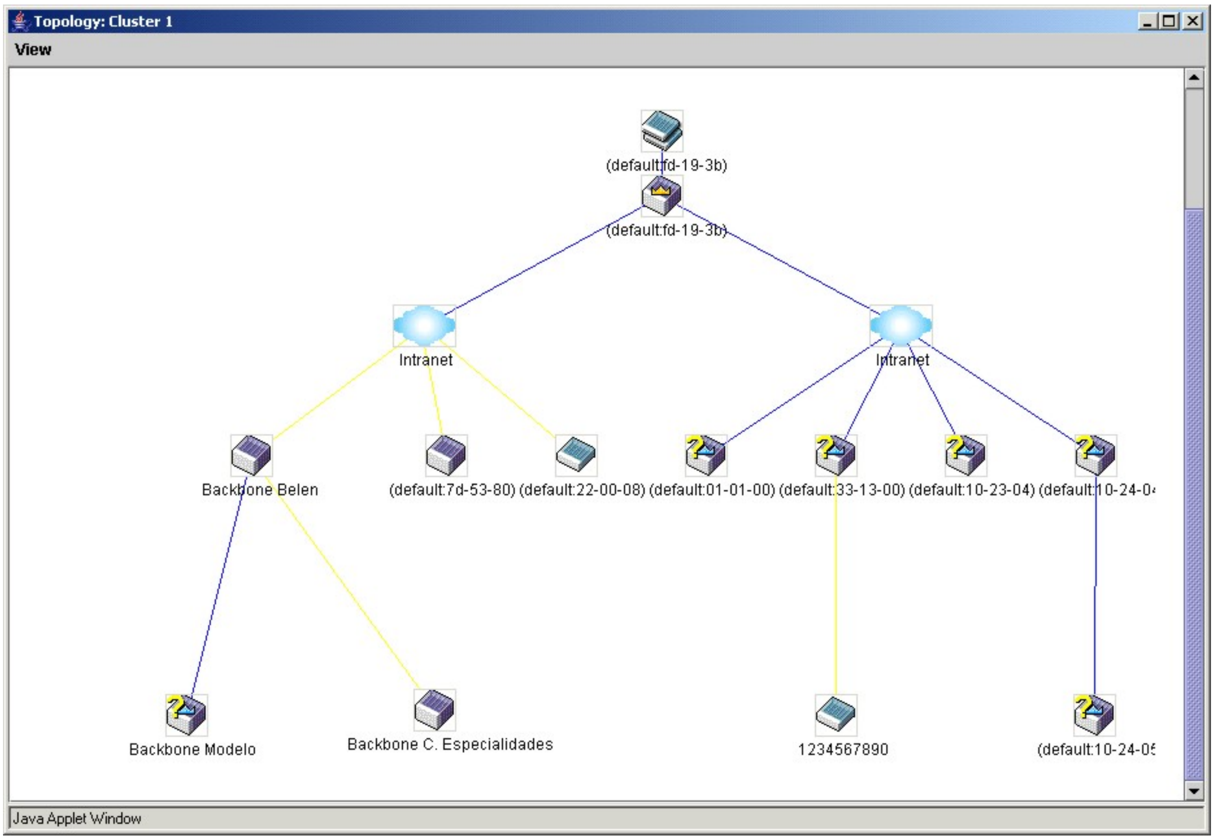
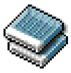
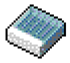
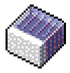
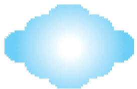


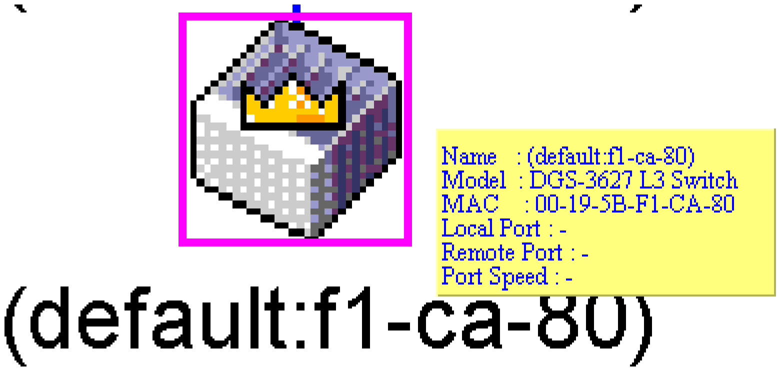
Figure 2- 98. Topology View window

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

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

Tool Tips

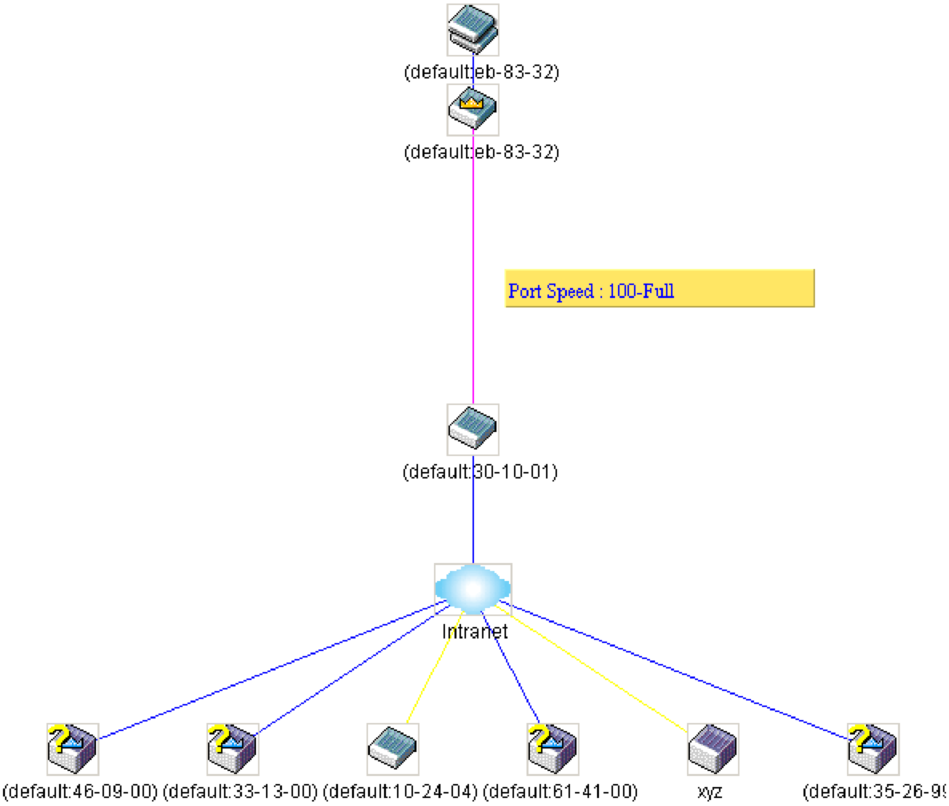
In the **Topology View** window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below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



Name : (default:f1-ca-80)
Model : DGS-3627 L3 Switch
MAC : 00-19-5B-F1-CA-80
Local Port : -
Remote Port : -
Port Speed : -

Figure 6- 99. 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:



Port Speed : 100-Full

Figure 2- 100. Port Speed Utilizing the Tool Tip

Right-Click

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

Group Icon

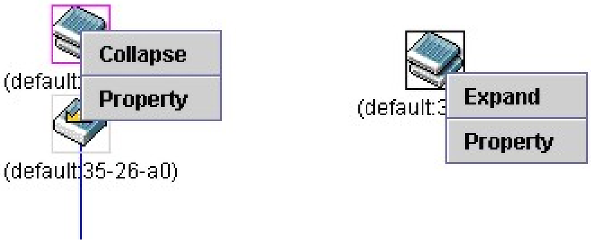


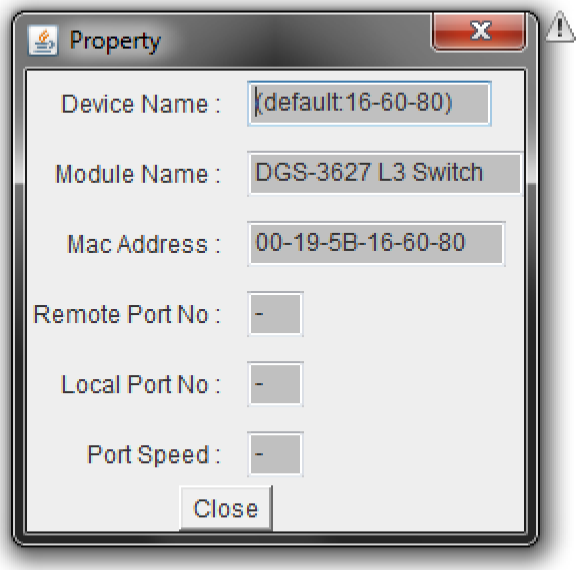
Figure 2- 101. Right-Clicking a Group Icon

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.



Property

Device Name : (default:16-60-80)

Module Name : DGS-3627 L3 Switch

Mac Address : 00-19-5B-16-60-80

Remote Port No : -

Local Port No : -

Port Speed : -

Figure 2- 102. 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

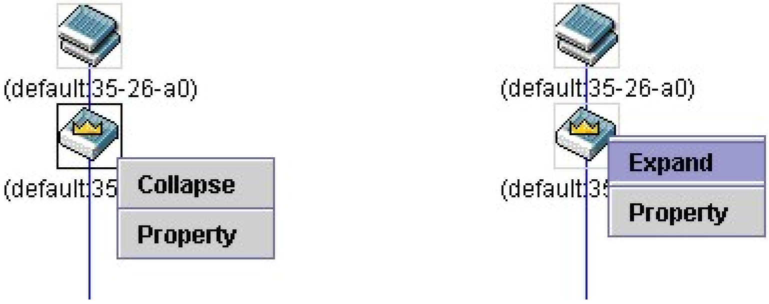


Figure 2- 103. Right-Clicking a Commander Icon

The following options may appear for the user to configure:

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

Expand - To expand the SIM group, in detail.

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

Member Switch Icon

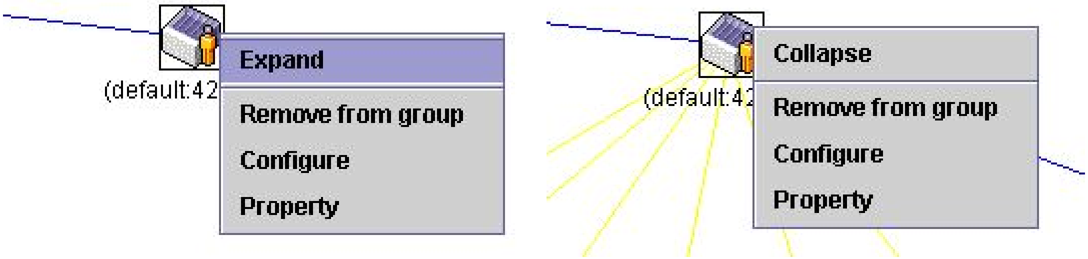


Figure 2- 104. Right-Clicking a Member icon

The following options may appear for the user to configure:

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

Expand - To expand the SIM group, in detail.

Remove from group - Remove a member from a group.

Configure - Launch the web management to configure the Switch.

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

Candidate Switch Icon

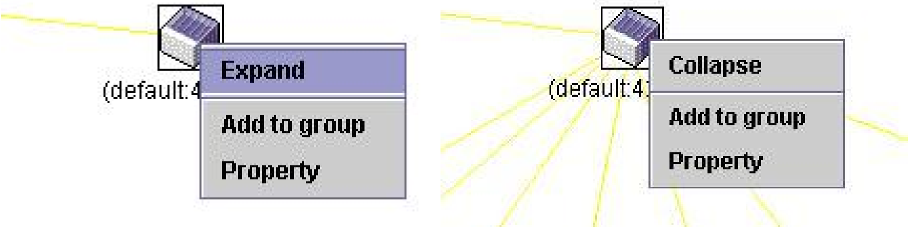


Figure 2- 105. Right-Clicking a Candidate icon

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 window for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the window.

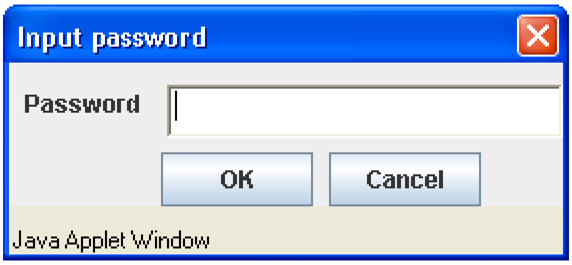


Figure 2- 106. Input password window

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

Menu Bar

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

Figure 2- 107. 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.

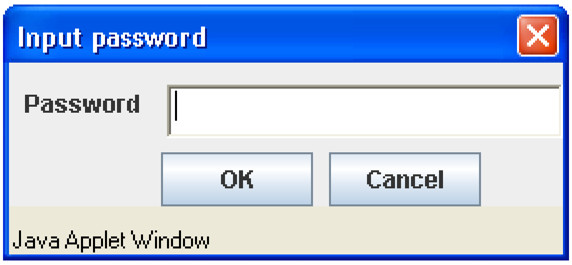


Figure 2- 108. Input password window

Remove from Group - Remove an MS from the group.

Device

Configure - Will open the Web manager for the specific device.

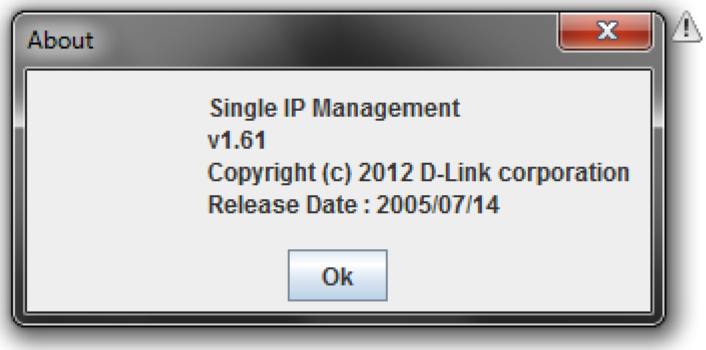
View

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.



Single IP Management
v1.61
Copyright (c) 2012 D-Link corporation
Release Date : 2005/07/14

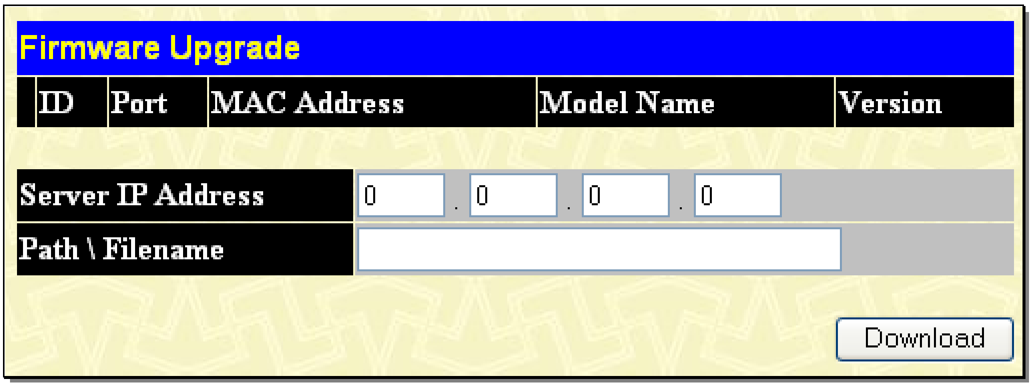
Figure 2- 109. About window

NOTE: Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the ***DGS-3600 Series CLI Refence Guide*** for more information on SIM and its configurations.

Firmware Upgrade

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

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



ID	Port	MAC Address	Model Name	Version

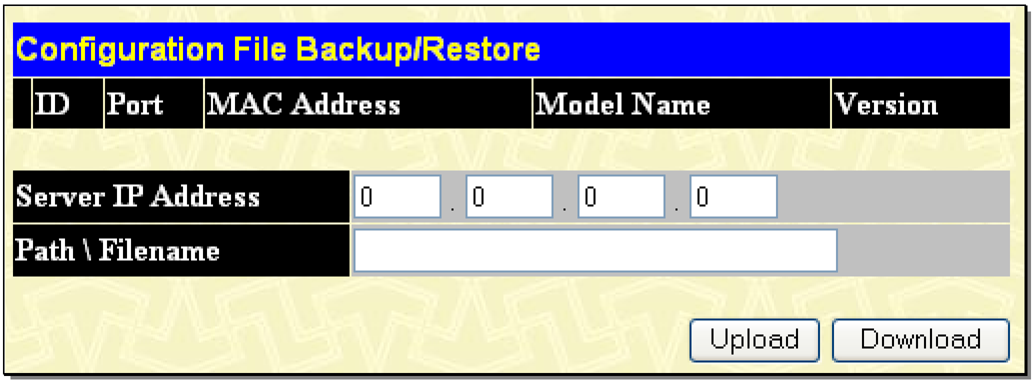
Server IP Address	0 . 0 . 0 . 0
Path \ Filename	

Figure 2- 110. Firmware Upgrade window

Configuration File Backup/Restore

This screen is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the Port heading. To update the configuration file, enter the Server IP Address where the file resides and enter the

Path/Filename of the configuration file. Click **Download** to initiate the file transfer from a TFTP server to the Switch. Click **Upload** to backup the configuration file to a TFTP server.



Configuration File Backup/Restore

ID	Port	MAC Address	Model Name	Version

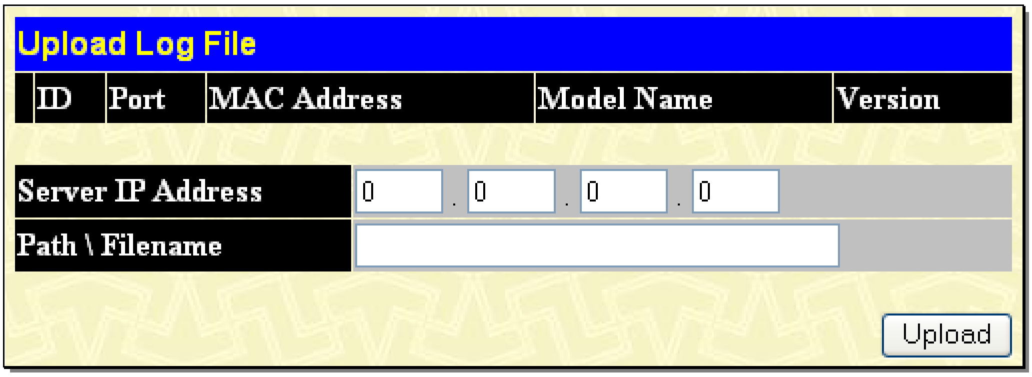
Server IP Address: 0 . 0 . 0 . 0

Path \ Filename:

Figure 2- 111. Configuration File Backup/Restore window

Upload Log

The following window is used to upload log files from SIM member switches to a specified PC. To upload a log file, enter the IP address of the SIM member switch and then enter a path on your PC where you wish to save this file. Click **Upload** to initiate the file transfer.



Upload Log File

ID	Port	MAC Address	Model Name	Version

Server IP Address: 0 . 0 . 0 . 0

Path \ Filename:

Figure 2- 112. Upload Log File window

Section 3

L2 Features

VLAN

Trunking

IGMP Snooping

MLD Snooping

Loopback Detection Global Settings

Spanning Tree

Forwarding & Filtering

LLDP

Q-in-Q

ERPS

DULD Settings

NLB Multicast FDB Settings

The following section will aid the user in configuring security functions for the Switch all functions are discussed in detail in the following section.

VLAN

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 also allows further tailoring of how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows users 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 Switch

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

The Switch supports IEEE 802.1Q VLANs. 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.

IEEE 802.1Q VLANs

Some relevant terms:

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

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

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

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

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

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

The main characteristics of IEEE 802.1Q are as follows:

Assigns packets to VLANs by filtering.

Assumes the presence of a single global spanning tree.

Uses an explicit tagging scheme with one-level tagging.

802.1Q VLAN Packet Forwarding

Packet forwarding decisions are made based upon the following three types of rules:

Ingress rules - rules relevant to the classification of received frames belonging to a VLAN.

Forwarding rules between ports - decides whether to filter or forward the packet.

Egress rules - determines if the packet must be sent tagged or untagged.

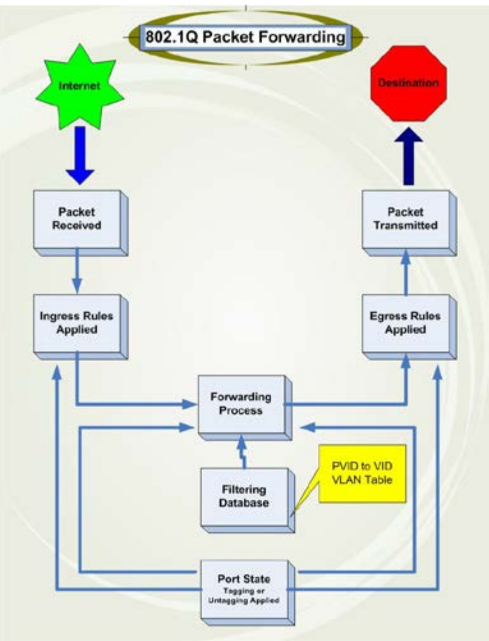


Figure 3- 1. IEEE 802.1Q Packet Forwarding

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.

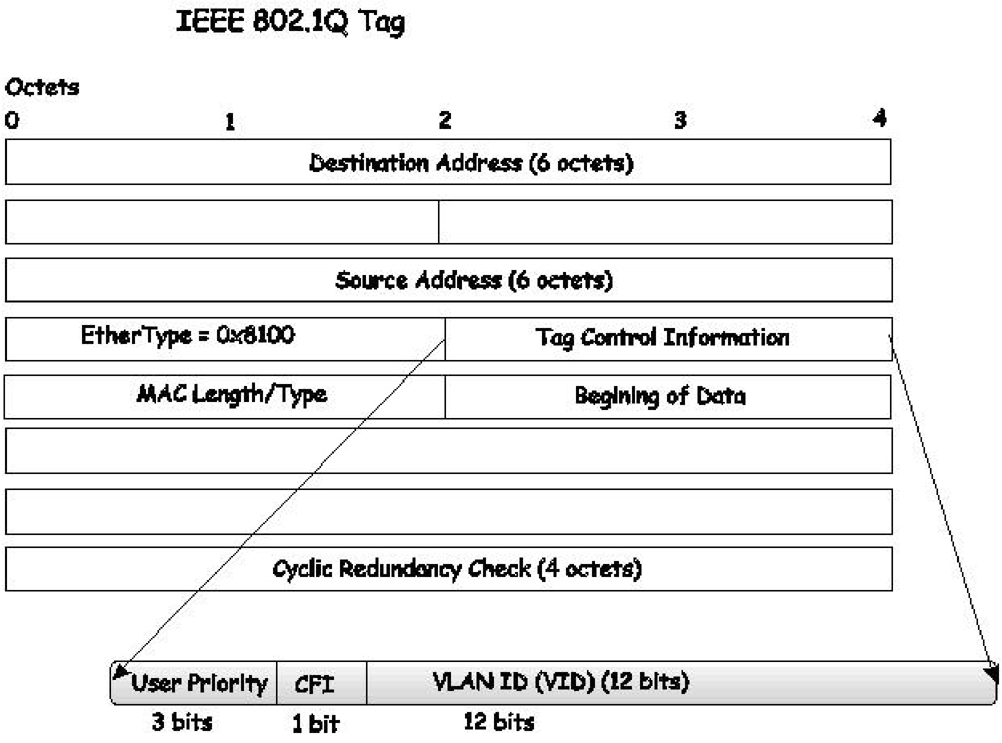


Figure 3- 2. IEEE 802.1Q Tag

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.

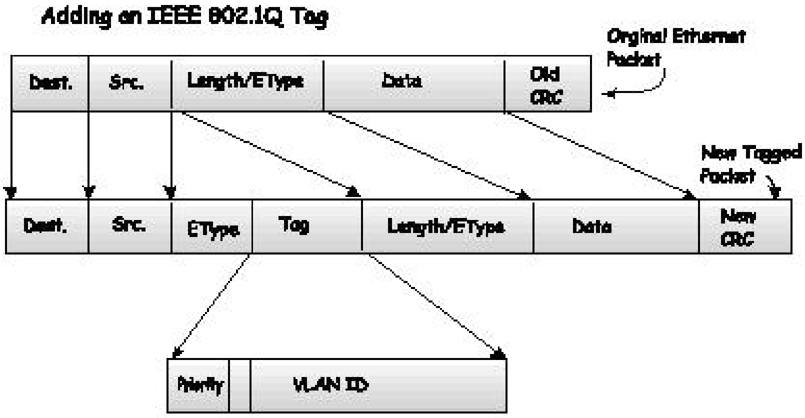


Figure 3- 3. Adding an IEEE 802.1Q Tag

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,
Engineering	2	9, 10
Marketing	3	3, 4
Finance	4	11, 12
Sales	5	1, 2, 3, 4

Figure 3- 4. VLAN Example - Assigned Ports

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 such as printers and servers 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

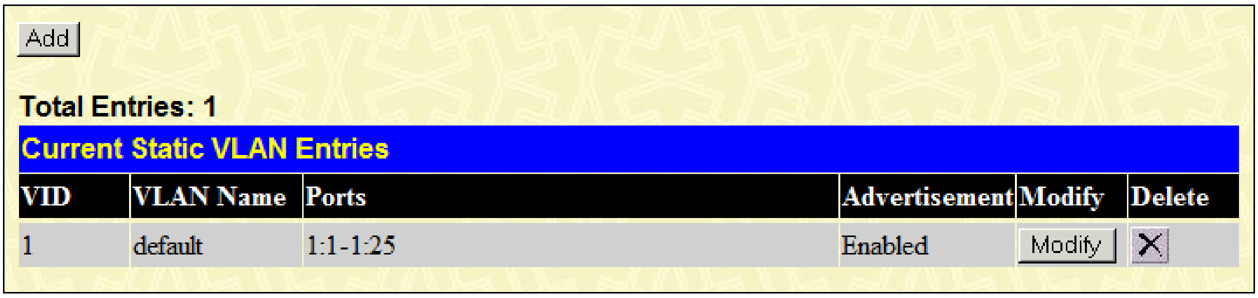
The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

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 users wish to change the port trunk grouping with VLANs already in place, there will be no 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.

Static VLAN Entries

This window is used to create static VLAN entries on the switch.

To view this window, click **L2 Features > VLAN > Static VLAN Entries**, as shown below:



Total Entries: 1

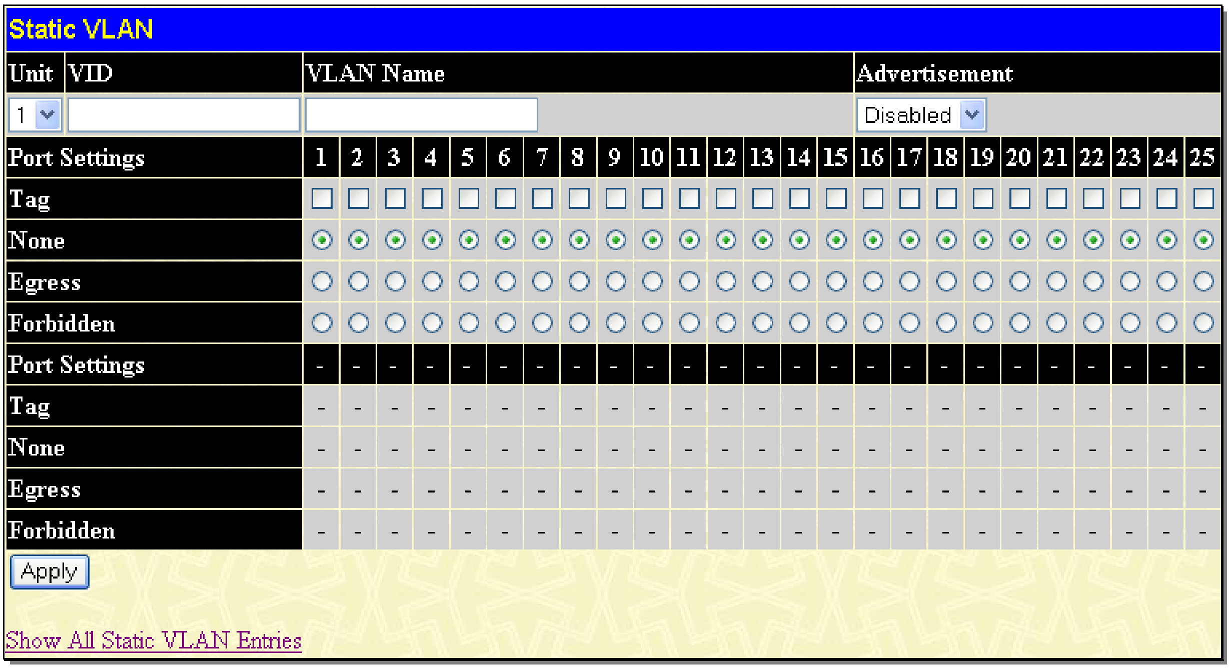
Current Static VLAN Entries

VID	VLAN Name	Ports	Advertisement	Modify	Delete
1	default	1:1-1:25	Enabled	Modify	☒

Figure 3- 5. Current Static VLAN Entries window

The **Current 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, 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.



Static VLAN

Unit	VID	VLAN Name	Advertisement
1			Disabled

Port Settings	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
Tag	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Egress	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Port Settings	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Tag	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Egress	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Figure 3- 6. Static VLAN window - Add

To return to the **Current Static VLAN Entries** window, click the Show All Static VLAN Entries link. To change an existing 802.1Q VLAN entry, click the corresponding **Modify** button, a new window will appear which will allow the user to configure the port settings and assign a unique name and number to the new VLAN.

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

NOTE: When the PVID Auto Assign function is disabled, users must manually configure the PVID for untagged ports or the host may not connect to the Switch correctly.

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

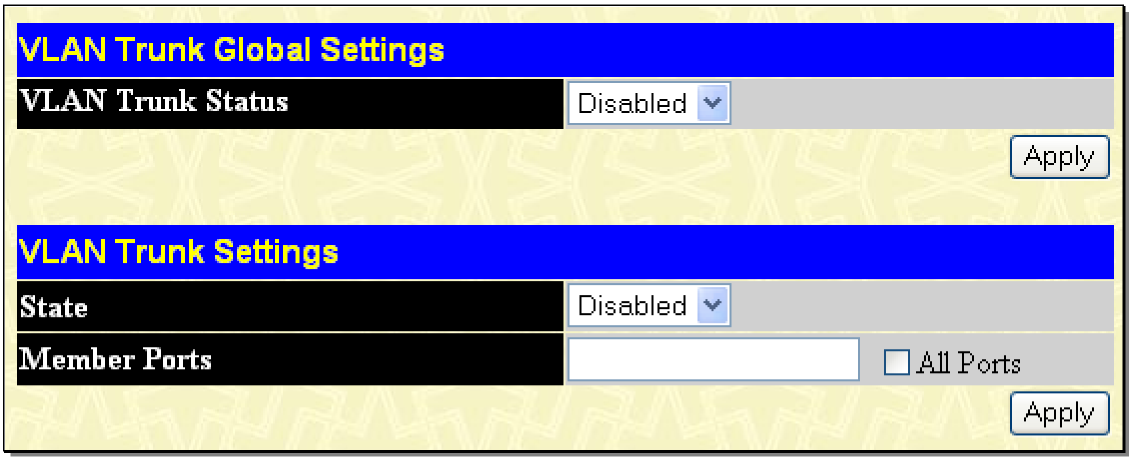
Parameter	Description
Unit	Select the unit you wish to configure.
VID (VLAN ID)	Allows the entry of a VLAN ID in the **Add** window, or displays the VLAN ID of an existing VLAN in the **Modify** window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the **Add** window, or displays 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.

VLAN Trunk

This window is used to configure VLAN trunk settings.

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



VLAN Trunk Global Settings

VLAN Trunk Status: Disabled

VLAN Trunk Settings

State: Disabled

Member Ports: □ All Ports

Figure 3- 7. VLAN Trunk Global Settings window

The following parameters can be configured:

Parameter	Description
VLAN Trunk Status	Use the pull-down menu to enable or disable VLAN trunk global status.

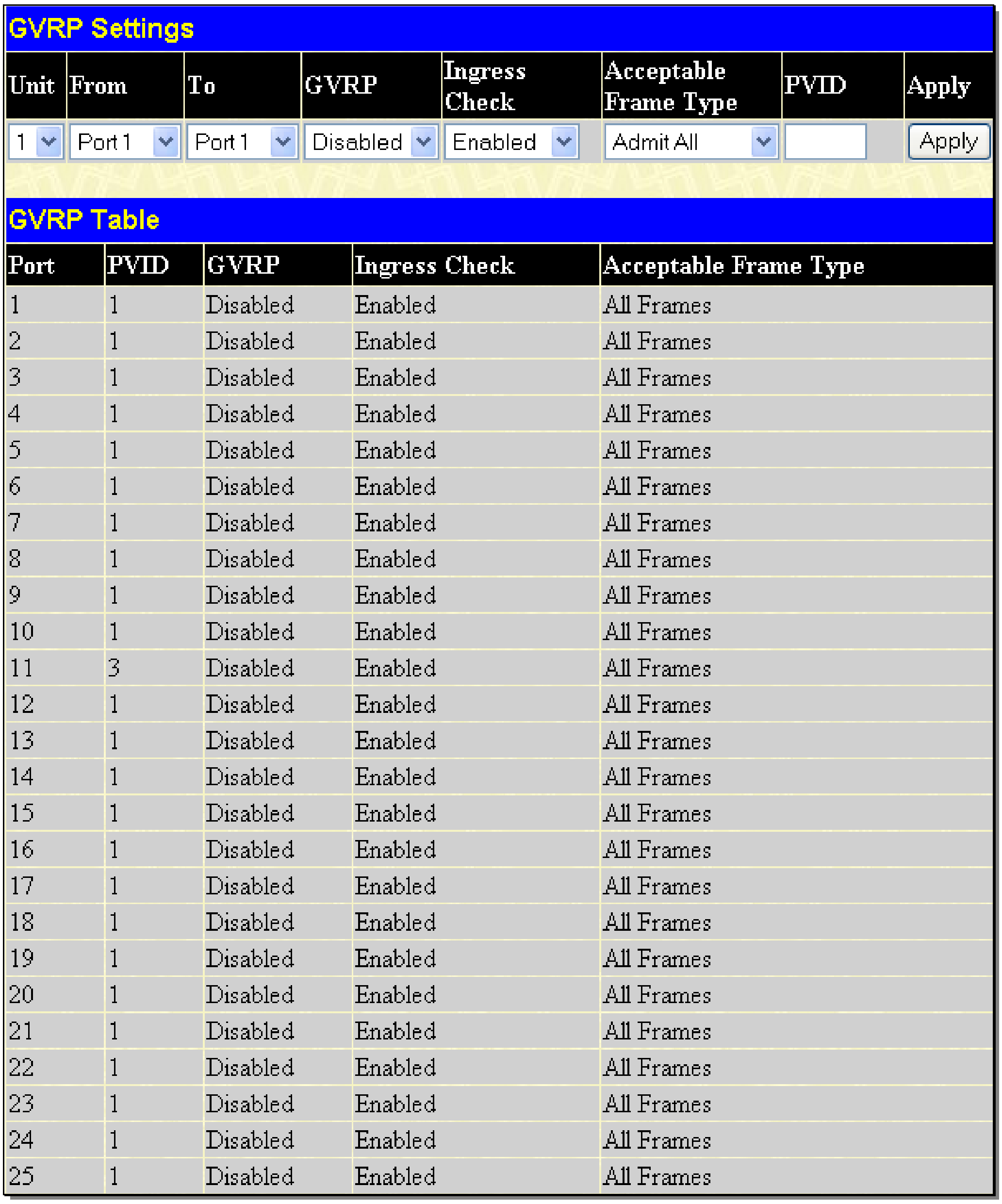
State	Use the pull-down menu to enable or disable VLAN trunk port state.
Member Ports	Enter the ports for VLAN trunk. Tick the **All Ports** check box to select all ports.

Click **Apply** to implement the changes.

GVRP Settings

This window 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 VID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

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



GVRP Settings

Unit	From	To	GVRP	Ingress Check	Acceptable Frame Type	PVID	Apply
1	Port 1	Port 1	Disabled	Enabled	Admit All		Apply

GVRP Table

Port	PVID	GVRP	Ingress Check	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
4	1	Disabled	Enabled	All Frames
5	1	Disabled	Enabled	All Frames
6	1	Disabled	Enabled	All Frames
7	1	Disabled	Enabled	All Frames
8	1	Disabled	Enabled	All Frames
9	1	Disabled	Enabled	All Frames
10	1	Disabled	Enabled	All Frames
11	3	Disabled	Enabled	All Frames
12	1	Disabled	Enabled	All Frames
13	1	Disabled	Enabled	All Frames
14	1	Disabled	Enabled	All Frames
15	1	Disabled	Enabled	All Frames
16	1	Disabled	Enabled	All Frames
17	1	Disabled	Enabled	All Frames
18	1	Disabled	Enabled	All Frames
19	1	Disabled	Enabled	All Frames
20	1	Disabled	Enabled	All Frames
21	1	Disabled	Enabled	All Frames
22	1	Disabled	Enabled	All Frames
23	1	Disabled	Enabled	All Frames
24	1	Disabled	Enabled	All Frames
25	1	Disabled	Enabled	All Frames

Figure 3- 8. GVRP Settings window

The following parameters may be configured.

Parameter	Description
Unit	Select the unit to configure.
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.

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 - and the tagging packet is forwarded to the port for transmission, then the untagged packets will be dropped. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The GARP 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 using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables ingress filtering. Ingress Checking is *Enabled* by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *Admit_All*, which mean both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.

Click **Apply** to implement changes made.

Double VLAN

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

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

Here is an example Double VLAN tagged packet.

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

Consider the example below:

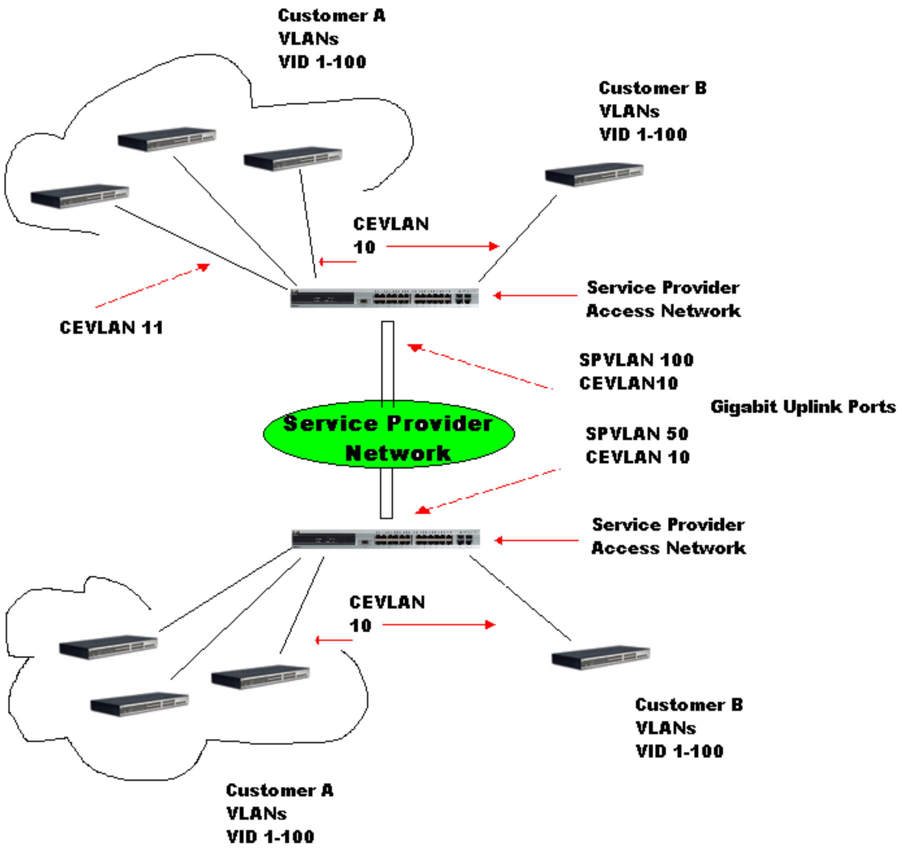


Figure 3- 9. Double VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs. Both CEVLANs (Customer VLANs), 10 and 11, are tagged with the SPVID 100 on the Service Provider Access Network and therefore belong to one VLAN on the Service Provider's network, thus being a member of two VLANs. In this way, the Customer can retain its normal VLAN and the Service Provider can congregate multiple Customer VLANs within one SPVLAN, 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

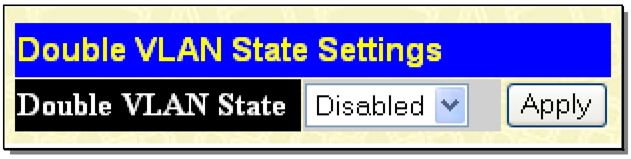
Some rules and regulations apply with the implementation of the Double VLAN procedure.

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

Double VLAN Settings

This window is used to enable the double VLAN settings on the Switch.

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

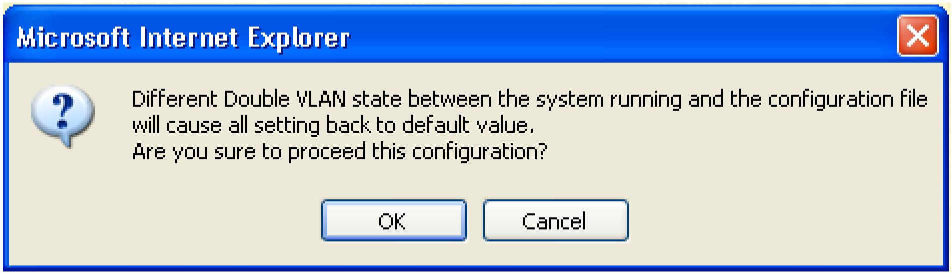


Double VLAN State Settings

Double VLAN State: Disabled

Figure 3- 10. Double VLAN State Settings window

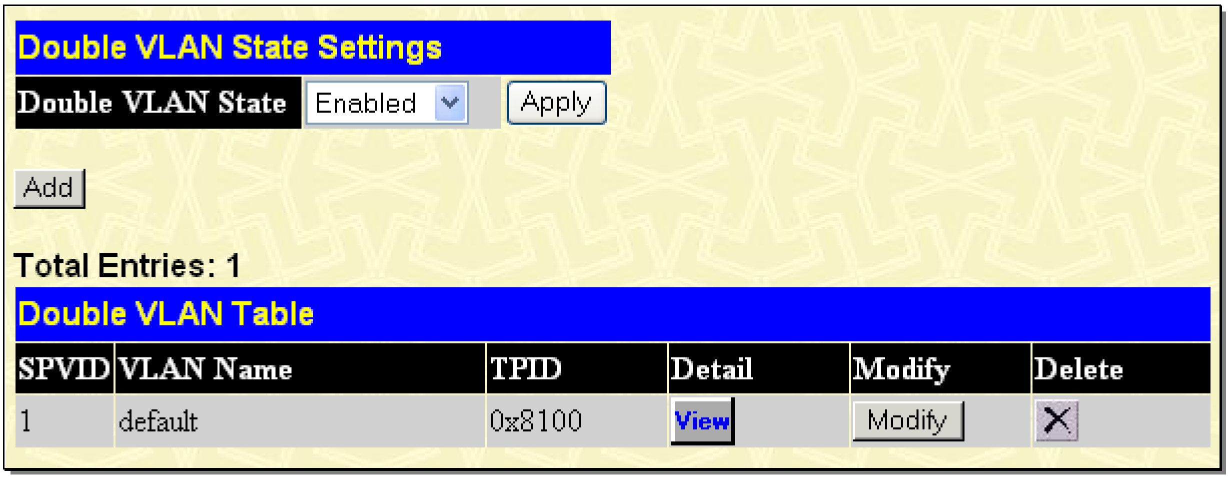
Choose *Enabled* using the pull-down menu and click **Apply**. The user will be prompted with the following warning window. Click **OK** to continue.



Microsoft Internet Explorer

Different Double VLAN state between the system running and the configuration file will cause all setting back to default value.
Are you sure to proceed this configuration?

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



Double VLAN State Settings

Double VLAN State: Enabled

Total Entries: 1

Double VLAN Table

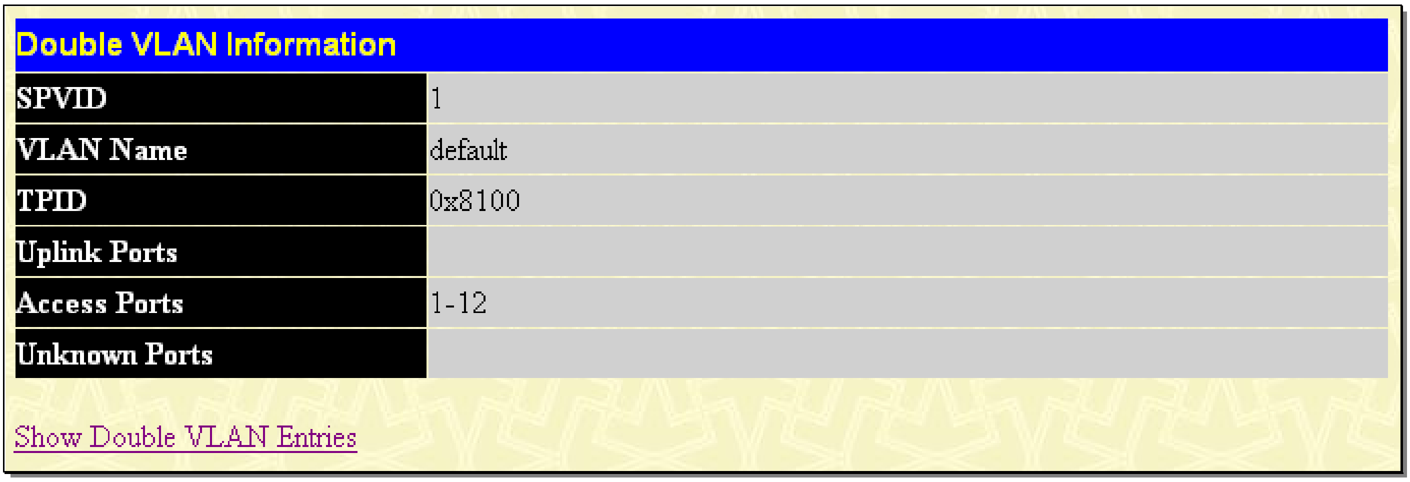
SPVID	VLAN Name	TPID	Detail	Modify	Delete
1	default	0x8100	View	Modify	✕

Figure 3- 11. Double VLAN State Settings window (*Enabled*)

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.

The user may view configurations for a Double VLAN by clicking its corresponding View button, which will display the following read-only window.



Double VLAN Information

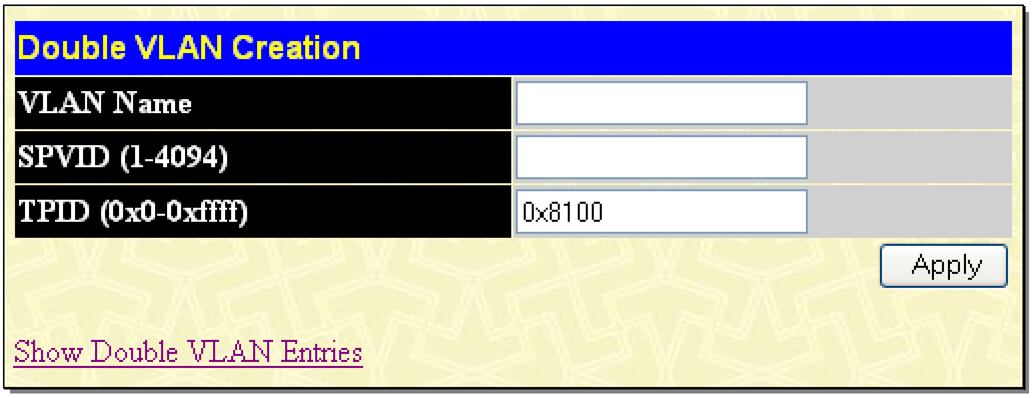
SPVID	1
VLAN Name	default
TPID	0x8100
Uplink Ports	
Access Ports	1-12
Unknown Ports	

Figure 3- 12. Double VLAN Information window

Parameters shown in the previous window are explained below:

Parameter	Description
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	These ports are set as uplink ports on the Switch. Uplink ports are for connecting Switch VLANs to the Service Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports.
Access Ports	These are the ports that are set as access ports on the Switch. Access ports are for connecting Switch VLANs to customer VLANs. Gigabit ports cannot be configured as access ports.
Unknown Ports	These are the ports that are a part of the VLAN but have yet to be defined as Access or Uplink ports.

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



Double VLAN Creation

VLAN Name	
SPVID (1-4094)	
TPID (0x0-0xffff)	0x8100

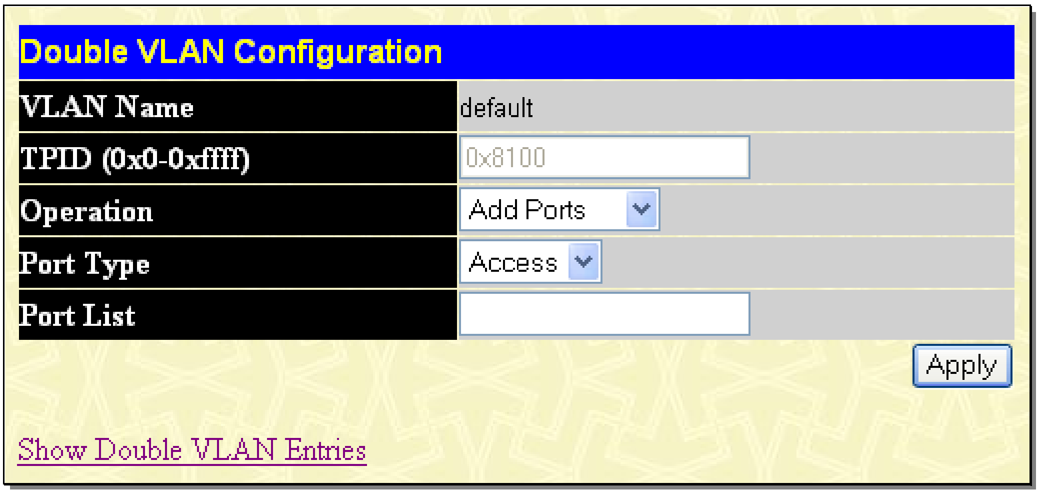
Figure 3- 13. Double VLAN Creation window

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.

Click **Apply** to implement changes made.

To configure the parameters for a previously created Service Provider VLAN, click the Modify button of the corresponding SPVID in the Double VLAN Table. The following window will appear for the user to configure.



Double VLAN Configuration

VLAN Name	default
TPID (0x0-0xffff)	0x8100
Operation	Add Ports
Port Type	Access
Port List	

Figure 3- 14. Double VLAN Configuration window

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

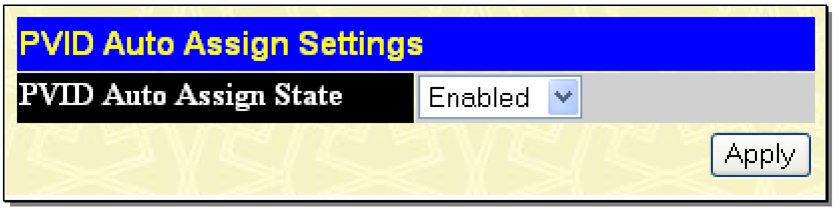
Parameter	Description
VLAN Name	The name of the pre-configured VLAN name to be configured.
TPID (0x0-0xffff)	The tagged protocol ID. Enter the new TPID in hex form to aid in packet identification of the Service Provider VLAN.
Operation	Allows one of the following three acts to be performed: *Add Ports* – Will allow users to add ports to this Service Provider VLAN using the Port List field below. *Delete Ports* – Will allow users to remove ports from the Service Provider VLAN configured, using the Port List field below. *Config TPID* – Will allow users to configure the Tagged Protocol ID of the Service Provider VLAN, in hex form.
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. The beginning and end of the port list range are separated by a dash.

PVID Auto Assign

This enables the PVID Auto Assign features on the switch.

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



PVID Auto Assign Settings

PVID Auto Assign State	Enabled

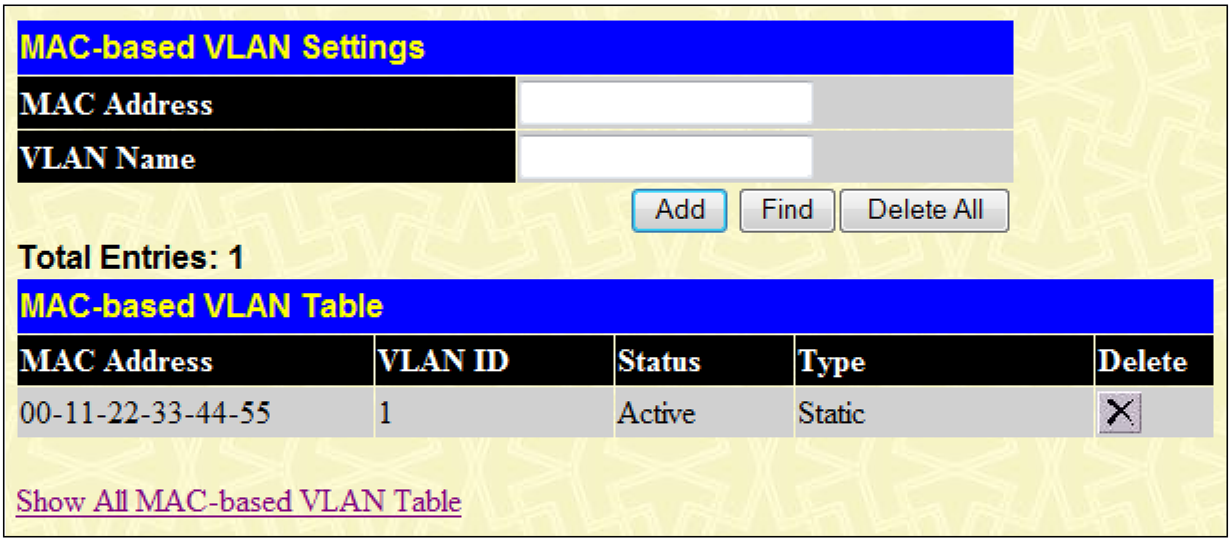
Figure 3- 15. PVID Auto Assign Settings window

When *Enabled*, PVID will be automatically assigned when adding a port to a VLAN as an untagged member port.

MAC-based VLAN Settings

This table is used to create MAC-based VLAN entries on the switch. A MAC Address can be mapped to any existing static VLAN and multiple MAC addresses can be mapped to the same VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user is able to be serviced under the specified VLAN regardless of the authentiucation function operated on the port.

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



MAC-based VLAN Settings

MAC Address	
VLAN Name	

Total Entries: 1

MAC-based VLAN Table

MAC Address	VLAN ID	Status	Type	Delete
00-11-22-33-44-55	1	Active	Static	☒

Figure 3- 16. MAC-based VLAN Settings window

The following parameters can be configured

Parameter	Description
MAC Address	Specifies the MAC Address of the entry you wish to **Add** or **Find**.
VLAN Name	Specifies the VLAN to be associated with the MAC Address.

To delete a specific entry click the corresponding ☒ button, to clear all entries click **Delete All**.

Protocol VLAN

The Switch 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 pre-defined protocols for configuration. The user can define a protocol by properly configuring the protocol value.

The following is a list of protocol values for some common protocols.

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
decLAT	0x6004
SNA 802.2	0x0404
netBios	0xF0F0
XNS	0x0600
VINES	0x0BAD
IPV6	0x86DD
AppleTalk	0x809B
RARP	0x8035
SNA over Ethernet2	0x80D5

Table 3- 1. Protocol VLAN and the corresponding protocol value

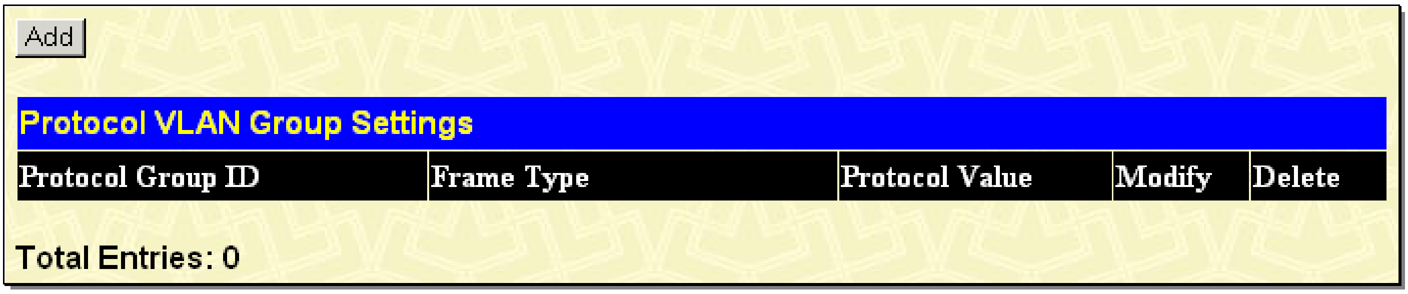
The following windows are used to create Protocol VLAN groups on the switch. The purpose of these Protocol VLAN groups is to identify ingress untagged packets and quickly and accurately send them to their destination. Ingress untagged packets can be identified by a protocol value in the packet header, which has been stated here by the user. Once identified, these packets can be tagged with the appropriate tags for VLAN and priority and then relayed to their destination.

To achieve this goal, users must first properly set the type of protocol, along with the identifying value located in the packet header and apply it to a protocol group, which is identified by an ID number. Once the group has been created and configured, then users must add it to a port or set of ports using the **Protocol VLAN Port Settings** window, and configure the appropriate VLAN and priority tags for these untagged packets. When these actions are completed and saved to the switch, then the ingress and untagged packets can be appropriately dealt with and forwarded through the switch.

Protocol VLAN Group Settings

This window is used to begin the Protocol Group VLAN configurations.

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



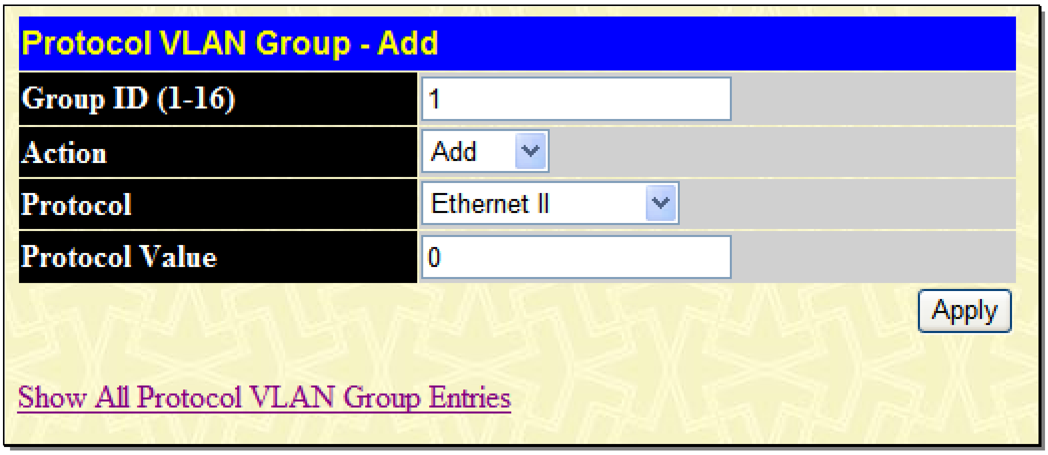
Protocol VLAN Group Settings

Protocol Group ID	Frame Type	Protocol Value	Modify	Delete

Total Entries: 0

Figure 3- 17. Protocol VLAN Group Settings window

Click the **Add** button to reveal the following window for the user to configure:



Protocol VLAN Group - Add

Group ID (1-16)	1
Action	Add
Protocol	Ethernet II
Protocol Value	0

Figure 3- 18. Protocol VLAN Group – Add window

The Add and Modify windows of the **Protocol VLAN Group** hold the following fields to be configured:

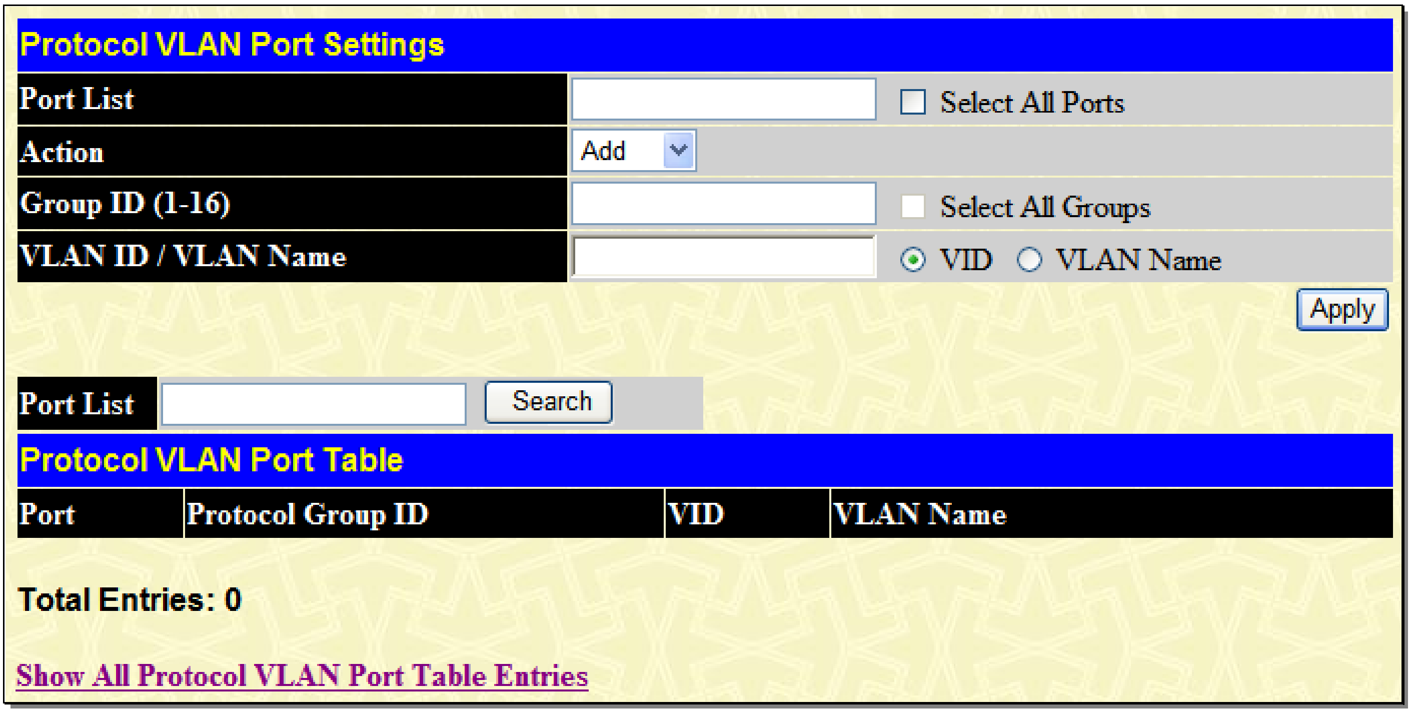
Parameter	Description
Group ID (1-16)	Enter an integer from *1* to *16* to identify the protocol VLAN group being created here. For the Modify window, this field will display the Protocol Group ID number of the group being configured.
Action	Use the pull-down menu to add or delete the protocol to this group. This protocol is identified using the following Protocol field.
Protocol	Use the pull-down menu to select the frame type to be added or deleted from this profile. The frame type indicates the frame format. The user has three choices for frame type: *Ethernet II* – Choose this parameter if you wish this protocol group to employ the Ethernet II frame type. In this frame type, the protocol is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following Protocol Value. *IEEE802.3 SNAP* – Choose this parameter if you wish this protocol group to employ the Sub Network Access Protocol (SNAP) frame type. For this frame type, the protocol is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following Protocol Value. *IEEE802.3 LLC* – Choose this parameter if you wish this protocol group to employ the Link Logical Control (LLC) frame type. For this frame type, the protocol is identified by the 2-octet IEEE802.3 Link Service Access Point (LSAP) pair field in the packet header, which is to be stated using the following Protocol Value. The first octet defines the Destination Service Access Point value and the second octet is the Source Service Access Point (SSAP) value.
Protocol Value	Enter the corresponding protocol value of the protocol identified in the previous field. This value must be stated in a hexadecimal form.

Click **Apply** to implement changes made.

Protocol VLAN Port Settings

The following window is used to add a Protocol VLAN Group profile to a port or list of ports and adjust the tags for incoming untagged packets before being relayed through the Switch.

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



Protocol VLAN Port Settings

Port List	□ Select All Ports
Action	Add
Group ID (1-16)	□ Select All Groups
VLAN ID / VLAN Name	● VID ○ VLAN Name

Protocol VLAN Port Table

Port	Protocol Group ID	VID	VLAN Name

Total Entries: 0

Show All Protocol VLAN Port Table Entries

Figure 3- 19. Protocol VLAN Port Settings window

The following fields may be configured:

Parameter	Description
Port List	Use this parameter to assign ports to a Protocol VLAN Group or remove them from the Protocol VLAN Group. Ticking the Select All Ports check box will configure this Protocol VLAN Group to all ports on the switch.
Action	Use the pull-down menu to add or delete the following Group ID to or from the ports selected in the previous field.
Group ID (1-16)	Enter the ID number of the Protocol VLAN Group for which to add or remove from the selected ports. Ticking the Select All Groups check box will apply all Protocol VLAN groups to the ports listed in the Port List field.
VLAN ID / VLAN Name	Use this field to add a VLAN to be associated with this configuration. Select the correct radio button if you are using a VLAN Name or a VID (VLAN ID).

Click **Apply** to implement changes made. The Protocol VLAN Port Table in the bottom half of the window will display correctly configured ports to Protocol Group configurations, along with associated VLANs and priorities. Users may use the Port List Search in the middle of the window to display configurations based on ports on the switch. Clicking the Show All Protocol VLAN Port Table Entries link will display all Protocol VLAN Port Table entries.

Subnet VLAN

The Subnet VLAN section includes Subnet VLAN Settings and VLAN Precedence Settings. Subnet VLAN is used to assign VIDs for untagged or priority-tagged frames based on source IPv4 or IPv6 address. If the ingress frame is untagged or priority-tagged frame, the source IPv4 address or the upper 64 bits of the IPv6 source address of the frame will be used as a key to look up the subnet VLAN table. If there is a matched entry, the VID of the frame will be picked up from the matched entry. If the frame is untagged, the priority will be picked up from it too. For priority-tagged packet, its priority will not change.

Subnet VLAN can support making an IP address map to any existing static VLAN, but it can’t support making the same IP address mapping to more than one VLAN. The VLAN classification precedence is configurable on each port. The default value is MAC-based VLAN classification precedence.

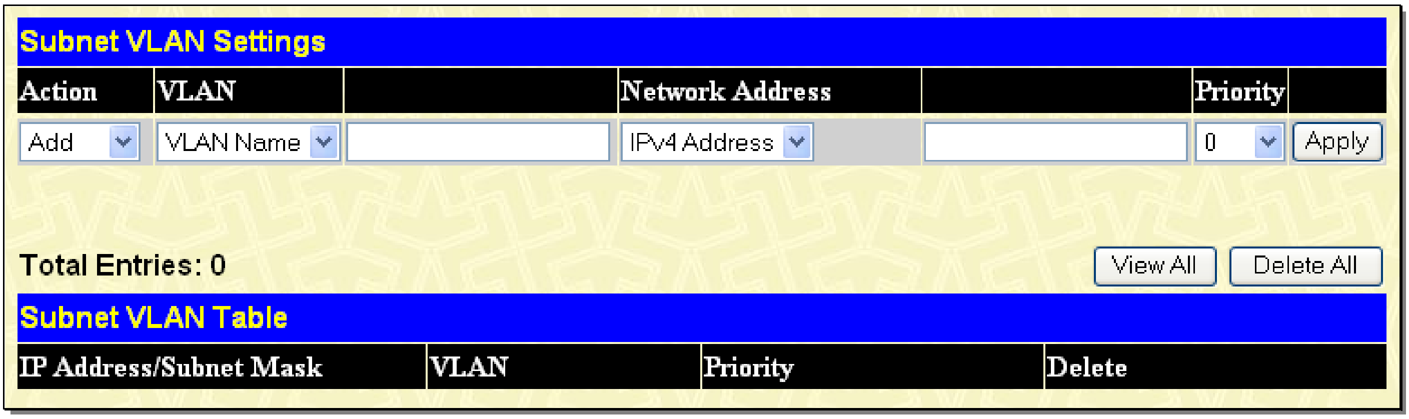
Note:

1. If the IP address of the received untagged packet matches two entries in the table, the longest-prefix match order is used.
2. To make the subnet VLAN work well, users must add the ingress port to the VLAN member ports.

3. The subnet VLAN may affect the authorization protocol, such as 802.1X, WAC, JWAC, MAC-based access control, and compound authentication. Since the authorized port will be assigned to target VLANs and set its PVID to the target VLAN ID, if the subnet VLAN takes effect, the ingress packets on this port may not be classified to target VLANs and may cause the authorization protocol to work less efficiently.

Subnet VLAN Settings

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



Subnet VLAN Settings

Action	VLAN		Network Address		Priority	
Add	VLAN Name		IPv4 Address		0	Apply

Total Entries: 0

Subnet VLAN Table

IP Address/Subnet Mask	VLAN	Priority	Delete

Figure 3- 20. Subnet VLAN Settings window

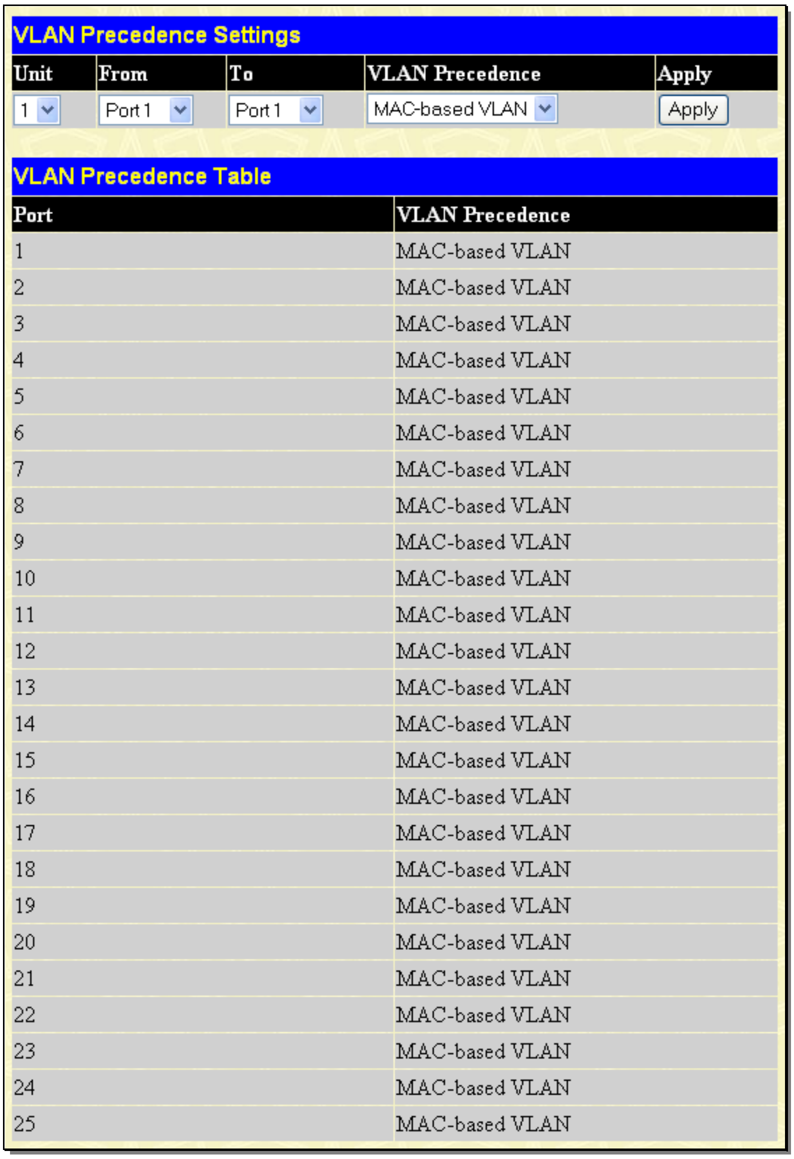
Parameter	Description
Action	Use the pull-down menu to *Add*, *Delete* or *Find* the subnet VLAN.
VLAN	Use the pull-down menu to select *VLAN Name* or *VID* to enter in the field next to it.
Network Address	Use the pull-down menu to select *IPv4 Address* or *IPv6 Address* to enter in the field next to it.
Priority	Use the pull-down menu to select priority *0* to *7*.

Click **Apply** to implement the changes. Click **View All** to see all the entries. Click **Delete All** to remove all the entries.

VLAN Precedence Settings

This window is used to configure VLAN precedence settings.

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



VLAN Precedence Settings

Unit	From	To	VLAN Precedence	Apply
1	Port 1	Port 1	MAC-based VLAN	Apply

VLAN Precedence Table

Port	VLAN Precedence
1	MAC-based VLAN
2	MAC-based VLAN
3	MAC-based VLAN
4	MAC-based VLAN
5	MAC-based VLAN
6	MAC-based VLAN
7	MAC-based VLAN
8	MAC-based VLAN
9	MAC-based VLAN
10	MAC-based VLAN
11	MAC-based VLAN
12	MAC-based VLAN
13	MAC-based VLAN
14	MAC-based VLAN
15	MAC-based VLAN
16	MAC-based VLAN
17	MAC-based VLAN
18	MAC-based VLAN
19	MAC-based VLAN
20	MAC-based VLAN
21	MAC-based VLAN
22	MAC-based VLAN
23	MAC-based VLAN
24	MAC-based VLAN
25	MAC-based VLAN

Figure 3- 21. VLAN Precedence Settings window

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From/To	These two fields allow the range of ports that will be included in the VLAN precedence.
VLAN Precedence	Use the pull-down menu to select the VLAN precedence as *MAC-based VLAN* or *Subnet VLAN*.

Click **Apply** to implement the changes.

Super VLAN

This section is used to create a super VLAN. The specified VLAN must be an 802.1Q VLAN. If the specified VLAN does not exist, the operation will not be successful.

NOTE:

1. If a user specifies the super VLAN name, the VLAN must be an existing 802.1Q VLAN.

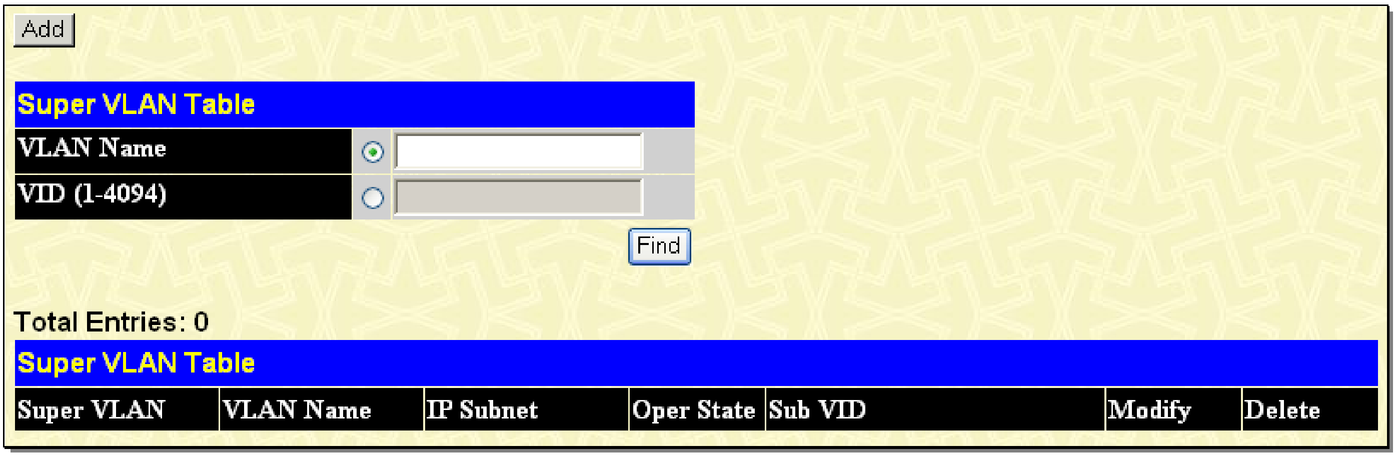
2. L3 route protocols, VRRP, multicast protocols, and IPV6 protocols cannot run on a super VLAN interface.

A super VLAN is used to aggregate multiple sub VLANs in the same IP subnet. A sub-VLAN is a L2 separate broadcast domain. The super VLAN cannot have any physical member ports; hosts reside on sub VLANs. Once an IP interface is bound to a super VLAN, the proxy ARP will enable automatically on the interface for communication between its sub VLANs. If an IP interface is bound to a super VLAN, it cannot bind to other VLANs. A super VLAN cannot be a sub VLAN of other super VLANs.

Super VLAN Settings

This window is used to configure a super VLAN.

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



Super VLAN Table

VLAN Name	●	
VID (1-4094)	○	

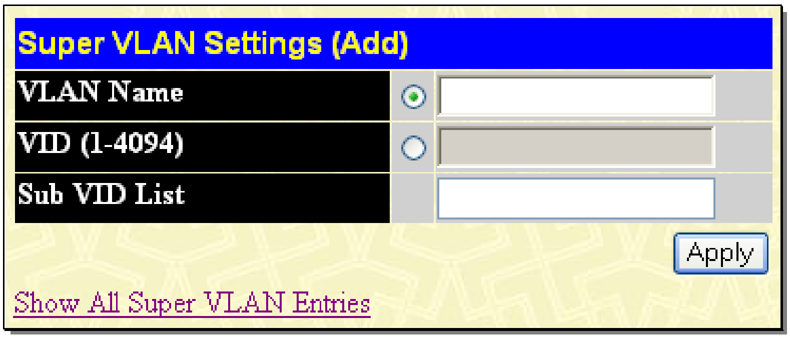
Total Entries: 0

Super VLAN Table

Super VLAN	VLAN Name	IP Subnet	Oper State	Sub VID	Modify	Delete

Figure 3- 22. Super VLAN Table window

Click the **Add** button to reveal the following window for the user to configure:



Super VLAN Settings (Add)

VLAN Name	●	
VID (1-4094)	○	
Sub VID List		

Figure 3- 23. Super VLAN Settings (Add) window

The following fields may be configured:

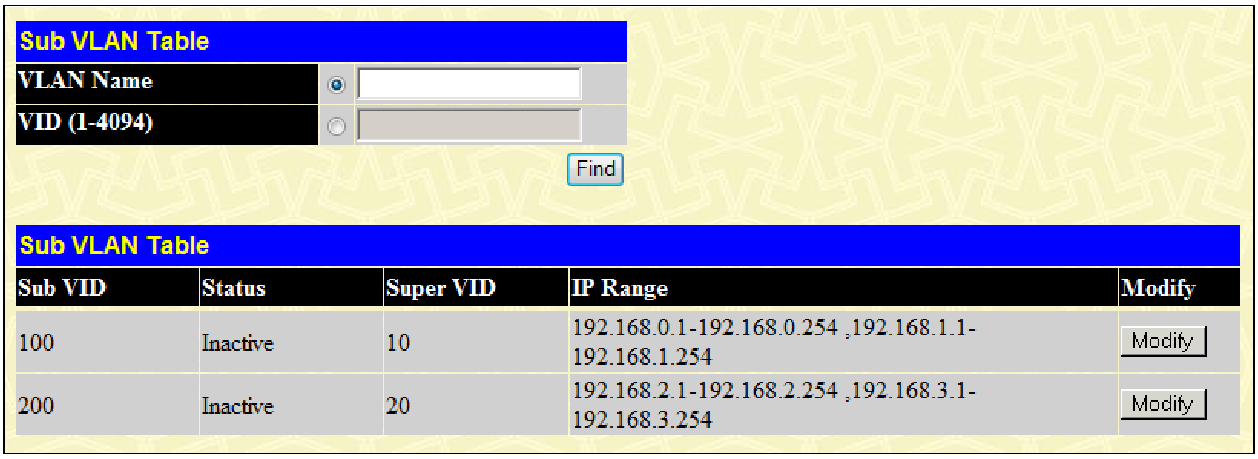
Parameter	Description
VLAN Name	Enter the name of the super VLAN. The VLAN name must be an existing 802.1Q VLAN.
VID (1-4094)	Enter the VLAN ID of the super VLAN.
Sub VID List	Enter the sub VLANs of the super VLAN. By default, a newly created super VLAN does not have any sub VLANs configured.

Click **Apply** to implement changes made.

Sub VLAN Settings

This window is used to configure the sub VLANs of a super VLAN. A sub VLAN only can belong to one super VLAN and users cannot bind an IP interface to it. The maximum number of sub VLANs for a super VLAN is 80.

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



Sub VLAN Table

VLAN Name	●
VID (1-4094)	○

Sub VLAN Table

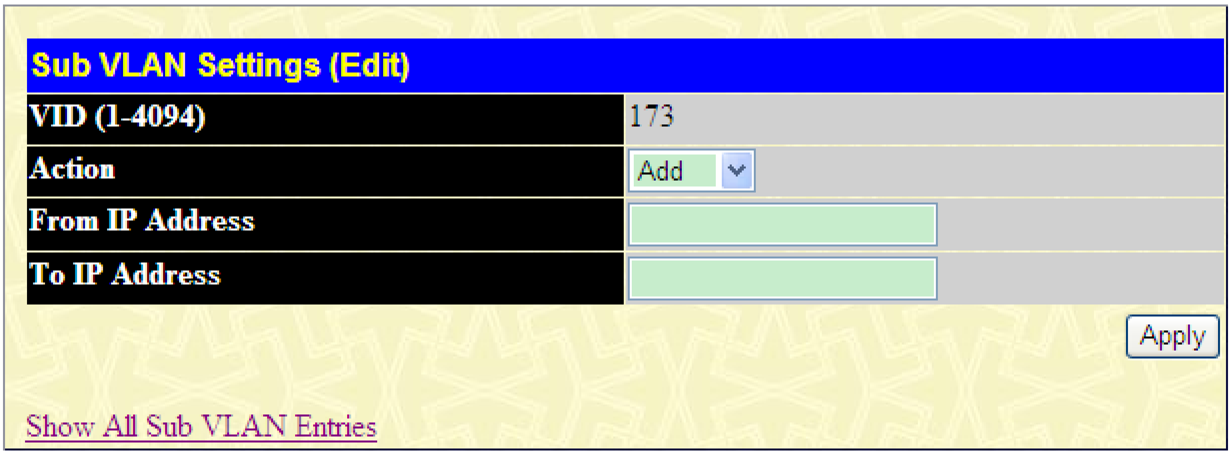
Sub VID	Status	Super VID	IP Range	Modify
100	Inactive	10	192.168.0.1-192.168.0.254 ,192.168.1.1-192.168.1.254	Modify
200	Inactive	20	192.168.2.1-192.168.2.254 ,192.168.3.1-192.168.3.254	Modify

Figure 3- 24. Sub VLAN Table window

The following fields may be configured:

Parameter	Description
VLAN Name	Enter the name of the sub VLAN.
VID (1-4094)	Enter the VLAN ID of the sub VLAN.

Clicking the **Modify** button will open the **Sub VLAN Table – Edit** window, shown below:



Sub VLAN Settings (Edit)

VID (1-4094)	173
Action	Add
From IP Address	
To IP Address	

Figure 3- 25. Sub VLAN Table – Edit window

The following fields may be configured:

Parameter	Description
Action	Use the drop-down menu to choose the desired action.
From IP Address	Enter the IP address to start from.
To IP Address	Enter the IP address to end with.

Trunking

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports this function on all its 10/100/1000 Ethernet Ports and on all its 10G interfaces. The 10/100/1000 ports support up to 32 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved when using the 10/100/1000Mbps Ethernet ports. The 10G interfaces also support port trunk groups with 2 interfaces in each group.

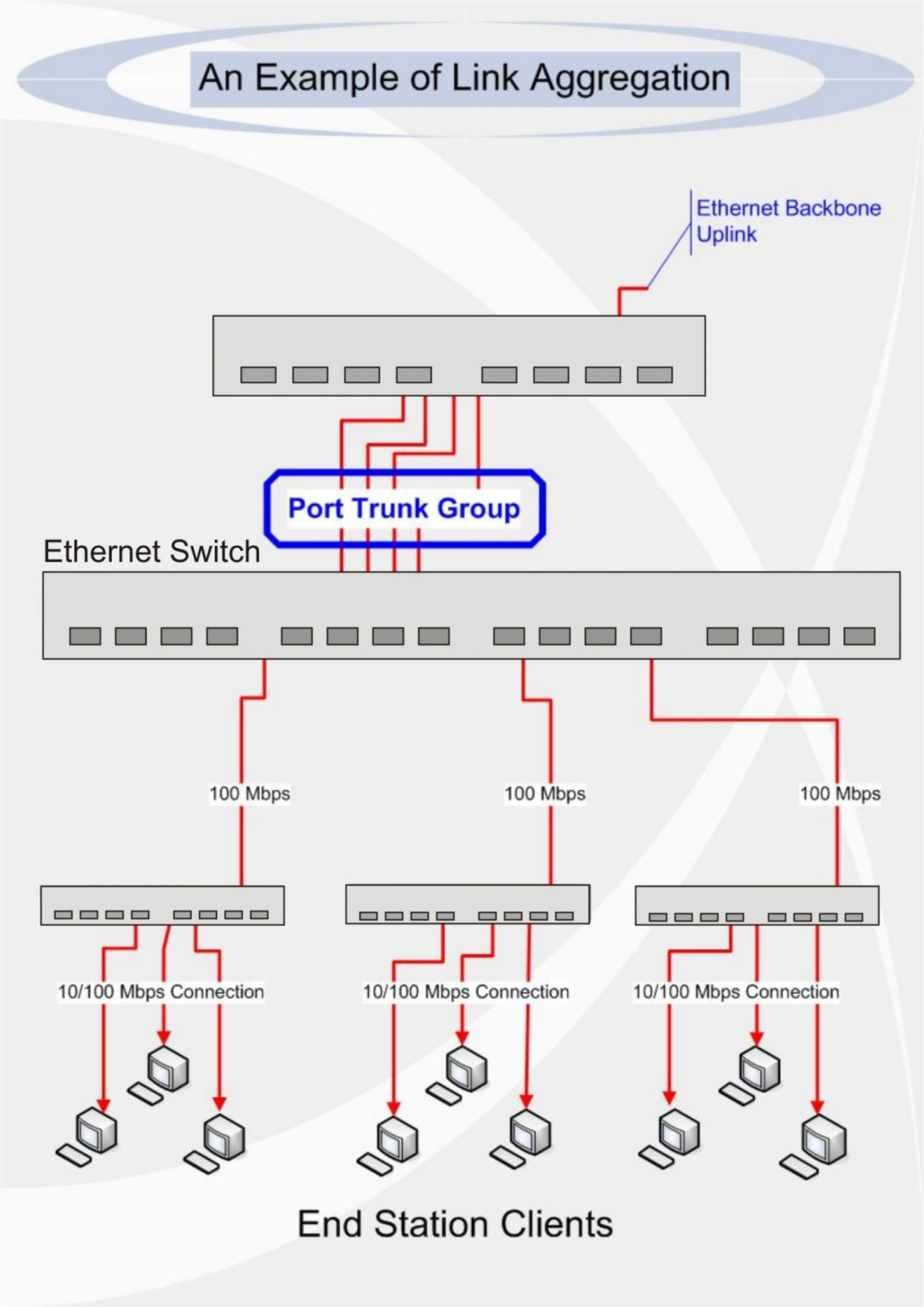


Figure 3- 26. Example of Port Trunk Group

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 linked 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 two to eight links (ports). All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control, traffic segmentation, port bandwidth and 802.1p default priority configurations must be identical. Port security, and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed when in the LACP state 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.

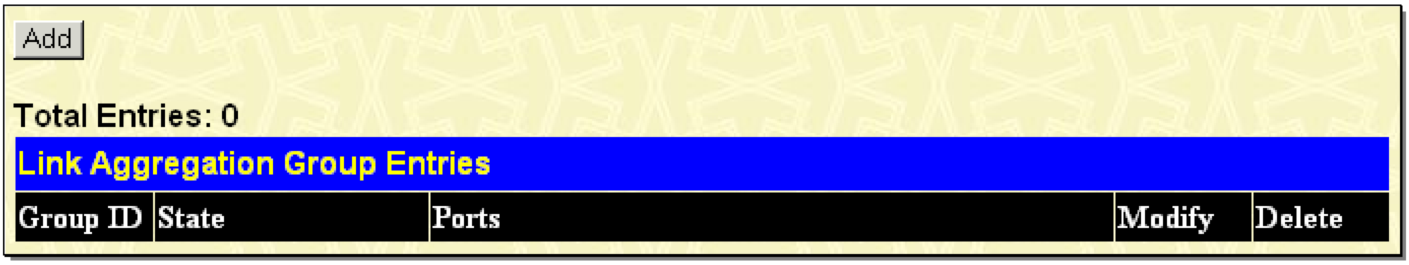
Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

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

This table is used to configure port trunking on the switch.

To view this table, click **L2 Features** > **Trunking** > **Link Aggregation**, as shown below:



Add

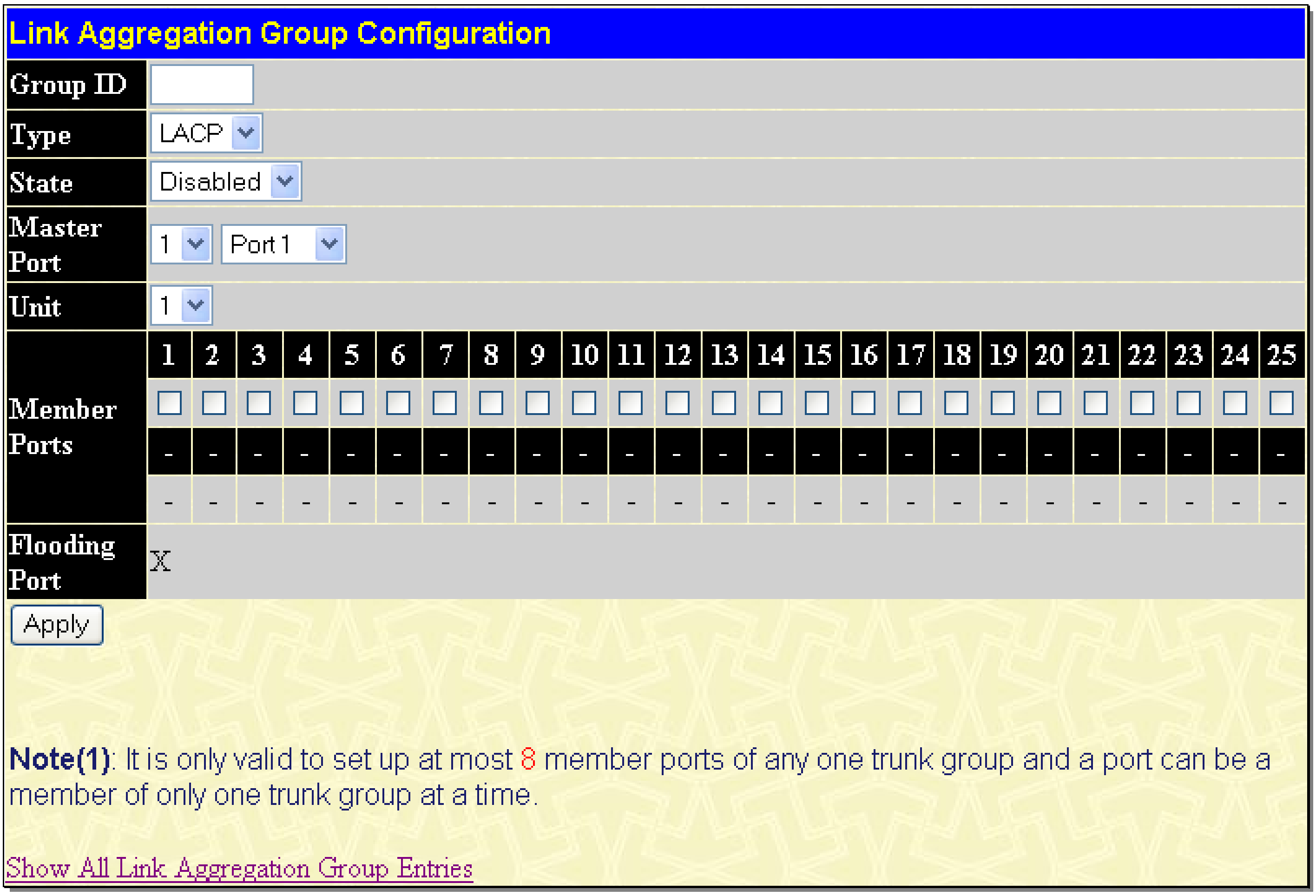
Total Entries: 0

Link Aggregation Group Entries

Group ID	State	Ports	Modify	Delete

Figure 3- 27. Link Aggregation Group Entries window

To configure port trunk groups, add a new trunk group and use the **Link Aggregation Group Configuration** window (see example below). 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** window.



Link Aggregation Group Configuration

Group ID	
Type	LACP
State	Disabled
Master Port	1 Port 1
Unit	1

Member 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
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Flooding Port X

Apply

Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.

Show All Link Aggregation Group Entries

Figure 3- 28. Link Aggregation Group Configuration window

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group, between *1* and *32*.
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.
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.
Unit	Select the unit you wish to configure.
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.

After setting the parameters, click **Apply** to allow changes to be implemented. Successfully created trunk groups will be shown in the **Link Aggregation Group Entries** table.

LACP Port Settings

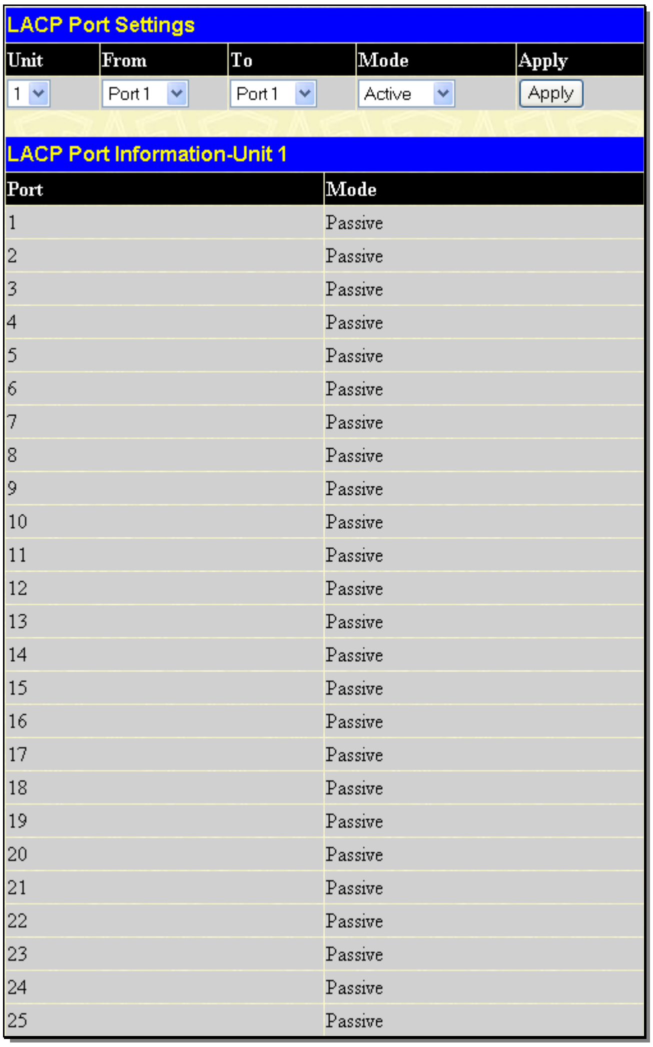
This window is used in conjunction with the **Link Aggregation** window to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames.

To view this window, click **L2 Features** > **Trunking** > **LACP Port Settings**, as shown.

The user may set the following parameters:

Parameter	**Description**
Unit	Select the unit you wish to configure.
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.



LACP Port Settings

Unit	From	To	Mode	Apply
1	Port 1	Port 1	Active	Apply

LACP Port Information-Unit 1

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

Figure 3- 29. LACP Port Settings window

IGMP Snooping

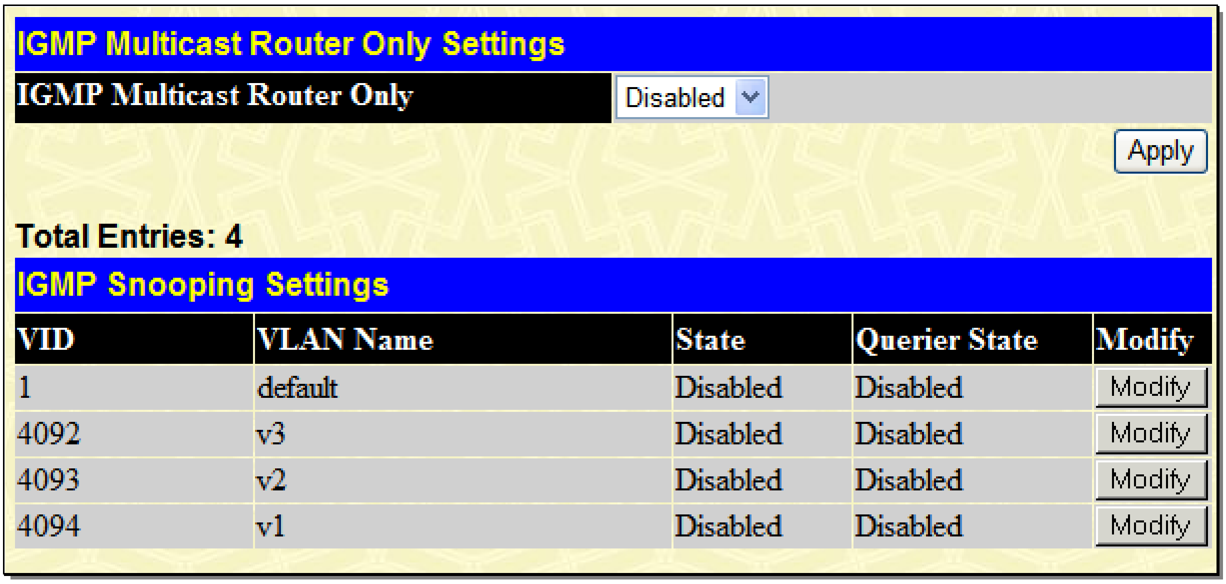
Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on an IGMP message passing through the Switch.

In order to use IGMP snooping, it must first be enabled for the entire Switch (see the **DGS-3600 Web Management Tool**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link in the **L2 Features** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

IGMP Snooping Settings

Use the **IGMP Snooping Settings** window to view IGMP snooping configurations.

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



IGMP Multicast Router Only Settings

IGMP Multicast Router Only: Disabled

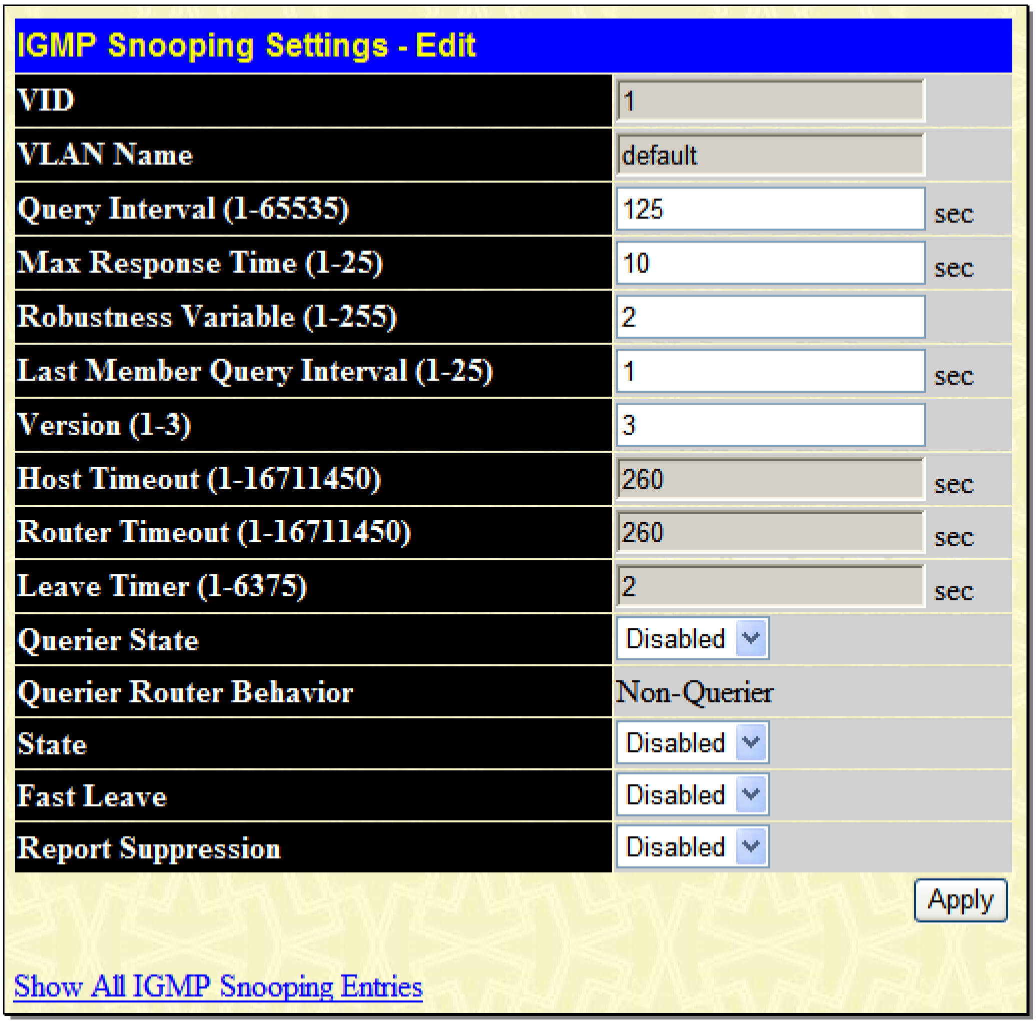
Total Entries: 4

IGMP Snooping Settings

VID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify
4092	v3	Disabled	Disabled	Modify
4093	v2	Disabled	Disabled	Modify
4094	v1	Disabled	Disabled	Modify

Figure 3- 30. IGMP Snooping Settings window

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



IGMP Snooping Settings - Edit

VID	1
VLAN Name	default
Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec
Robustness Variable (1-255)	2
Last Member Query Interval (1-25)	1 sec
Version (1-3)	3
Host Timeout (1-16711450)	260 sec
Router Timeout (1-16711450)	260 sec
Leave Timer (1-6375)	2 sec
Querier State	Disabled
Querier Router Behavior	Non-Querier
State	Disabled
Fast Leave	Disabled
Report Suppression	Disabled

Figure 3- 31. 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 to modify the IGMP Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which to modify the IGMP Snooping Settings.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between *1* and *65535* seconds are allowed. The default is *125*.
Max Response Time (1-25 sec)	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between *1* and *25* (seconds). The default is *10*.
Robustness Variable (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. The default is *2*.
Last Member Query Interval (1-25 sec)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is *1*.
Version (1-3)	Configure the IGMP version of the query packet which will be sent by the router.
Host Timeout (1-16711450 sec)	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. The default is

	260.
Router Timeout (1-16711450 sec)	This is the maximum amount of time in seconds a router is kept in the forwarding table without receiving a membership report. The default is *260*.
Leave Timer (1-16711450 sec)	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. The default setting is *2* seconds.
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*.
Report Suppression	This parameter allows the user to enable the Report Suppression function. When IGMP report suppression is *Enabled*, the Switch sends the first IGMP report from all hosts for a group to all the multicast routers. The Switch does not send the remaining IGMP reports for the group to the multicast routers. If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the Switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the Switch forwards all IGMPv3 reports for a group to the multicast devices. 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.

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.

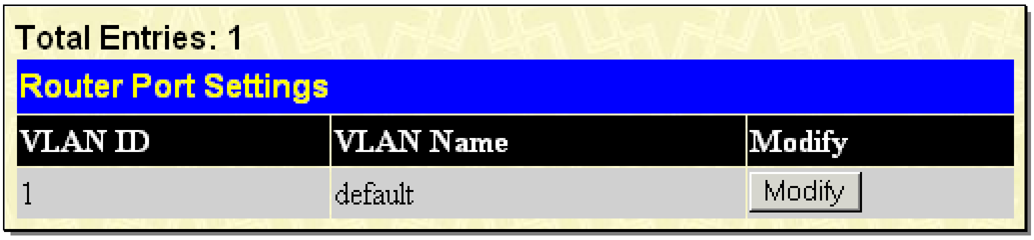
IGMP query packets – Internet Group Management Protocol query packets work by controlling the flow of multicast traffic. The IGMP query packets works by sending messages out to determine which devices are members of a particular multicast group, the devices will respond to the query and inform the querier of its membership status.

RIPv2 multicast – Routing Information Protocol Version 2 can be used for small networks or on the perifory of larger networks where VLSM is required. RIPv2 is used to support route authentication and multicasting of route updates. RIPv2 sends updates every 30 seconds and it uses triggered updates to carry out loop-prevention and poison reverse or counting to infinity.

DVMRP multicast – Distance Vector Multicast Routing Protocol uses reverse path flooding. Messages are flooded out of all interfaces except the one that returns to the souce, this is to prevent any packets traveling to members of the multicast VLAN. The DVMRP uses periodic flooding so as to establish if there are other or potentially new group members.

PIM-DM multicast – Protocol Independent Multicast Dense Mode works by flooding the multicast packets to all routers and eliminates groups or members of groups that don't have an efficient path or route to their members. This mode is generally used if the volume of multicast traffic is large and constant.

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



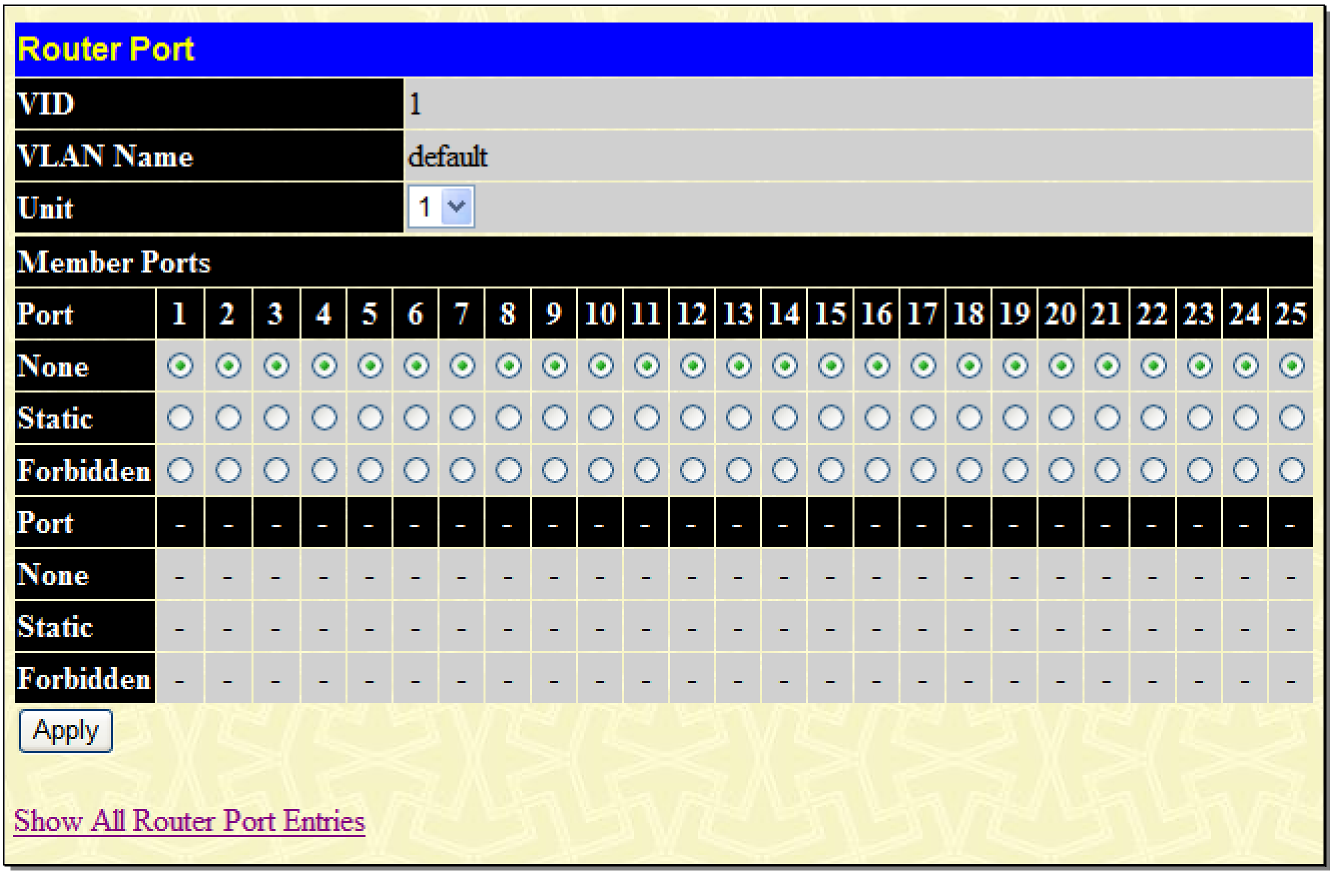
Total Entries: 1

Router Port Settings

VLAN ID	VLAN Name	Modify
1	default	Modify

Figure 3- 32. Router Port 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 **Router Port** window, as shown below:



Router Port

VID	1
VLAN Name	default
Unit	1

Member Ports

Port	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
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Port	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Static	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Apply

Show All Router Port Entries

Figure 3- 33. Router Port (Modify) 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.
Unit	This is the stacking unit where the VLAN is located where the multicast router is attached.
Member Ports	Ports on the Switch that will have a multicast router attached to them. There are three options for which to configure these ports: *None* – Click this option to not set these ports as router ports *Static* – Click this option to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router.

	Forbidden – Click this option to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets.

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

IGMP Snooping Static Group Settings

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

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

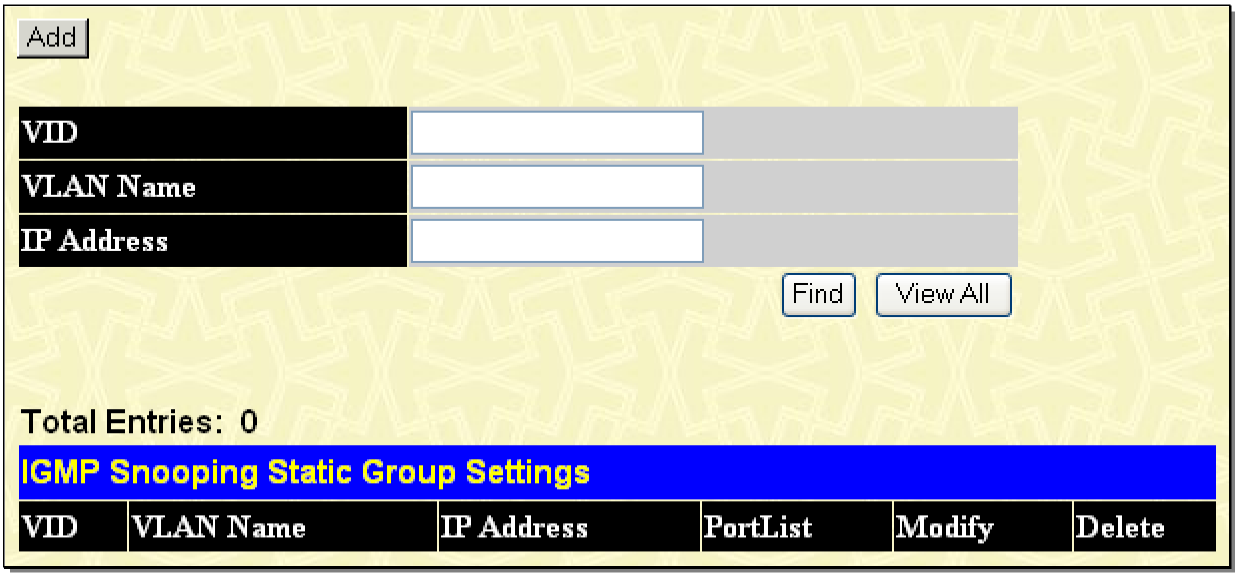


Figure 3- 34. IGMP Snooping Static Group Settings window

The following parameters can be configured:

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

To search for an entry enter the appropriate information and click **Find**, to display all current entries on the Switch click **View All**. To add a new entry click **Add**, the following window will be displayed:

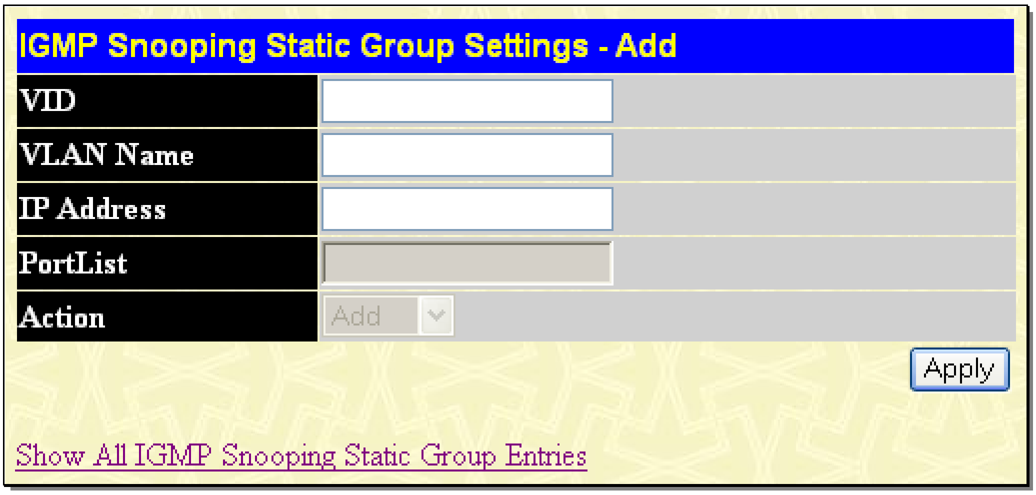

IGMP Snooping Static Group Settings - Add
VID
VLAN Name
IP Address
PortList
Action
Add
Apply
Show All IGMP Snooping Static Group Entries

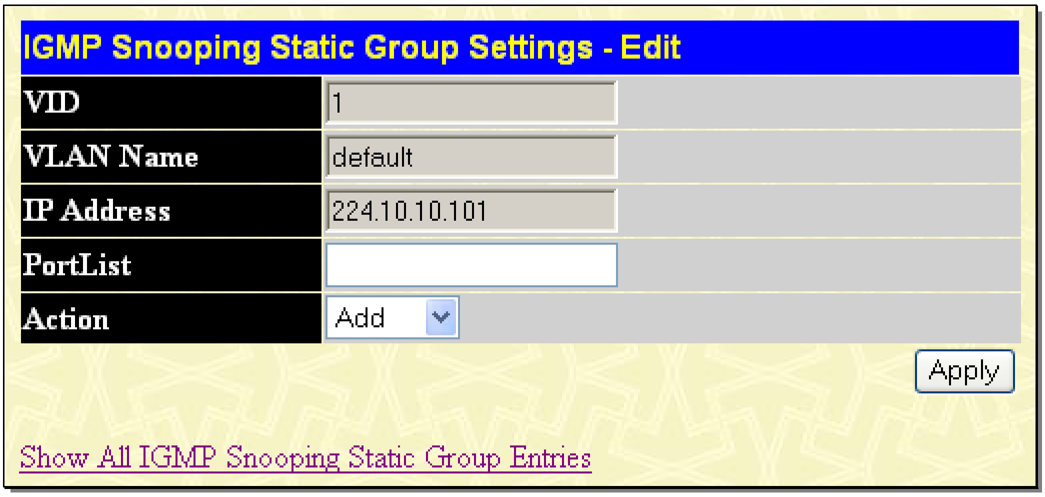
Figure 3- 35. IGMP Snooping Static Group Settings - Add window

The following fields can be configured:

Parameter	Description
VID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to add.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to add.
IP Address	The static group address for which to create IGMP snooping static group information.
PortList	The ports that will belong to this group.
Action	Specifies to *Add* or *Delete* the IGMP Static group entry.

Click **Apply** to implement changes made.

To modify an entry, click the corresponding **Modify** button on the **IGMP Snooping Static Group Settings** window, the following window will be displayed:



IGMP Snooping Static Group Settings - Edit

VID	1
VLAN Name	default
IP Address	224.10.10.101
PortList	
Action	Add

Figure 3- 36. IGMP Snooping Static Group Settings - Edit window

The following fields can be configured:

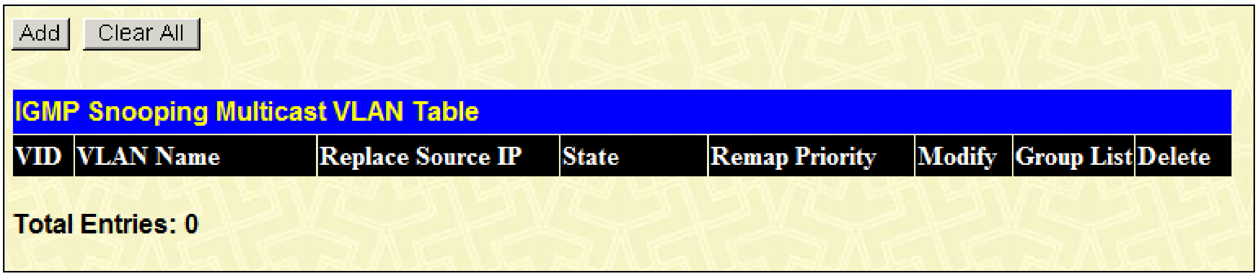
Parameter	Description
PortList	Enter the port number of the entry to add or delete.
Action	Specify to *Add* or *Delete* the IGMP static group entry member ports.

Click **Apply** to implement changes made.

ISM VLAN Settings

Use this page to view and configure the ISM VLAN settings.

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



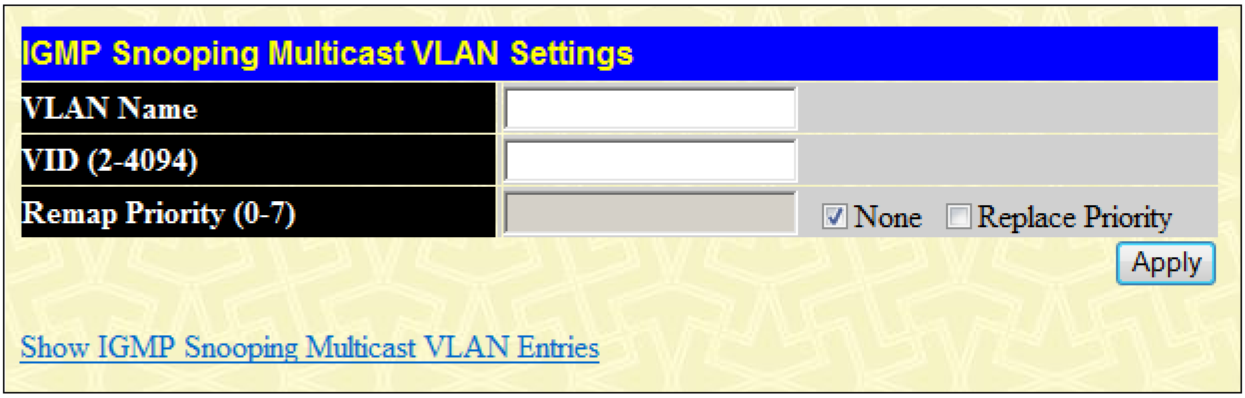
IGMP Snooping Multicast VLAN Table

VID	VLAN Name	Replace Source IP	State	Remap Priority	Modify	Group List	Delete

Total Entries: 0

Figure 3- 37. ISM VLAN Settings window

To clear all the entries from the list, click **Clear** All. To add a new entry click **Add**, the following window will be displayed:



IGMP Snooping Multicast VLAN Settings

VLAN Name	
VID (2-4094)	
Remap Priority (0-7)	☑ None ☐ Replace Priority

Figure 3- 38. ISM VLAN Settings (Add) window

The following parameters can be set:

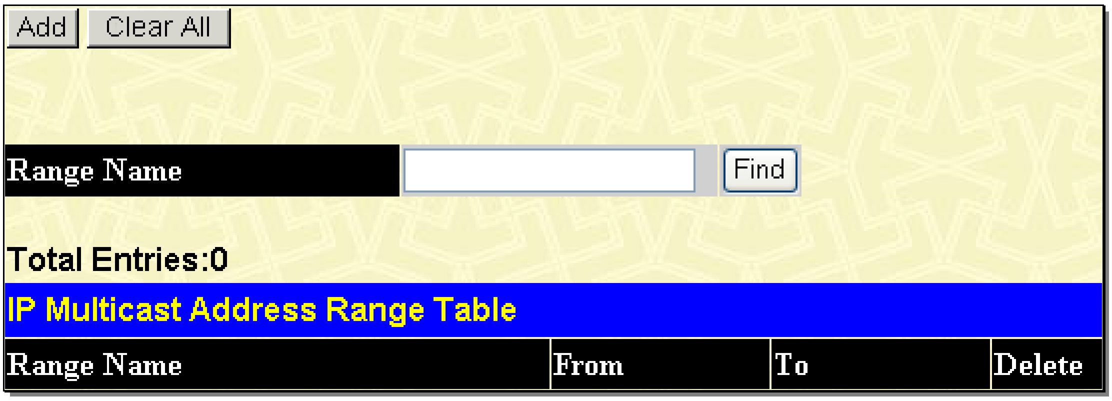
Parameter	Description
VLAN Name	Enter the VLAN name here.
VID (2-4094)	Enter the VLAN ID here.
Remap Priority (0-7)	Enter the remap priority value used here. When **None** is selected, no value can be entered. Tick the **Replace Priority** option, to replace the original value with the entered value.

Click **Apply** to implement changes made.

IP Multicast Address Range Settings

Users can configure the range of multicast addresses that will be accepted by the source port to be forwarded to the receiver ports. The following window will be displayed for the user.

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



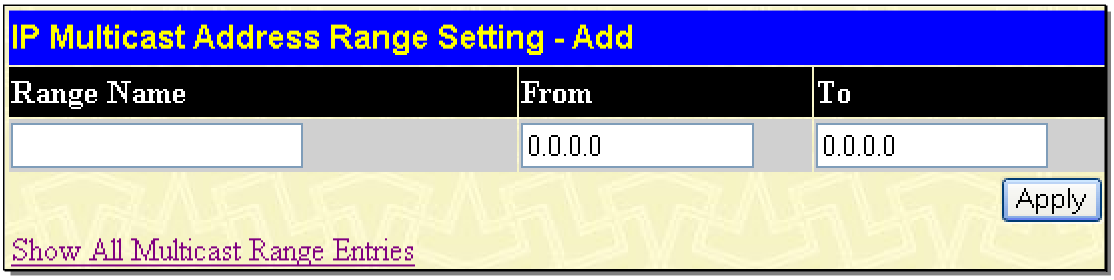
Total Entries:0

IP Multicast Address Range Table

Range Name	From	To	Delete

Figure 3- 39. IP Multicast Address Range Table window

To display a previously created IP Multicast Address enter the Range Name and click **Find**, the information will be displayed on the **IP Multicast Address Range Table**. To create a new range, click the **Add** button which will display the following window.



IP Multicast Address Range Setting - Add

Range Name	From	To
	0.0.0.0	0.0.0.0

Figure 3- 40. IP Multicast Address Range Setting – Add window

The following parameters can be set:

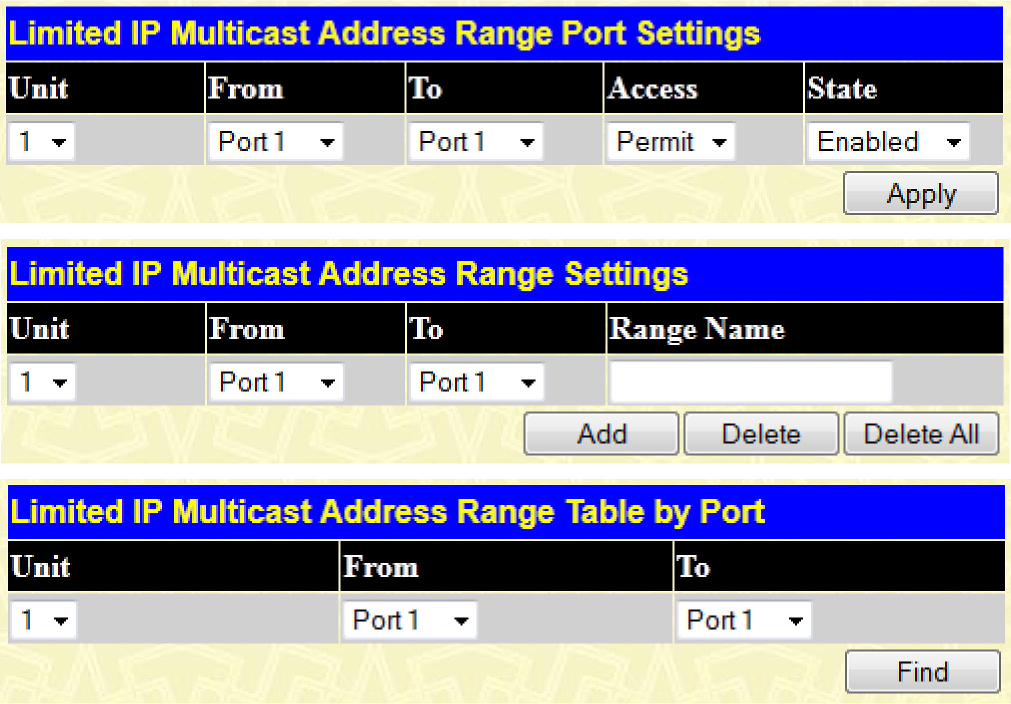
Parameter	Description
Range Name	Enter an alphanumeric name of no more than 32 characters to define the Multicast Address range. This name will be used to define the multicast address range when it is added to a multicast port.
From/To	Enter the range of multicast addresses that will be accepted by the multicast port using this range name. A range of multicast addresses may be separated by a dash (Ex. 224.0.0.0-239.255.255.255).

Click **Apply** to set this Range Name with these multicast addresses.

Limited Multicast Address Range Settings

This window allows the user to specify which multicast address(es) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP address or range of IP addresses, by entering a pre-configured Range Name, to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view this window, click **L2 Features > IGMP Snooping > Limited Multicast Address Range Settings**, as shown.



Limited IP Multicast Address Range Port Settings

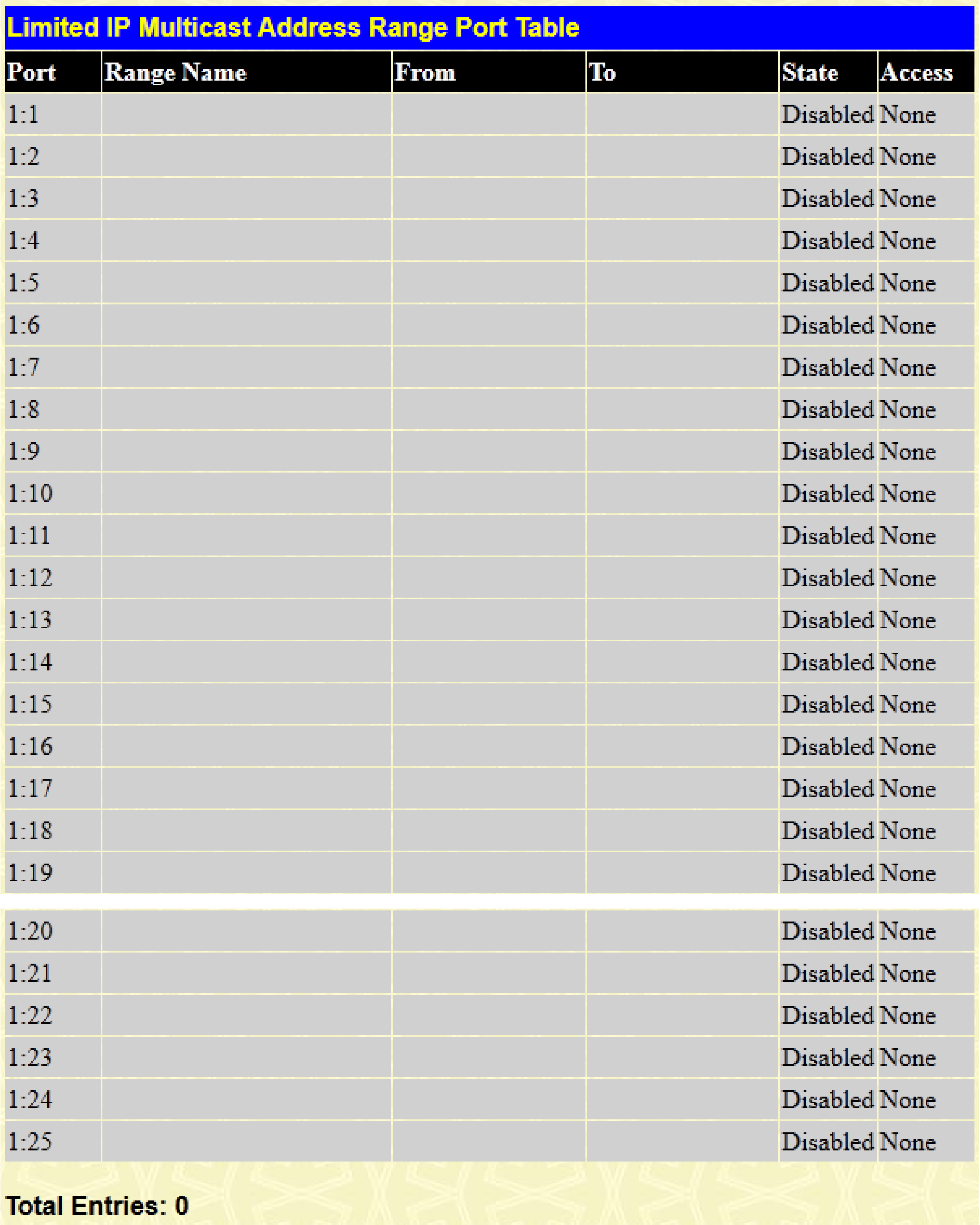
Unit	From	To	Access	State
1	Port 1	Port 1	Permit	Enabled

Limited IP Multicast Address Range Settings

Unit	From	To	Range Name
1	Port 1	Port 1	

Limited IP Multicast Address Range Table by Port

Unit	From	To
1	Port 1	Port 1



Limited IP Multicast Address Range Port Table

Port	Range Name	From	To	State	Access
1:1				Disabled	None
1:2				Disabled	None
1:3				Disabled	None
1:4				Disabled	None
1:5				Disabled	None
1:6				Disabled	None
1:7				Disabled	None
1:8				Disabled	None
1:9				Disabled	None
1:10				Disabled	None
1:11				Disabled	None
1:12				Disabled	None
1:13				Disabled	None
1:14				Disabled	None
1:15				Disabled	None
1:16				Disabled	None
1:17				Disabled	None
1:18				Disabled	None
1:19				Disabled	None
1:20				Disabled	None
1:21				Disabled	None
1:22				Disabled	None
1:23				Disabled	None
1:24				Disabled	None
1:25				Disabled	None

Total Entries: 0

Figure 3- 41. Limited IP Multicast Address Range Port Settings window

Users may view the Limited Multicast IP Range settings on a port-by-port basis using the pull-down menus under Limited IP Multicast Address Range Table by Port. Configured entries will be displayed in the Limited IP Multicast Address Range Port Table at the bottom of the window.

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

Parameter	Description
Unit	Enter the unit you wish to configure.
From/To	Select a range of ports to be granted access or denied access from receiving multicast information.
Access	Toggle the Access field to either Permit or Deny access to a specified range of Multicast addresses on a particular port or range of ports.
State	Select this option to enable or disable the specified feature.
Range Name	Enter the pre-configured Range Name denoting a range of multicast IP addresses for the ports listed in the previous fields.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add the Range Name to these ports.

Click the **Delete** button to delete the range name from the list of ports.

Click the **Delete All** button to delete all configured range names from the list of ports.

Click the **Find** button to locate the specified entry.

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

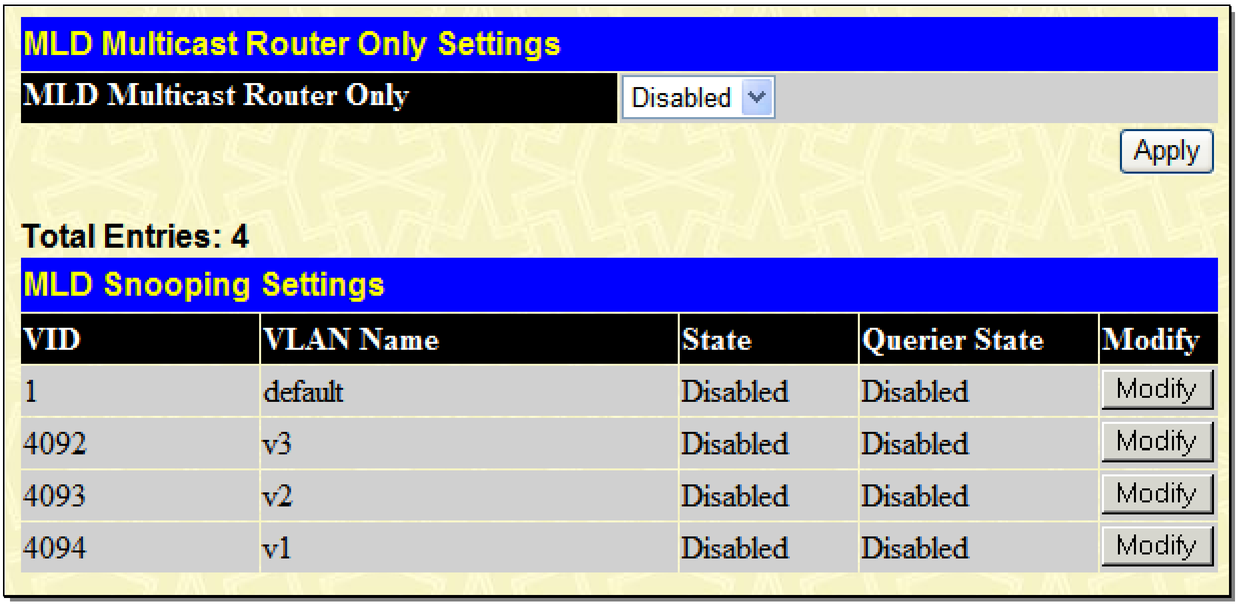
Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131 and 132.

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 also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
2. **Multicast Listener Report** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

MLD Snooping Settings

This window is used to configure the settings for MLD snooping.

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



MLD Multicast Router Only Settings

MLD Multicast Router Only	Disabled

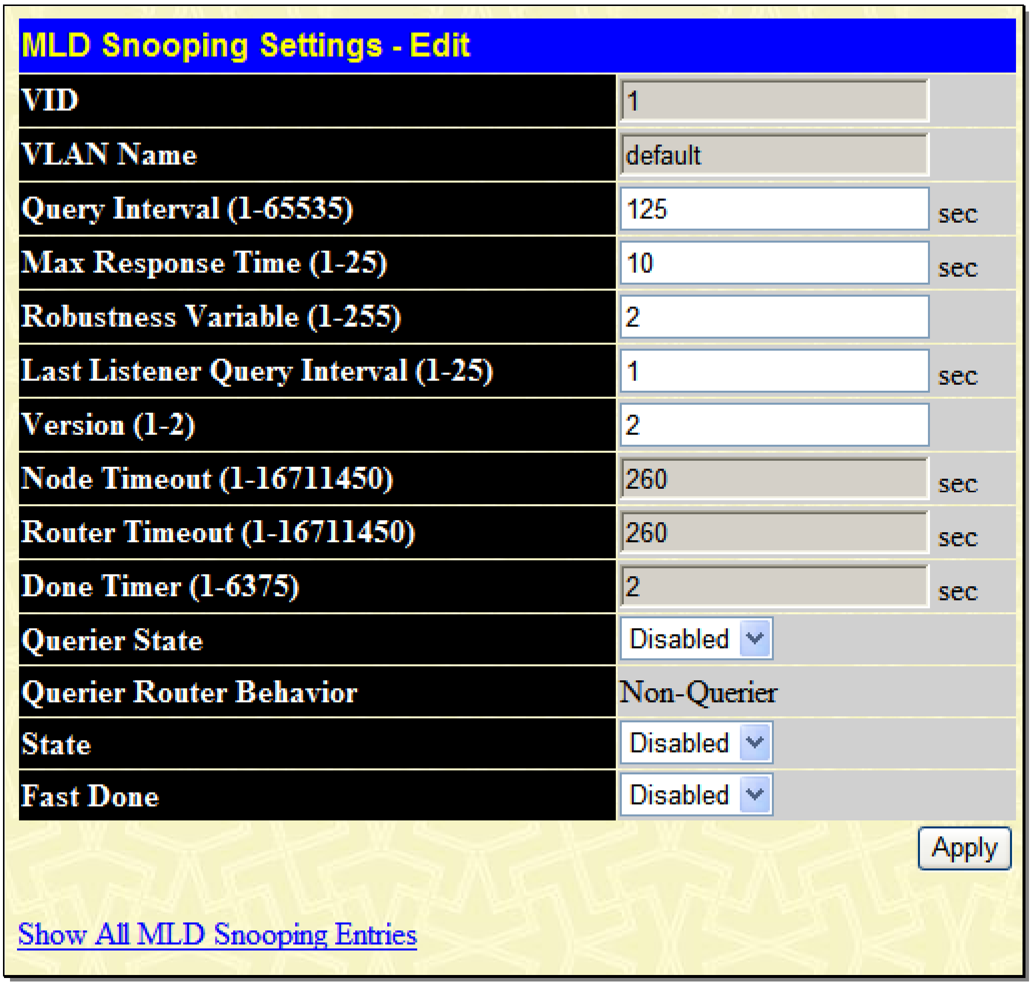
Total Entries: 4

MLD Snooping Settings

VID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify
4092	v3	Disabled	Disabled	Modify
4093	v2	Disabled	Disabled	Modify
4094	v1	Disabled	Disabled	Modify

Figure 3- 42. 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.



MLD Snooping Settings - Edit

VID	1
VLAN Name	default
Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec
Robustness Variable (1-255)	2
Last Listener Query Interval (1-25)	1 sec
Version (1-2)	2
Node Timeout (1-16711450)	260 sec
Router Timeout (1-16711450)	260 sec
Done Timer (1-6375)	2 sec
Querier State	Disabled
Querier Router Behavior	Non-Querier
State	Disabled
Fast Done	Disabled

Figure 3- 43. MLD Snooping Settings - Edit window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which

	to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which to modify the MLD Snooping Settings.
Query Interval (1-65535 sec)	The Query Interval field is used to set the time (in seconds) between transmitting MLD queries. Entries between *1* and *65535* seconds are allowed. Default = *125*.
Max Response Time (1-25 sec)	This determines the maximum amount of time in seconds allowed 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 Variable (1-255)	Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between *1* and *255* with a default setting of *2*. If a subnet is expected to be lossy, the user may wish to increase this interval.
Last Listener Query Interval (1-25 sec)	The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between *1* and *25* seconds with a default setting of *1* second.
Version <value 1-2>	Configure the MLD version of the query packet which will be sent by the router.
Node Timeout (1-16711450 sec)	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	Choose *Enabled* to enable transmitting MLD Snooping Query packets or *Disabled* to disable. The default is *Disabled*.
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 Done	This parameter allows the user to enable the *fast done* function. Enabled, this function will allow members of a multicast group to leave the group immediately when a *done* 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 response 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).

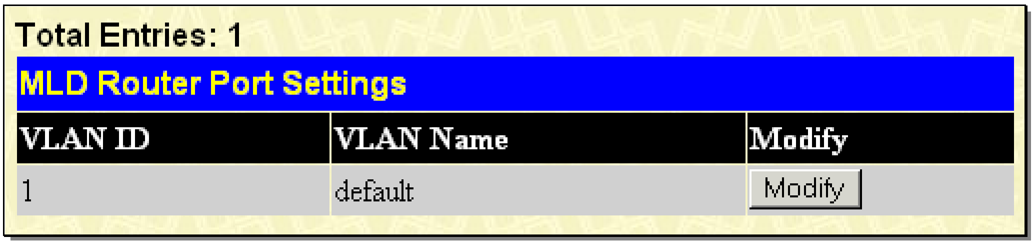
Last Listener Query Count – The amount of group-specific queries sent before the router assumes there are no local listeners in this group. The default value is the value of the robustness variable.

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

MLD 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 OSPFv3 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 these settings, click **L2 Features** > **MLD Snooping** > **MLD Router Port Settings**, as shown below:



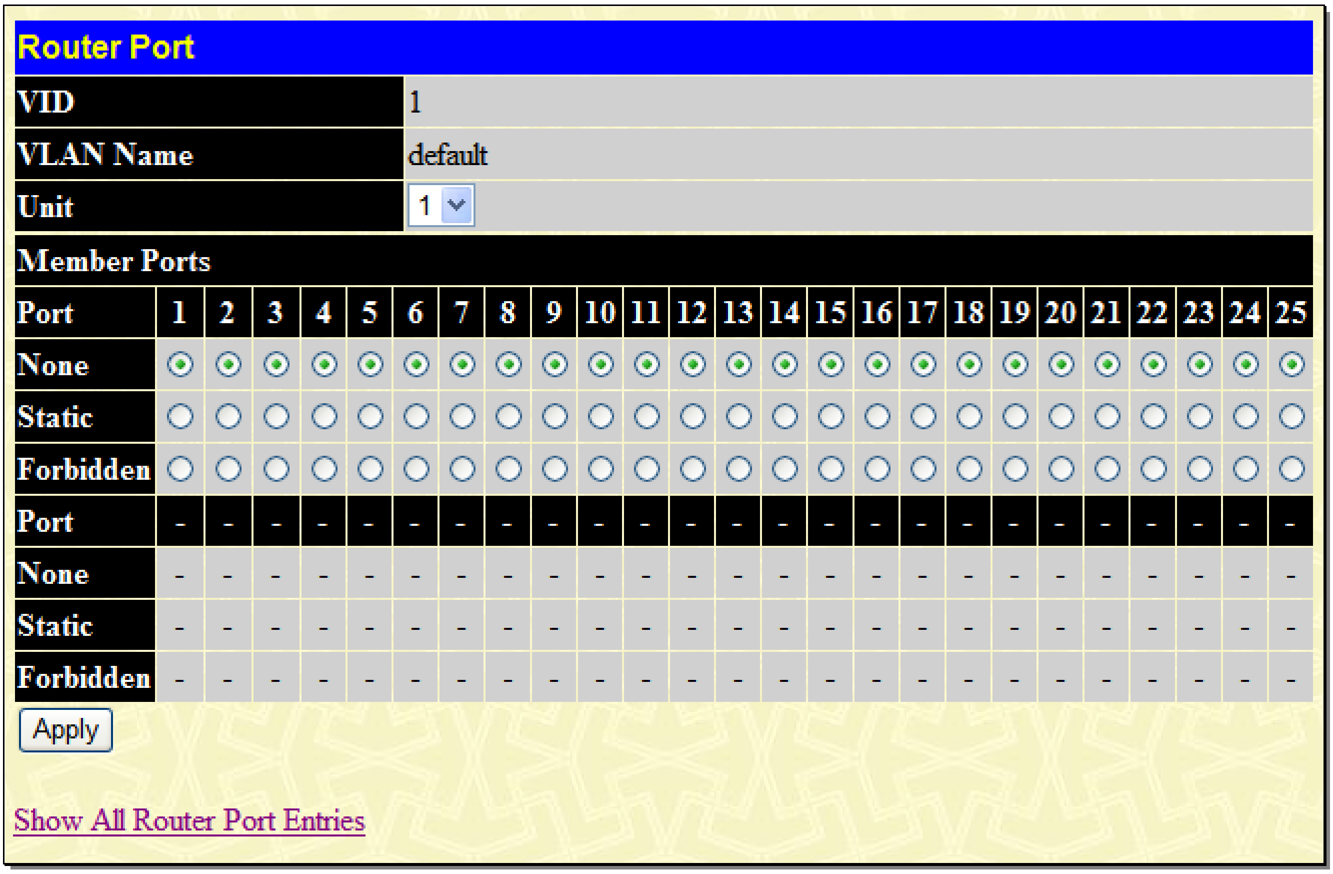
Total Entries: 1

MLD Router Port Settings

VLAN ID	VLAN Name	Modify
1	default	Modify

Figure 3- 44. MLD 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.



Router Port

VID	1
VLAN Name	default
Unit	1

Member Ports

Port	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
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Static	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Port	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Static	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Show All Router Port Entries

Figure 3- 45. Router Port window (Modify)

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 MLD multicast router is attached.
VLAN Name	This is the name of the VLAN where the MLD multicast router is attached.
Unit	Select the unit you wish to configure.
Member Ports	Ports on the Switch that will have a multicast router attached to them. There are three options for which to configure these ports:

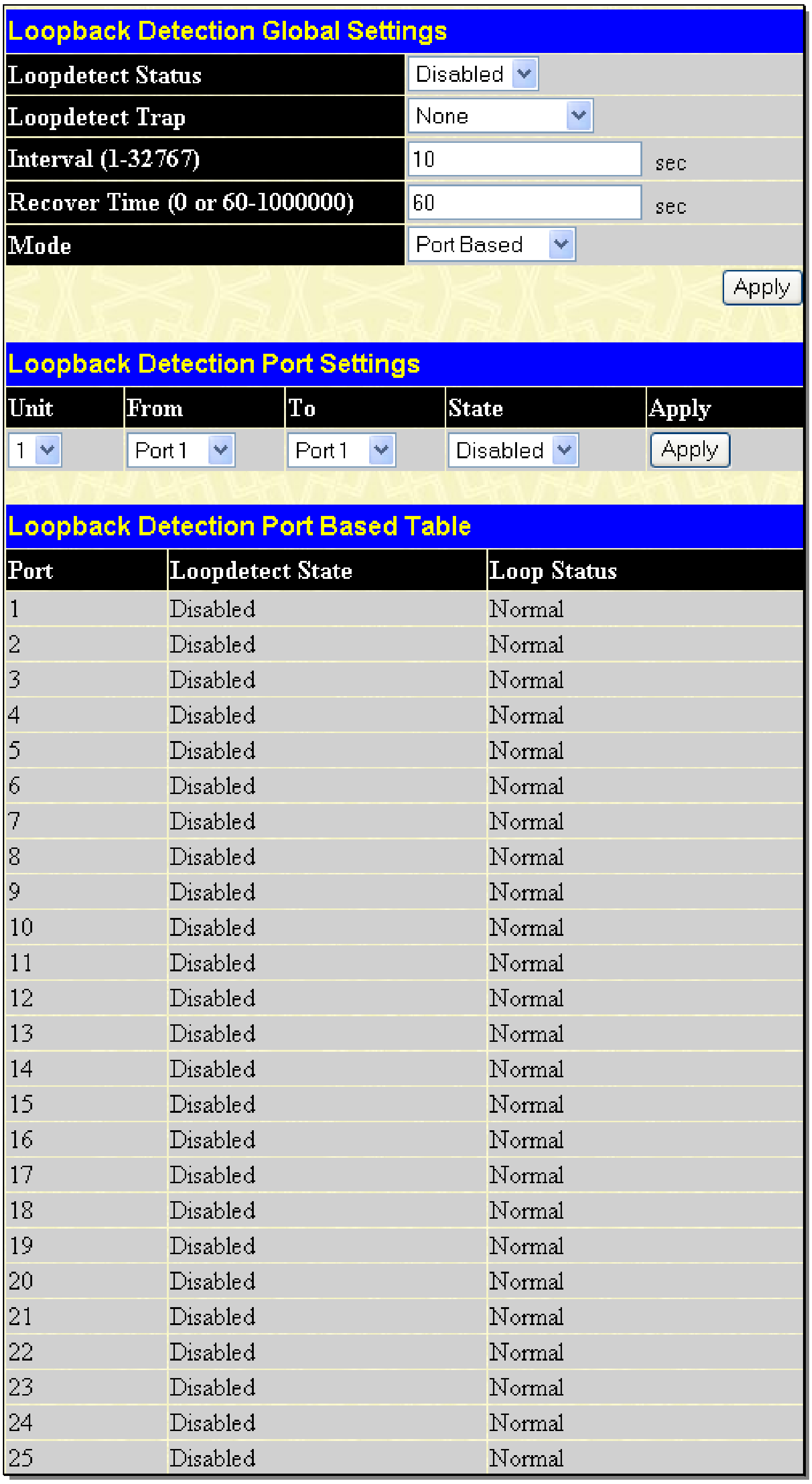
	None – Click this option to not set these ports as router ports *Static* – Click this option to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router. *Forbidden* – Click this option to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets.

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

Loopback Detection Global Settings

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

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



Loopback Detection Global Settings

Loopdetect Status	Disabled
Loopdetect Trap	None
Interval (1-32767)	10 sec
Recover Time (0 or 60-1000000)	60 sec
Mode	Port Based

Loopback Detection Port Settings

Unit	From	To	State	Apply
1	Port 1	Port 1	Disabled	Apply

Loopback Detection Port Based Table

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

Figure 3- 46. Loopback Detection Global Settings window

The following parameters can be configured.

Parameter	Description
Loopdetect Status	Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*

Loopdetect Trap	*None* – The trap will not be sent in any situation. *Loop Detected* – The trap is sent when the loop condition is detected. *Loop Cleared* – The trap is sent when the loop condition is cleared. *Both* – The trap will be sent for both conditions.
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	Select the mode you wish to use either *Port Based* or *VLAN Based.* *Port Based* – This mode can detect loopback based on the Port. If the Switch detects loopback on the Port, the loopback detection will only block the traffic which belongs to this Port. Other VLAN traffic should not be affected by this. *VLAN Based* – This mode can detect loopback based on the VLAN. If the Switch detects loopback on the VLAN, the loopback detection will only block the traffic which belongs to this VLAN. Other VLAN traffic should not be affected by this. Loopback detection will send the CTP packets periodically per port per VLAN in VLAN-based mode.
Unit	Select the unit you wish to configure.
From/To	Use the drop-down menu to select a port or range of ports to be configured.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*

Click **Apply** to implement changes made.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 802.1Q-2005 MSTP have been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

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

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

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

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).

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

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

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

802.1D-2004 Rapid Spanning Tree

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

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 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-1998 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 3-2 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-1998 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

Table 3- 2. Comparing Port States

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant 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-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 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 Loopback Detection

When connected to other switches, STP is an important configuration in consistency for delivering packets to ports and can greatly improve the throughput of your switch. Yet, even this function can malfunction with the emergence of STP BPDU packets that occasionally loop back to the Switch, such as BPDU packets looped back from an unmanaged switch connected to a DGS-3600 Series switch. To maintain the consistency of the throughput, the DGS-3600 Series switch implements the STP Loopback Detection function.

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

Setting the Loopback Timer

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

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

Regulations and Restrictions for the Loopback Detection Function

- All three versions of STP (STP, RSTP and MSTP) can enable this feature.
- May be configured globally (STP Global Bridge Settings), or per port (MSTP Port Information).
- Neighbor switches of the Switch must have the capability to forward BPDU packets. Switches that the fail to meet this requirement will disable this function for the port in question on the Switch.
- Loopback Detection is globally enabled for the switch, yet the port-by-port default setting is disabled.
- The default setting for the Loopback timer is 60 seconds.

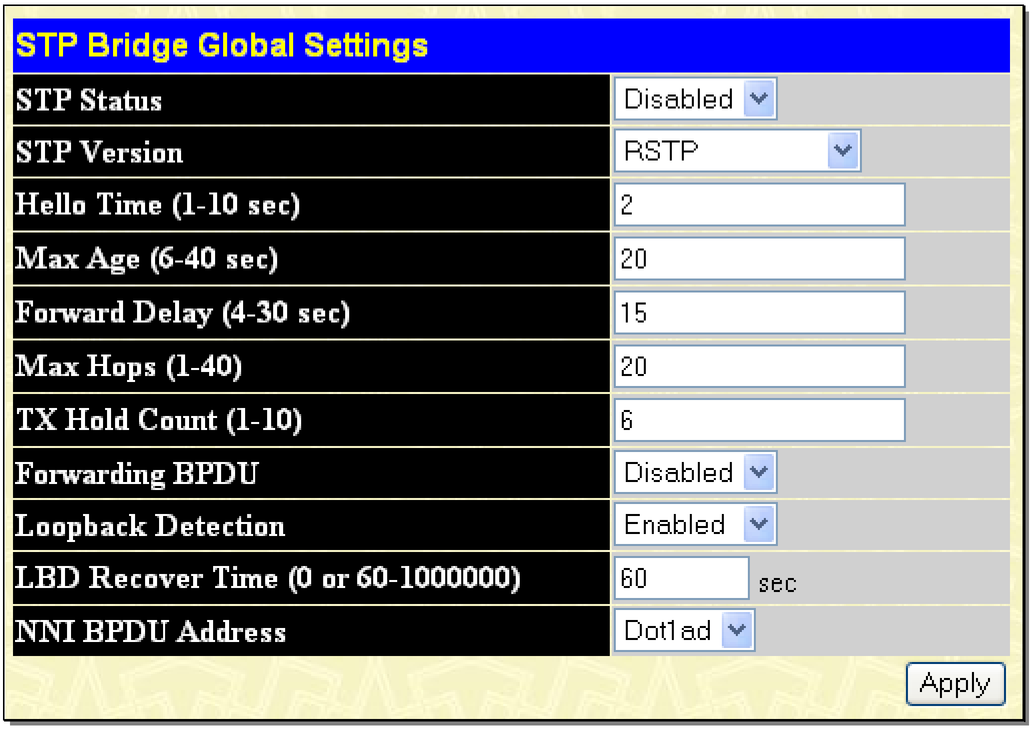
- This setting will only be operational if the interface is STP-enabled.

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

STP Bridge Global Settings

This window is used to configure the STP Bridge Global Settings on the Switch.

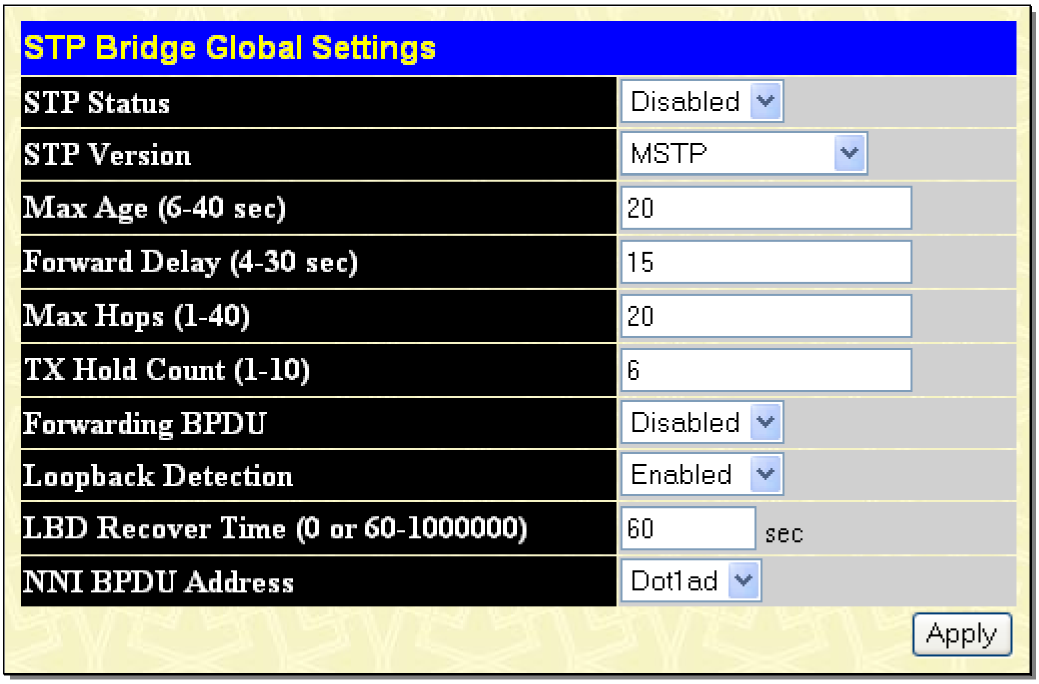
To view the following window, click **L2 Features > Spanning Tree > STP Bridge Global Settings**, as shown below:



STP Bridge Global Settings

STP Status	Disabled
STP Version	RSTP
Hello Time (1-10 sec)	2
Max Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Max Hops (1-40)	20
TX Hold Count (1-10)	6
Forwarding BPDU	Disabled
Loopback Detection	Enabled
LBD Recover Time (0 or 60-1000000)	60 sec
NNI BPDU Address	Dot1ad

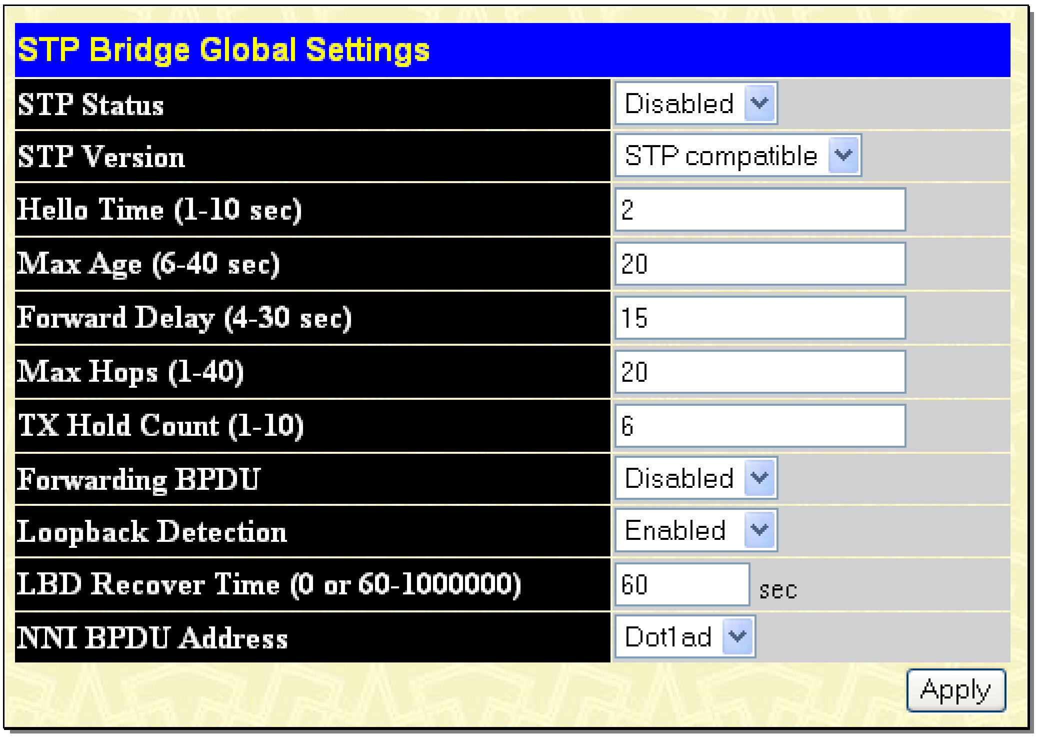
Figure 3- 47. STP Bridge Global Settings window – RSTP (default)



STP Bridge Global Settings

STP Status	Disabled
STP Version	MSTP
Max Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Max Hops (1-40)	20
TX Hold Count (1-10)	6
Forwarding BPDU	Disabled
Loopback Detection	Enabled
LBD Recover Time (0 or 60-1000000)	60 sec
NNI BPDU Address	Dot1ad

Figure 3- 48. STP Bridge Global Settings window - MSTP



STP Bridge Global Settings

STP Status	Disabled
STP Version	STP compatible
Hello Time (1-10 sec)	2
Max Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Max Hops (1-40)	20
TX Hold Count (1-10)	6
Forwarding BPDU	Disabled
Loopback Detection	Enabled
LBD Recover Time (0 or 60-1000000)	60 sec
NNI BPDU Address	Dot1ad

Figure 3- 49. 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 *STP compatible*, *RSTP*, and *MSTP*. RSTP is the default.
Hello Time (1-10 sec)	The Hello Time can be set from *1* to *10* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge.
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 (1-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from *1* to *40*. The default is *20*.

TX Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *3*.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is Disabled.
Loopback Detection	This feature is used to temporarily shutdown a port on the Switch when a BPDU packet has been looped back to the switch. When the Switch detects its own BPDU packet coming back, it signifies a loop on the network. STP will automatically be blocked and an alert will be sent to the administrator. The LBD STP port will restart (change to discarding state) when the LBD Recover Time times out. The Loopback Detection function will only be implemented on one port at a time. The user may enable or disable this function using the pull-down menu. The default is Enabled.
LBD Recover Time () or 60-1000000)	This field will set the time the STP port will wait before recovering the STP state set. 0 will denote that the LBD will never time out or restart until the administrator personally changes it. The user may also set a time between *60* and *1000000* seconds. The default is *60* seconds.
NNI BPDU Address	Use the drop-down menu to choose *Dot1d* or *Dot1ad*.

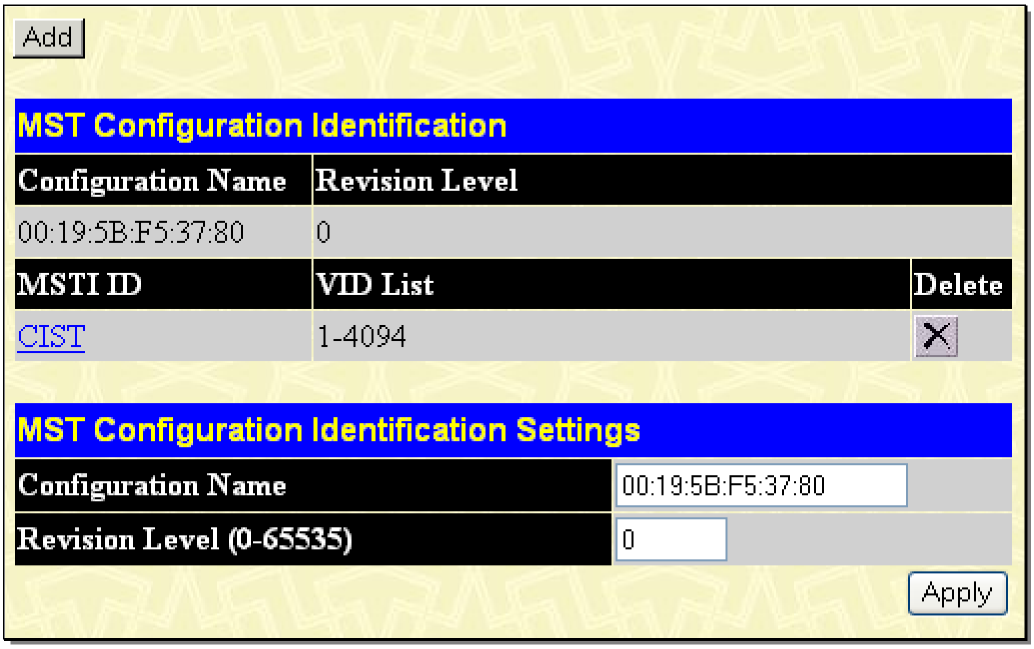
NOTE: The Loopback Detection function can only be implemented on the Switch if it is configured both on the **STP Global Settings** window, and on the **STP Port Settings** window. Enabling this feature through only one of these windows will not fully enable the Loopback Detection function.

Click **Apply** to implement changes made.

MST Configuration Identification

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

To view this window, click **L2 Features > Spanning Tree > MST Configuration Identification**, as shown below:



MST Configuration Identification

Configuration Name	Revision Level
00:19:5B:F5:37:80	0

MSTI ID	VID List	Delete
CIST	1-4094	☒

MST Configuration Identification Settings

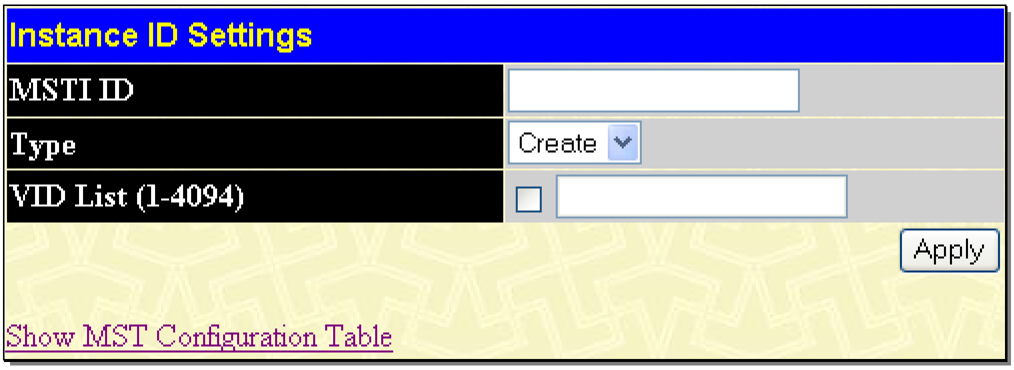
Configuration Name	00:19:5B:F5:37:80
Revision Level (0-65535)	0

Figure 3- 50. MST Configuration Identification window

The window above contains the following information:

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

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



Instance ID Settings

MSTI ID

Type: Create

VID List (1-4094): □

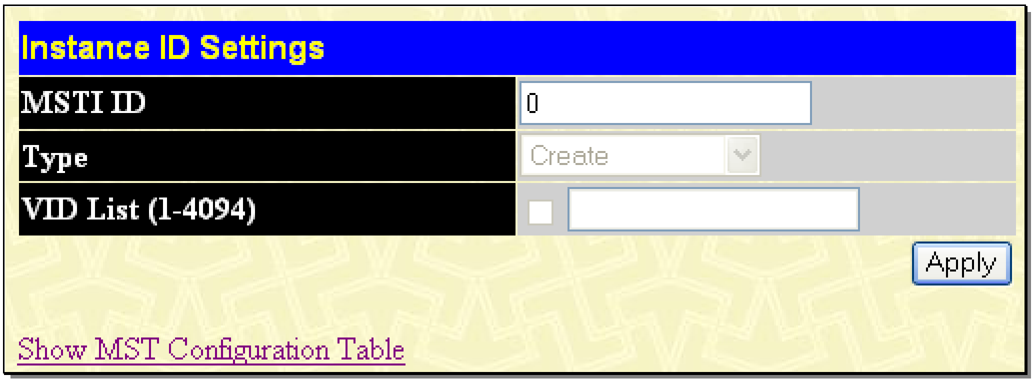
Figure 3- 51. Instance ID Settings window (Add)

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

Parameter	Description
MSTI ID	Enter a number between *1* and *15* 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:



Instance ID Settings

MSTI ID: 0

Type: Create

VID List (1-4094): □

Figure 3- 52. Instance ID Settings window (CIST modify)

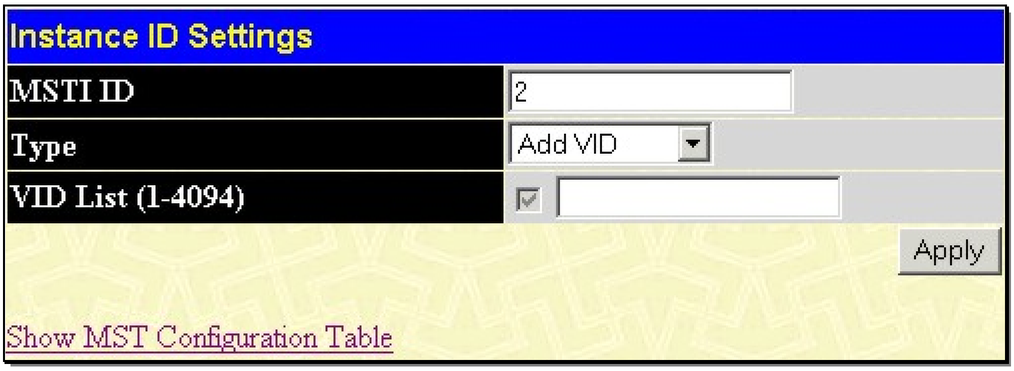
The user may configure the following parameters to configure the CIST on the Switch.

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.



Instance ID Settings

MSTI ID: 2

Type: Add VID

VID List (1-4094): ☑

Figure 3- 53. Instance ID Settings window (Modify)

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

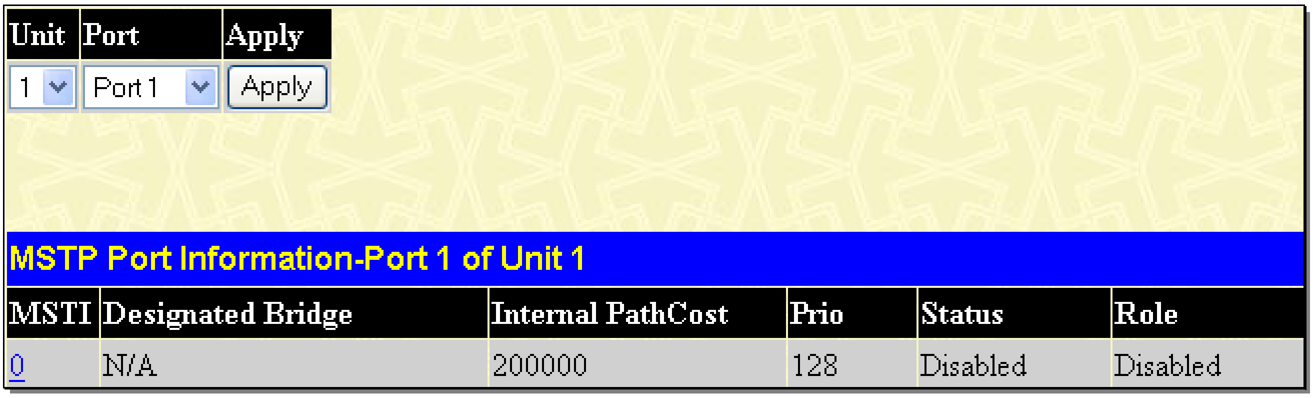
Parameter	Description
MSTI ID	Displays the MSTI ID previously set by the user.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has four choices. *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *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 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**, as shown below:



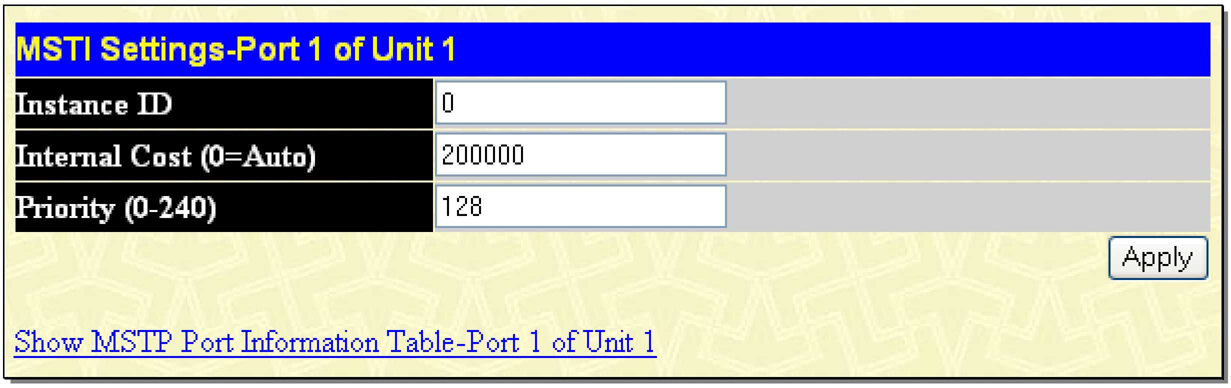
Unit	Port	Apply
1	Port 1	Apply

MSTP Port Information-Port 1 of Unit 1

MSTI	Designated Bridge	Internal PathCost	Prio	Status	Role
0	N/A	200000	128	Disabled	Disabled

Figure 3- 54. 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.



MSTI Settings-Port 1 of Unit 1

Instance ID	0
Internal Cost (0=Auto)	200000
Priority (0-240)	128

Show MSTP Port Information Table-Port 1 of Unit 1

Figure 3- 55. MSTI Settings window

The user may configure the following parameters.

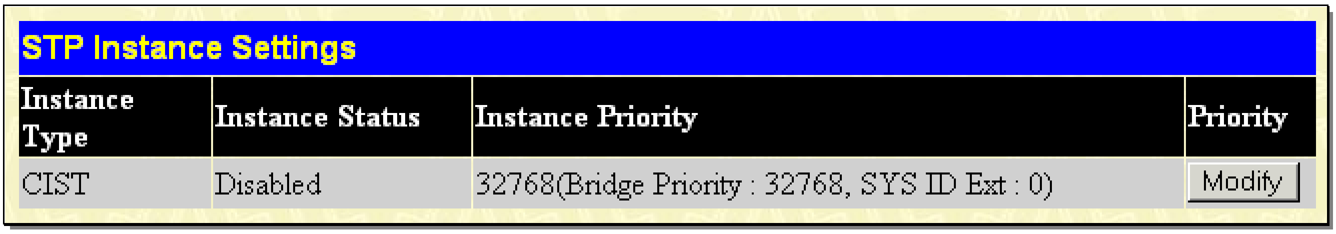
Parameter	Description
Instance ID	Displays the MSTI ID of the instance being configured. An entry of 0 in this field denotes the CIST (default MSTI).
Internal cost (0=Auto)	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within 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 1-200000000* - Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.
Priority (0-240)	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**, as shown below:



STP Instance Settings

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

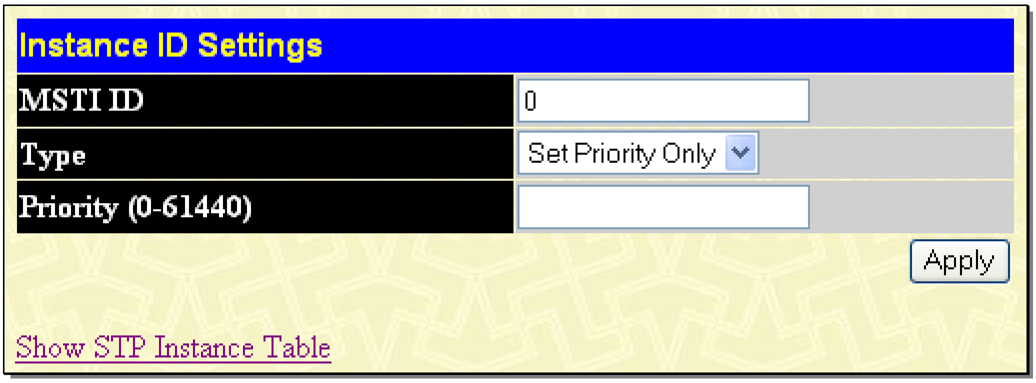
Figure 3- 56. STP Instance Settings window

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.



Instance ID Settings

MSTI ID	0
Type	Set Priority Only
Priority (0-61440)	

Figure 3- 57. Instance ID Settings - Modify priority window

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* and *61440*.

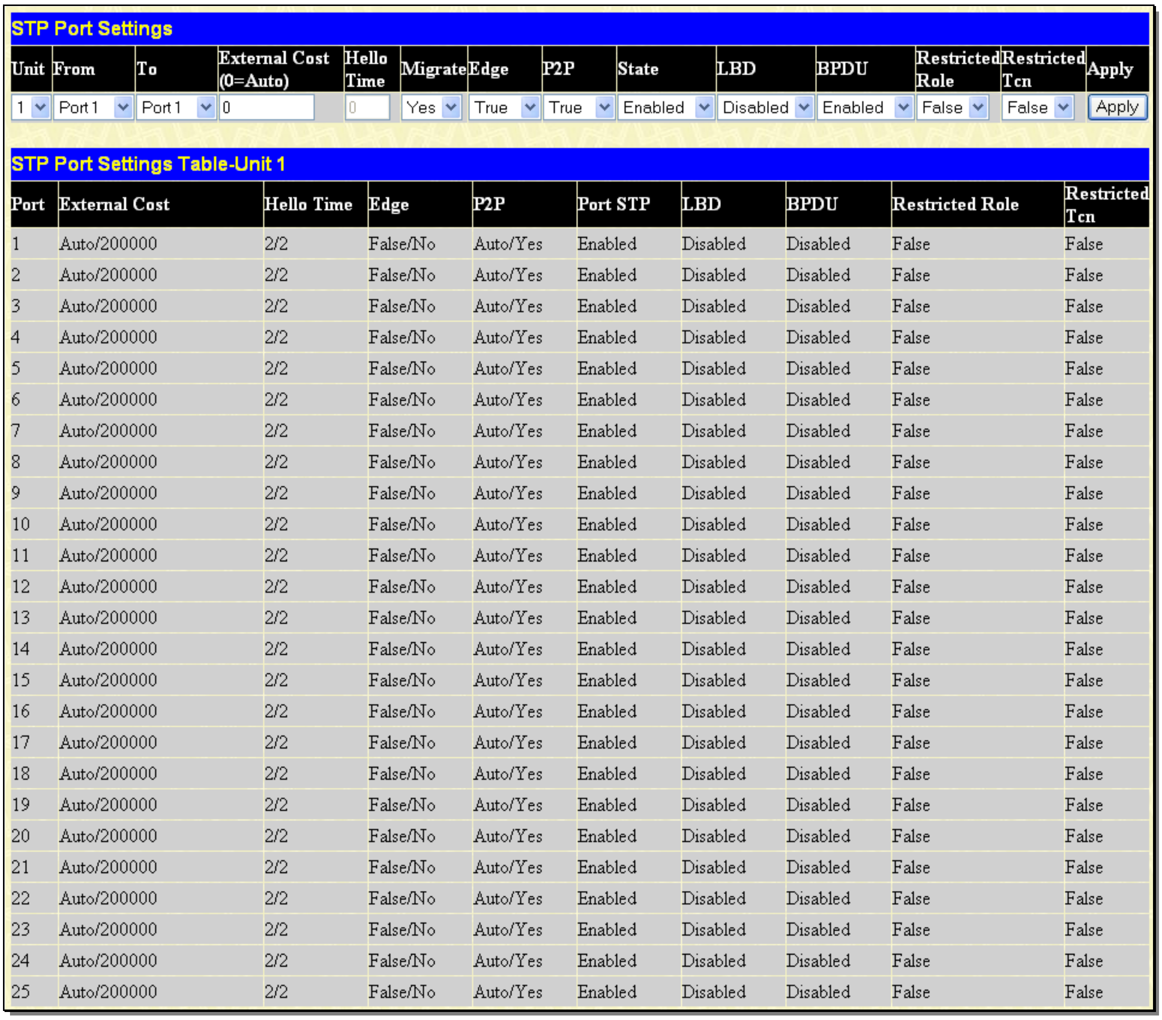
Click **Apply** to implement the new priority setting.

STP Port Settings

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

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



STP Port Settings

Unit	From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	P2P	State	LBD	BPDU	Restricted Role	Restricted Tcn	Apply
1	Port 1	Port 1	0	0	Yes	True	True	Enabled	Disabled	Enabled	False	False	Apply

STP Port Settings Table-Unit 1

Port	External Cost	Hello Time	Edge	P2P	Port STP	LBD	BPDU	Restricted Role	Restricted Tcn
1	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
2	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
3	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
4	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
5	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
6	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
7	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
8	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
9	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
10	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
11	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
12	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
13	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
14	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
15	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
16	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
17	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
18	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
19	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
20	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
21	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
22	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
23	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
24	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False
25	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False

Figure 3- 58. STP Port Settings window

The following STP Port Settings fields can be set:

Parameter	Description
Unit	Select the unit to configure.
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*.
State	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is *Enabled*.
LBD	Use the pull-down menu to enable or disable the Loopback Detection function on the Switch for the ports configured above. For more information on this function, see the Loopback Detection field in the **STP Bridge Global Settings** window, mentioned earlier in this section.
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 the **STP Bridge Global Settings** window above). The default setting *Disabled*, does not forward BPDU packets when STP is disabled.
Restricted Role	Toggle between *True* and *False* to set the restricted role state of the packet. If *True* causes the port not to be selected as the root port for the CIST or any MSTI, even if it has the best spanning tree priority vector, such a port will be selected as an Alternate Port after the Root Port has been selected. Setting this variable can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This parameter is *False* by default.
Restriced TCN	Toggle between *True* and *False* to set the restricted TCN of the packet. If *True* causes the port not to be selected as the root port for the CIST or any MSTI, even if it has the best spanning tree priority vector, such a port will be selected as an Alternate Port after the Root Port has been selected. Setting this variable can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This parameter should be *False* by default.

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** window discussed previously.

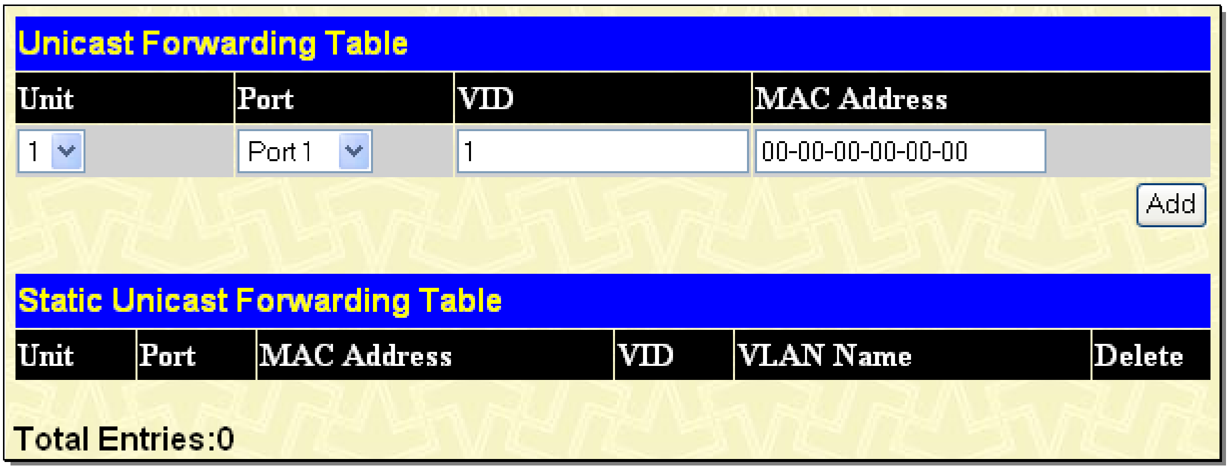
Forwarding & Filtering

The Forwarding & Filtering section is made up of Unicast Forwarding, Multicast Forwarding, and Multicast Filtering Mode.

Unicast Forwarding

The following window is used to set up unicast forwarding on the Switch.

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



Unicast Forwarding Table

Unit	Port	VID	MAC Address
1	Port 1	1	00-00-00-00-00-00

Static Unicast Forwarding Table

Unit	Port	MAC Address	VID	VLAN Name	Delete

Total Entries:0

Figure 3- 59. Unicast Forwarding Table window

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

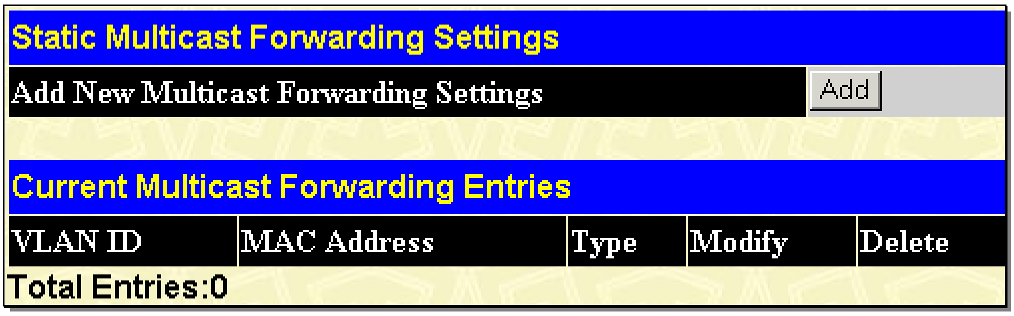
Parameter	Description
Unit	Enter the unit to configure.
Port	Allows the selection of the port number on which the MAC address entered above resides.
VID	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.

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

Multicast Forwarding

The following window is used to set up multicast forwarding on the Switch.

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



Static Multicast Forwarding Settings

Add New Multicast Forwarding Settings [Add]

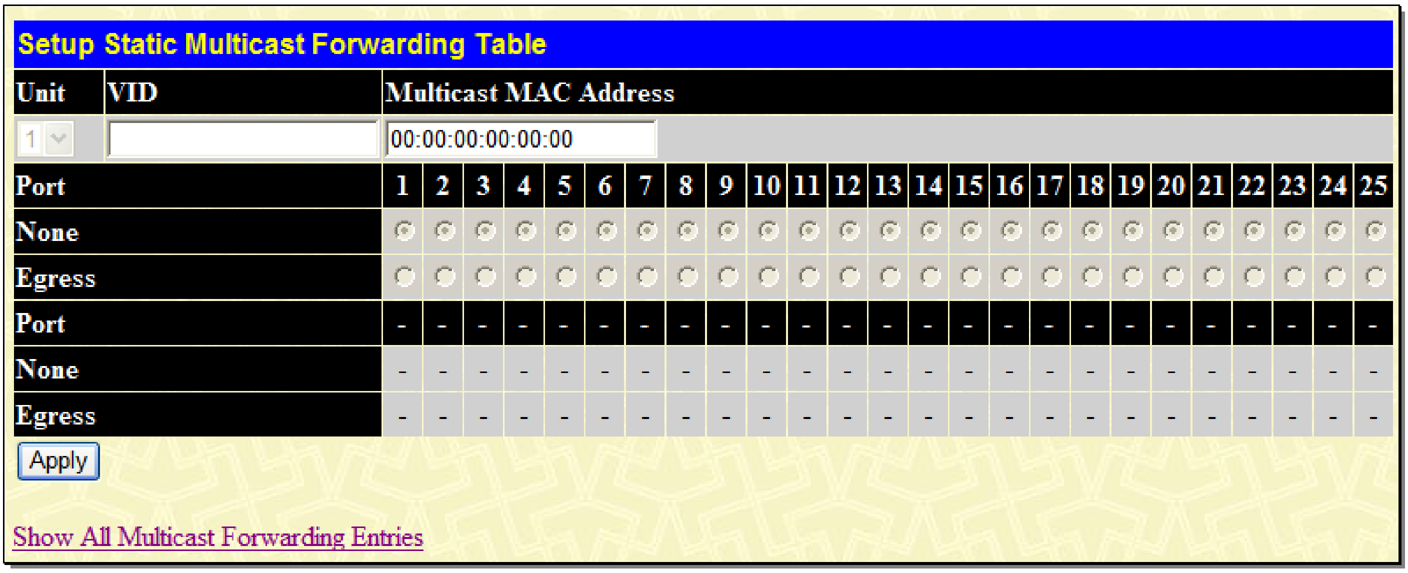
Current Multicast Forwarding Entries

VLAN ID	MAC Address	Type	Modify	Delete

Total Entries:0

Figure 3- 60. 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:



Setup Static Multicast Forwarding Table

Unit	VID	Multicast MAC Address
1		00:00:00:00:00:00

Port	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
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Egress	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Port	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Egress	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

[Apply]

Show All Multicast Forwarding Entries

Figure 3- 61. Setup Static Multicast Forwarding Table window

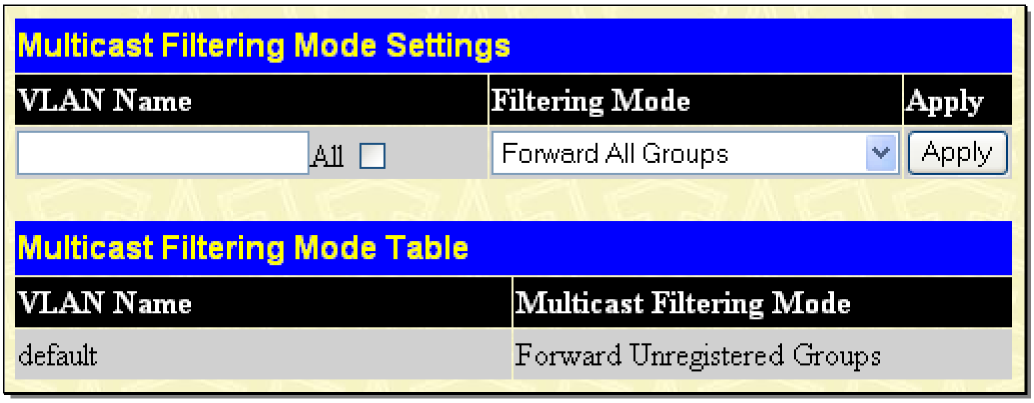
The following parameters can be set:

Parameter	Description
Unit	Select the unit to configure.
VID	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	Allows the selection of ports that will be members of the static multicast group and ports 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.

Multicast Filtering Mode

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



Multicast Filtering Mode Settings

VLAN Name	Filtering Mode	Apply
All □	Forward All Groups	Apply

Multicast Filtering Mode Table

VLAN Name	Multicast Filtering Mode
default	Forward Unregistered Groups

Figure 3- 62. Multicast Filtering Mode Settings window

The following parameters can be set:

Parameter	Description
VLAN Name	The VLAN to which the specified filtering action applies. Tick the All check box to apply the action to all VLANs on the Switch.
Filtering Mode	This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN. *Forward All Groups* – This will instruct the Switch to forward a multicast packet to all multicast groups residing within the range of ports specified above. *Forward Unregistered Groups* – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. *Filter Unregistered Groups* – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above but it will forward the multicast reserved address. For example: 224.0.0.x/24 and FF0x::/16 can be forwarded in Filter Unregistered Groups mode

Click **Apply** to implement changes made.

LLDP

The Link Layer Discovery Protocol (LLDP) allows stations attached to a LAN to advertise, to other stations attached to the same LAN segment, the connectivity and management information necessary to identify, to those management entities, the station's point of attachment to the LAN or network. The information distributed via this protocol is stored by its recipients in a standard management information base (MIB), making it possible for the information to be accessed by a network management system (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP standard specifies the necessary protocol and management elements to:

1. Facilitate multi-vendor inter-operability and the use of standard management tools to discover and make available physical topology information for network management
2. Make it possible for network management to discover certain configuration inconsistencies or malfunctions that can result in impaired communication at higher layers.
3. Provide information to assist network management in making resource changes and/or reconfigurations that correct configuration inconsistencies or malfunctions identified above.

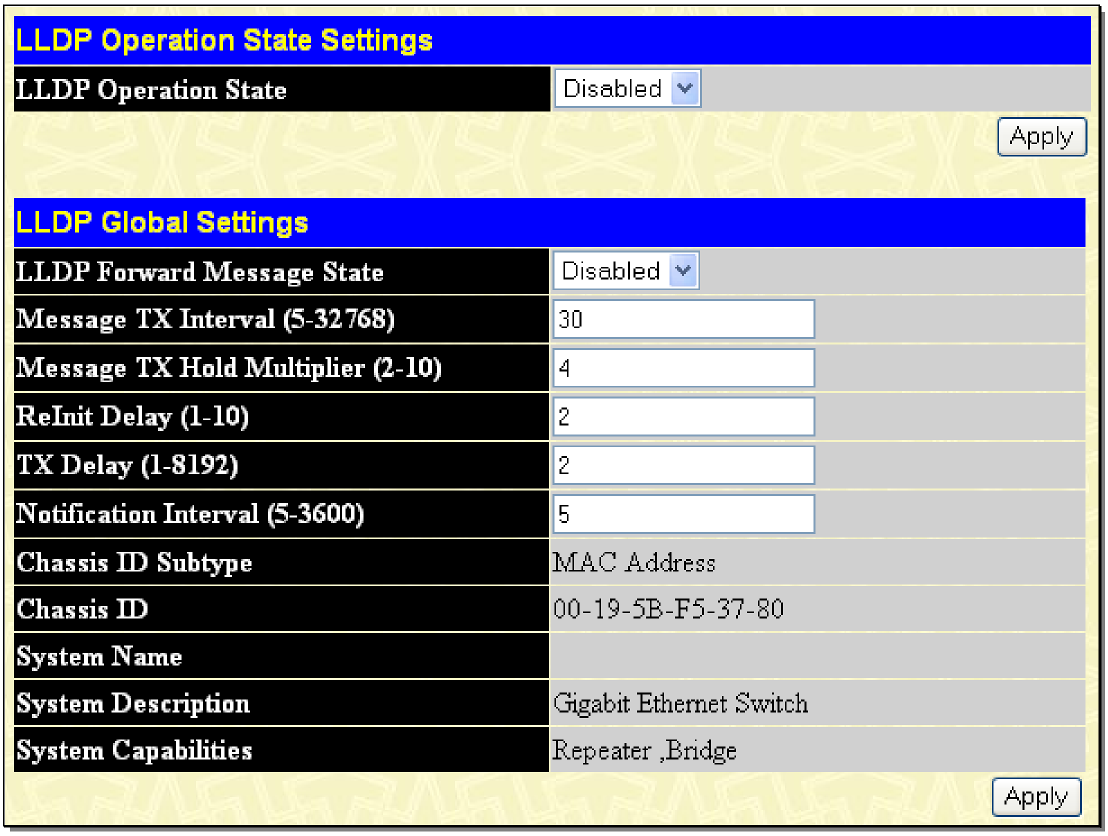
LLDP is a one way protocol (transmit and receive are separated). An LLDP agent can transmit information about the capabilities and current status of the system associated with its MSAP identifier. The LLDP agent can also receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, LLDP agents are not provided any means of soliciting information from other LLDP agents via this protocol.

LLDP allows the transmitter and the receiver to be separately enabled, making it possible to configure an implementation to restrict the local LLDP agent either to transmit only or receive only, or to allow the local LLDP agent to both transmit and receive LLDP information

LLDP Global Settings

The following window is used to set up LLDP on the Switch.

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



LLDP Operation State Settings

LLDP Operation State	Disabled

LLDP Global Settings

LLDP Forward Message State	Disabled
Message TX Interval (5-32768)	30
Message TX Hold Multiplier (2-10)	4
ReInit Delay (1-10)	2
TX Delay (1-8192)	2
Notification Interval (5-3600)	5
Chassis ID Subtype	MAC Address
Chassis ID	00-19-5B-F5-37-80
System Name	
System Description	Gigabit Ethernet Switch
System Capabilities	Repeater ,Bridge

Figure 3- 63. LLDP Operation State Settings window

The following parameters can be set:

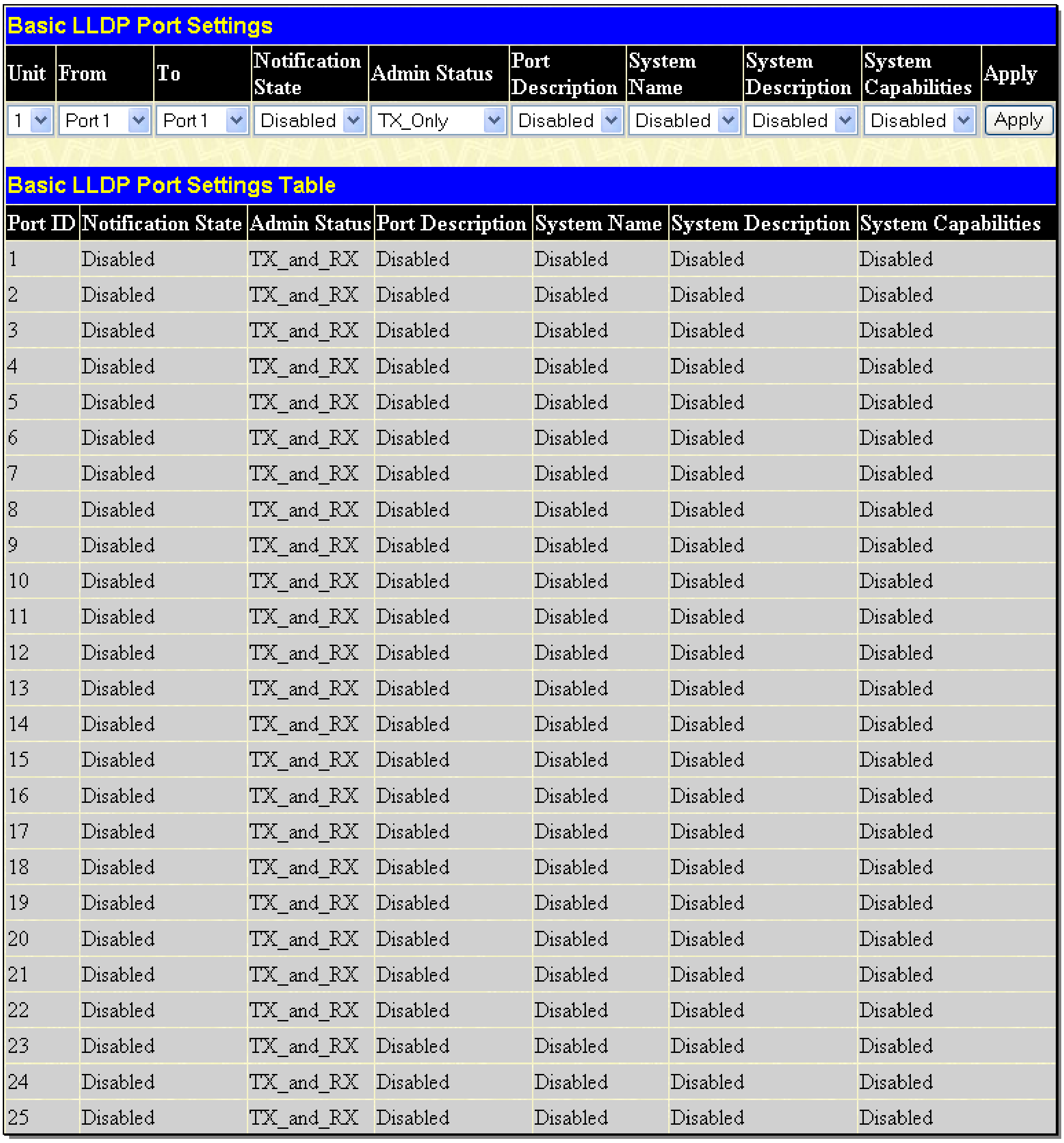
Parameter	Description
LLDP Operation State	When this function is *Enabled*, the switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table.
LLDP Forward Message State	Use the drop-down menu to disable or enable the LLDP forward message state.
Message TX Interval (5-32768)	This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is *30* seconds.
Message TX Hold Multiplier (2-10)	This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is *4*.
ReInit Delay (1-10)	This parameter indicates the amount of delay from when adminStatus becomes "disabled" until re-initialization will be attempted. The default value is *2* seconds.
TX Delay (1-8192)	This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: 1 < txDelay < (0.25 × msgTxInterval) The default value is *2* seconds.
Notification Interval (5-3600)	Used to configure the timer of notification interval for sending notification to configured SNMP trap receiver(s). The default value is *5* seconds.

Click **Apply** to implement changes made.

Basic LLDP Port Settings

The following window is used to set up LLDP on individual port(s) on the Switch.

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



Basic LLDP Port Settings

Unit	From	To	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities	Apply
1	Port 1	Port 1	Disabled	TX_Only	Disabled	Disabled	Disabled	Disabled	Apply

Basic LLDP Port Settings Table

Port ID	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
2	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
3	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
4	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
5	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
6	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
7	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
8	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
9	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
10	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
11	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
12	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
13	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
14	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
15	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
16	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
17	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
18	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
19	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
20	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
21	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
22	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
23	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
24	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
25	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled

Figure 3- 64. Basic LLDP Port Settings window

The following parameters can be set or displayed:

Parameter	Description
Unit	Select the desired stacking unit, if applicable.
From/To	Select a port or group of ports using the pull-down menus.
Notification State	Used to configure each port for sending notification to configured SNMP trap receiver(s). Enable or disable each port for sending change notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, and information update. In addition, the changed type includes any data update /insert/remove.

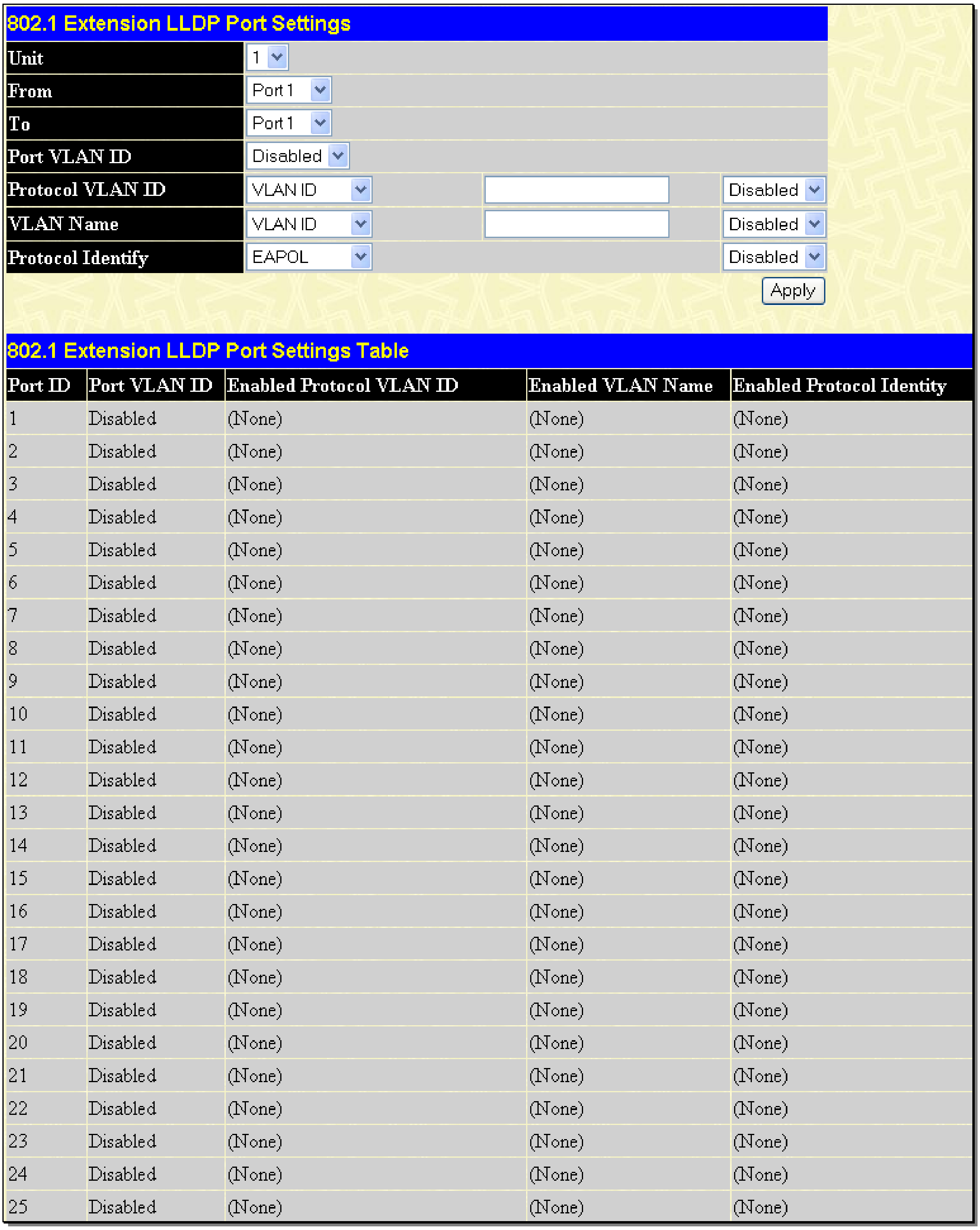
Admin Status	Use the drop-down menu to choose: *TX_Only*, *RX_Only*, *TX_and_RX*, or *Disabled*.
Port Description	Use the drop-down menu to toggle Port Description between *Enabled* and *Disabled*.
System Name	Use the drop-down menu to toggle System Name between *Enabled* and *Disabled*.
System Description	Use the drop-down menu to toggle System Description between *Enabled* and *Disabled*.
System Capabilities	Use the drop-down menu to toggle System Capabilities between *Enabled* and *Disabled*.

Click **Apply** to implement changes made.

802.1 Extension LLDP Port Settings

The following window is used to set up 802.1 Extension LLDP on individual port(s) on the Switch.

To view this window, click **L2 Features** > **LLDP** > **802.1 Extension LLDP Port Settings**, as shown below:



802.1 Extension LLDP Port Settings

Unit	1		
From	Port 1		
To	Port 1		
Port VLAN ID	Disabled		
Protocol VLAN ID	VLAN ID		Disabled
VLAN Name	VLAN ID		Disabled
Protocol Identify	EAPOL		Disabled

802.1 Extension LLDP Port Settings Table

Port ID	Port VLAN ID	Enabled Protocol VLAN ID	Enabled VLAN Name	Enabled Protocol Identity
1	Disabled	(None)	(None)	(None)
2	Disabled	(None)	(None)	(None)
3	Disabled	(None)	(None)	(None)
4	Disabled	(None)	(None)	(None)
5	Disabled	(None)	(None)	(None)
6	Disabled	(None)	(None)	(None)
7	Disabled	(None)	(None)	(None)
8	Disabled	(None)	(None)	(None)
9	Disabled	(None)	(None)	(None)
10	Disabled	(None)	(None)	(None)
11	Disabled	(None)	(None)	(None)
12	Disabled	(None)	(None)	(None)
13	Disabled	(None)	(None)	(None)
14	Disabled	(None)	(None)	(None)
15	Disabled	(None)	(None)	(None)
16	Disabled	(None)	(None)	(None)
17	Disabled	(None)	(None)	(None)
18	Disabled	(None)	(None)	(None)
19	Disabled	(None)	(None)	(None)
20	Disabled	(None)	(None)	(None)
21	Disabled	(None)	(None)	(None)
22	Disabled	(None)	(None)	(None)
23	Disabled	(None)	(None)	(None)
24	Disabled	(None)	(None)	(None)
25	Disabled	(None)	(None)	(None)

Figure 3- 65. 802.1 Extension LLDP Port Settings Table window

The following parameters can be set or displayed:

Parameter	Description
Unit	Select the desired stacking unit, if applicable.

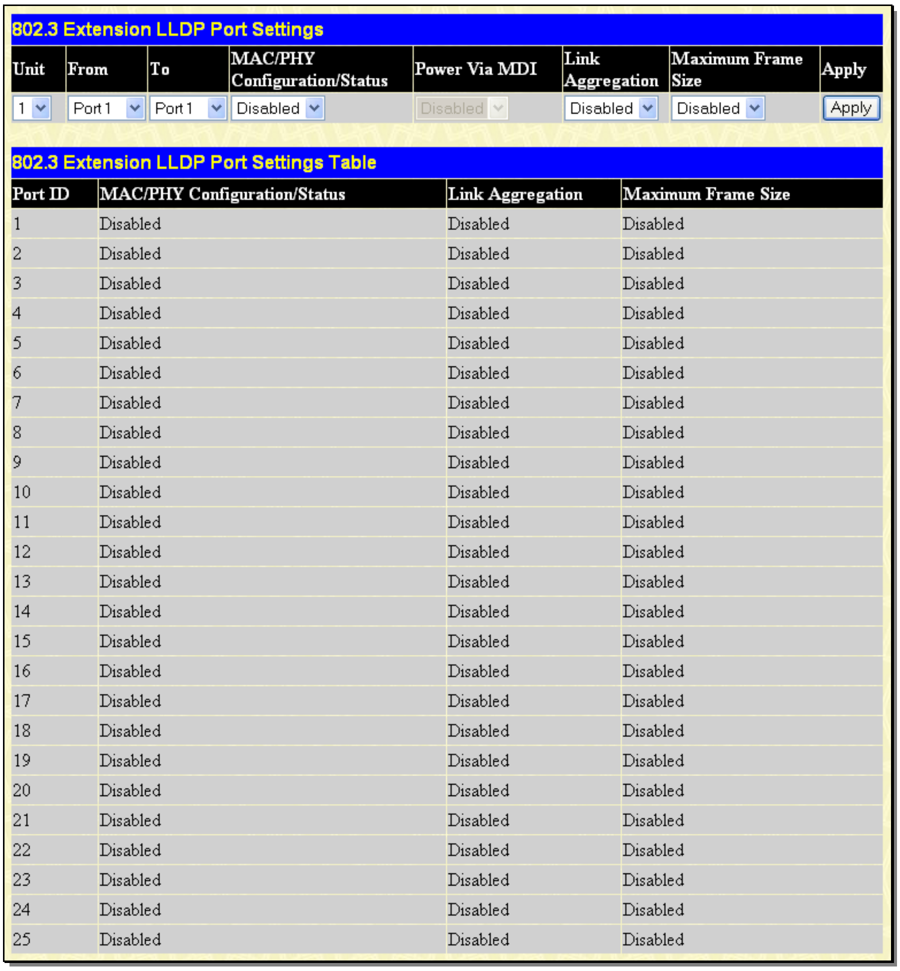
From/To	Select a port or group of ports using the pull-down menus.
Port VLAN ID	Use the drop-down menu to toggle Port VLAN ID between *Enabled* and *Disabled*.
Protocol VLAN ID	Use the drop-down menu to toggle among *VLAN ID*, *VLAN Name*, and *All*. Use the drop-down menu to toggle between *Enabled* and *Disabled.*
VLAN Name	Use the drop-down menu to toggle among *VLAN ID*, *VLAN Name*, and *All*. Use the drop-down menu to toggle between *Enabled* and *Disabled.*
Protocol Identity	Use the drop-down menu to toggle among *EAPOL*, *LACP*, *GVRP*, *STP*, and *All*. Use the drop-down menu to toggle between *Enabled* and *Disabled.*

Click **Apply** to implement changes made.

802.3 Extension LLDP Port Settings

The following window is used to set up 802.3 Extension LLDP on individual port(s) on the Switch.

To view this window, click **L2 Features** > **LLDP** > **802.3 Extension LLDP Port Settings**, as shown below:



802.3 Extension LLDP Port Settings

Unit	From	To	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size	Apply
1	Port 1	Port 1	Disabled	Disabled	Disabled	Disabled	Apply

802.3 Extension LLDP Port Settings Table

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

Figure 3- 66. 802.3 Extension LLDP Port Settings Table window

The following parameters can be set or displayed:

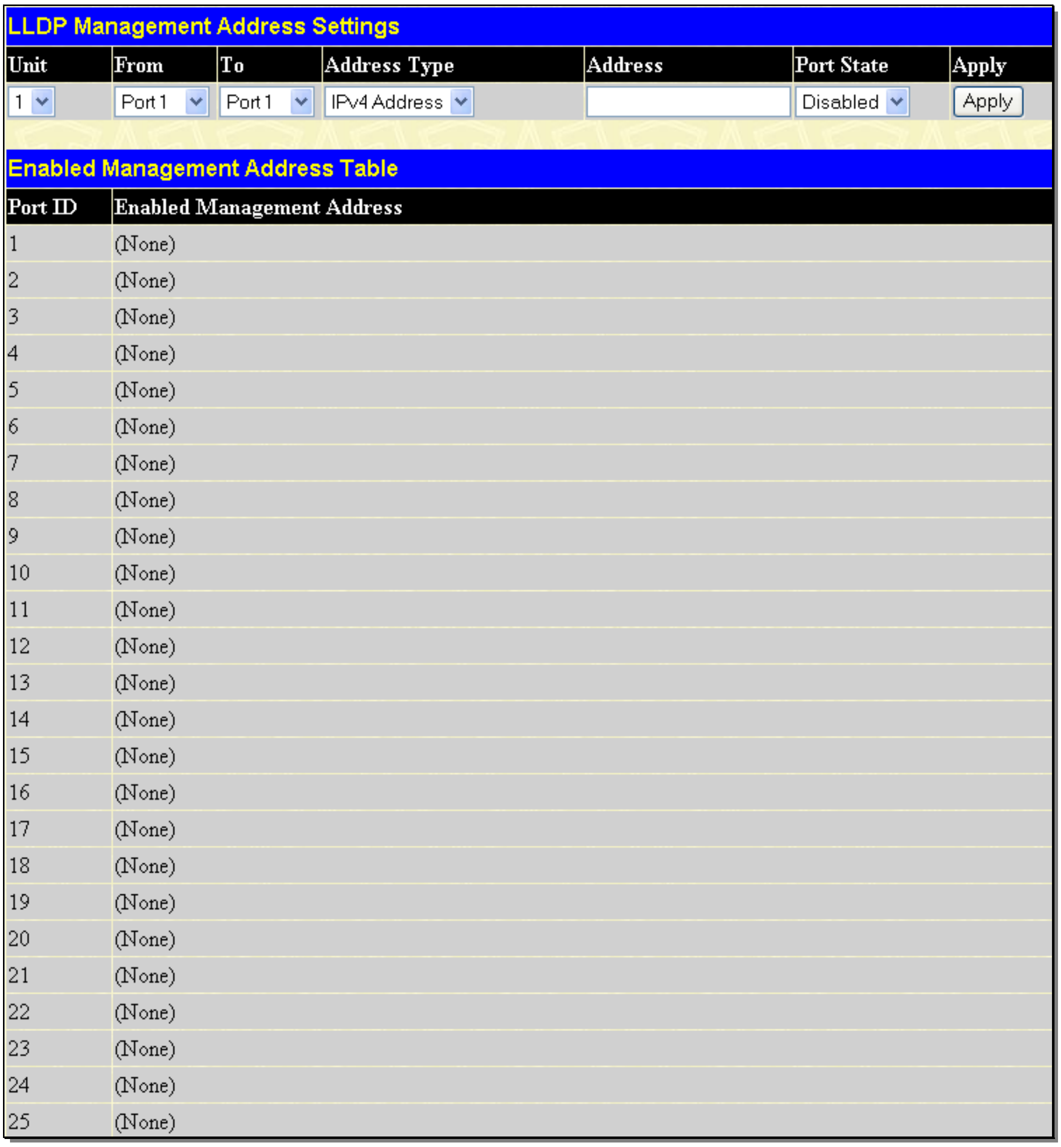
Parameter	Description
Unit	Select the desired stacking unit, if applicable.
From/To	Select a port or group of ports using the pull-down menus.
MAC/PHY Configuration/Status	Use the drop-down menu to toggle the MAC/PHY Configuration/Status between *Enabled* and *Disabled*.
Power Via MDI	This TLV optional data type indicates that LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is *Disabled*.
Link Aggregation	Use the drop-down menu to toggle Link Aggregation between *Enabled* and *Disabled*.
Maximum Frame Size	Use the drop-down menu to toggle Maximum Frame Size between *Enabled* and *Disabled*.

Click **Apply** to implement changes made.

LLDP Management Address Settings

The following window is used to set up LLDP management address settings on the Switch.

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



LLDP Management Address Settings

Unit	From	To	Address Type	Address	Port State	Apply
1	Port 1	Port 1	IPv4 Address		Disabled	Apply

Enabled Management Address Table

Port ID	Enabled Management Address
1	(None)
2	(None)
3	(None)
4	(None)
5	(None)
6	(None)
7	(None)
8	(None)
9	(None)
10	(None)
11	(None)
12	(None)
13	(None)
14	(None)
15	(None)
16	(None)
17	(None)
18	(None)
19	(None)
20	(None)
21	(None)
22	(None)
23	(None)
24	(None)
25	(None)

Figure 3- 67. LLDP Management Address Settings window

The following parameters can be set or displayed:

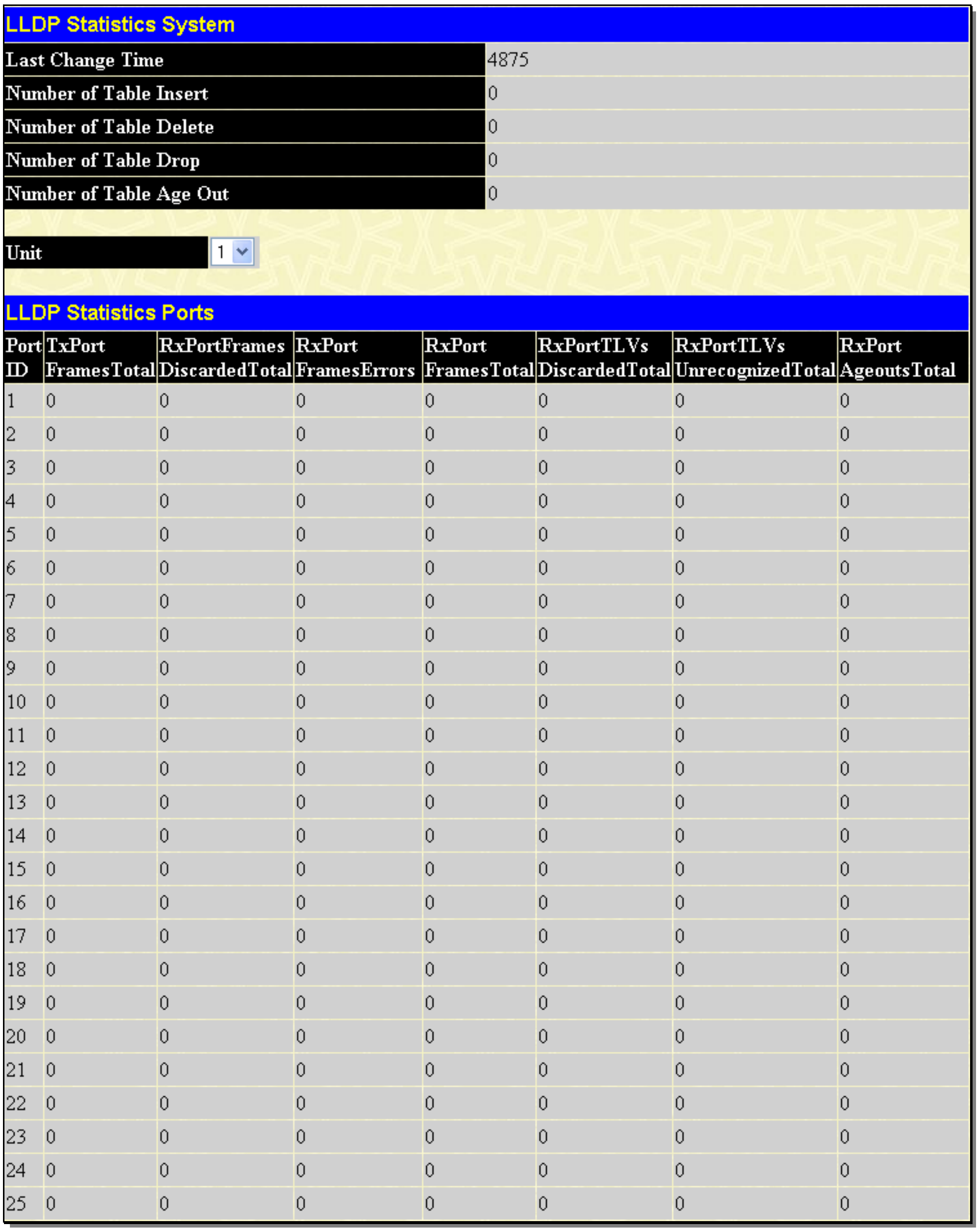
Parameter	Description
Unit	Select the desired stacking unit, if applicable.
From/To	Select a port or group of ports using the pull-down menus.
Address Type	Use the drop-down menu to toggle between *IPV4 Address* and *IPV6 Address*.
Address	Enter the LLDP management address in this field.
Port State	Use the drop-down menu to toggle the Port State between *Enabled* and *Disabled*.

Click **Apply** to implement changes made.

LLDP Statistics

The following window is used to display LLDP statistics.

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



LLDP Statistics System

Last Change Time	4875
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Age Out	0

Unit 1

LLDP Statistics Ports

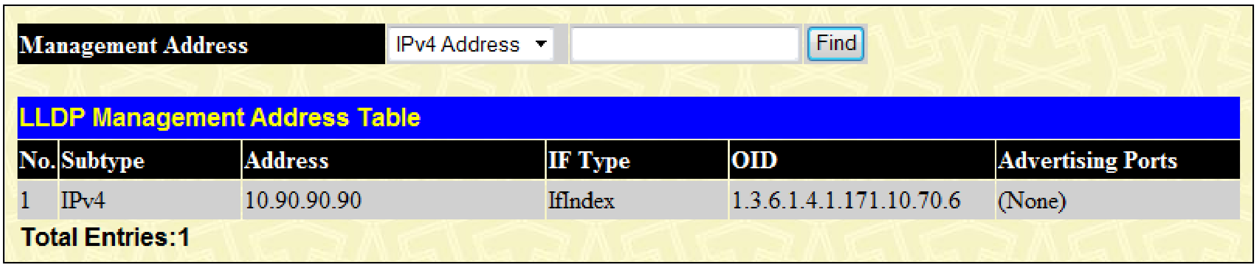
Port ID	TxPort FramesTotal	RxPortFrames DiscardedTotal	RxPort FramesErrors	RxPort FramesTotal	RxPortTLVs DiscardedTotal	RxPortTLVs UnrecognizedTotal	RxPort AgeoutsTotal
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0

Figure 3- 68. LLDP Statistics System window

LLDP Management Address Table

The following window is used to make entries to and display the LLDP Management Address Table.

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



Management Address: IPv4 Address

LLDP Management Address Table

No.	Subtype	Address	IF Type	OID	Advertising Ports
1	IPv4	10.90.90.90	IfIndex	1.3.6.1.4.1.171.10.70.6	(None)

Total Entries:1

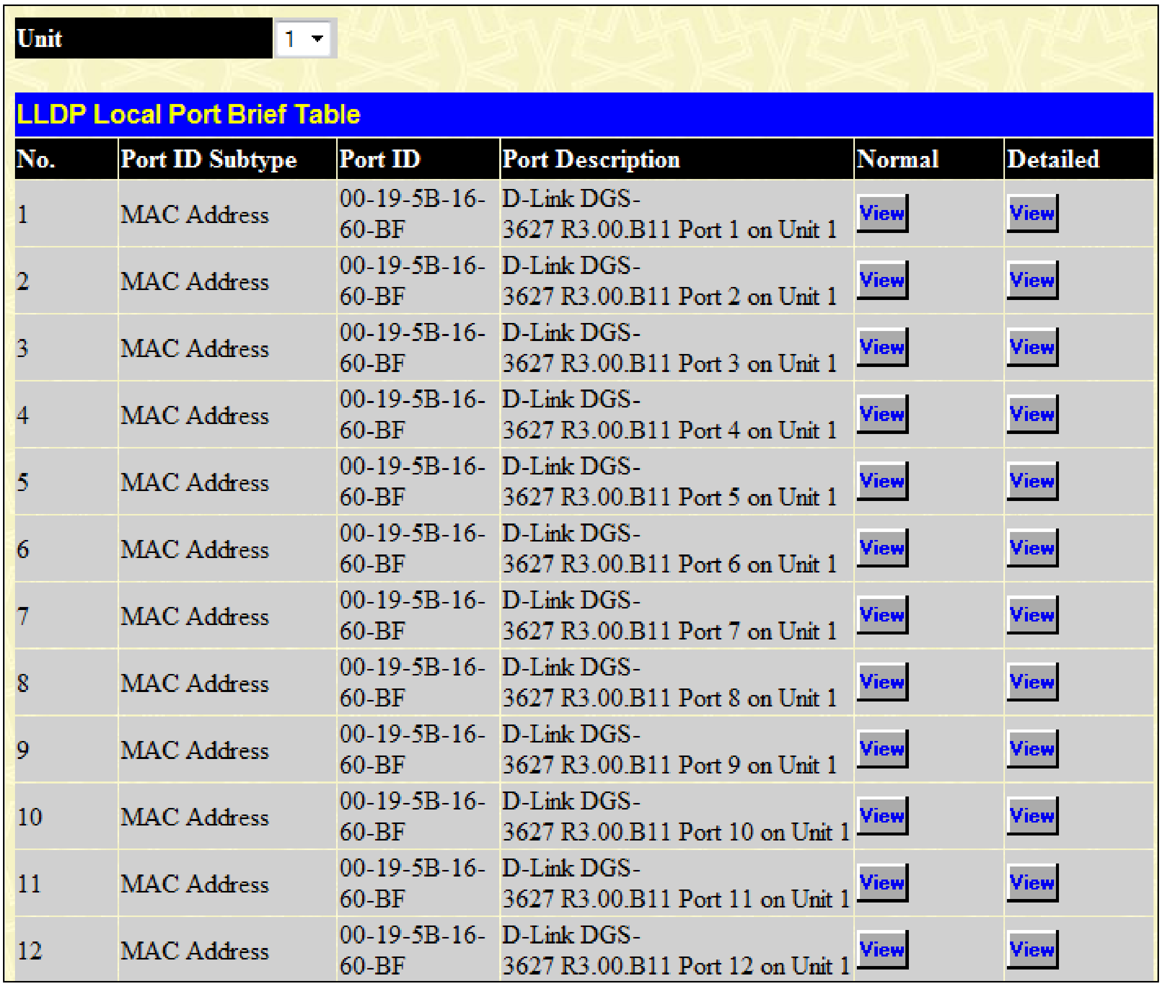
Figure 3- 69. LLDP Management Address Table window

Use the drop-down menu to select the type of Management Address, enter an IP address in the field provided, and then click the **Find** button.

LLDP Local Port Table

The following window is used to display the LLDP Local Port Brief Table.

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



Unit: 1

LLDP Local Port Brief Table

No.	Port ID Subtype	Port ID	Port Description	Normal	Detailed
1	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 1 on Unit 1	View	View
2	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 2 on Unit 1	View	View
3	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 3 on Unit 1	View	View
4	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 4 on Unit 1	View	View
5	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 5 on Unit 1	View	View
6	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 6 on Unit 1	View	View
7	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 7 on Unit 1	View	View
8	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 8 on Unit 1	View	View
9	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 9 on Unit 1	View	View
10	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 10 on Unit 1	View	View
11	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 11 on Unit 1	View	View
12	MAC Address	00-19-5B-16-60-BF	D-Link DGS-3627 R3.00.B11 Port 12 on Unit 1	View	View

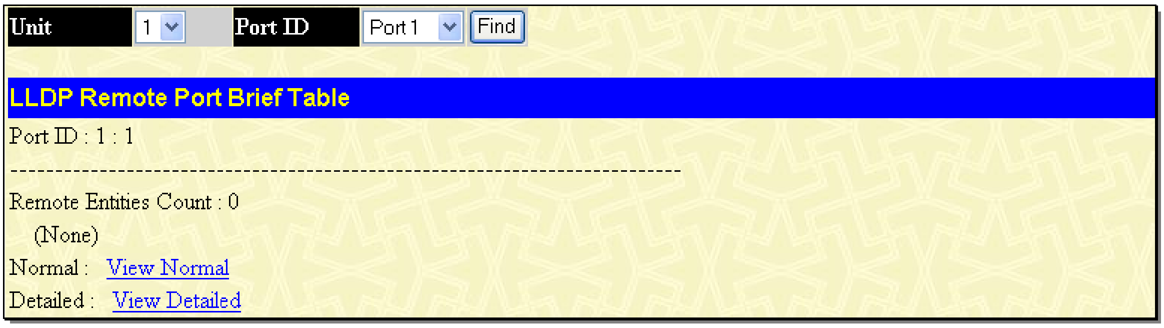
Figure 3- 70. LLDP Local Port Brief Table window

Click the **View** button to display additional information about entries on the LLDP Local Port Brief Table.

LLDP Remote Port Table

The following window is used to display the LLDP Remote Port Brief Table.

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



LLDP Remote Port Brief Table

Port ID : 1 : 1

Remote Entities Count : 0

(None)

Normal : View Normal

Detailed : View Detailed

Figure 3- 71. LLDP Remote Port Brief Table window

Click the View Normal and View Detailed hyperlinks to display additional information.

Q-in-Q

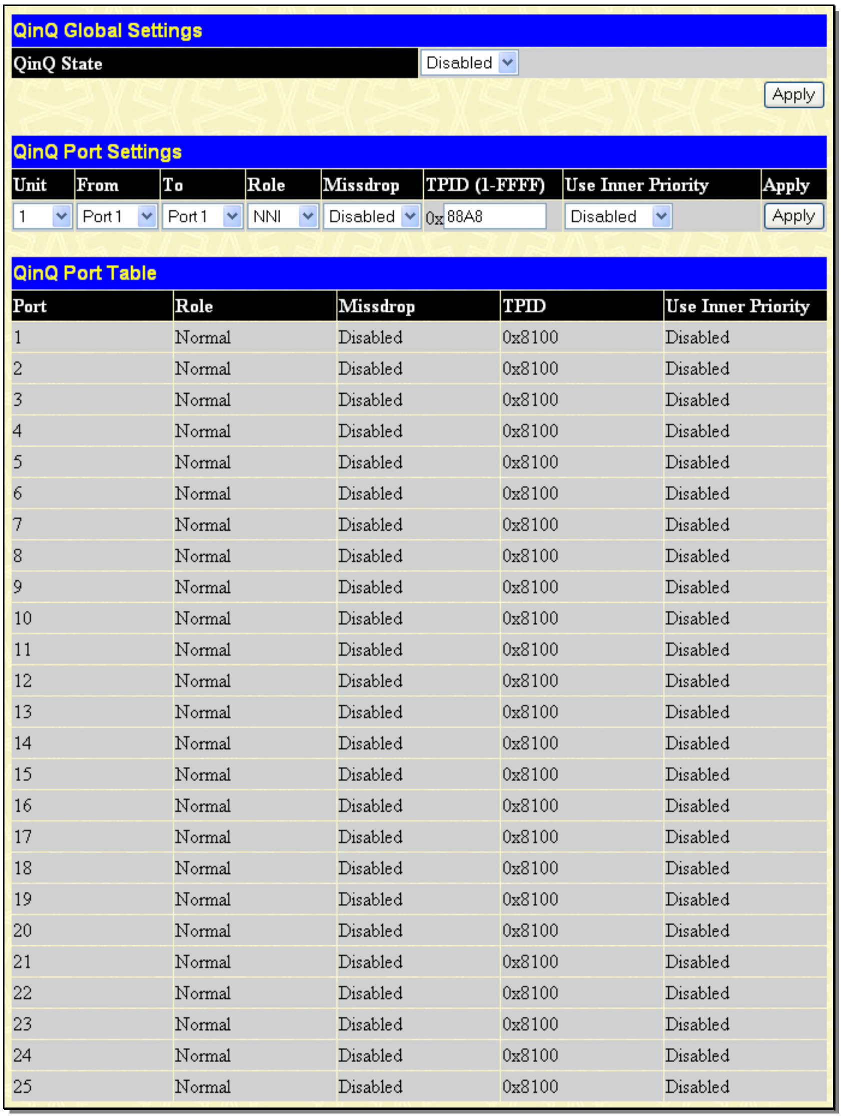
Q-in-Q is designed for service providers to carry traffic from multiple users across a network. Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's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

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

Q-in-Q Settings

This function allows the user to enable or disable the Q-in-Q function.

To view this window click **L2 Features > Q-in-Q > Global Settings**, as shown.



QinQ Global Settings

QinQ State	Disabled

QinQ Port Settings

Unit	From	To	Role	Missdrop	TPID (1-FFFF)	Use Inner Priority	Apply
1	Port 1	Port 1	NNI	Disabled	0x 88A8	Disabled	Apply

QinQ Port Table

Port	Role	Missdrop	TPID	Use Inner Priority
1	Normal	Disabled	0x8100	Disabled
2	Normal	Disabled	0x8100	Disabled
3	Normal	Disabled	0x8100	Disabled
4	Normal	Disabled	0x8100	Disabled
5	Normal	Disabled	0x8100	Disabled
6	Normal	Disabled	0x8100	Disabled
7	Normal	Disabled	0x8100	Disabled
8	Normal	Disabled	0x8100	Disabled
9	Normal	Disabled	0x8100	Disabled
10	Normal	Disabled	0x8100	Disabled
11	Normal	Disabled	0x8100	Disabled
12	Normal	Disabled	0x8100	Disabled
13	Normal	Disabled	0x8100	Disabled
14	Normal	Disabled	0x8100	Disabled
15	Normal	Disabled	0x8100	Disabled
16	Normal	Disabled	0x8100	Disabled
17	Normal	Disabled	0x8100	Disabled
18	Normal	Disabled	0x8100	Disabled
19	Normal	Disabled	0x8100	Disabled
20	Normal	Disabled	0x8100	Disabled
21	Normal	Disabled	0x8100	Disabled
22	Normal	Disabled	0x8100	Disabled
23	Normal	Disabled	0x8100	Disabled
24	Normal	Disabled	0x8100	Disabled
25	Normal	Disabled	0x8100	Disabled

Figure 3- 72. Q-in-Q Global Settings window

The following fields can be set:

Parameter	Description
Q-in-Q State	Use the pull-down menu to enable or disable the Q-in-Q Global State. When Q-in-Q is *Enabled*, all network port roles will have NNI ports and their outer TPID set to 0x88a8. All existing static VLANs will run as SP-VLANs. All dynamically learned L2 addresses and all dynamically registered VLAN entries will be cleared, GVRP will be disabled. According

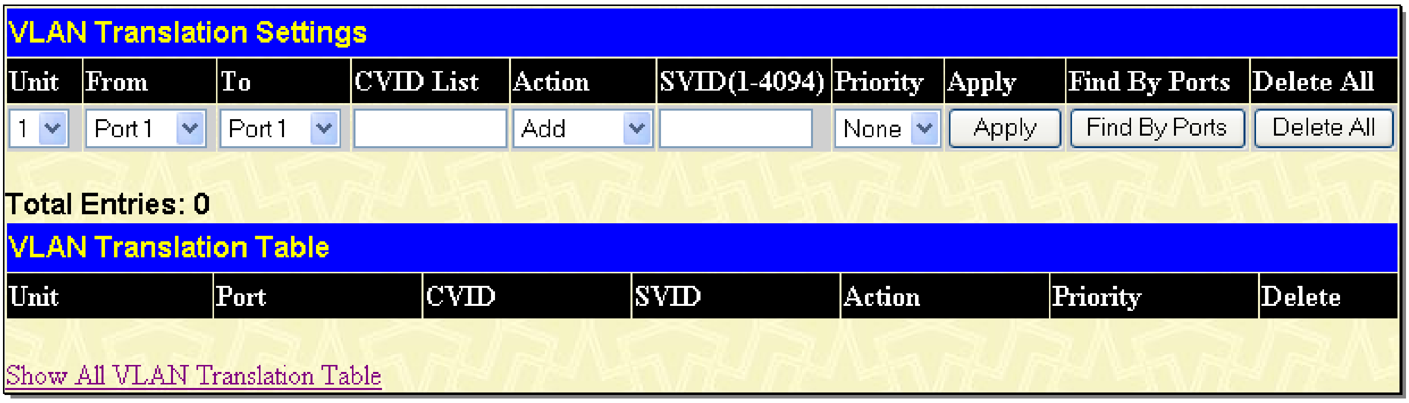
	802.1ad, the address 01-80-c2-00-00-08 will be used for STP in the provider's network. So the user shall disable STP first, and then use the new address for STP state machine. The default setting is *Disabled*.
Unit	Select the Switch to be configured.
From/To	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
Role	The user can choose between UNI or NNI role. *UNI* – To select a user-to-network interface which specifies that communication between the specified user and a specified network will occur. *NNI* – To select a network-to-network interface specifies that communication between two specified networks will occur.
Missdrop	*Enable* or *Disable* C-VLAN based on SP-VLAN assignment miss drop. When enabled the tagged packet will be dropped if the VLAN translation look up misses. When disabled the packet will not be dropped if the VLAN translation loop up misses. If VLAN translation table lookup misses, the packet can be either dropped or add an outer VLAN based on MAC/SUBNET/PROTOCOL/PORT based VLAN configuration. This will make the packet as a double tagged packet. Note: The result will be Transparent Mode behavior.
TPID(0x1-0xffff)	The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID.
Use Inner Priority	Specify whether to use the priority in the C-VLAN tag as the priority in the S-VLAN tag. By default, the setting is *Disabled*.

Click **Apply** to implement changes.

VLAN Translation Settings

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

To view this window, click **L2 Features > Q-in-Q > VLAN Translation Settings**, as shown below:



VLAN Translation Settings

Unit	From	To	CVID List	Action	SVID(1-4094)	Priority	Apply	Find By Ports	Delete All
1	Port 1	Port 1		Add		None	Apply	Find By Ports	Delete All

Total Entries: 0

VLAN Translation Table

Unit	Port	CVID	SVID	Action	Priority	Delete

Show All VLAN Translation Table

Figure 3- 73. VLAN Translation Settings window

The following fields can be set:

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

Click **Apply** to create a new entry, click **Find By Ports** to view the current entries by ports and **Delete All** to remove a VLAN Translation entry. To view the VLAN translation table, click the hyperlinked Show All VLAN Translation Table.

ERPS

The Switch supports ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) to provide a reliable mechanism of malfunction recovery in an Ethernet ring topology network.

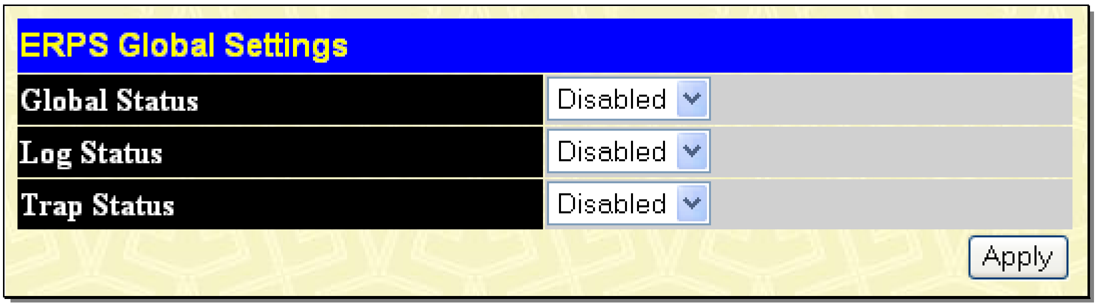
ERPS Global Settings

This window is used to enable global ERPS function on the Switch. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. The global ERPS function cannot be enabled when any ERPS ring on the device is enabled and the integrity of any ring parameter is not available. For each ring, with the individual ring state enabled and ERPS enabled globally, the following integrity will be checked:

1. The Ring-Automatic Protection Switching (R-APS) VLAN is created.
2. The Ring port is a tagged member port of the R-APS VLAN.
3. The Ring Protection Link (RPL) port is specified if the RPL owner is enabled.

The default state is disabled.

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



ERPS Global Settings

Global Status	Disabled
Log Status	Disabled
Trap Status	Disabled

Figure 3- 74. ERPS Global Settings window

The following fields can be set:

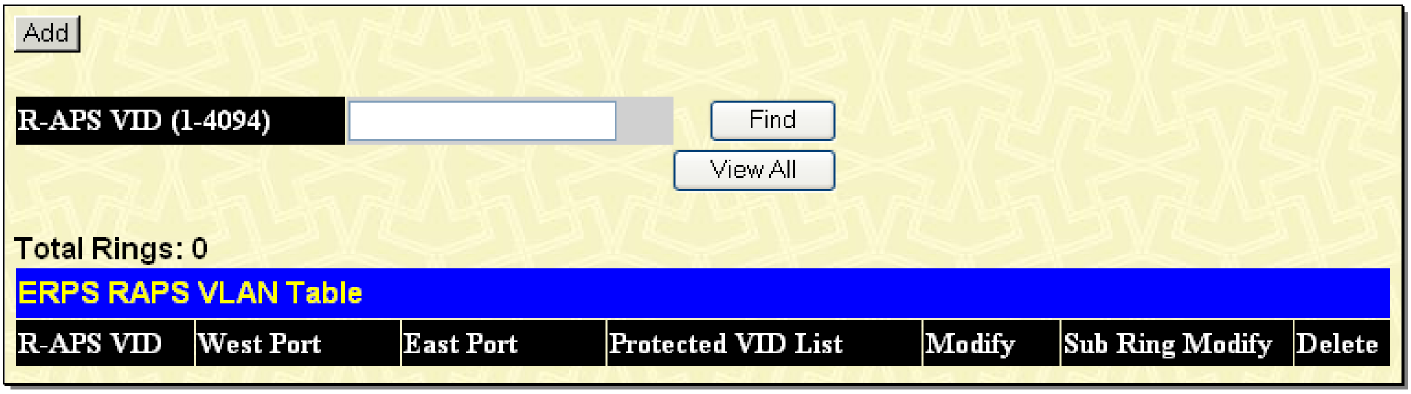
Parameter	Description
Global Status	Enable the global ERPS function on a switch.
Log Status	Enable or disable the log state of ERPS events. The default value is *Disabled*.
Trap Status	Enable or disable the trap state of ERPS events. The default value is *Disabled*

Click **Apply** to implement changes made.

ERPS RAPS VLAN Settings

This window allows users to search for and display ERPS RAPS information. Enter an R-APS VLAN ID in the field provided.

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



R-APS VID (1-4094)

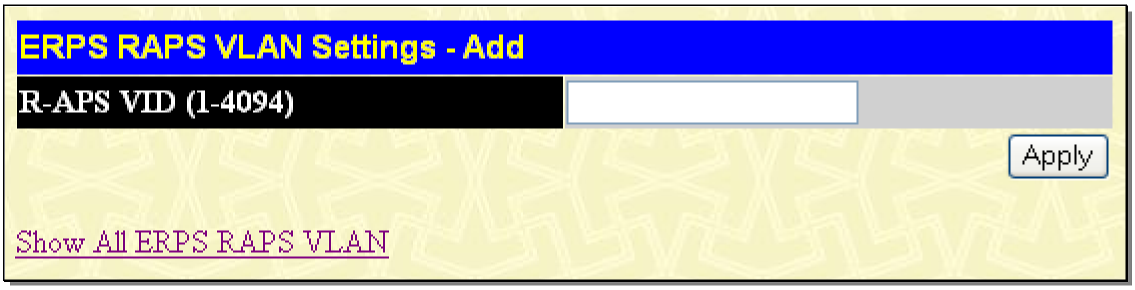
Total Rings: 0

ERPS RAPS VLAN Table

R-APS VID	West Port	East Port	Protected VID List	Modify	Sub Ring Modify	Delete

Figure 3- 75. ERPS RAPS VLAN Settings window

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



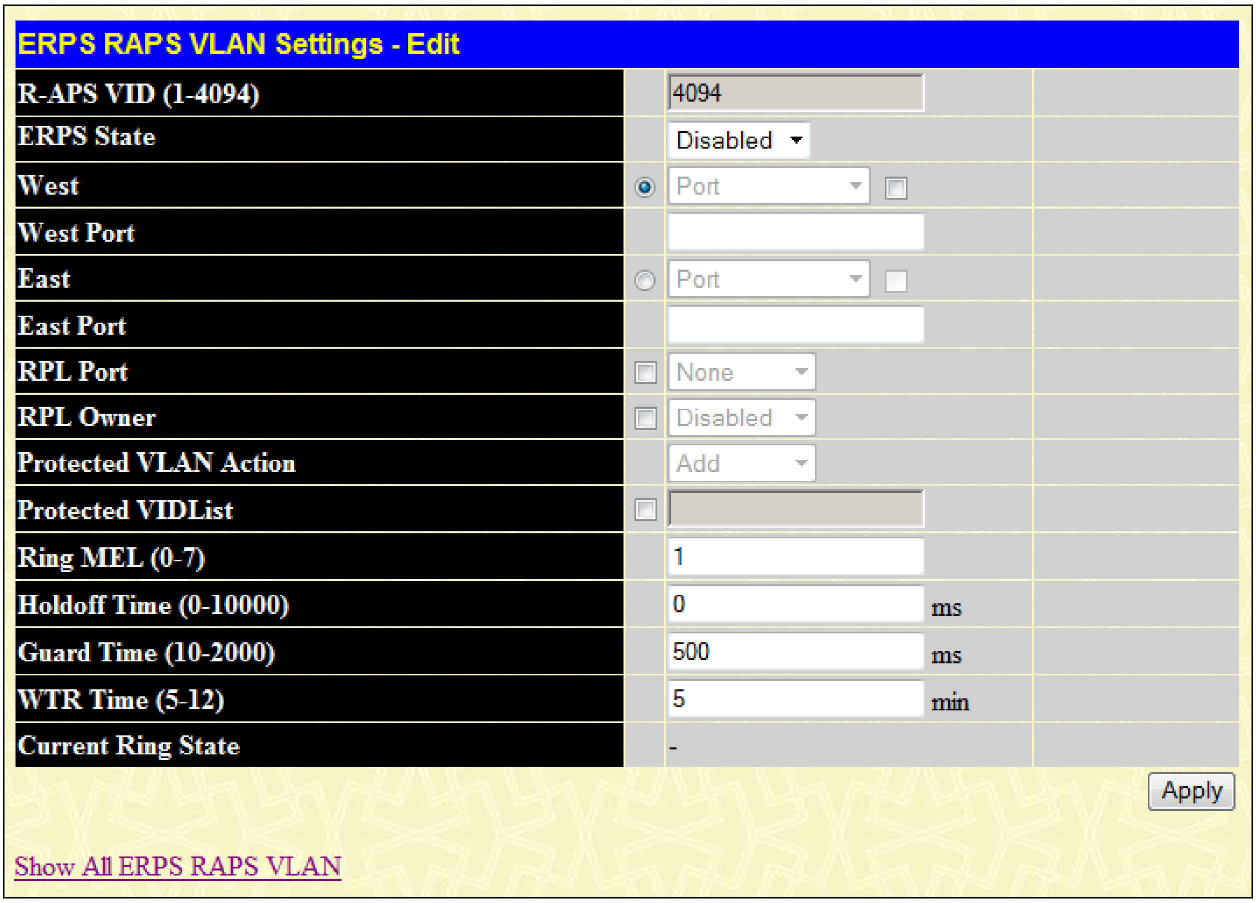
ERPS RAPS VLAN Settings - Add

R-APS VID (1-4094)	

Figure 3- 76. ERPS RAPS VLAN Settings – Add window

Enter an R-APS VLAN ID in the field provided and click **Apply** to make a new entry for the ERPS RAPS VLAN Table.

To edit an exisiting ERPS RAPS VLAN Table entry, click the **Modify** button in the Modify column in the ERPS RAPS VLAN Table. The following window will open:



ERPS RAPS VLAN Settings - Edit

R-APS VID (1-4094)		4094
ERPS State		Disabled
West	●	Port □
West Port		
East	○	Port □
East Port		
RPL Port	□	None
RPL Owner	□	Disabled
Protected VLAN Action		Add
Protected VIDList	□	
Ring MEL (0-7)		1
Holdoff Time (0-10000)		0 ms
Guard Time (10-2000)		500 ms
WTR Time (5-12)		5 min
Current Ring State		-

Figure 3- 77. ERPS RAPS VLAN Settings – Edit window

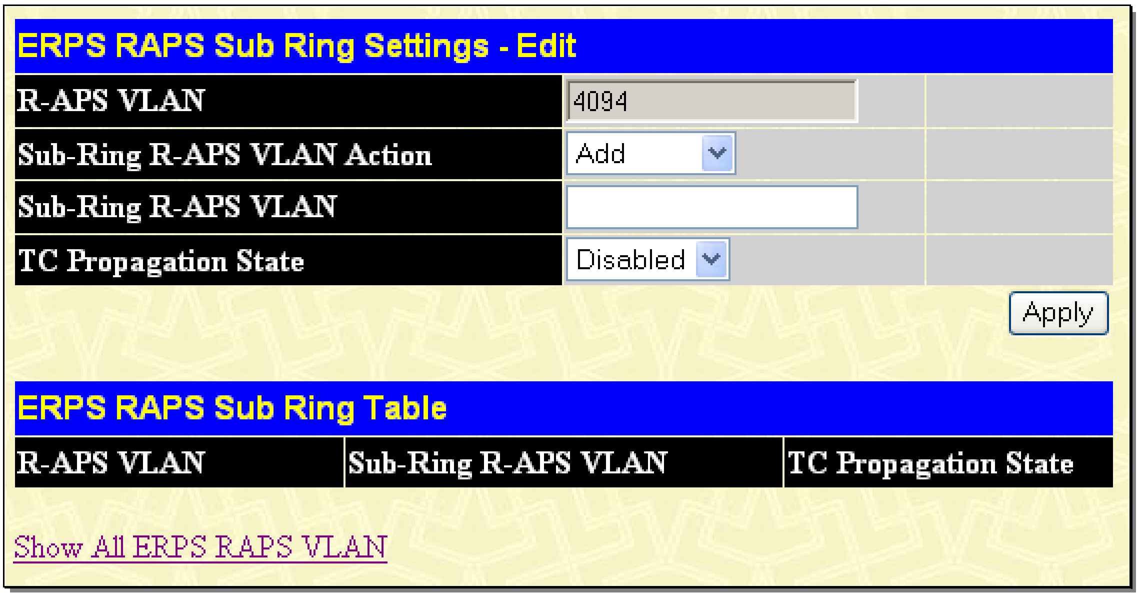
The following fields can be set:

Parameter	Description
ERPS State	This is used to configure ring state of the specified ring. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated. The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when the ring is activated. The default ring state is *Disabled*.
West	Click to specify the port as the west ring port. To specify as a Virtual Channel, tick the check and toggle from *Port* to *Virtual Channel*.
West Port	If Port is set above, enter the port to be configured.

East	Click to specify the port as the east ring port. To specify as a Virtual Channel, tick the check and toggle from *Port* to *Virtual Channel*.
East Port	If Port is set above, enter the port to be configured.
RPL Port	Tick the check box and use the drop-down menu to select *West*, *East*, or *None*. *West* - Specify the west ring port as the RPL port. *East* - Specify the east ring port as the RPL port. *None* - This indicates that there is no RPL port on this node. By default, the node has no RPL port.
RPL Owner	Tick the check box and use the drop-down menu to select *Enabled* or *Disabled*. *Enabled* specifies the device as an RPL owner node. *Disabled* indicates the node is not an RPL owner. By default, the RPL owner is disabled.
Protected VLAN Action	This is used to configure the VLANs that are protected by the ERPS function. The R-APS VLAN cannot be the protected VLAN. The protected VLAN can be one that has already been created, or it can be used for a VLAN that has not yet been created. Toggle between *Add* or *Delete*. *Add* - This adds VLANs to the protected VLAN group. *Delete* - This removes VLANs from the protected VLAN group.
Protected VIDList	Tick this check box and enter the VLANs to be added or deleted.
Ring MEL (0-7)	Enter the ring MEL of the R-APS function. The range is from *0* to *7*. The default ring MEL is *1*.
Holdoff Time (0-10000)	The Holdoff timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the holdoff timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified. The range is from 0 to 10000 milliseconds. The default holdoff time is 0 milliseconds.
Guard Time (10-2000)	The Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case, the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring. The range is from *10* to *2000* milliseconds. The default guard time is *500* milliseconds.
WTR Time (5-12)	The WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block the original unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time. The range is from *5* to *12* minutes. The default WTR time is *5* minutes.

Click **Apply** to implement changes made.

To edit ERPS RAPS Sub Ring Settings for an ERPS RAPS VLAN Table entry, click the **Modify** button in the Sub Ring Modify column in the ERPS RAPS VLAN Table. The following window will open:



ERPS RAPS Sub Ring Settings - Edit

R-APS VLAN	4094
Sub-Ring R-APS VLAN Action	Add
Sub-Ring R-APS VLAN	
TC Propagation State	Disabled

ERPS RAPS Sub Ring Table

R-APS VLAN	Sub-Ring R-APS VLAN	TC Propagation State

Figure 3- 78. ERPS RAPS Sub Ring Settings – Edit window

The following fields can be set:

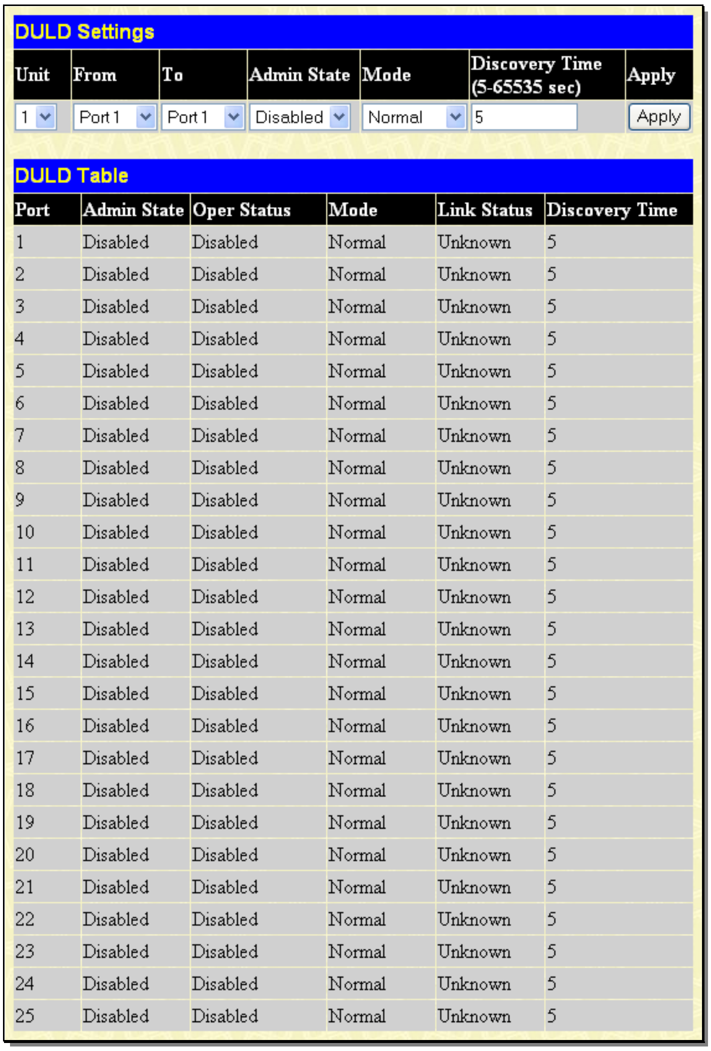
Parameter	Description
Sub-Ring R-APS VLAN Action	Toggle between *Add* or *Delete*. *Add* connects the sub-ring to another ring. *Delete* disconnects the sub-ring from a connected ring.
Sub-Ring R-APS VLAN	Enter the sub-ring R-APS VLAN.
TC Propagation State	This is used to configure the state of topology change propagation for the sub-ring. This setting is applied on the interconnection node.

Click **Apply** to implement changes made.

DULD Settings

The Switch features a D-Link Unidirectional Link Detection (DULD) module. The unidirectional link detection provides a mechanism that can be used to detect unidirectional link for Ethernet switches whose PHYs do not support unidirectional OAM operation. This function is established based on OAM, so OAM should be enabled before starting detection.

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



DULD Settings

Unit	From	To	Admin State	Mode	Discovery Time (5-65535 sec)	Apply
1	Port 1	Port 1	Disabled	Normal	5	Apply

DULD Table

Port	Admin State	Oper Status	Mode	Link Status	Discovery Time
1	Disabled	Disabled	Normal	Unknown	5
2	Disabled	Disabled	Normal	Unknown	5
3	Disabled	Disabled	Normal	Unknown	5
4	Disabled	Disabled	Normal	Unknown	5
5	Disabled	Disabled	Normal	Unknown	5
6	Disabled	Disabled	Normal	Unknown	5
7	Disabled	Disabled	Normal	Unknown	5
8	Disabled	Disabled	Normal	Unknown	5
9	Disabled	Disabled	Normal	Unknown	5
10	Disabled	Disabled	Normal	Unknown	5
11	Disabled	Disabled	Normal	Unknown	5
12	Disabled	Disabled	Normal	Unknown	5
13	Disabled	Disabled	Normal	Unknown	5
14	Disabled	Disabled	Normal	Unknown	5
15	Disabled	Disabled	Normal	Unknown	5
16	Disabled	Disabled	Normal	Unknown	5
17	Disabled	Disabled	Normal	Unknown	5
18	Disabled	Disabled	Normal	Unknown	5
19	Disabled	Disabled	Normal	Unknown	5
20	Disabled	Disabled	Normal	Unknown	5
21	Disabled	Disabled	Normal	Unknown	5
22	Disabled	Disabled	Normal	Unknown	5
23	Disabled	Disabled	Normal	Unknown	5
24	Disabled	Disabled	Normal	Unknown	5
25	Disabled	Disabled	Normal	Unknown	5

Figure 3- 79. DULD Settings window

The following fields can be set:

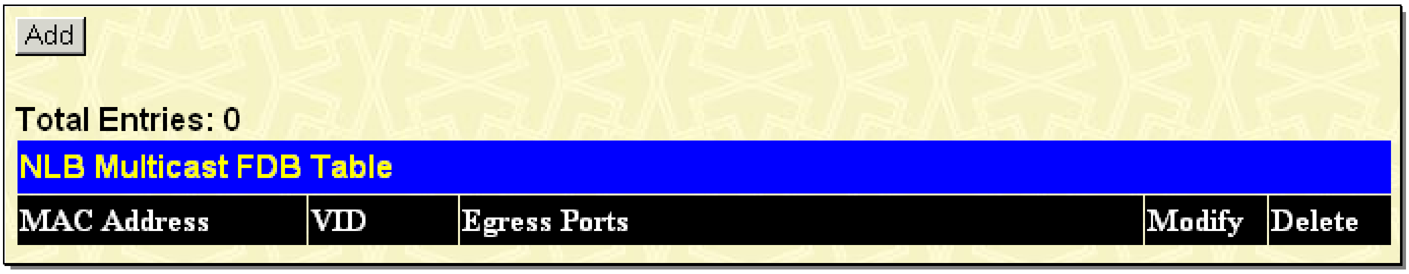
Parameter	Description
Unit	Select the unit to configure.
From/To	Select a range of ports.
Admin State	Enable or disable the administration state. This indicates these ports unidirectional link detection status. The default state is *Disabled*.
Mode	Toggle between *Shutdown* and *Normal*. When *Shutdown* is selected, if any unidirectional link is detected, this feature will disable the port and log an event. When *Normal* is selected, this feature will only log an event when a unidirectional link is detected.
Discovery Time (5-65535 sec)	Enter the port neighbor discovery time between *5* and *65535* seconds. If the discovery is timed out, the unidirectional link detection will start. The default discovery time is *5* seconds

Click **Apply** to create a new entry.

NLB Multicast FDB Settings

The Switch supports Network Load Balancing (NLB). This is a MAC forwarding control for supporting the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. The server can work in two different modes – unicast mode and multicast mode. In unicast mode, the client uses a unicast MAC address as the destination MAC to reach the server. In multicast mode, the client uses a multicast MAC address as the destination MAC to reach the server. The destination MAC is the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.The NLB multicast FDB entry will be mutually exclusive with the L2 multicast entry. At the current time, only multicase mode is supported.

To view this window, click **L2 Features > NLB Multicast FDB Settings**, as shown below:



Total Entries: 0

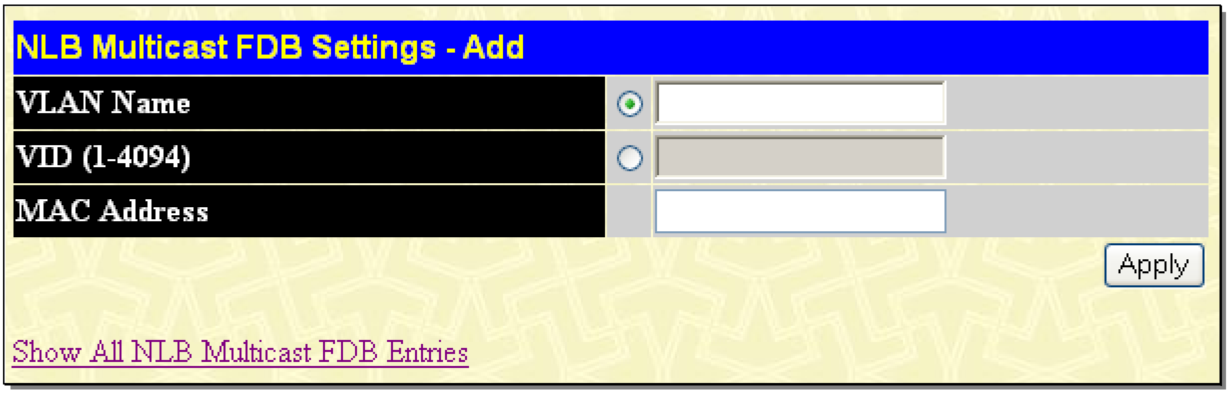
NLB Multicast FDB Table

MAC Address	VID	Egress Ports	Modify	Delete

Figure 3- 80. NLB Multicast FDB Table window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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



NLB Multicast FDB Settings - Add

VLAN Name	●	
VID (1-4094)	○	
MAC Address		

Figure 3- 81. NLB Multicast FDB Settings - Add window

The following fields can be set:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN of the NLB multicast FDB entry to be created.
VID (1-4094)	Click the radio button and enter the VLAN by the VLAN ID.
MAC Address	Enter the MAC address of the NLB multicast FDB entry to be created.

Click **Apply** to create a new entry. To view the NLB Multicast FDB Table, click the hyperlinked Show All NLB Multicast FDB Entries.

Section 4

L3 Features

The following section will aid the user in configuring security functions for the Switch.

The Switch has the capability to support the following:

- IPv6 unicast, multicast and anycast addresses
- Allow for IPv6 packet forwarding
- IPv6 fragmentation and re-assembly
- Processing of IPv6 packet and extension headers
- Static IPv6 route configuration
- IPv6 Neighbor Discovery
- Link-Layer Address resolution, Neighbor Unreachability Detection and Duplicate Address Detection over broadcast mediums (ex: Ethernet)
- Send Router Advertisement
- ICMPv6 functionality

The following sections will briefly explain IPv6, its functionality and how IPv6 is implemented on this Switch.

Overview

IP version 6 is the logical successor to IP version 4. It was known that IPv4 could not support the amount of addresses that would eventually be needed for not only each person, but each device that would require an IP address, and therefore a system with a larger pool of IP addresses was required. IPv6 has addressed that issue, along with other issues that enhance routing over the network, provide better security and improve Quality of Service for Internet users. Some of the improvements made were:

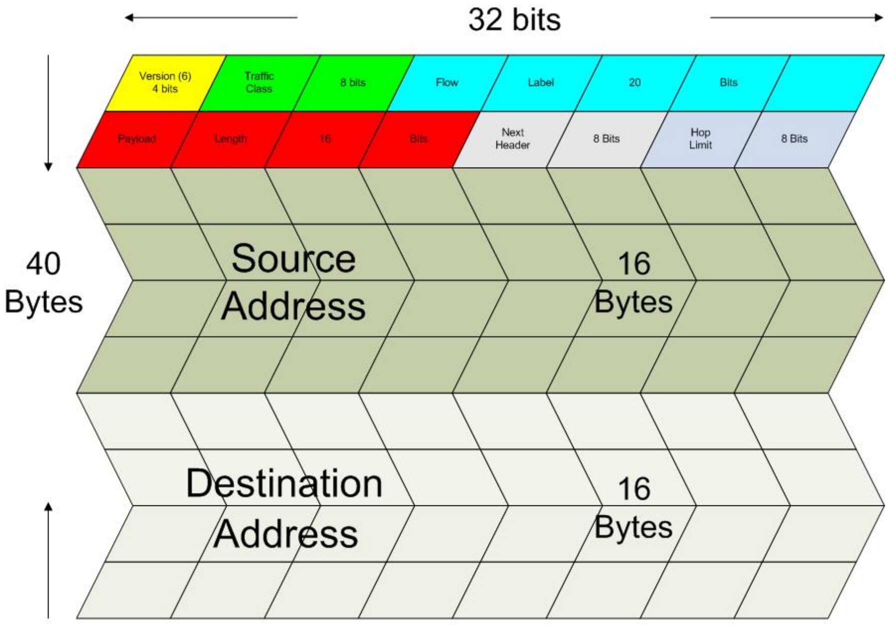
- **Expanding the Capabilites for IP Addressing** – IPv6 has increased the size of the IP address from 32 bits to 128 bits. As a result, the addressing hierarchy has been greatly expanded, more nodes now have the capability of having a unique IP address and the method of assigning an IP address to an interface has become cleaner and quicker. Unicast and multicast addresses still exist but in a purer form and multicast addresses now have a scope field that increases the scalability of multicast routing. Also, an anycast address has been added, which will send packets to the closest node that is a part of a group of nodes, thereby eliminating a specified device for a particular group.
- **Simplifying the Packet Header** – The IPv6 packet header has been simplified from IPv4 as some headers have been modified or dropped altogether, which improves processing speed and cost. The IPv6 header now has a fixed length of 40 bytes consisting of an 8-byte header and two 16-byte IP addresses (source and destination).
- **Extensions and Options Enhan**cement – Packet header option fields encoding has been enhanced to allow for proficient forwarding of packets due to lesser restrictions on packet option length and encoding method. This enhancement will also allow new option fields to be integrated into the IPv6 system without hassles and limitations. These optional headers are placed between the header and the payload of a packet, if they are necessary at all.
- **Authentication and Privacy Extension Support** – New authentication capabilities use extensions for data integrity and data confidentiality for IPv6.
- **Flow Labeling** – This new capability allows packets to be streamlined into certain traffic “flows” if labeled by the sender. In this way, services such as “real time services or non-default quality of service can receive special attention for improved flow quality.

Packet Format

As in IPv4, the IPv6 packet consists of the packet header and the payload, but the difference occurs in the packet header that has been amended and improved for better packet flow and processing. The following will outline and detail the IPv6 enhancements and parts of the IPv6 packet, with special attention to the packet header.

IPv6 Header

The IPv6 packet header has been modified and simplified from IPv4. The header length, identification, flags, fragment offset and header checksum have all been removed in the IPv6 header due to lack of necessity or improvement to a better function of the header. The minimum header length is now 20 bytes but may be increased to as much as 60 bytes, using 4-byte increment extensions. The following picture is an example of an IPv6 packet header.



Standard IPv6 Packet Header

Eight fields make up the basic IPv6 packet header:

1. **Version** – This 4-bit field defines the packet version, which is IPv6 and is defined as the number 6.
2. **Traffic Class** – This 1-byte field replaces the Type of Service field used in IPv4 and is used to process real-time data and other data requiring special packet management. This field defines the Class of Service priority of an IPv6 packet.
3. **Flow Label** – This 20-bit field is used to facilitate the handling of real-time traffic. Hosts sending data can place a flow label into this field to identify a sequence of packets that have an identical set of options. In this way, router can process these packets more efficiently once the flow class has been identified and the rest of the packet header no longer needs to be fully processed, just the flow label and the source address. All flow label packets must have identical source and destination addresses.
4. **Payload Length** – Known as the datagram length in IPv4, this 16-bit field specifies the length of the IPv6 data carried after the header of the packet. Extension headers are considered part of the payload and are included in the length specified here.
5. **Next Header** – This 8-bit field is used to identify the header immediately following the IPv6 header. When this field is set after the hop by-hop header, it defines the extension header that will appear after the destination address. Each extension header must be preceded by a Next Header field. Integers used to define extension headers in the next Header field use the same values as IPv4 (ex: 6=TCP, 17=UDP, etc.).
6. **Hop Limit** - Similar to the TTL field in IPv4, this 8-bit field defines the number of hops remaining after the packet has been processed by a node, instead of the number of seconds left to live as on an IPv4 network. This field will decrement by one after every node it passes and the packet will be discarded once this field reaches zero.
7. **Source Address** – This 16-byte field defines the IPv6 address of the source node sending the packet.
8. **Destination Address** – This 16-byte field defines the IPv6 address of the destination node receiving the packet. This may or may not be the final destination node of this packet, depending on the routing header, if present.

Extension Headers

Extension headers are used to identify optional parameters regarding IPv6 packets such as routing, fragmentation of packets or authentication parameters. The types of extension headers supported are Hop-by-Hop, Routing, Fragment, Destination Options, Authentication and Encapsulating Security Payload. These extension headers are placed between the IPv6 packet header and the payload and are linked together by the aforementioned Next Header, as shown below:

IPv6 header **Next Header = TCP**	**TCP header + data**

IPv6 header **Next Header = Routing**	**Routing Header** **Next Header = TCP**	**TCP header + data**

IPv6 header **Next Header = Destination Options**	**Destination Options Header** **Next Header = Routing**	**Routing Header** **Next Header = TCP**	**TCP header + data**

Each header has a specific place in the header chain and must follow the following order:

- IPv6 Header
- Hop-By-Hop Header (Must follow the IPv6 header)
- Destination Options
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulating Security Payload Header
- Destination Options Header
- Upper Layer Header

There may be zero, one or more extension headers in the IPv6 header, they must be processed in order and they are to be in increments of 8 octets in the IPv6 packet. Nodes that do not recognize the field of the extension header will discard the packet and send a relevant ICMPv6 message back to the source.

Packet Fragmentation

At times, packets are sent out to a destination that exceed the size of the Path MTU, so the source node is required to split these packets into fragments in individual packets which will be rebuilt when it reaches its final destination. Each of the packets that will be fragmented is given an Identification value, by the source node. It is essential that each of these Identification values is different than any other fragmented packet recently sent that include the same source and destination address. The original packet is divided into two parts, a fragmentable part and an unfragmentable part. The unfragemntable part of the packet consists of the IPv6 header and any extension headers present, up to the routing extension header. The fragmentable part has the payload plus any extension headers that must be processed by the final destination node. This part will be divided into multiple packets that are of a size that can be accepted by the Path MTU. The IPv6 header is then included with this fragmented part and sent to its destination. Once all parts of the fragmented packet reach its destination, they are reassembled using the Fragment Identification value, provided that the source and destination addresses are identical.

Address Format

To address the problem of finding a larger pool of IP addresses for IPv6, the size and format of the IPv4 format needed to be changed. Quadrupling the size of the address, from 32 bits to 128 bits, and encoding addresses using the hexadecimal form were used to solve the problem. In IPv4, the format of the address looked like xxx.xxx.xxx.xxx, where the x’s represent integers from 0-9 (ex. 136.145.225.121). Now in IPv6, the format of the address resembles xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where a set of xxxx represents a 16-bit hexadecimal value (ex. 2D83:0C76:3140:0000:0000:020C:417A:3214). Although this address looks long and cumbersome, there are some compression rules that will shorten the format of the IPv6 address to make it more compatible to the user.

One such compression rule that is used is to remove leading zeros from any 16-bit hexadecimal value. This is only for zeros that begin the value, not for zeros within the value or ones that are ending the value. Therefore, if we take the previous example IPv6 address and use the compression rules, our IPv6 address would look like this:

2D83:0C76:3140:**0000:0000:020C**:417A:3214 → 2D83:C76:3140:**0:0:20C**:417A:3214

The second compression method is to change a string of zero bits into two colons. At times, there may be strings of empty values in the IPv6 address that are unused for this address, but are necessary for the format of other IPv6 addresses with alternate purposes. To compress these zero strings, the format "::" is used to represent multiple zero fields in the address. This double colon can only be used once in the IPv6 address because when a computer finds a colon, it will expand this field with as many zeros as is necessary to reach the 128-bit address size. If two strings of zeros are present, separated by another non-zero field, a zero must be used to represent one of the two zero fields. So, if we reduce our example using this compression, it would look like this:

2D83:0C76:3140**:0000:0000:020C:**417A:3214 → 2D83:C76:3140**:0:0:20C:**417A:3214 →2D83:C76:3140**::20C:**417A:3214

When IPv4 and IPv6 nodes are mixed in a network, the IPv6 notation overcomes the difficulty of using an IPv4 address by converting it to the IPv6 format using zeros at the beginning of the IPv4 address. For example, an IP address of 192.168.1.1 is represented in IPv6 format x:x:x:x:d.d.d.d where the x's are a string of zeros and the d's represent the normal IPv4 address. (ex. 0:0:0:0:192.168.1.1 or condensed ::192.168.1.1 or hex form ::C0A8:1:1).

Types

IPv6 addresses are classified into three main categories, unicast, multicast and anycast.

Unicast – This address represents a single interface on an IPv6 node. Any packet with a unicast address as its destination address will only be sent to that specific node. Two types of unicast addresses are mainly used for IPv6.

- *Link-Local* – Defined by the IPv6 address prefix FE80::/10, link-local addresses allow for communication to occur between devices on a local link. These addresses are used in neighbor discovery and stateless autoconfiguration.
- *Global Aggregateable* - Defined using a global routing prefix in the range of 2000::/3 to E000::/3, global addresses are aggregated using these routing prefixes to produce unique IPv6 addresses, which will limit global routing table entries. The MAC address of the device is used to produce this address in this form:

  Global Unicast Address: **global prefix + interface identifier** (the interface indentifier is based on IEEE EUI-64: **xxxxxxux xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx**, this is the 48 bit MAC address format, thereinto, u bit is universal/local bit, we need to change the u bit to 1, and then insert the "FFFE") between the (first 3 bytes) of the MAC address and the (last 3 bytes) of the MAC address.

  For example, **00-0C-6E-6B-EB-0C >>> 00000000-0C-6E-6B-EB-0C >>> 00000010-0C-6E-6B-EB-0C >>> 02-0C-6E-6B-EB-0C >>> 020C:6EFF:FE6B:EB0C**, this is the 64 bits interface ID. When received the prefix will be **2000::/3**, so the ipv6 address will be **2000::20C:6EFF:FE6B:EB0C**

Multicast – Like IPv4, multicast addresses are used to send packets to multiple destinations on a network. These interfaces must be a part of the multicast group. IPv6 multicast prefixes begin with the prefix FF00::/8. FF represents the binary 1111 1111 which identifies a multicast address. The first zero, which is a 4-bit integer, represents the lifetime of the packet. An entry of zero in this field represents a permanent multicast address and an entry of one represents a temporary multicast address. The second zero, which is also a 4-bit integer, defines the scope of the multicast address. This scope defines to what places the multicast address is valid. For example, a value of 1 defines the node, 2 defines the link, 5 defines a site, 8 defines a organization and so on. Not all integers are in use for the scope field. An example of this would be FF02 where the 2 represents a multicast packet going to all the nodes on a local link.

Anycast – The anycast address will send messages to the nearest node of a particular group. This address is assigned to multiple interfaces in the group but only the node with the closest proximity will receive the message. These anycast addresses are allocated from the unicast address space and therefore have no real defined prefix to distinguish it from other IPv6 addresses. The main purpose of the anycast address is to identify a set of routers owned by an organization providing Internet service. It could also be used to identify a set of routers connected to a particular subnet or permitting entrance to a specific routing domain.

Two other special types of addresses exist in IPv6. The **unspecified address** has a value of 0:0:0:0:0:0:0:0 which is comparable to the 0.0.0.0 address in IPv4. This address is used to indicate the lack of a valid IP address on a node and may be used by a device when booting and requesting address configuration notification. In its IPv6 condensed form, it appears as "**::**" and should not be statically or dynamically assigned to an interface, nor should it be the destination address of an IPv6 packet, or located within the routing header.

The second type of special address is the **loopback address** which is represented by 0:0:0:0:0:0:0:1, or ::1 in its compressed form. It is akin to the 127.0.0.1 address in IPv4 and is used in troubleshooting and testing IP stacks. This address, like the unspecified address, and should not be statically or dynamically assigned to an interface.

ICMPv6

Network professionals are already very familiar with ICMP for IPv4, which is an essential tool in the IPv4 network, relaying messages about network problems and the general condition of the network. ICMPv6 is the successor to the IPv4 version and performs many of the same basic functions as its precursor, yet is not compatible with ICMPv4. ICMPv6 has made improvements over its forerunner, with such enhancements as managing multicast group memberships and allowing for neighbor discovery by resolving link-layer addresses attached to the same link and identifying changes in those addresses. ICMP can also discover routers, determine which neighbors can be reached and map IP addresses to MAC addresses within the network. ICMPv6 is a vital part of the IPv6 network and must be implemented on every IPv6 node for operations to function normally.

Two kinds of ICMP messages are apparent on the IPv6 network:

Error Messages – ICMP error messages are sent out on the network when packet sizes exceed the path MTU (Maximum Transfer Unit), when the hop count of the IPv6 packet has been surpassed, when messages cannot reach their intended destination and when there are parameter problems within the IPv6 packet.

Informational Messages – ICMP informational messages send out packets describing current network information valuable to devices on the network. A common and useful ICMPv6 informational message is the ping program use to discover the availability a device, by using a ping request and reply format. Other informational messages include Path MTU discovery that is used to determine the maximum size of data packets that can be allowed to be transferred, and Neighbor Discovery messages which discover routers that can forward packets on the network. Neighbor discovery will be discussed in greater detail later in the next section.

Neighbor Discovery

Neighbor discovery is a new feature incorporated in IPv6. In IPv4, no means were available to tell if a neighbor could be reached. Now, combining ICMP messages and ARP, neighbors can be detected and their layer 2 addresses (MAC Address) can be identified. This feature can also discover neighboring routers that can forward packets and keep track of the reachability of routers, as well as if changes occur within link-layer addresses of nodes on the network or identical unicast addresses are present on the local link.

The functionality of the Neighbor Discovery feature is based on ICMPv6 packets, Neighbor Solicitation and Router Advertisement messages circulating on the network. When a node wishes to determine link layer addresses of other nodes on the same link, it produces a Neighbor Solicitation message to be circulated on the local link. When received by a neighbor, this neighbor will produce Router Advertisements immediately to be returned. These Router Advertisements will contain a multicast address as the destination address and have an ICMP type of 134 (the specified number for Router Advertisements), as well as having the link-layer address of the node sending the advertisement. Router Advertisement messages may be periodic, specified in the advertisement by having the all-nodes multicast address FF02::1, or sent out as a result of receiving a Neighbor Solicitation message, specified in the advertisement by having the address of the interface that first sent the solicitation message. Once confirmation of the Neighbor has been reached, packets can now be exchanged on the link.

Neighbor Unreachability Detection

At times on the network, problems occur in reaching the Neighbor node or getting a response from the Neighbor. A neighbor is considered reachable when it has received and processed packets sent to it, and in return sends a packet back notifying a affirmative response. This response may come in the form of an indication from an upper-layer protocol, like TCP, noting that progress is being made, or in response from a Neighbor Solicitation message in the form of a Router Advertisement message. If responses are not received from the node, it is considered unreachable and a Destination Unreachable message is received in the form of an ICMP packet. This Destination Unreachable ICMP packet will contain the reason for the fault, located in the code field of the ICMP header. Five possible reasons for the failure can be stated:

1. There is no route or destination (Code 0).
2. Communication has been administratively prohibited, such as a firewall or filter (Code 1)
3. Beyond the scope of the source address, when the multicast scope of the source address is smaller than the scope of the destination address (Code 2)
4. The address is unreachable (Code 3)
5. The port is unreachable (Code 4)

Duplicate Address Detection (DAD)

DAD messages are used to specify that there is more than one node on a local link possessing the same IP address. IPv6 addresses are only leased for a defined period of time. When that time expires, the address will become invalid and another address must be addressed to the node. To ensure that this new address is unique on the local link, a node runs a DAD process to determine the uniqueness of the new address. This is done through the use of a Neighbor Solicitation message containing a Tentative address. This message will detect if another node on the local link has this Tentative address. If the Tentative address is found on another node, that node will send out a Neighbor Advertisement message, the process will be terminated, and manual configuration will be necessary. If no answer is forthcoming regarding this Neighbor Solicitation message containing the tentative address, the address is allotted to the node and connectivity is established.

Assigning IP Addresses

For IPv4 addresses, users may only assign one address per interface and only one address may be used on a particular VLAN. Yet, IPv6 addresses are different. All IPv6 interfaces on the switch must have at least one IPv6 link-local unicast address, if the user is employing the IPv6 addressing scheme. Multiple IPv6 addresses may be configured for IPv6 interfaces, regardless of type, whether it is unicast, multicast or anycast. The scope of the address has some bearing on the assigning multiple addresses to a single interface as well. If multiple physical interfaces are considered as one interface on the Internet layer, multiple unicast addresses may be allotted to multiple physical interfaces, which would be beneficial for load sharing on these interfaces. This is dependent on these unicast addresses having a scope smaller than the link-local address, if these unicast addresses are not the source or destination address for IPv6 packets to or from address that are not IPv6 neighbors of the interface in question.

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 256 interfaces per VLAN (one primary, and up to 255 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.

Interface Settings

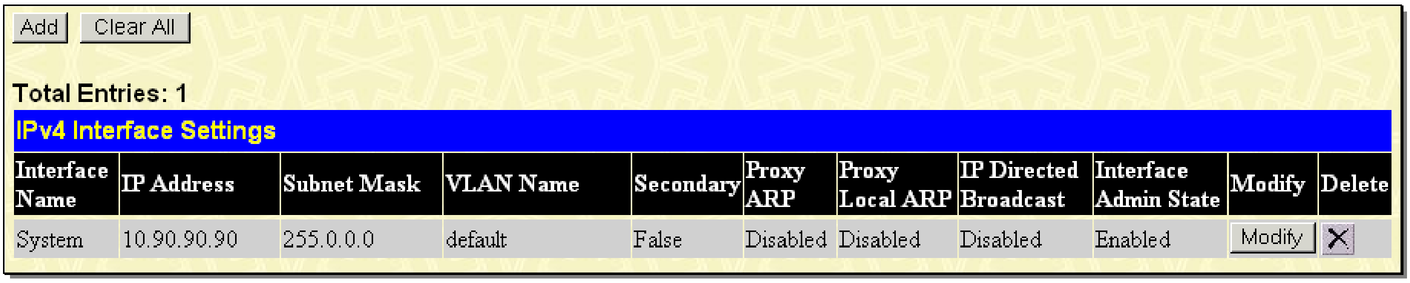
The IP Address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the introduction of the ***DGS-3600 Series CLI Reference Guide*** or return to Section 4 of this manual for more information. To change IP settings using the Web manager users must access the **IP Address** window located in the **Administration** folder.

The Web manager contains two folders for which to set up IP interfaces on the switch, one for IPv4 addresses, named **IPv4 Interfaces Settings**, and one for IPv6 addresses, named **IPv6 Interfaces Settings**.

NOTE: After properly configuring an IP interface on the Switch, each VLAN can be routed without any additional steps.

IPv4 Interfaces Settings

To view this window, click **L3 Features** > **Interface Settings > IPv4 Interfaces Settings**, as shown below:



Total Entries: 1

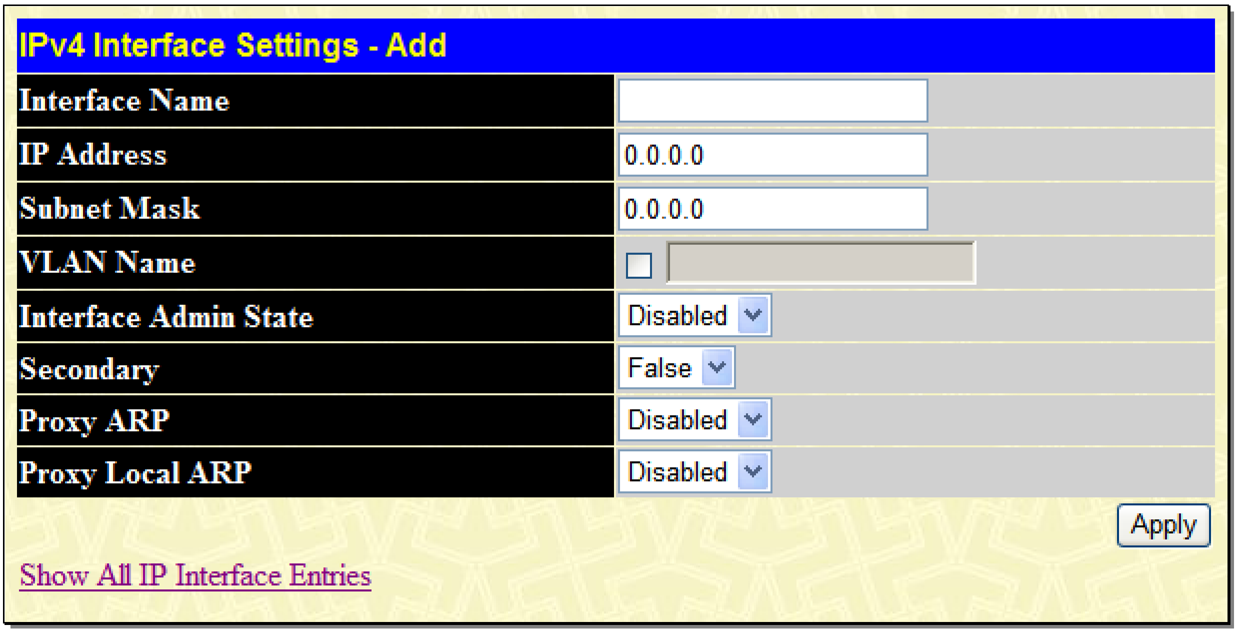
IPv4 Interface Settings

Interface Name	IP Address	Subnet Mask	VLAN Name	Secondary	Proxy ARP	Proxy Local ARP	IP Directed Broadcast	Interface Admin State	Modify	Delete
System	10.90.90.90	255.0.0.0	default	False	Disabled	Disabled	Disabled	Enabled	Modify	☒

Figure 4- 1. IPv4 Interface Settings window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To manually assign the Switch's IPv4 address and its related configurations, click the **Add** button, revealing the following window to configure:

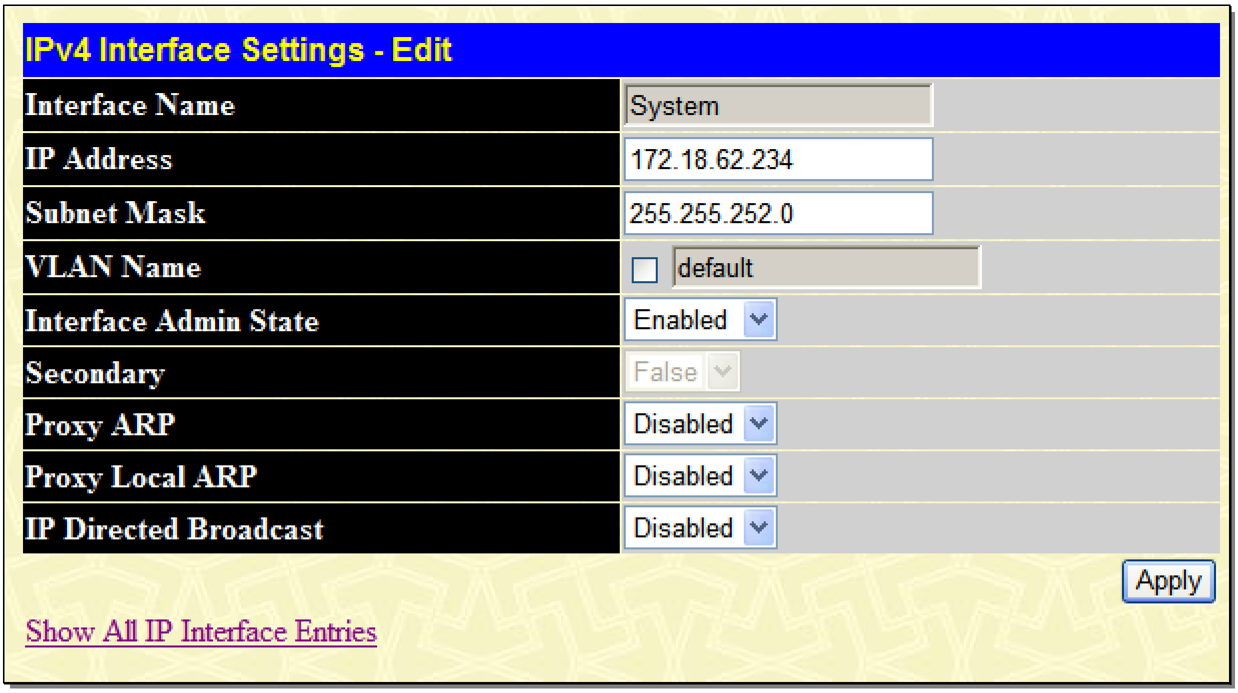


IPv4 Interface Settings - Add

Interface Name	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
VLAN Name	□
Interface Admin State	Disabled
Secondary	False
Proxy ARP	Disabled
Proxy Local ARP	Disabled

Figure 4- 2. IPv4 Interface Settings – Add window

To modify an existing Interface, click that interface’s **Modify** button, which will produce this window:



IPv4 Interface Settings - Edit

Interface Name	System
IP Address	172.18.62.234
Subnet Mask	255.255.252.0
VLAN Name	□ default
Interface Admin State	Enabled
Secondary	False
Proxy ARP	Disabled
Proxy Local ARP	Disabled
IP Directed Broadcast	Disabled

Figure 4- 3. IPv4 Interface Settings – Edit window

Enter a name for the new interface to be added in the Interface Name field (if 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 Interface Admin State pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. To view entries in the **IPv4 Interface Settings** window, click the Show All IP Interface Entries hyperlink. Use the **Save Changes** window to enter the changes into NV-RAM.

The following fields can be set or modified:

Parameter	Description
Interface Name	This field displays the name for the IP interface or is used to add a new interface to be created by the user. The default IP interface is named "System".
IP Address	This field allows the entry of an IPv4 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 states the VLAN Name directly associated with this interface.
Interface Admin. State	Use the pull-down menu to enable or disable configuration on this interface.
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.
Proxy ARP	Use the pull-down menu to *Enable* or *Disable* the proxy ARP state on the IP interface.
Proxy Local ARP	Use the pull-down menu to *Enable* or *Disable* the proxy local ARP. This function allows the Switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.
IP Directed Broadcast	Use the pull-down menu to enable or disable the IP directed broadcast on a specified interface. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address of some IP subnet, but which originates from a node that is not a part of that destination subnet. The switch that is not directly connected to its destination subnet and forwards an IP directed broadcast in the same way that it would forward unicast IP packets to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, and that packet is "exploded" as a broadcast on the destination subnet. This only works on layer 3 switches.

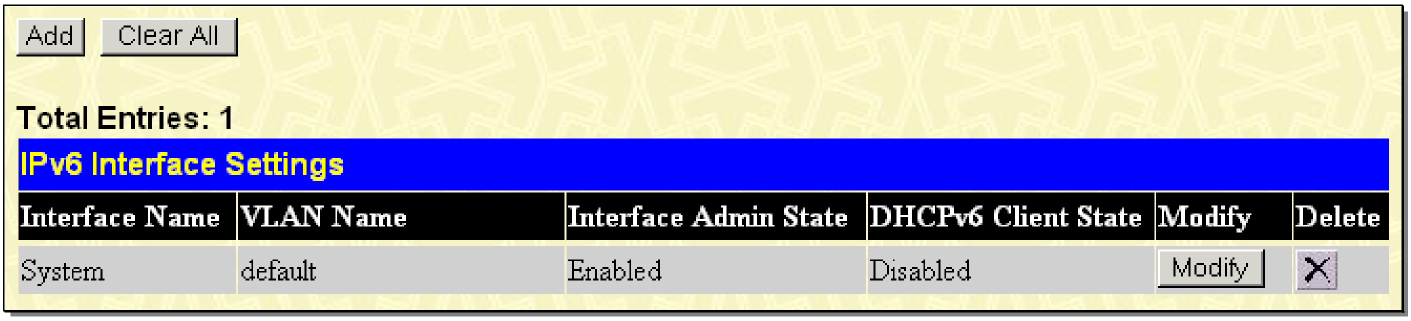
Click **Apply** to implement changes made.

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.

IPv6 Interface Settings

The following window is used to setup IPv6 interfaces and addresses for the switch.

To view this window, click **L3 Features** > **Interface Settings > IPv6 Interfaces Settings**, as shown below:



Total Entries: 1

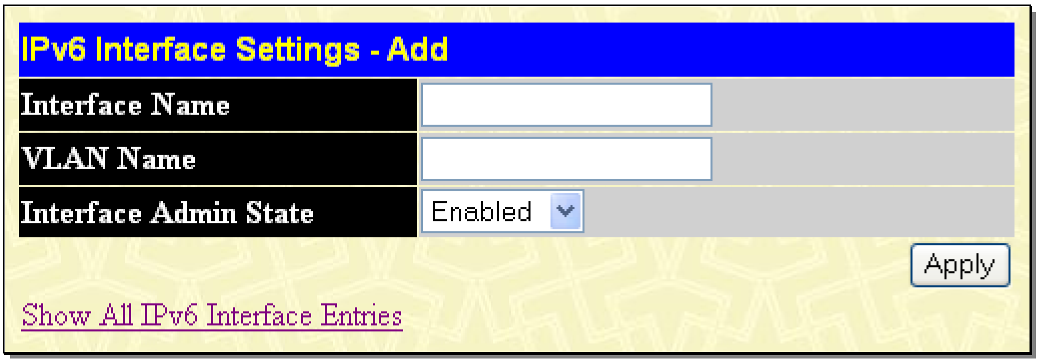
IPv6 Interface Settings

Interface Name	VLAN Name	Interface Admin State	DHCPv6 Client State	Modify	Delete
System	default	Enabled	Disabled	Modify	☒

Figure 4- 4. IPv6 Interface Settings window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To add a new IPv6 interface, click the **Add** button, which will display the following window.



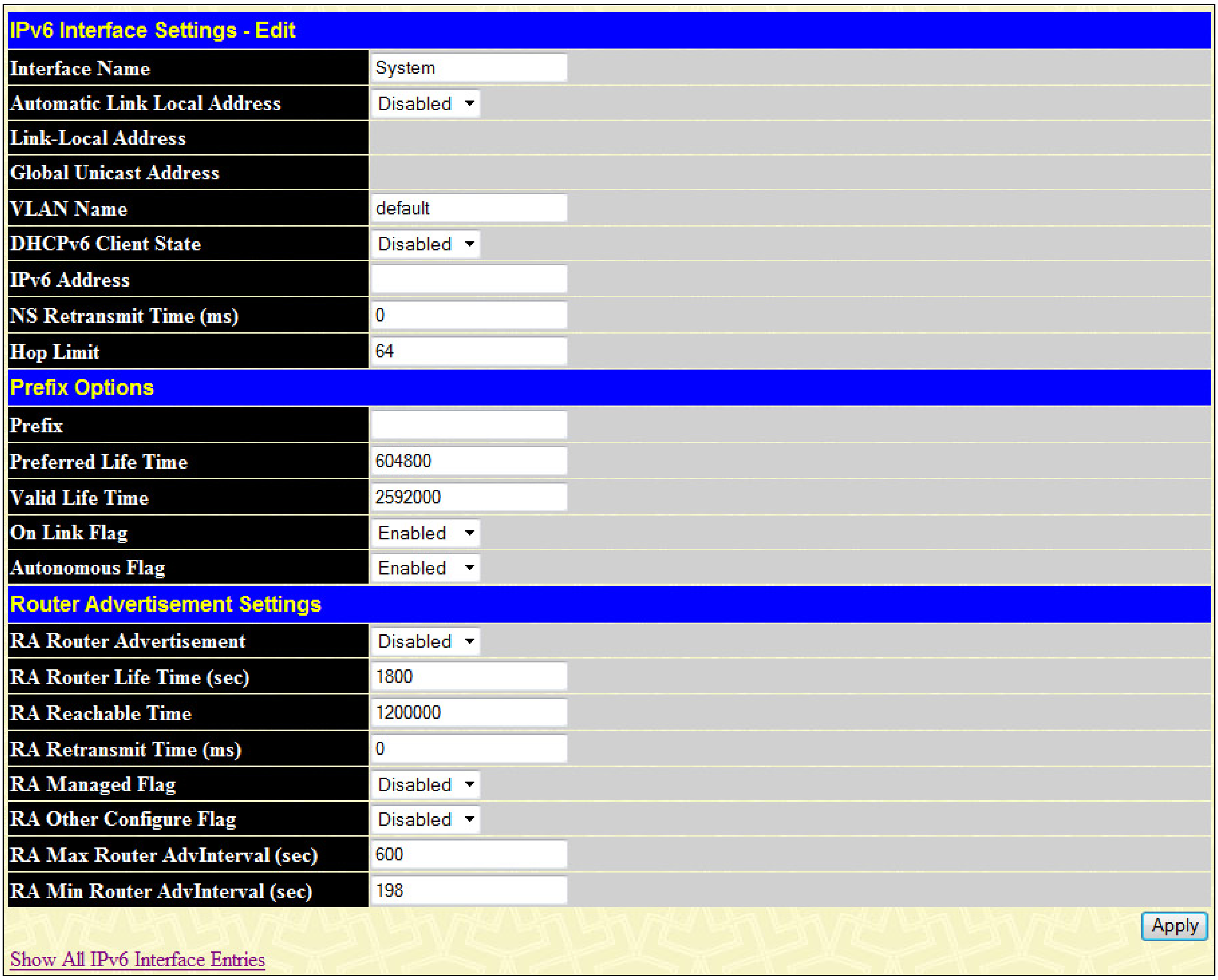
IPv6 Interface Settings - Add

Interface Name	
VLAN Name	
Interface Admin State	Enabled

Figure 4- 5. IPv6 Interface Settings – Add window

To add an Interface, enter an Interface Name in the field provided, along with a corresponding VLAN Name, set the Interface Admin. State to *Enabled* and click **Apply**. Newly created interfaces will appear in the **IPv6 Interface Settings** window.

To change the settings for a configured Interface, click the corresponding **Modify** button, which will display the following window for the user to configure.



IPv6 Interface Settings - Edit

Interface Name	System
Automatic Link Local Address	Disabled
Link-Local Address	
Global Unicast Address	
VLAN Name	default
DHCPv6 Client State	Disabled
IPv6 Address	
NS Retransmit Time (ms)	0
Hop Limit	64

Prefix Options

Prefix	
Preferred Life Time	604800
Valid Life Time	2592000
On Link Flag	Enabled
Autonomous Flag	Enabled

Router Advertisement Settings

RA Router Advertisement	Disabled
RA Router Life Time (sec)	1800
RA Reachable Time	1200000
RA Retransmit Time (ms)	0
RA Managed Flag	Disabled
RA Other Configure Flag	Disabled
RA Max Router AdvInterval (sec)	600
RA Min Router AdvInterval (sec)	198

Figure 4- 6. IPv6 Interface Settings – Edit window

The following fields may be viewed or modified. Click **Apply** to set changes made.

Parameter	Description
Interface Name	This field displays the name for the IP interface or is used to add a new interface or change an existing interface name.
Automatic Link Local Address	Use this pull-down menu to enable or disable this feature. When enabled, the switch will automatically create an IPv6 link-local address for the switch. Once the user enables this feature and clicks **Apply**, an IPv6 address will be produced based on the MAC address of the switch and the new entry will appear in the following Link-Local Address field.
Link-local Address	This field displays the IPv6 address created automatically by the Switch, based on the MAC Address of the Switch. This is a site local address used only for local routing.
Global Unicast Address	This field is the unicast address that will be used by the Switch for packets coming from outside the site-local address, or the public IPv6 address, when connected directly to the Internet.
VLAN Name	This field states the VLAN Name directly associated with this interface and may be modified by entering a new pre-configured VLAN Name.
DHCPv6 Client State	Use the pull-down menu to enable or disable configuration on this interface.
IPv6 Address	Use this field to set a Global Unicast Address for the Switch. This address will be used to access the network outside of the local link.
NS Retransmit Time	Use this field to set the interval, in seconds that this Switch will produce Neighbor

(ms)	Solicitation packets to be sent out over the local network. This is used to discover IPv6 neighbors on the local link. The user may select a time between *0* and *65535* milliseconds. Very fast intervals, represented by a low number, are not recommended for this field.
Hop Limit	This field sets the number of nodes that this Router Advertisement packet will pass before being dropped. This number is set to depreciate by one after every node it reaches and will be dropped once the Hop Limit reaches 0. The user may set the Hop Limit between *0* and *255*. The default value is *64*.
Prefix Options	
Prefix	Use this field to set a prefix for Global Unicast IPv6 addresses to be assigned to other nodes on the link-local network. This prefix is carried in the Router Advertisement message to be shared on the link-local network. The user must first have a Global Unicast Address set for the Switch.
Preferred Life Time	This field states the time that this prefix is advertised as being preferred on the link local network, when using stateless address configuration. The user may configure a time between *0* and *4294967295* milliseconds, with a default setting of *604800* milliseconds.
Valid Life Time	This field states the time that this prefix is advertised as valid on the link local network, when using stateless address configuration. The user may configure a time between *0* and *4294967295* milliseconds, a default setting of *2592000* milliseconds.
On Link Flag	Setting this field to *Enabled* will denote, within the IPv6 packet, that the IPv6 prefix configured here is assigned to this link-local network. Once traffic has been successfully sent to these nodes with this specific IPv6 prefix, the nodes will be considered reachable on the link-local network.
Autonomous Flag	Setting this field to *Enabled* will denote that this prefix may be used to autoconfigure IPv6 addresses on the link-local network.
Router Advertisement Settings	
RA Router Advertisement	Use this pull-down menu to enable or disable the switch as being capable of accepting solicitation from a neighbor, and thus becoming an IPv6 neighbor. Once enabled, this Switch is now capable of producing Router Advertisement messages to be returned to querying neighbors.
RA Router Life Time (sec)	This time represents the validity of this interface to be the default router for the link-local network. A value of 0 represents that this Switch should not be recognized as the default router for this link-local network. The user may set a time between *0* and *9000* seconds. The default setting is *1800* seconds.
RA Reachable Time	This field will set the time that remote IPv6 nodes are considered reachable. In essence, this is the Neighbor Unreachability Detection field once confirmation of the access to this node has been made. The user may set a time between *0* and *3600000* milliseconds. The default setting is *1200000* milliseconds. A very low value is not recommended.
RA Retransmit Time (ms)	Used to set an interval time between *0* and *4294967295* milliseconds for the dispatch of router advertisements by this interface over the link-local network, in response to a Neighbor Solicitation message. If this Switch is set as the default router for this local link, this value should not exceed the value stated in the Life Time field previously mentioned. Setting this field to zero will specify that this switch will not specify the Retransmit Time for the link-local network. (and therefore will be specified by another router on the link-local network. The default value is *0* milliseconds.
RA Managed Flag	Use the pull-down menu to enable or disable the Managed flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get both Global and link-local IPv6 addresses for the Switch. The default setting is *Disabled*.
RA Other Configure Flag	Use the pull-down menu to enable or disable the Other Configure flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get configuration information that is not address information, yet is important to the IPv6 settings of the Switch. The default setting is *Disabled*.

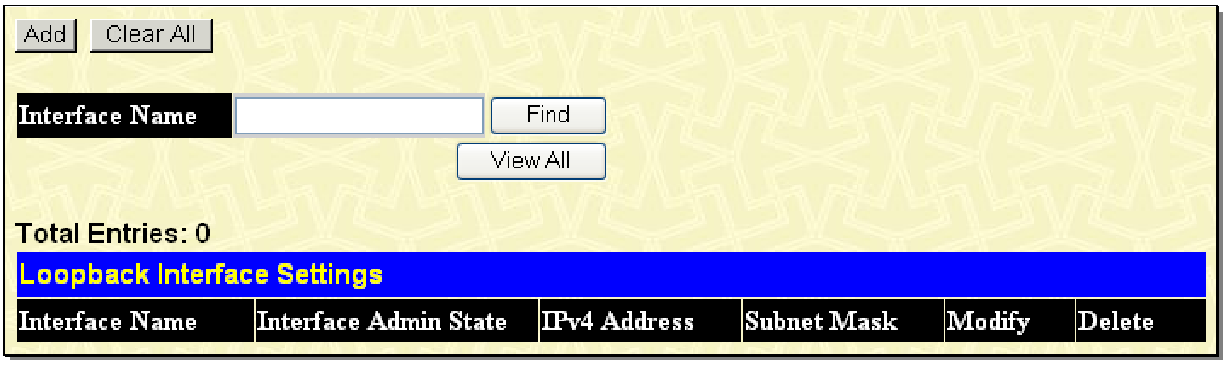
RA Max Router AdvInterval (sec)	Used to set the maximum interval time between the dispatches of router advertisements by this interface over the link-local network. This entry must be no less than *4* seconds (4000 milliseconds) and no more than *1800* seconds. The user may configure a time between *4* and *1800* seconds. The default setting is *600* seconds.
RA Min Router AdvInterval (sec)	Used to set the minimum interval time between the dispatches of router advertisements by this interface over the link-local network. This entry must be no less then 3 seconds and no more than .75 (3/4) of the MaxRtrAdvInterval. The user may configure a time between *3* and *1350* seconds. The default setting is *198* seconds.

Click **Apply** to save changes made.

Loopback Interfaces Settings

This window is used to configure loopback interfaces. A loopback interface is a logical IP interface which is always active, until a user disables or deletes it. It is independent of the state of any physical interfaces.

To view this window, click **L3 Features** > **Interface Settings > Loopback Interfaces Settings**, as shown below:



Total Entries: 0

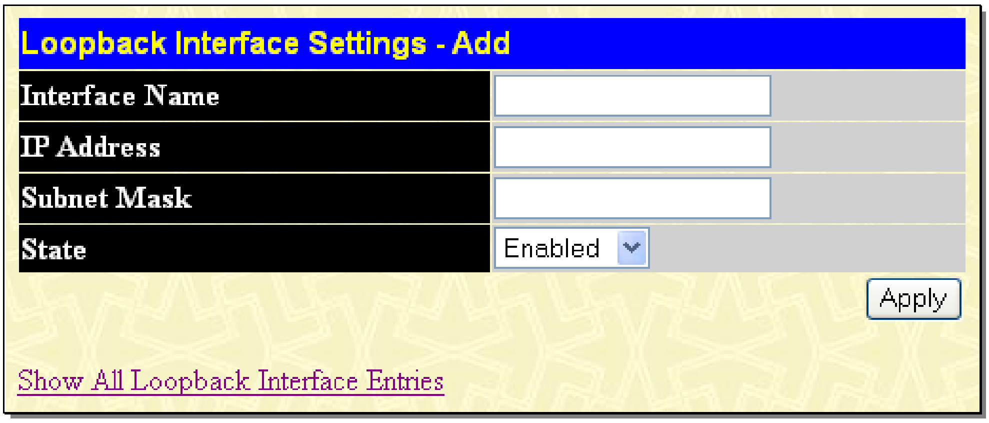
Loopback Interface Settings

Interface Name	Interface Admin State	IPv4 Address	Subnet Mask	Modify	Delete

Figure 4- 7. Loopback Interface Settings window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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



Loopback Interface Settings - Add

Interface Name	
IP Address	
Subnet Mask	
State	Enabled

Figure 4- 8. Loopback Interface Settings – Add window

The following fields can be set or modified:

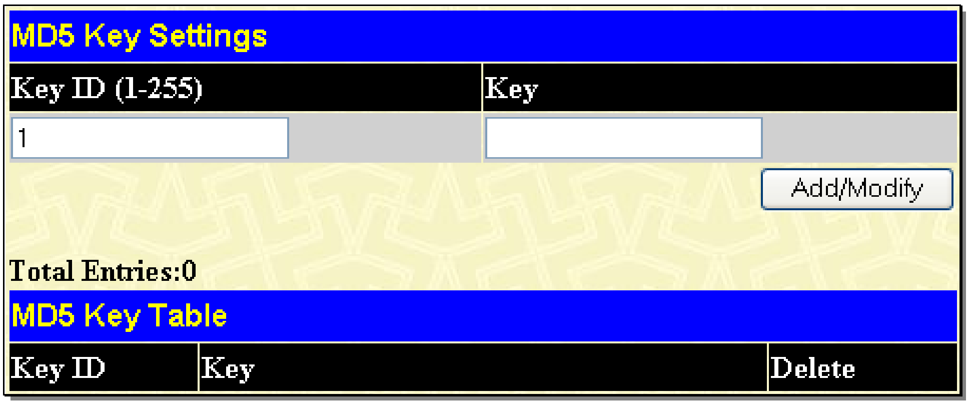
Parameter	Description
Interface Name	The name of the loopback interface. Note: The loopback ipif has the same name domain space with the regular ipif, so its name can’t be a duplicate with the regular ipif.
IP Address	Enter a 32-bit IPv4 address for the loopback interface.
Subnet Mask	This field allows the entry of a subnet mask to be applied to the loopback interface.
State	Use the pull-down menu to enable or disable the loopback interface.

Click **Apply** to implement changes made.

MD5 Key Settings

This window allows the entry of a 16-character Message Digest – version 5 (MD5) key that 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 windows below.

To configure an **MD5 Key**, click **L3 Features** > **MD5 Key Settings**, as shown below:



MD5 Key Settings

Key ID (1-255)	Key
1	

Total Entries:0

MD5 Key Table

Key ID	Key	Delete

Figure 4- 9. MD5 Key Settings 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	A 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.

Click **Add/Modify** to enter the new Key ID settings. To delete a Key ID entry, click the corresponding ☒ under the Delete heading.

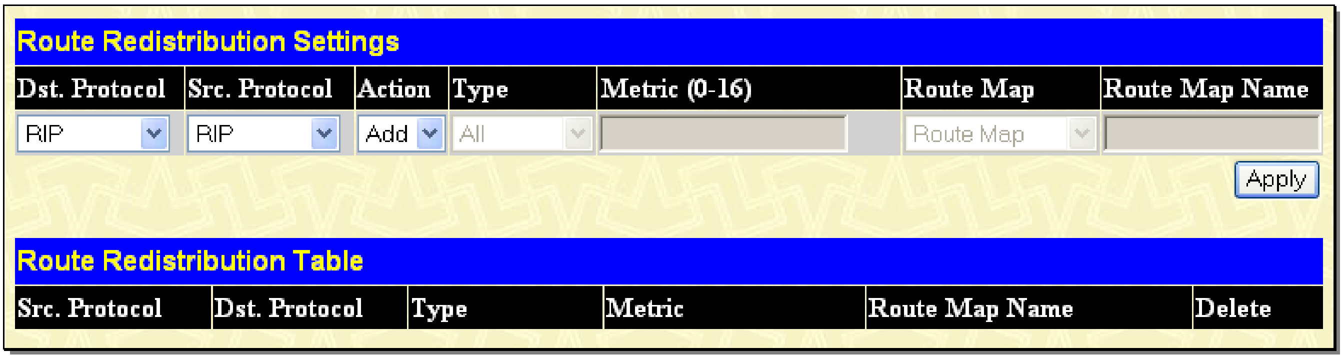
Route Redistribution Settings

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 among OSPF, RIP, and BGP routing protocols to all routers on the network that are running OSPF, RIP, and BGP. Routing information entered into the Static Routing Table on the local Switch is also redistributed.

Entering the metric 0 specifies transparency.

This window will redistribute routing information among the OSPF, RIP, and BGP routing protocols to all routers on the network that are running OSPF, RIP, and BGP.

To access the **Route Redistribution Settings** window, click **L3 Features** > **Route Redistribution Settings**, as shown below:



Route Redistribution Settings

Dst. Protocol	Src. Protocol	Action	Type	Metric (0-16)	Route Map	Route Map Name
RIP	RIP	Add	All		Route Map	

Route Redistribution Table

Src. Protocol	Dst. Protocol	Type	Metric	Route Map Name	Delete

Figure 4- 10. Route Redistribution Settings 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 among *RIP*, *OSPF*, and *BGP.*
Src. Protocol	Allows for the selection of the protocol for the source device. Choose between *RIP*, *OSPF, BGP*, *Static* and *Local*.
Action	Toggle the drop-down menu to *Add* or *Edit* the router redistribution setting being configured.
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-E2*.
Metric (0-16)	Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol. The user may specify a cost between *0* and *16*.
Route Map	Use the pull-down menu to add or delete a route map. Specify a route map, which will be used as the criteria to determine whether to redistribute specific routes.
Route Map Name	Enter the route map name to add or delete.

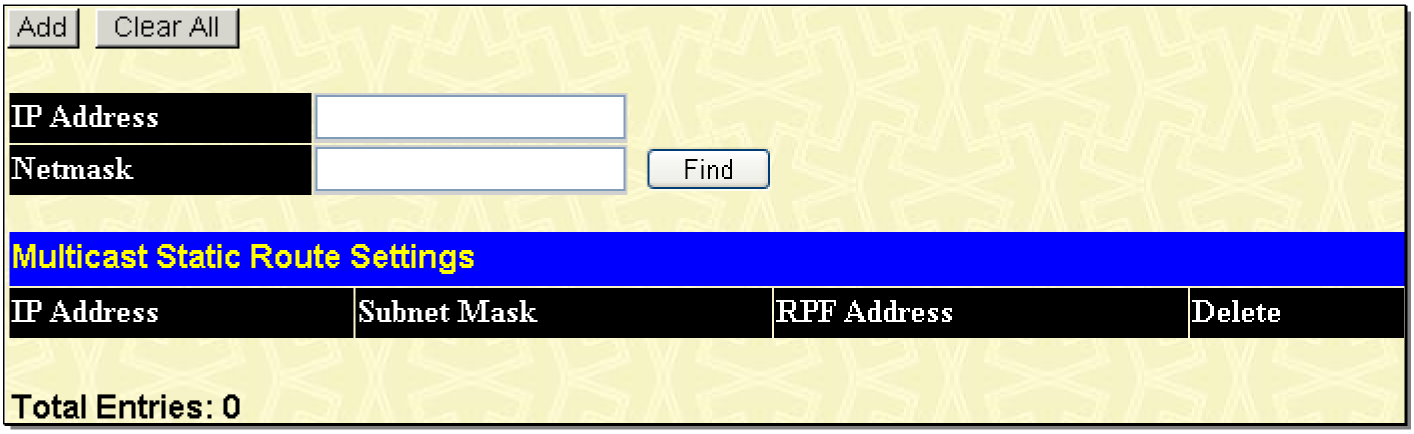
Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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

Multicast Static Route Settings

This window is used to create an IP multicast static route configuration entry.

To access the **Multicast Static Route Settings** window, click **L3 Features > Multicast Static Route Settings**, as shown below:



IP Address	
Netmask	

Multicast Static Route Settings

IP Address	Subnet Mask	RPF Address	Delete

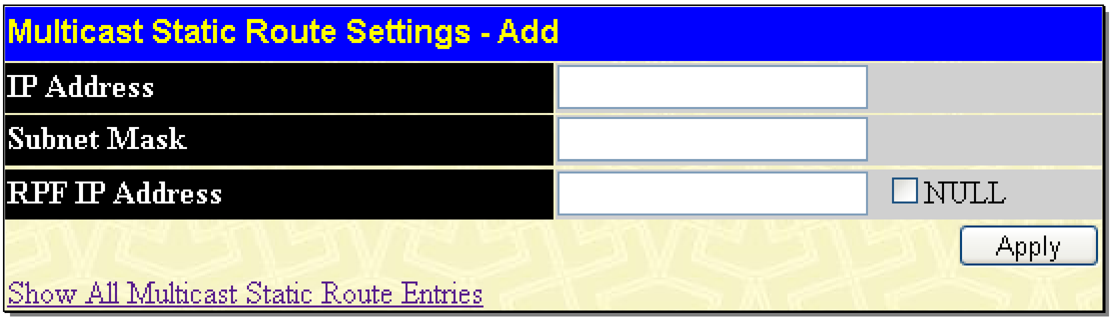
Total Entries: 0

Figure 4- 11. Multicast Static Route Settings window

The following parameters may be configured:

Parameter	Description
IP Address	Enter the IP address you wish to find.
Netmask	Enter the subnet mask of the entry to find.

Enter the appropriate information and click **Find**, the information will appear in the Multicast Static Route Settings table To remove an entry from the table, click its corresponding ☒ under the Delete heading. To clear all the entries click the **Clear All** button. To add a new entry click **Add**, the following window will be displayed for the user to configure.



Multicast Static Route Settings - Add

IP Address		
Subnet Mask		
RPF IP Address		□ NULL

Figure 4- 12. Multicast Static Route Settings - Add window

The following parameters may be configured:

Parameter	Description
IP Address	Enter the IP address of the entry you wish to add. If the source IP address of the received IP multicast packet matches this address, the RPF address is used to complete the RPF check.
Subnet Mask	Enter the Subnet Mask of the entry to add.
RFP IP Address	Enter the RFP IP Address of the entry you wish to add. This specifies that the IP address entered, uses the source IP address of the received IP multicast packet to match the network_address. The rpf_address will be used to check whether packets are received from a legal interface. If it is set to null, and the source IP address in the received IP multicast packet matches the network_address, the RPF check will always fail.

Enter the appropriate information and click **Apply**. To return to the Multicast Static Route Entries table, click the hyperlinked Show All Multicast Static Route Entries.

Static/Default Route Settings

The Switch supports static routing for IPv4 and IPv6 formatted addressing. Users can create up to 256 static route entries for IPv4 and IPv6 combined.

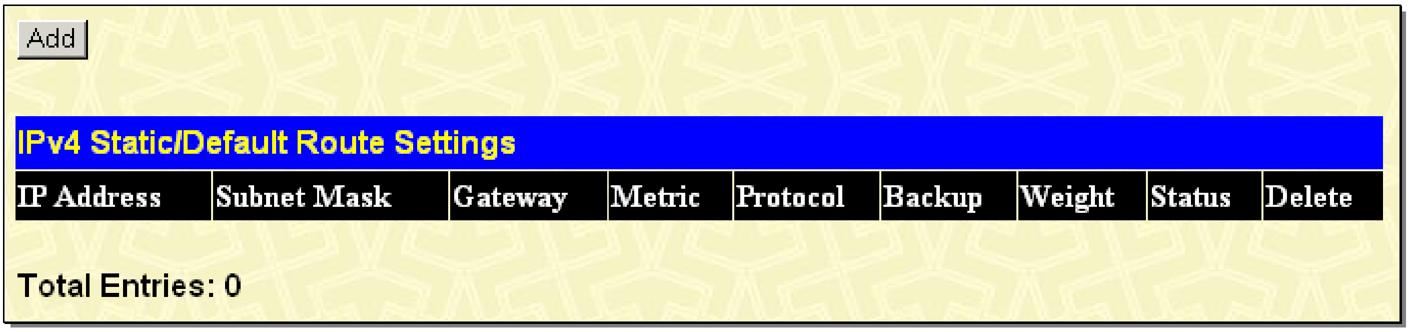
For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

IPv4 Static/Default Route Settings

Entries into the Switch’s forwarding table can be made using both an IP address subnet mask and a gateway. 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 > IPv4 Static/Default Route Settings**, as shown below:



IPv4 Static/Default Route Settings

IP Address	Subnet Mask	Gateway	Metric	Protocol	Backup	Weight	Status	Delete

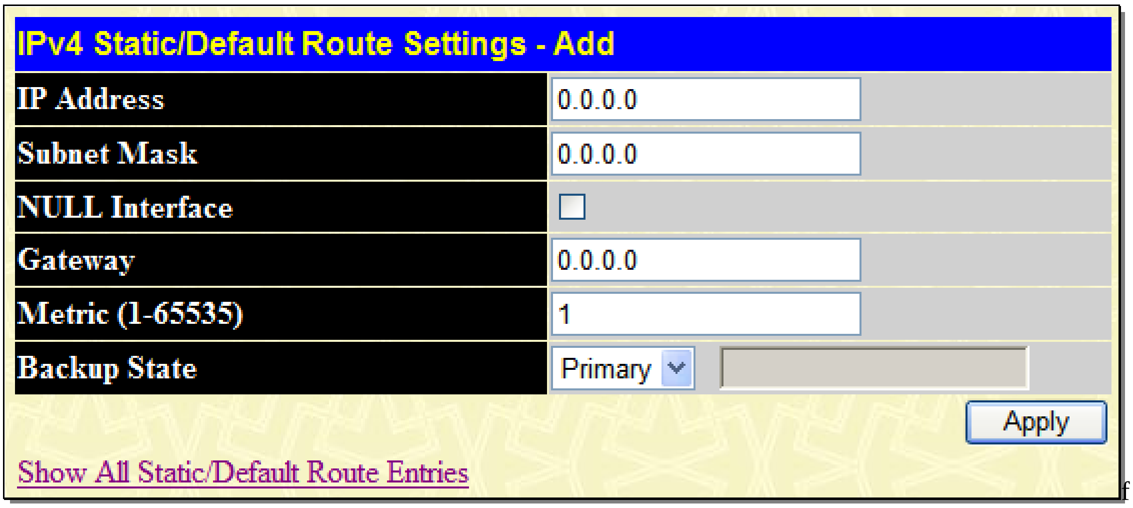
Total Entries: 0

Figure 4- 13. IPv4 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 route entered into the table.
Metric	Represents the metric value of the IP route entered into the table. This field may read a number between 1 and 65535.
Protocol	Represents the protocol used for the Routing Table entry of the IP route.
Backup	Represents the Backup state that this IP route is configured for. This field may read Primary, Backup or None.
Weight	This field is used to add a weight to the IP route. The rate will determine the ratio for forwarding data packets to a destination. 1= low 4=high.
Status	This field denotes the current active state of this IP route.
Delete	Click ☒ to delete this entry from the Static/Default Route Settings table.

To enter an IP route into the Switch's **IPv4 Static/Default Route Settings** window, click the **Add** button, revealing the following window to configure.



IPv4 Static/Default Route Settings - Add

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
NULL Interface	□
Gateway	0.0.0.0
Metric (1-65535)	1
Backup State	Primary

Figure 4- 14. IPv4 Static/Default Route Settings – Add window

The following fields can be set:

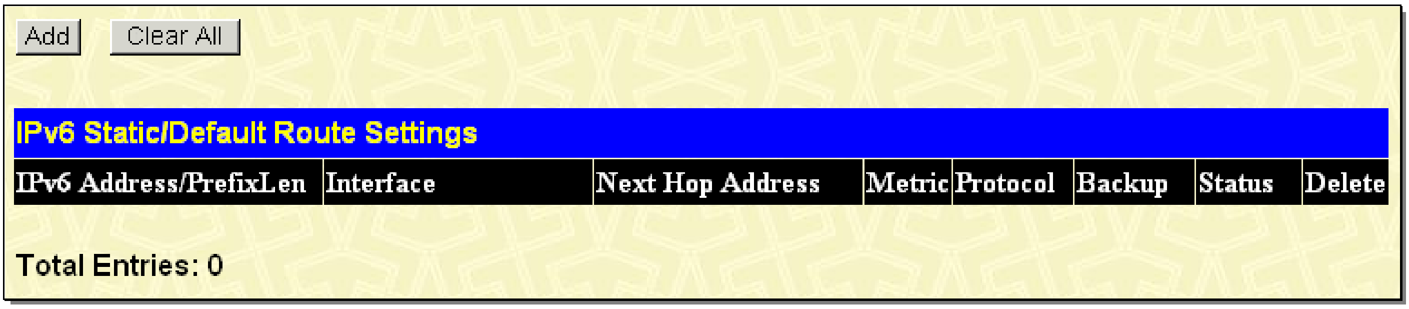
Parameter	Description
IP Address	Allows the entry of an IP address that will be a static entry into the Switch's Routing Table.
Subnet Mask	Allows the entry of a subnet mask corresponding to the IP address above.
NULL Interface	Tick the checkbox to select the null interface.
Gateway	Allows the entry of an IP address of a gateway for the IP route 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 among *Primary*, *Backup*, and *Weight*. 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. If *Weight* is selected, use the text box on the right to enter your own weight setting.

Click **Apply** to implement changes made.

IPv6 Static/Default Route Settings

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses.

To view the following window, click **L3 Features > Static/Default Route Settings > IPv6 Static/Default Route Settings**, as shown below:



IPv6 Static/Default Route Settings

IPv6 Address/PrefixLen	Interface	Next Hop Address	Metric	Protocol	Backup	Status	Delete

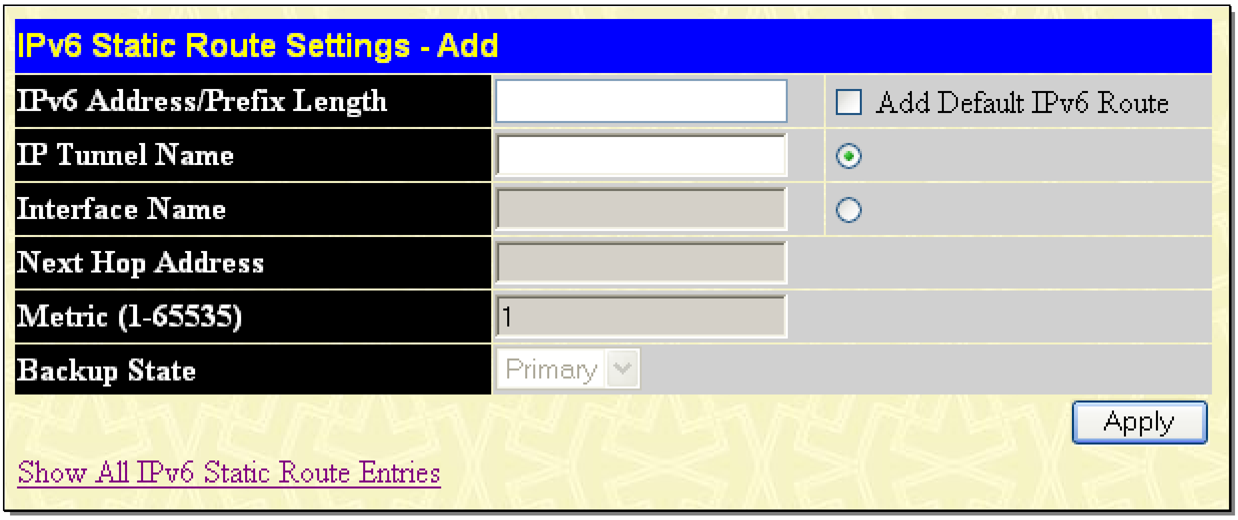
Total Entries: 0

Figure 4- 15. IPv6 Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IPv6 Address/PrefixLen	The IPv6 address and corresponding Prefix Length of the IPv6 static route entry.
Interface	The IP Interface where the static IPv6 route is created.
Next Hop Address	The corresponding IPv6 address for the next hop Gateway address in IPv6 format.
Metric	The metric of the IPv6 interface entered into the table representing the number of routers between the Switch and the IPv6 address above. Metric values allowed are between 1 and 65535.
Protocol	Represents the status for the IPv6 routing table entry.
Backup	This field will indicate the role of this interface for the IPv6 network connection for the switch, whether Primary or Backup.
Status	This field denotes the current active state of this IPv6 route.
Delete	Click the ☒ button to delete this entry from the list.

To enter an IPv6 Interface into the IPv6 Static Route list, click the **Add** button, revealing the following window to configure.


IPv6 Static Route Settings - Add

IPv6 Address/Prefix Length		□ Add Default IPv6 Route
IP Tunnel Name		●
Interface Name		○
Next Hop Address		
Metric (1-65535)	1	
Backup State	Primary	

Figure 4- 16. IPv6 Static Route Settings – Add window

Tick the default check box if this will be the default IPv6 route. Choosing this option will allow the user to configure the default gateway for the next hop router only.

The following fields can be set:

Parameter	Description

IPv6 Address/Prefix Length	Specify the address and mask information using the format as IPv6 address / prefix length (IPv6 address is hexadecimal number, prefix length is decimal number, for example 1234:5D7F/32). Ticking the default check box will set the IPv6 address as unspecified and the Switch will automatically find the default route. This defines the entry as a 1 hop IPv6 default route.
IP Tunnel Name	The IP tunnel interface name of the next hop. When this option is specified, it is indicated that this new created route is an IP tunnel route.
Interface Name	The IP Interface where the static IPv6 route is to be created.
Next Hop Address	Enter the IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric representing the number of routers between the Switch and the IPv6 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 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
Default	1 - 999	1
OSPF Intra	1 - 999	80
OSPF Inter	1 - 999	90
RIP	1 - 999	100
OSPF ExtT1	1 - 999	110
OSPF ExtT2	1 - 999	115
EBGP	1 - 999	70
IBGP	1 - 999	130

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.

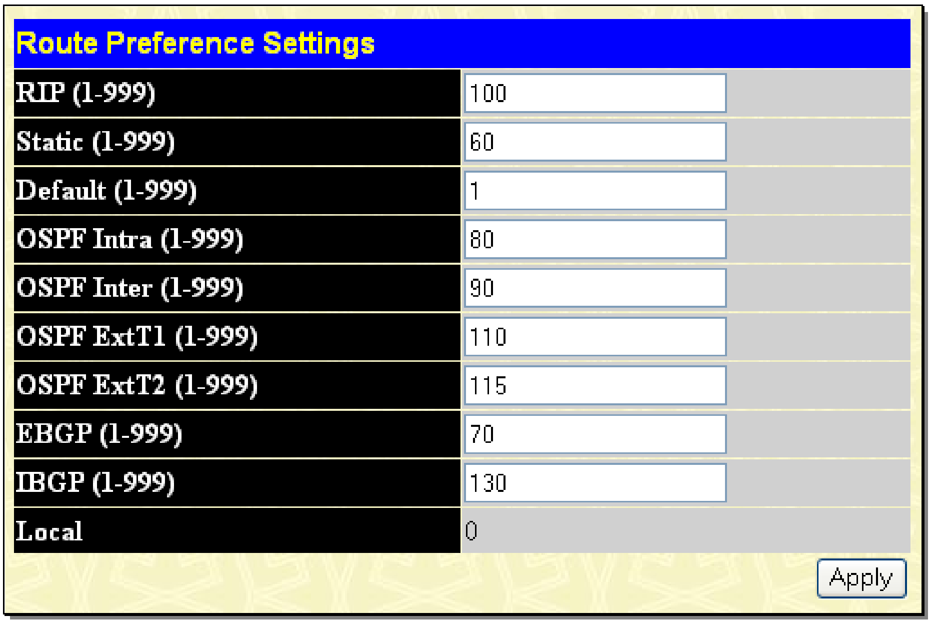
The user should be aware of three points before configuring the route preference:

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**, as shown below:



Route Preference Settings

RIP (1-999)	100
Static (1-999)	60
Default (1-999)	1
OSPF Intra (1-999)	80
OSPF Inter (1-999)	90
OSPF ExtT1 (1-999)	110
OSPF ExtT2 (1-999)	115
EBGP (1-999)	70
IBGP (1-999)	130
Local	0

Figure 4- 17. Route Preference Settings window

The following fields can be 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*.
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*.
Default (1-999)	Enter a value between *1* and *999* to set the route preference for Default. 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 1.
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*.
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*.
EBGP (1-999)	Enter a value between *1* and *999* to set the route preference for EBGP. 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 *70*.
IBGP (1-999)	Enter a value between *1* and *999* to set the route preference for IBGP. 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 *130*.

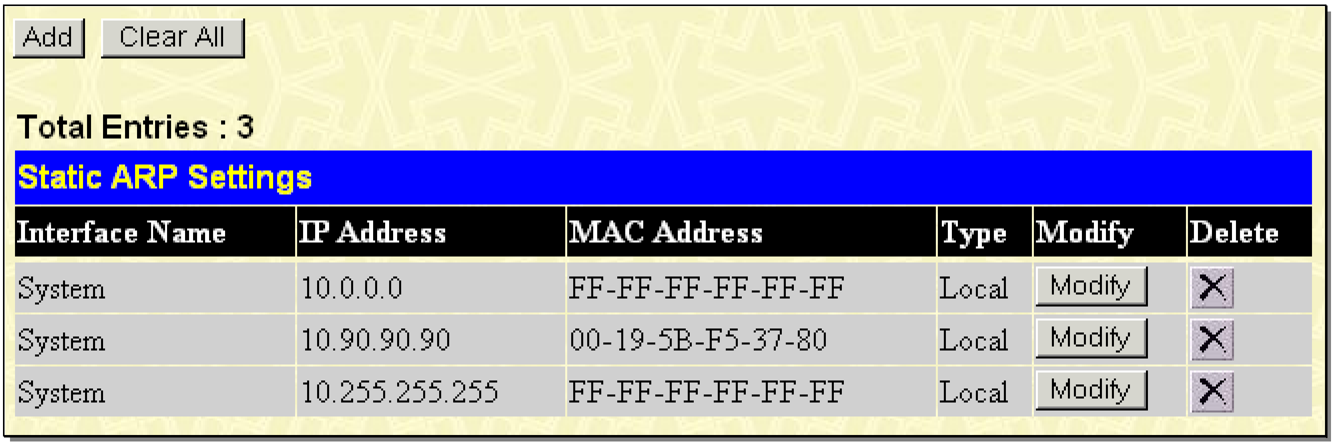
Click **Apply** to implement changes made.

Static ARP Settings

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 Settings** window, click **L3 Features** > **Static ARP Settings**, as shown below:



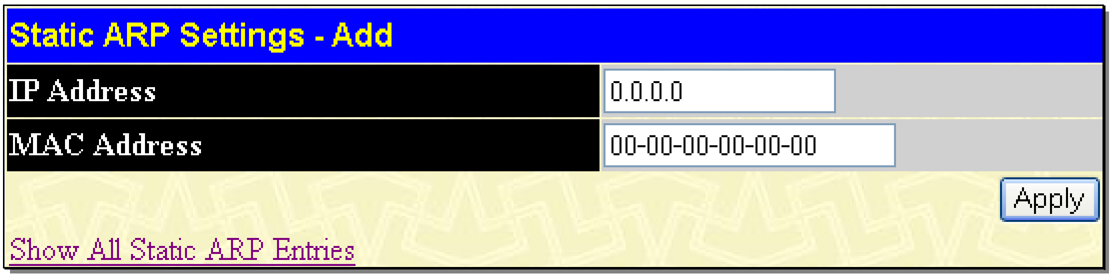
Total Entries : 3

Static ARP Settings

Interface Name	IP Address	MAC Address	Type	Modify	Delete
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local	Modify	☒
System	10.90.90.90	00-19-5B-F5-37-80	Local	Modify	☒
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local	Modify	☒

Figure 4- 18. Static ARP Settings window

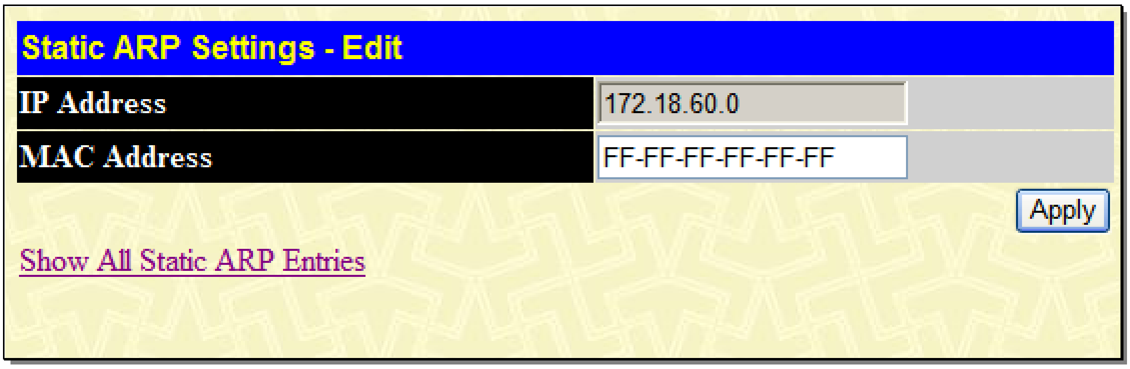
To add a new entry, click the **Add** button, revealing the following screen to configure:


Static ARP Settings - Add

IP Address	0.0.0.0
MAC Address	00-00-00-00-00-00

Figure 4- 19. Static ARP Settings – Add window

To modify a current entry, click the corresponding **Modify** button of the entry to be modified, revealing the following window to configure:



Static ARP Settings - Edit

IP Address	172.18.60.0
MAC Address	FF-FF-FF-FF-FF-FF

Figure 4- 20. Static ARP Settings – Edit window

The following fields can be set or viewed:

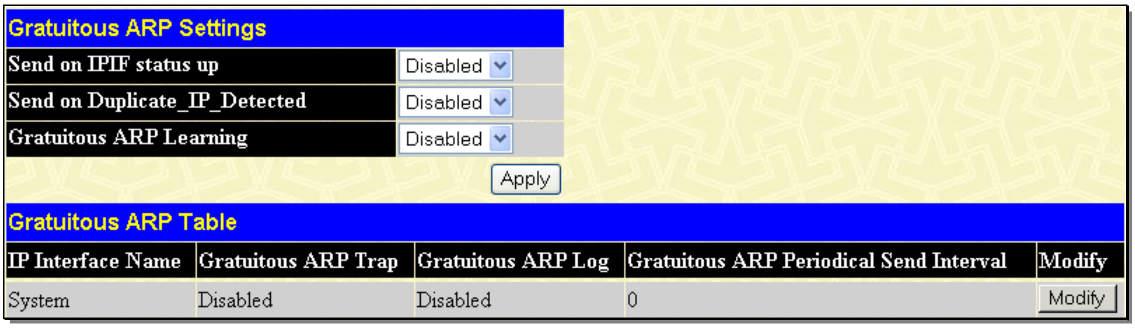
Parameter	Description
IP Address	The IP address of the ARP entry. This field cannot be edited in the **Static ARP Settings – Edit** window.
MAC Address	The MAC address of the ARP entry.

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.

Gratuitous ARP Settings

An ARP announcement (also known as Gratuitous ARP) is a packet (usually an ARP Request) containing a valid SHA and SPA for the host which sent it, with TPA equal to SPA. Such a request is not intended to solicit a reply, but merely updates the ARP caches of other hosts which receive the packet. This is commonly done by many operating systems on startup, and helps to resolve problems which would otherwise occur if, for example, a network card had recently been changed (changing the IP address to MAC address mapping) and other hosts still had the old mapping in their ARP cache

To open the **Gratuitous ARP Settings** window, click **L3 Features** > **Gratuitous ARP Settings**, as shown below:



Gratuitous ARP Settings

Send on IPIF status up	Disabled
Send on Duplicate_IP_Detected	Disabled
Gratuitous ARP Learning	Disabled

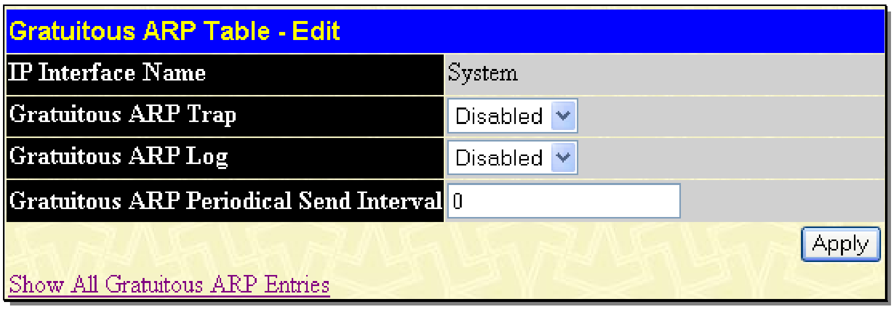
Gratuitous ARP Table

IP Interface Name	Gratuitous ARP Trap	Gratuitous ARP Log	Gratuitous ARP Periodical Send Interval	Modify
System	Disabled	Disabled	0	Modify

Figure 4- 21. Gratuitous ARP Settings window

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

To modify a current entry, click the corresponding **Modify** button of the entry, which will reveal the following window to be configured:



Gratuitous ARP Table - Edit

IP Interface Name	System
Gratuitous ARP Trap	Disabled
Gratuitous ARP Log	Disabled
Gratuitous ARP Periodical Send Interval	0

Figure 4- 22. Gratuitous ARP Table – Edit window

The following fields can be set or viewed:

Parameter	Description
Send on IPIF status up	This is used to enable/disable the sending of gratuitous ARP request packets while an IPIF interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is *Disabled*, and only one ARP packet will be broadcast.
Send on Duplicate_IP-_Detected	This is used to enable/disable the sending of gratuitous ARP request packets while a duplicate IP is detected. By default, the state is *Disabled*. Duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address.
Gratuitous ARP Learning	This is used to enable/disable updating ARP cache based on the received gratuitous ARP packet. If a switch receives a gratuitous ARP packet, it should add or update the ARP entry. This is *Disabled* by default.
Gratuitous ARP Trap & Log	The switch can trap and log IP conflict events to inform the administrator. By default, trap is Disabled and event log is also disabled.
Gratuitous ARP Periodical Send Interval	This is used to configure the interval for the periodical sending of gratuitous ARP request packets. By default, the interval is 0.

After making the desired changes, click **Apply** to implement the new Gratuitous ARP Table entry.

Policy Route Settings

Policy Based routing is a method used by the Switch to give specified devices a cleaner path to the Internet. Used in conjunction with the Access Profile feature, the Switch will identify traffic originating from a device using the Access Profile feature and forward it on to a next hop router that has a more direct connection to the Internet than the normal routing scheme of your network.

Take the example adjacent picture. Let's say that the PC with IP address 10.1.1.1 belongs to the manager of a company while the other PCs belong to employees. The network administrator hopes to circumvent network traffic by configuring the Policy Routing Switch to make a more direct connection to the Internet using a next hop router (10.2.2.2) that is directly attached to a Gateway router (10.3.3.3), thus totally avoiding the normal network and its related traffic. To accomplish this, the user must configure the Access Profile feature of the Switch to have the PC, with IP address 10.1.1.1 as the Source IP address and the Internet address as the destination IP address (learned through routing protocols), along with other pertinent information. Next, the administrator must configure the Policy Route window to be enabled for this Access Profile and its associated rule, and the Next Hop Router's IP address (10.2.2.2) must be set. Finally, this Policy Route entry must be enabled.

Once completed, the Switch will identify the IP address using the Access Profile function, recognize that is has a Policy Based route, and then forward the information on to the specified next hop router, that will, in turn, relay packets to the gateway router. Thus, the new, cleaner path to the Internet has been formed.

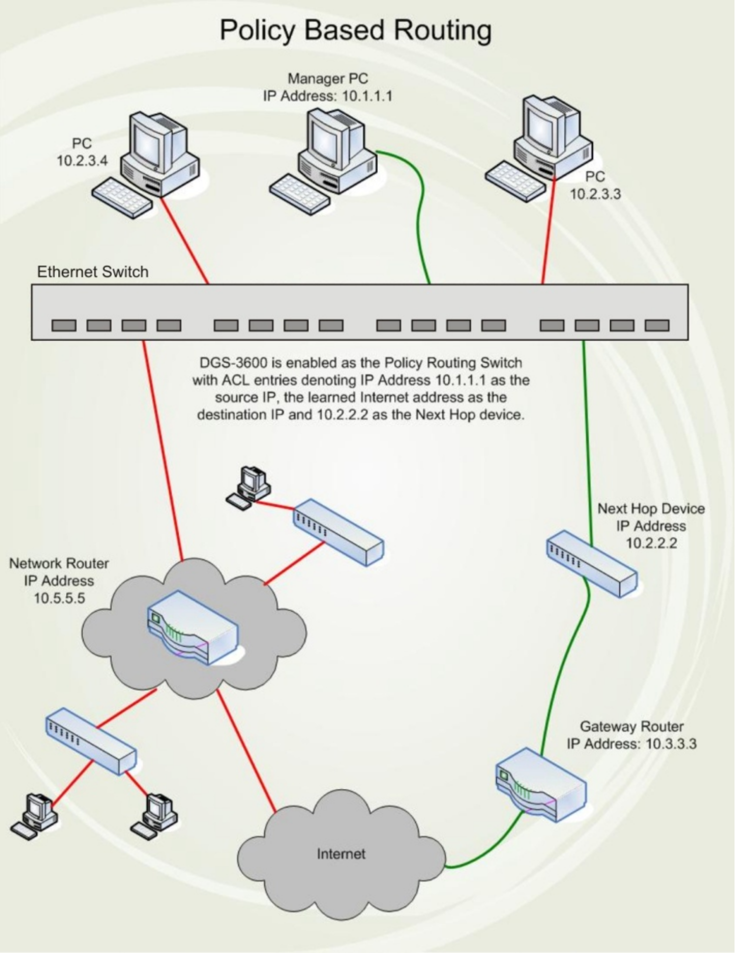
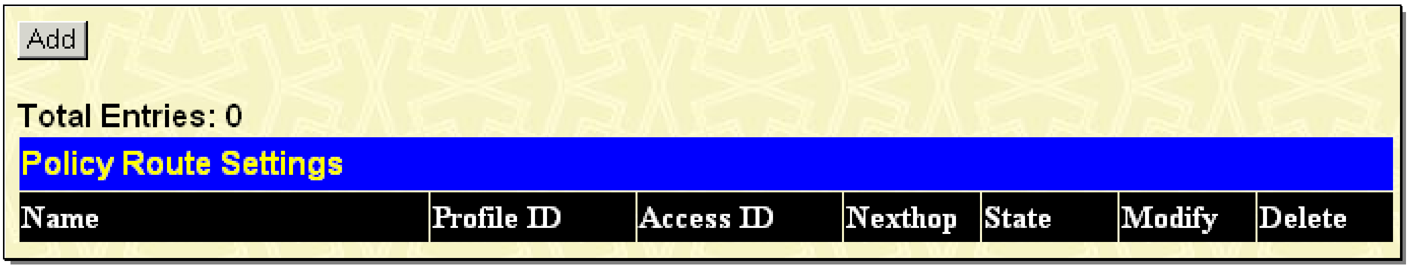

Policy Based Routing
Manager PC
IP Address: 10.1.1.1
PC
10.2.3.4
PC
10.2.3.3
Ethernet Switch
DGS-3600 is enabled as the Policy Routing Switch with ACL entries denoting IP Address 10.1.1.1 as the source IP, the learned Internet address as the destination IP and 10.2.2.2 as the Next Hop device.
Next Hop Device
IP Address
10.2.2.2
Network Router
IP Address
10.5.5.5
Gateway Router
IP Address: 10.3.3.3
Internet

Figure 4- 23. Policy-based Routing example

There are some restrictions and cautions when implementing this feature:

1. The access profile must first be created, along with the accompanying rule. If the administrator attempts to enable this feature without the access profile, an error message will be produced.
2. If the access profile is configured as Deny, the packet will be dropped and not forwarded to the next hop destination.
3. If the administrator deletes a rule or profile that is directly linked to a configured policy route, and error message will be prompted to the administrator.

To configure the Policy Route feature, click **L3 Features** > **Policy Route Settings**, as shown below:



Total Entries: 0

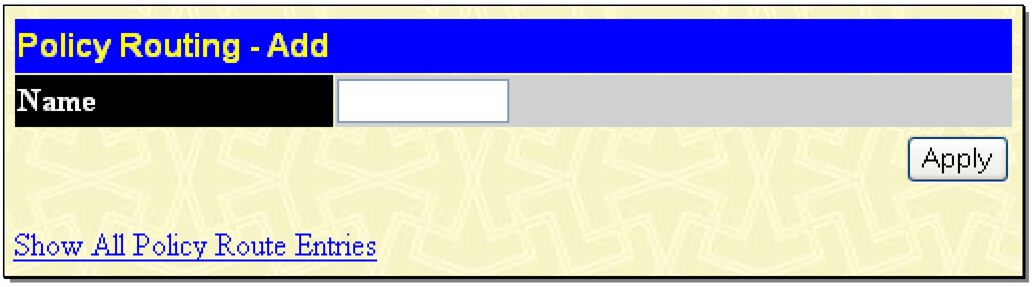
Policy Route Settings

Name	Profile ID	Access ID	Nexthop	State	Modify	Delete

Figure 4- 24. Policy Route Settings window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To add a new Policy Route, click the **Add** button, which will display the following window.


Policy Routing - Add

Name	

Figure 4- 25. Policy Route – Add window

Adjust the following parameters and click **Apply** to set the new Policy Route, which will be displayed in the **Policy Route Settings** window. Click Show All Policy Route Entries to return to the **Policy Route Settings** window.

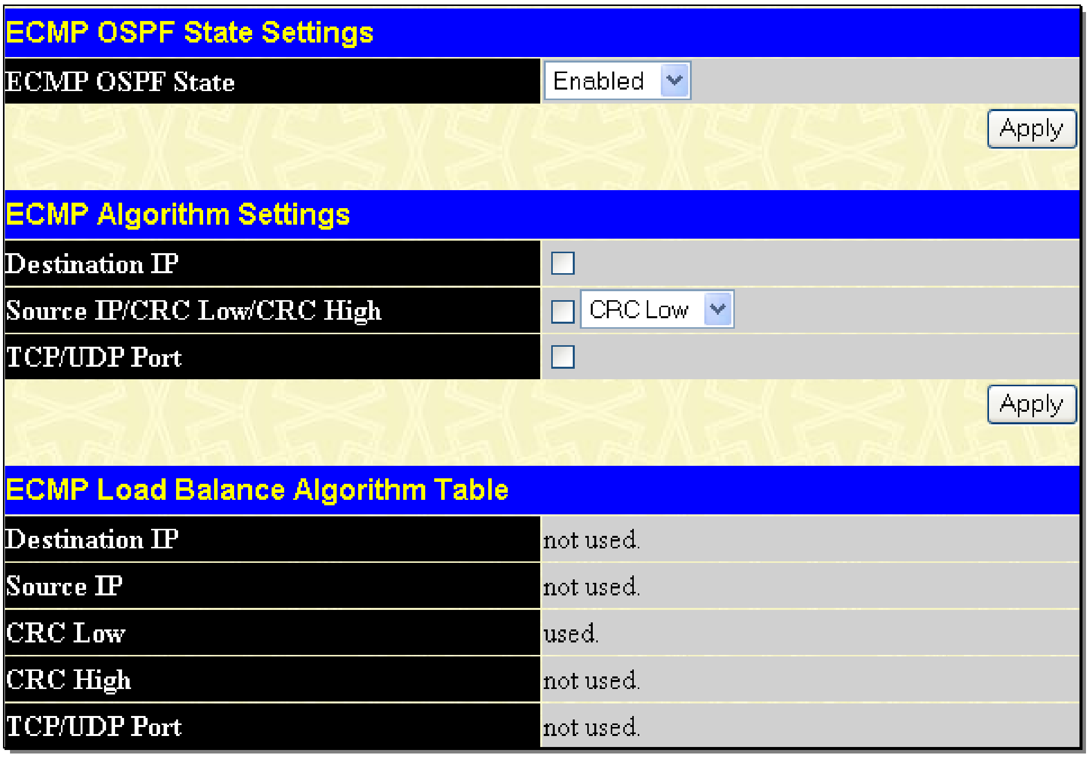
Parameter	Description
Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this policy route.
Profile ID	Enter the Profile ID number of the Access Profile, previously created, which will be used to identify packets as following this Policy Route. This access profile, along with the access rule, must first be constructed before this policy route can be created.
Access ID	Enter the Access ID number of the Access Rule, previously created, which will be used to identify packets as following this Policy Route. This access rule, along with the access profile, must first be constructed before this policy route can be created.
Nexthop	This is the IP address of the Next Hop router that will have a direct connection to the Gateway router connected to the Internet.
State	Use the pull-down menu to enable or disable this Policy Route.

ECMP Algorithm Settings

ECMP algorithm settings allow the user to set the ECMP load balance algorithm which makes it effective for ECMP routing. ECMP routing can be adopted by either OSPF dynamic routes or by static routes which are configured with equal cost. The OSPF protocol maintains multiple equal-cost routes to all destinations. Each one of the multiple routes will be of the same type (intra-area, inter-area, type 1 external or type 2 external), cost, and will have the same associated area. However, each route may specify a separate next hop and Advertising router.

There is no requirement that a router running OSPF can keep track of all possible equal-cost routes to a destination. An implementation may choose to keep only a fixed number of routes to any given destination. This does not affect any of the algorithms presented in this specification.

To configure these settings, click **L3 Features** > **ECMP Algorithm Settings**, as shown below:



ECMP OSPF State Settings

ECMP OSPF State: Enabled

ECMP Algorithm Settings

Destination IP: □

Source IP/CRC Low/CRC High: □ CRC Low

TCP/UDP Port: □

ECMP Load Balance Algorithm Table

Destination IP	not used.
Source IP	not used.
CRC Low	used.
CRC High	not used.
TCP/UDP Port	not used.

Figure 4- 26. ECMP Algorithm Settings window

The following settings can be configured:

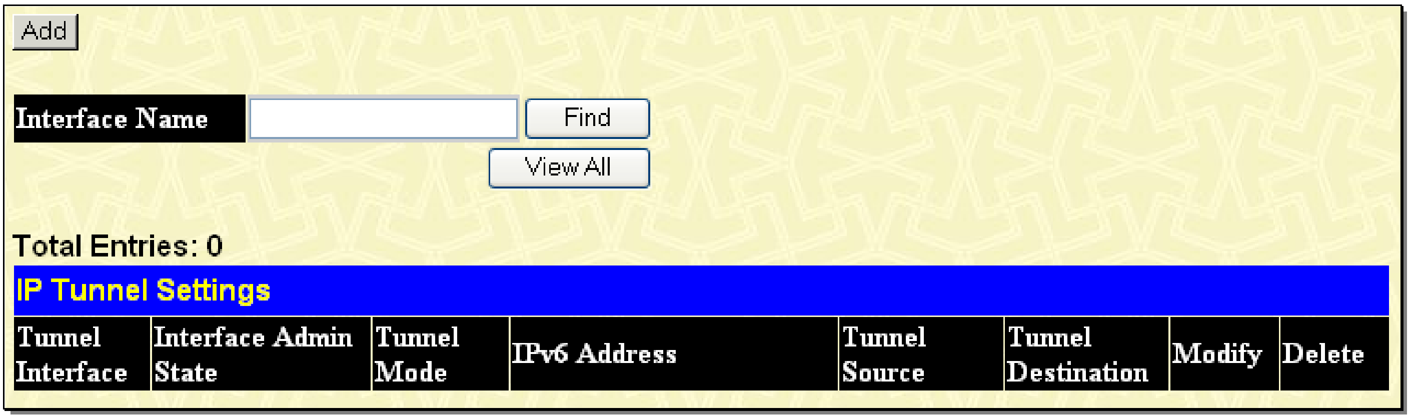
Parameter	**Description**
ECMP OSPF State	Use the drop-down menu to enable or disable the ECMP OSPF State.
Destination IP	Tick this check box to include the Destination IP in the ECMP Algorithm.
Source IP/CRC Low/CRC High	*Source IP* – If set, ECMP algorithm will include the source IP. This attribution is mutually exclusive with CRC Low and CRC High. If it is set, CRC Low and CRC High will be excluded. It is not set by default. *CRC Low* – If set, ECMP algorithm will include the lower 5 bits of CRC. This attribution is mutually exclusive from CRC High and IP source. If it is set, CRC High and IP source will be excluded. It is set by default. *CRC High* – If set, ECMP algorithm will include the upper 5 bits of CRC. This attribution is mutually exclusive with IP source and CRC Low. If it is set, CRC Low and IP source will be excluded. It is not set by default.
TCP/UDP Port	Tick this check box to include TCP/UDP Port in the ECMP Algorithm.

Click **Apply** to implement changes made.

IP Tunnel Settings

The Switch supports IP tunneling. The idea behind this feature is to be able to integrate IPv6 into and coexist with existing IPv4 networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start. This IPv6 tunneling mechanism is one of D-Link's strategies for solving the transition from IPv4 to IPv6.

To configure these settings, click **L3 Features** > **IP Tunnel Settings**, as shown below:



Total Entries: 0

IP Tunnel Settings

Tunnel Interface	Interface Admin State	Tunnel Mode	IPv6 Address	Tunnel Source	Tunnel Destination	Modify	Delete

Figure 4- 27. IP Tunnel Settings window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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

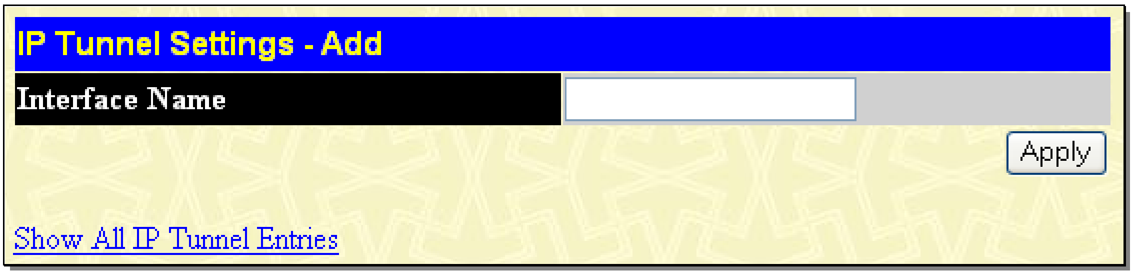
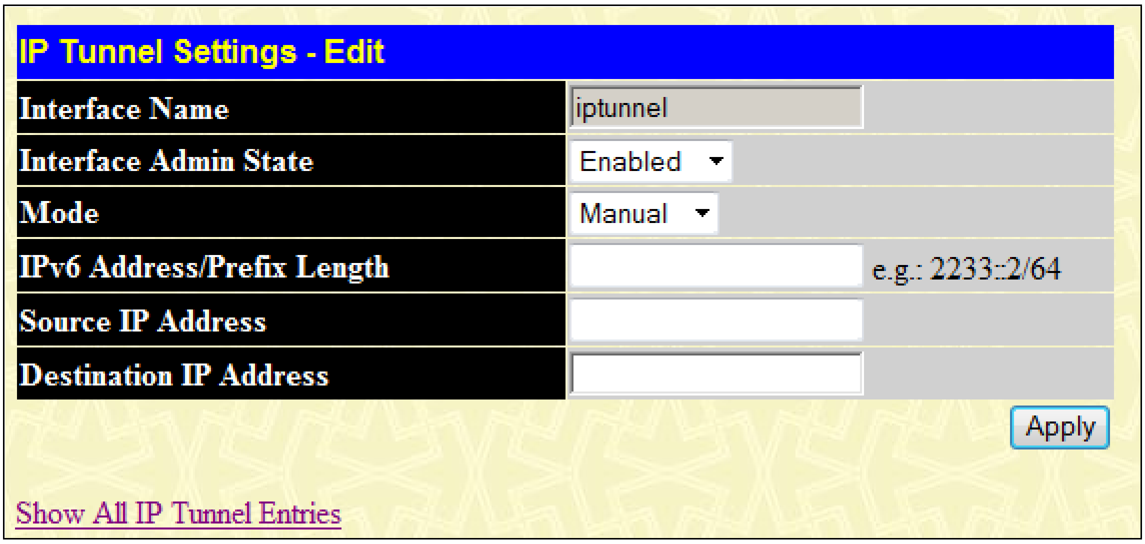


Figure 4- 28. IP Tunnel Settings – Add window

To modify an entry in the IP Tunnel Settings window, first use the Add window above to create an entry and then click the Modify. The following window will open:


IP Tunnel Settings - Edit

Interface Name	iptunnel
Interface Admin State	Enabled
Mode	Manual
IPv6 Address/Prefix Length	e.g.: 2233::2/64
Source IP Address	
Destination IP Address	

Figure 4- 29. IP Tunnel Settings – Edit window

The following settings can be configured:

Parameter	Description
Interface Name	This is the IPv6 tunnel interface name.

Interface Admin State	Enable or disable IP tunneling.
Mode	Select from Manual, 6to4, or ISATAP. Manual is used to configure an existing IPv6 tunnel as an IPv6 manual tunnel on the Switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not, will depend on the current mode. IPv6 Manual tunnels are simple point-to-point tunnels that can be used within a site or between sites 6to4 is used to configure an existing IPv6 tunnel as an IPv6 6to4 tunnel on the Switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not will depend on the current mode. A maximum of one IPv6 6to4 tunnel can exist on the system. IPv6 6to4 tunnels are point-to-multipoint tunnels that can be used to connect isolated IPv6 sites. Each IPv6 site has at least one connection to a shared IPv4 network and this IPv4 network could be the global Internet or a corporate backbone. The key requirement is that each site has a globally unique IPv4 address, which is used to construct a 48-bit globally unique 6to4 IPv6 prefix (It starts with the prefix 2002::/16). ISATAP is used to configure an existing IPv6 tunnel as an IPv6 ISATAP tunnel on the Switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not will depend on the current mode. IPv6 ISATAP tunnels are point-to-multipoint tunnels that can be used to connect systems within a site. An IPv6 ISATAP address is a well-defined unicast address that includes a 64-bit unicast IPv6 prefix (it can be link local or global prefixes), a 32-bit value 0000:5EFE and a 32-bit tunnel source IPv4 address.
IPv6 Address/Prefix Length	Enter the IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing would be enabled on this IPv6 tunnel interface when an IPv6 address is configured. This IPv6 address is not connected with tunnel source or destination IPv4 address.
Source IP Address	Enter the source IPv4 address of this IPv6 tunnel interface. It is used as the source address for packets in this IPv6 tunnel.
Destination IP Address	Enter the destination IPv4 address of this IPv6 tunnel interface. It is used as the destination address for packets in this IPv6 tunnel. It is not required for 6to4 and ISATAP tunnels.

Click **Apply** to implement changes made.

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.

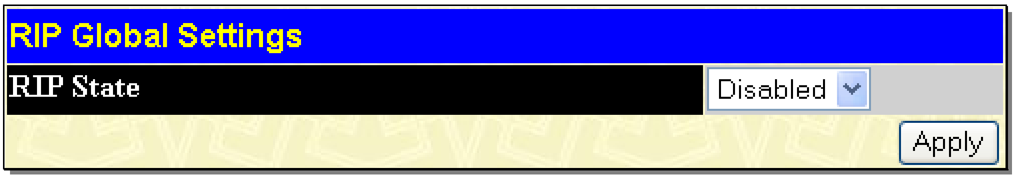
Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

RIP

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 > RIP Global Settings**, as shown below:



RIP Global Settings

RIP State: Disabled

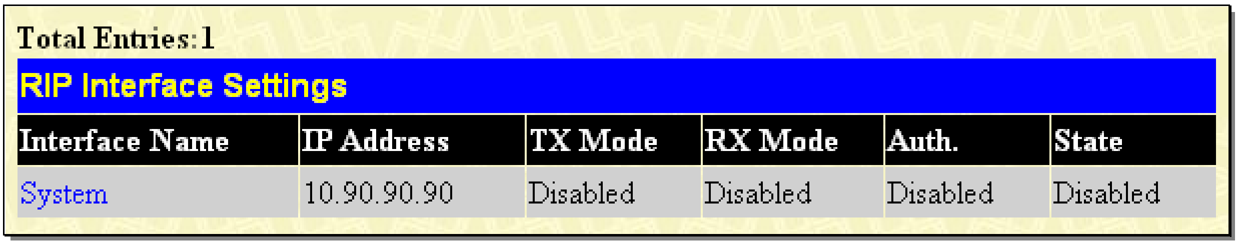
Figure 4- 30. RIP Global Settings window

To enable RIP, simply use the pull-down menu, select *Enabled* and click **Apply**.

RIP Interface Settings

RIP settings are configured for each IP interface on the Switch. This window 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 > RIP Interface Settings**, as shown below:



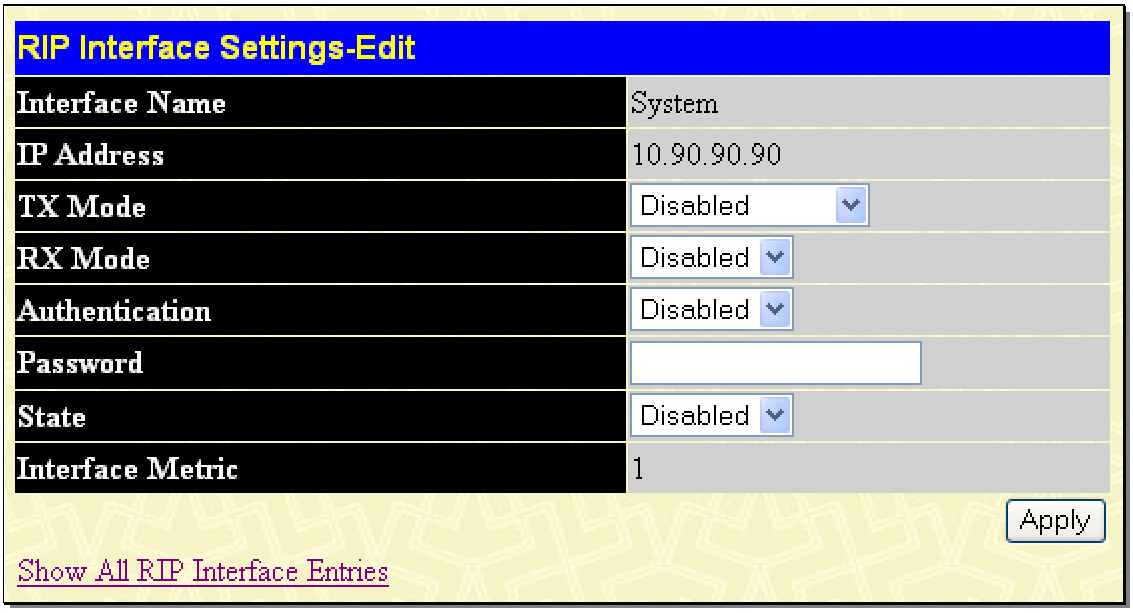
Total Entries: 1

RIP Interface Settings

Interface Name	IP Address	TX Mode	RX Mode	Auth.	State
System	10.90.90.90	Disabled	Disabled	Disabled	Disabled

Figure 4- 31. RIP Interface Settings window

Click the hyperlinked name of the interface to configure the settings for RIP, which will give access to the following window:



RIP Interface Settings-Edit

Interface Name	System
IP Address	10.90.90.90
TX Mode	Disabled
RX Mode	Disabled
Authentication	Disabled
Password	
State	Disabled
Interface Metric	1

Figure 4- 32. 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 use 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.

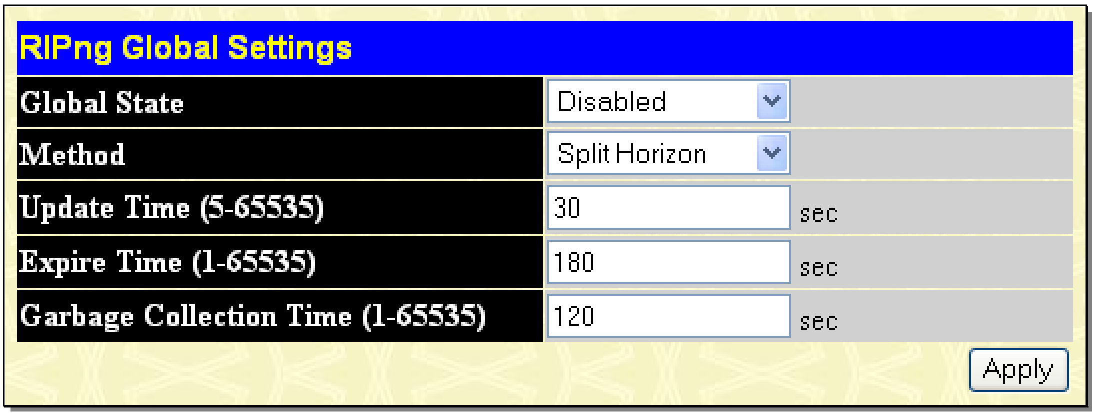
RIPng

The Switch supports Routing Information Protocol next generation (RIPng). RIPng is a routing protocol that exchanges routing information used to compute routes and is intended for IPv6-based networks.

RIPng Global Settings

This window allows users to set up RIPng.

To globally enable RIPng on the Switch, click **L3 Features** > **RIP** > **RIPng** > **RIPng Global Settings**, as shown below:



RIPng Global Settings

Global State	Disabled	
Method	Split Horizon	
Update Time (5-65535)	30	sec
Expire Time (1-65535)	180	sec
Garbage Collection Time (1-65535)	120	sec

Figure 4- 33. RIPng Global Settings window

The following settings can be configured:

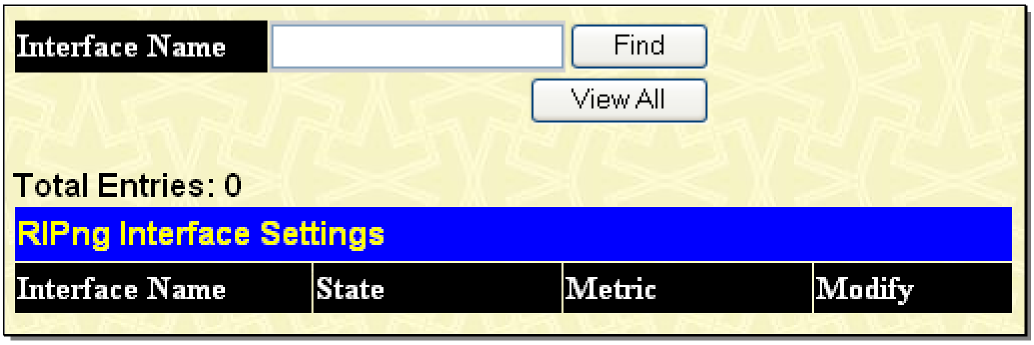
Parameter	Description
Global State	Enable or disable RIPng globally. The default setting is *Disabled*.
Method	Choose from *No Horizon*, *Split Horizon*, and *Poison Reverse*. *No Horizon* – Configured to not use any horizon. *Split Horizon* – Configured to use basic split horizon. This is the default setting. *Poison Reverse* – Configured to use split horizon with poison reverse.
Update Time (5-65535)	Enter the value (in seconds) of the update timer.
Expire Time (1-65535)	Enter the interval (in seconds) of the expire timer.
Garbage Collection Time (1-65535)	Enter the value (in seconds) of the garbage collection timer.

Click **Apply** to implement changes made.

RIPng Interface Settings

This window allows users to configure RIPng interface settings.

To view this window, click **L3 Features > RIP > RIPng > RIPng Interface Settings**, as shown below:



Interface Name

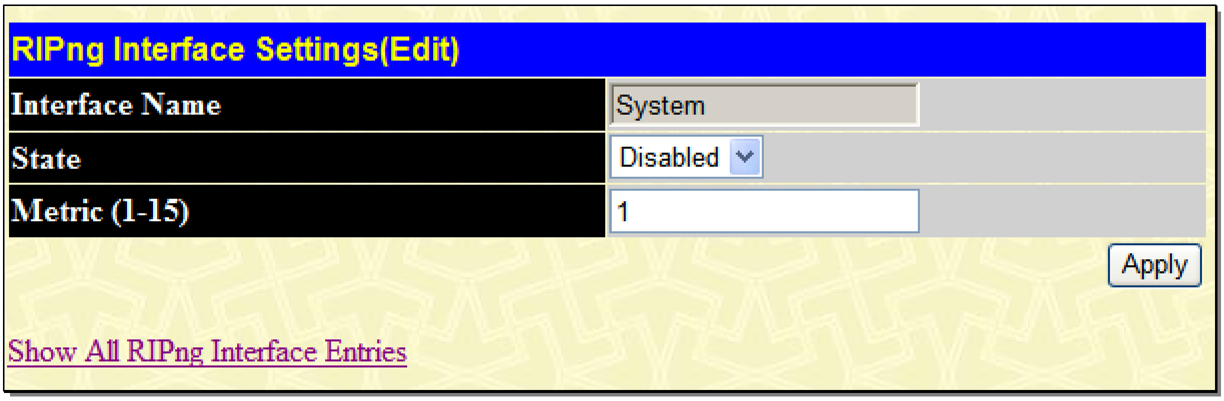
Total Entries: 0

RIPng Interface Settings

Interface Name	State	Metric	Modify

Figure 4- 34. RIPng Interface Settings window

Click the hyperlinked name of the interface to configure the settings for RIPng, which will give access to the following window:



RIPng Interface Settings(Edit)

Interface Name	System
State	Disabled
Metric (1-15)	1

Figure 4- 35. RIPng Interface Settings (Edit) window

The following settings can be configured:

Parameter	Description
Interface Name	The name of the interface for the RIPng configuration.
State	Enable or disable the RIPng state on the specific IP interface. If the state is *Disabled*, then RIPng packets will not be transmitted or received by the interface. The default setting is *Disabled*.
Metric	Enter the cost value of an interface. The RIPng route that was learned from the interface will add this value as a new route metric. The default value is *1*.

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 once 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:

1. 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.
2. This link-state advertisement is flooded to all routers in the area. Each router that receives the link-state advertisement will store the advertisement and then forward a copy to other routers.
3. 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.
4. 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 placed 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.

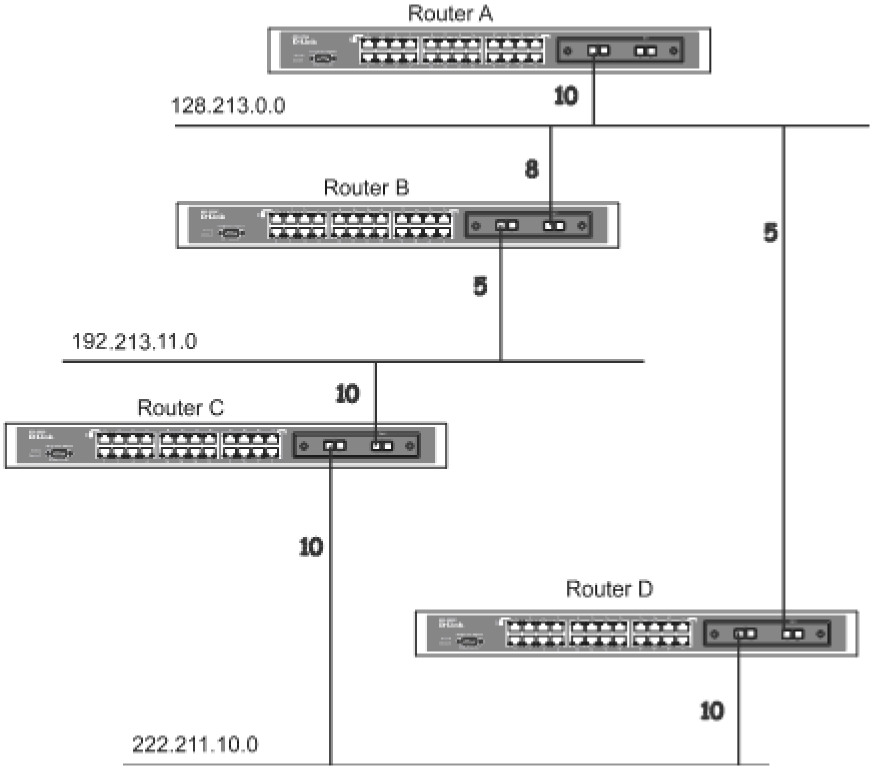


Figure 4- 36. Constructing a Shortest Path Tree

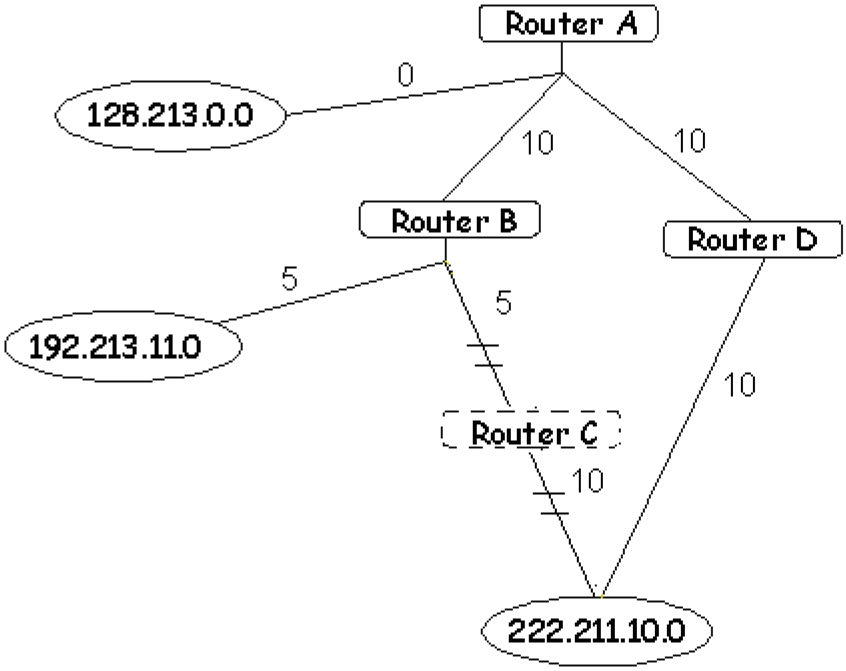


Figure 4- 37. Constructing a Shortest Path Tree

The diagram above shows the network from the viewpoint of Router A. Router A can reach 192.213.11.0 through Router B with a cost of 10 + 5 = 15. Router A can reach 222.211.10.0 through Router C with a cost of 10 + 10 = 20. Router A can also reach 222.211.10.0 through Router B and Router D with a cost of 10 + 5 + 10 = 25, but the cost is higher than the route through Router C. This higher-cost route will not be included in the Router A's shortest path tree. The resulting tree will look like this:

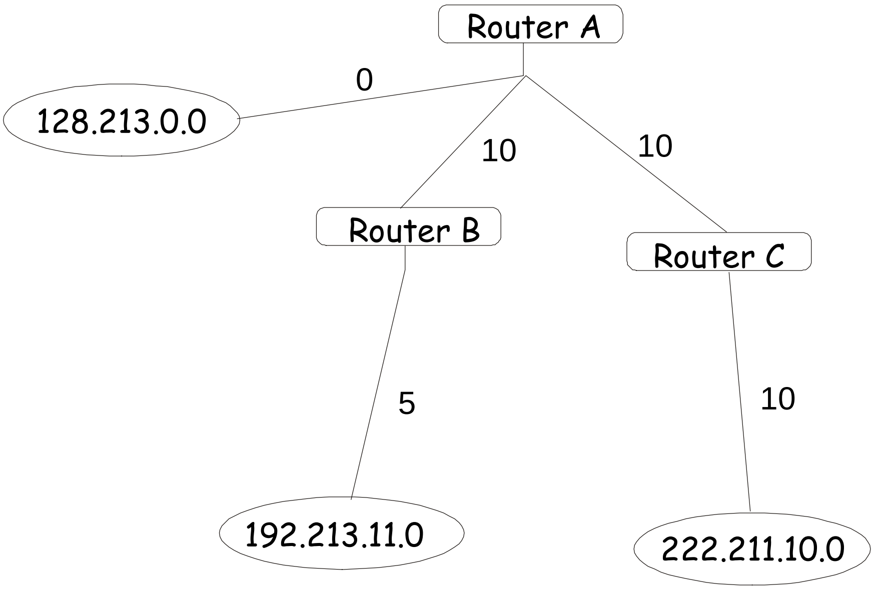


Figure 4- 38. Constructing a Shortest Path Tree - Completed

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 will 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:

1. **Router Link-State Updates** – These describe a router's links to destinations within an area.
2. **Summary Link-State Updates** – Issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).
3. **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.
4. **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 no 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 the 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 must 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:

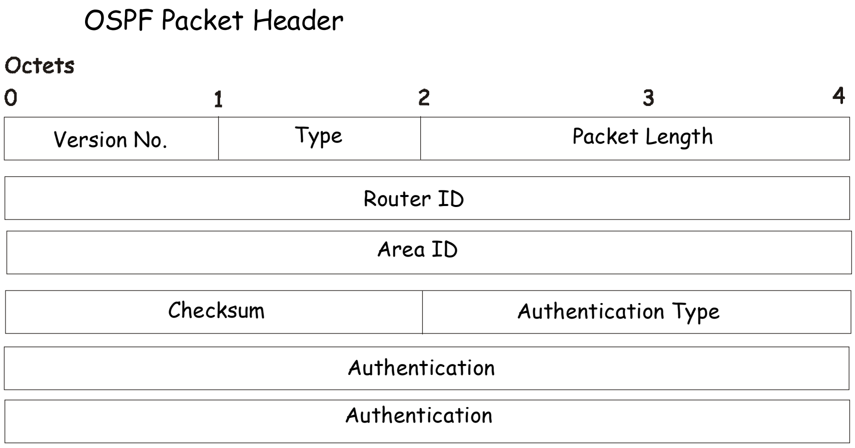


Figure 4- 39. OSPF Packet Header Format

Field	Description
Version No.	The OSPF version number

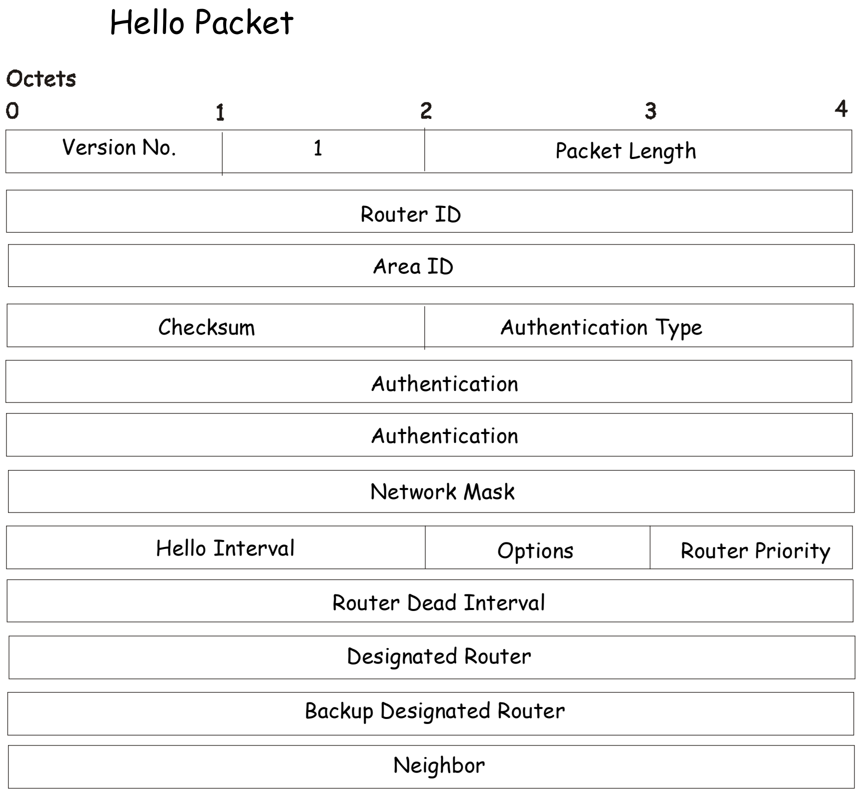
Type	The OSPF packet type. The OSPF packet types are as follows: Type Description Hello Database Description Link-State Request Link-State Update Link-State Acknowledgment
Packet Length	The length of the packet in bytes. This length includes the 24-byte header.
Router ID	The Router ID of the packet's 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 cannot inhibit the forming of neighbor relationships.

The format of the Hello packet is shown below:



Hello Packet

Octets

0	1	2	3	4
Version No.	1	Packet Length		
Router ID				
Area ID				
Checksum		Authentication Type		
Authentication				
Authentication				
Network Mask				
Hello Interval		Options	Router Priority	
Router Dead Interval				
Designated Router				
Backup Designated Router				
Neighbor				

Figure 4- 40. 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 to 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.
Field	Description
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 seconds 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.

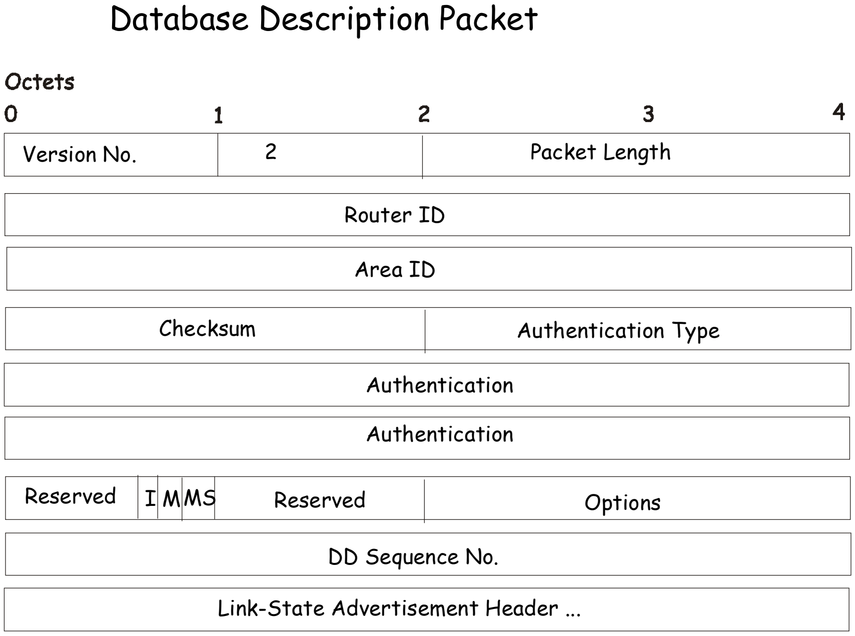


Figure 4- 41. Database Description Packet

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:

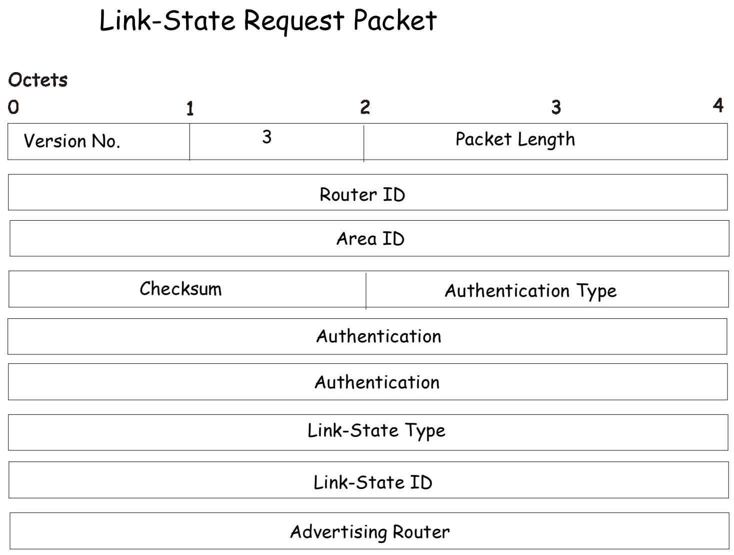


Figure 4- 42. Link-State Request Packet

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:

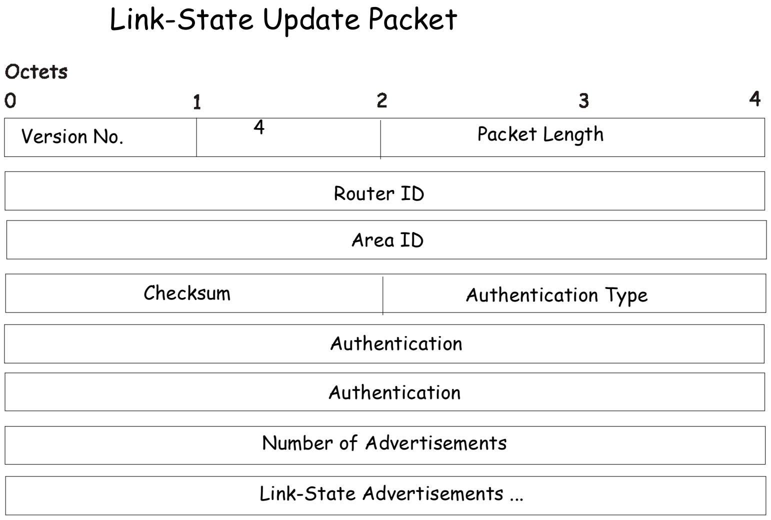


Figure 4- 43. Link-State Update Packet

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:

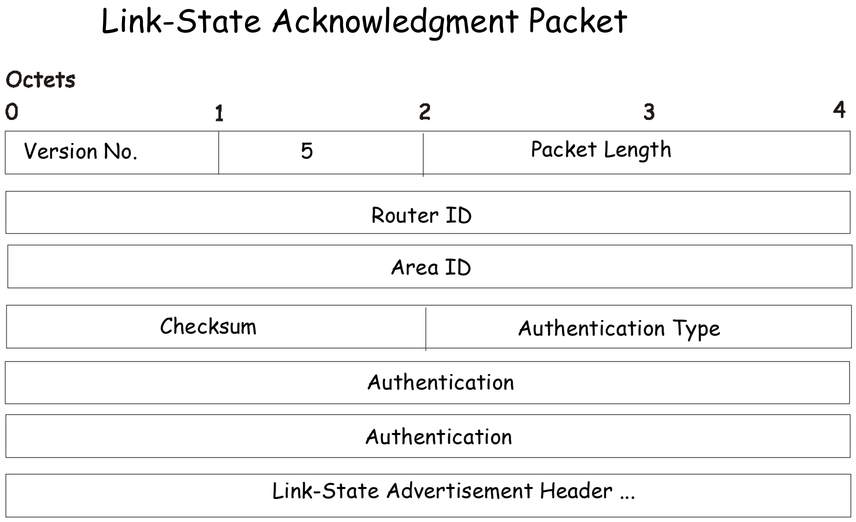


Figure 4- 44. Link State Acknowledge Packet

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:

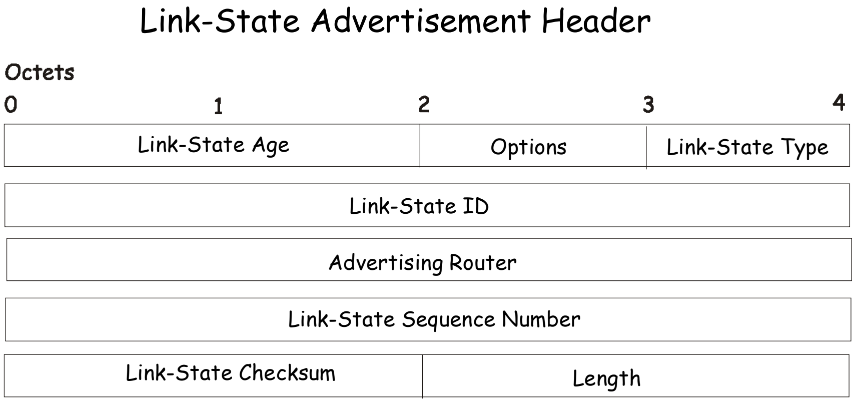


Figure 4- 45. Link State Advertisement Header

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 types 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:

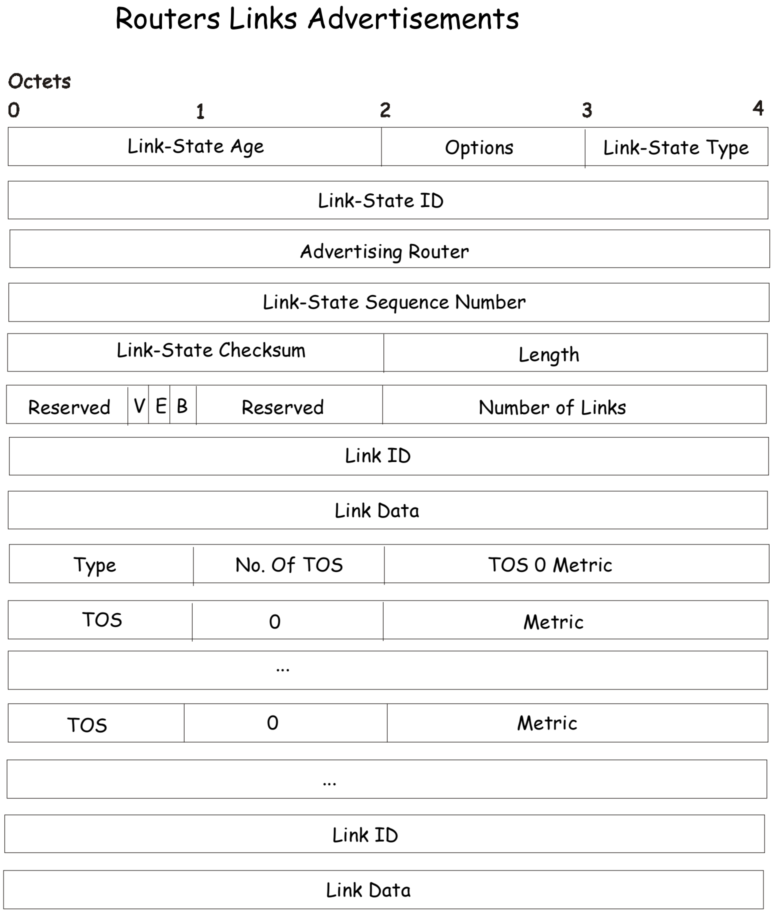


Figure 4- 46. Routers Links Advertisements

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
Type	A quick classification of the router link. One of the following: Type Description: Point-to-point connection to another router. Connection to a transit network. Connection to a stub network. Virtual link.
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:

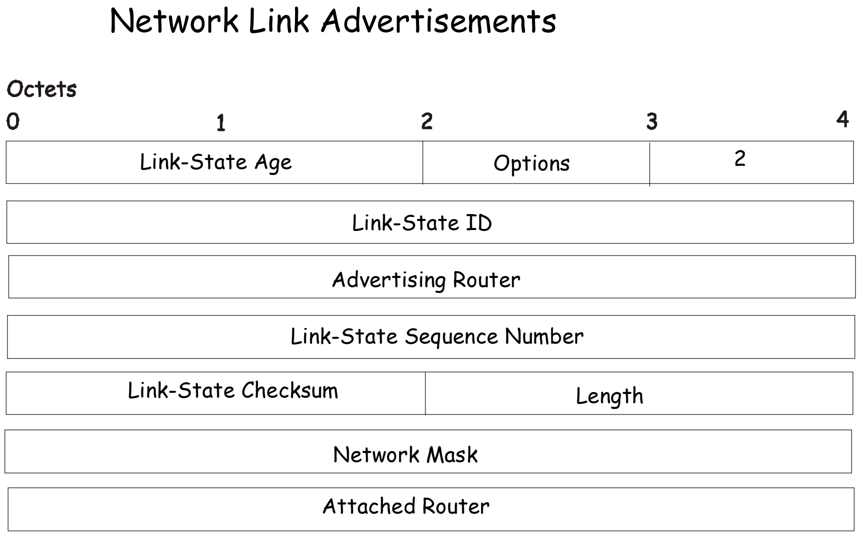


Figure 4- 47. Network Link Advertisements

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 that the difference in the Link State ID field, the format of Type 3 and 4 link state advertisements is identical.

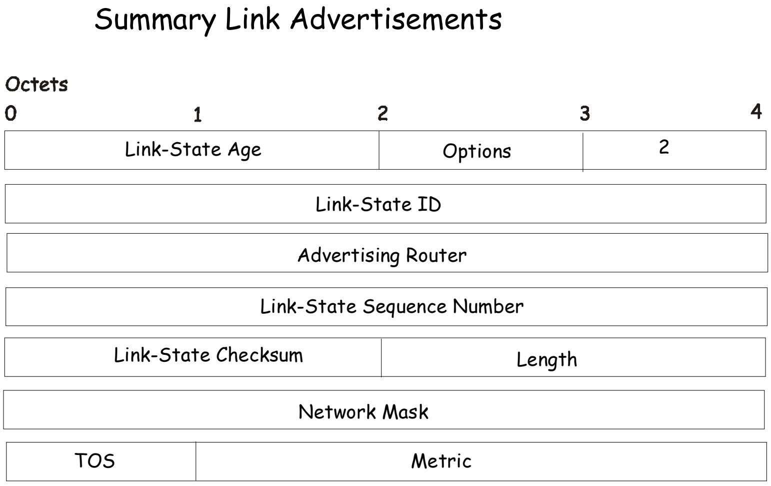


Figure 4- 48. Summary Link Advertisements

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 State ID is always set with 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:

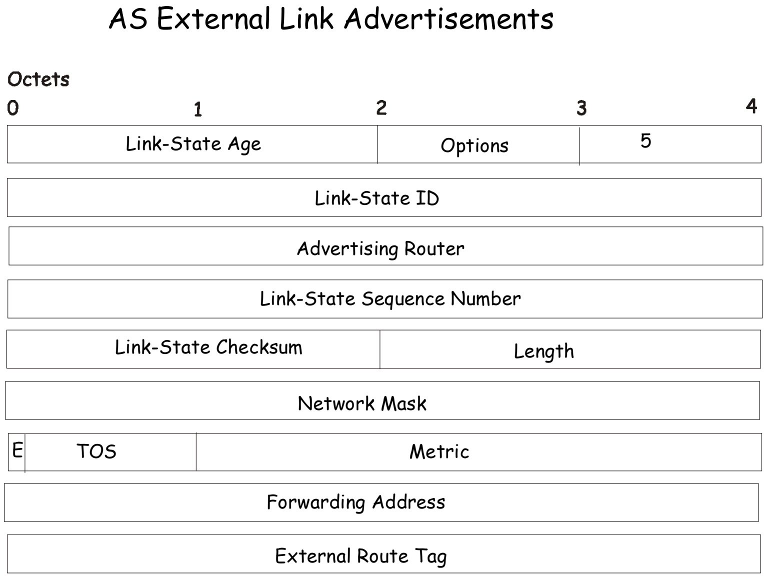


Figure 4- 49. AS External Link Advertisements

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.

Including the NSSA

The NSSA or Not So Stubby Area is a feature that has been added to OSPF so external routes from ASs (Autonomous Systems) can be imported into the OSPF area. As an extension of stub areas, the NSSA feature uses a packet translation system used by BRs (Border Routers) to translate outside routes into the OSPF area. Consider the following example:

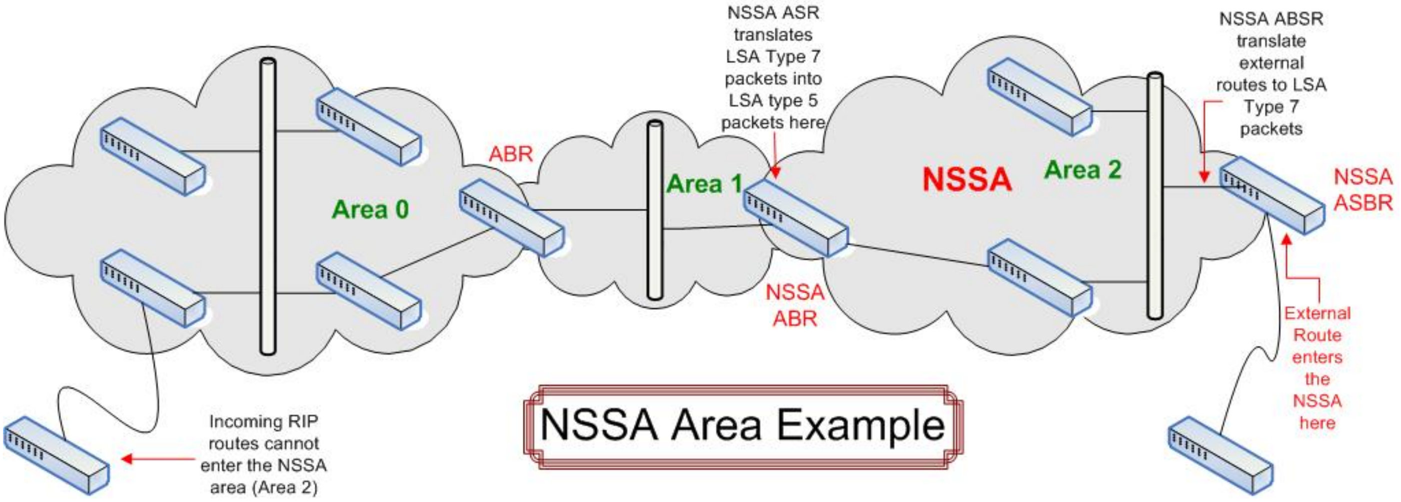

NSSA ASR translates LSA Type 7 packets into LSA type 5 packets here
NSSA ABSR translate external routes to LSA Type 7 packets
ABR
Area 0
Area 1
NSSA
Area 2
NSSA ASBR
NSSA ABR
External Route enters the NSSA here
Incoming RIP routes cannot enter the NSSA area (Area 2)
NSSA Area Example

Figure 4- 50. NSSA Area example

The NSSA ASBR (Not So Stubby Area Autonomous System Border Router) is receiving External Route information and translating it as an LSA Type-7 packet that will be distributed ONLY to switches within the NSSA (Area 2 in the example above). For this route's information to enter another area, the LSA Type-7 packet has to be translated into an LSA Type-5 packet by the NSSA ABR (Area Border Router) and then is distributed to other switches within the other OSPF areas (Area 1 and 2 in the example above). Once completed, new routes are learned and new shortest routes will be determined.

To alleviate any problems with OSPF summary routing due to new routes and packets, all NSSA area border routers (ABR) must support optional importing of LSA type-3 summary packets into the NSSA.

Type-7 LSA Packets

Type-7 LSA (Link State Advertisement) packets are used to import external routes into the NSSA. These packets can originate from NSSA ASBRs or NSSA ABRs and are defined by setting the P-Bit in the LSA type-7 packet header. Each destination network learned from external routes is converted into Type-7 LSA packets. These packets are specific for NSSA switches and the route information contained in these packets cannot leave the area unless translated into Type-5 LSA packets by Area Border Routers. See the following table for a better description of the LSA type-7 packet seen here.

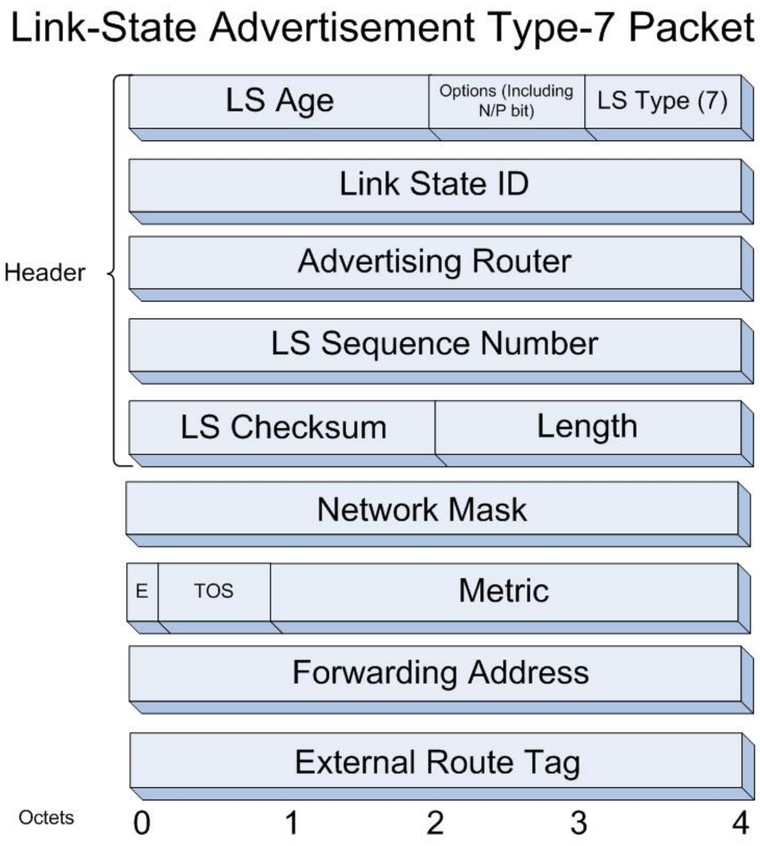


Figure 4- 51. LSA Type-7 Packet

Field	Description
Link State Packet Header	This field will hold information concerning information regarding the LS Checksum, length, LS sequence number, Advertising Router, Link State ID, LS age, the packet type (Type-7), and the options field. The Options byte contains information regarding the N-Bit and the P-Bit, which will be described later in this section.
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. Yet, if the network between the NSSA ASBR and the adjacent AS is advertised in the area as an internal OSFP route, this address will be the next hop address. Conversely, if the network is not advertised as internal, this field should be any of the router's active OSPF interfaces.
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.

The N-Bit

Contained in the options field of the Link State Packet header, the N-Bit is used to ensure that all members of an NSSA agree on the area configurations. Used in conjunction with the E-Bit, these two bits represent the flooding capability of an external LSA. Because type-5 LSAs cannot be flooded into the NSSA, the N-Bit will contain information for sending and receiving LSA type-7 packets, while the E-bit is to be cleared. An additional check must be created for the function that accepts these packets to verify these two bits (N and E-Bit). Bits matching the checking feature will be accepted, while other bit combinations will be dropped.

The P-Bit

Also included in the Options field of the LSA type-7 packet, the P-Bit (propagate) is used to define whether or not to translate the LSA type-7 packet into an LSA type-5 packet for distribution outside the NSSA.

LSA Type-7 Packet Features

- LSA Type-7 address ranges for OSPF areas are defined as a pair, consisting of an IP address and a mask. The packet will also state whether or not to advertise and it will also contain an external route tag.
- The NSSA ASBR will translate external routes into type-7 LSAs to be distributed on the NSSA. NSSA ABRs will optionally translate these type-7 packets into type-5 packets to be distributed among other OSPF areas. These type-5 packets are indiscernible from other type-5 packets. The NSSA does not support type-5 LSAs.
- Once border routers of the NSSA have finished translating or grouping type-7 LSAs into type-5 LSAs, type-5 LSAs should be flushed or reset as a translation or an aggregation of other type-7 LSAs.
- The forwarding addresses contained in translated type-5 LSAs must be set, with the exception of an LSA address range match.

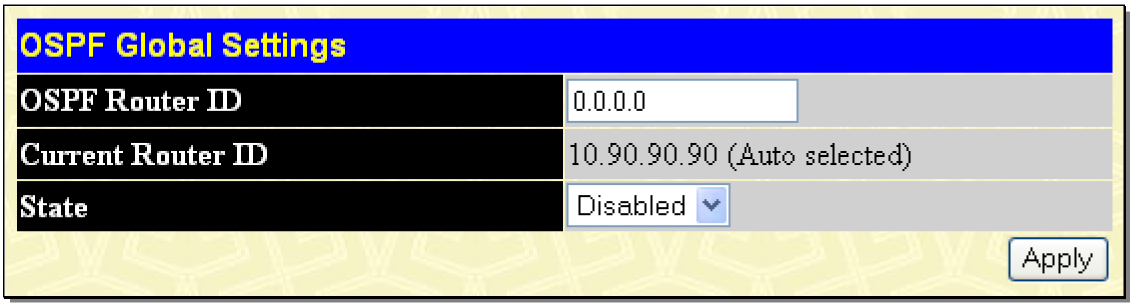
OSPF

The Switch supports Open Shortest Path First (OSPF), a dynamic routing protocol used in Internet Protocol (IP) networks.

OSPF Global Settings

This window allows OSPF to be enabled or disabled on the Switch – without changing the Switch's OSPF configuration. To enable OSPF, first supply an OSPF Router ID (see below), select *Enabled* from the State drop-down menu and click the **Apply** button.

To view the following window, click **L3 Features** > **OSPF** > **OSPF** > **OSPF Global Settings**, as shown below:



OSPF Global Settings

OSPF Router ID: 0.0.0.0

Current Router ID: 10.90.90.90 (Auto selected)

State: Disabled

Figure 4- 52. OSPF Global Settings window

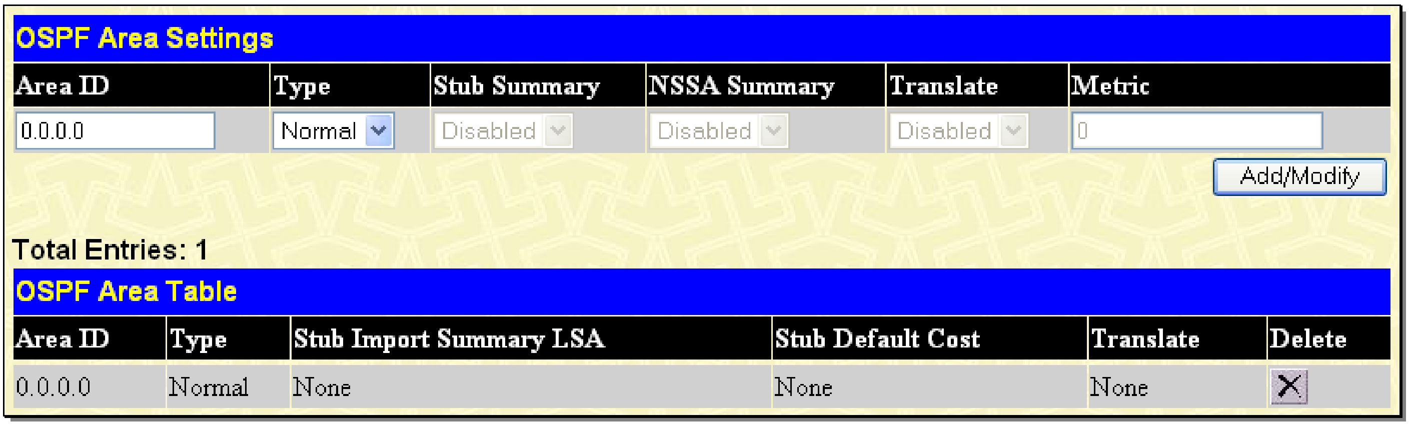
The following parameters are used for general OSPF configuration:

Parameter	Description
OSPF Router 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). If 0.0.0.0 is entered, the highest IP address assigned to the Switch will become the OSPF Router ID. If an active loopback interface exists on the device and the OSPF's router ID is auto-select, the active loopback interface's IP address will be preferred to use as router ID. If there are several active loopback interfaces, it will choose the largest IP address from all the active loopback interfaces as router ID. If there is no loopback interface, the highest IP address assigned to the Switch will become the OSPF Router ID.
Current Router ID	Displays the OSPF Router ID currently in use by the Switch. This Router ID is displayed as a convenience to the user when changing the Switch's OSPF Router ID.
State	Allows OSPF to be enabled or disabled globally on the Switch without changing the OSPF configuration.

OSPF Area Settings

This window allows the configuration of OSPF Area IDs and to designate these areas as Normal, Stub or NSSA. Normal OSPF areas allow Link-State Database (LSDB) advertisements of routes to networks that are external to the area. Stub areas do not allow the LSDB advertisement of external routes. Stub areas use a default summary external route (0.0.0.0 or Area 0) to reach external destinations.

To set up an OSPF area configuration, click **Layer 3 Features > OSPF > OSPF > OSPF Area Settings**, as shown below:



OSPF Area Settings

Area ID	Type	Stub Summary	NSSA Summary	Translate	Metric
0.0.0.0	Normal	Disabled	Disabled	Disabled	0

Total Entries: 1

OSPF Area Table

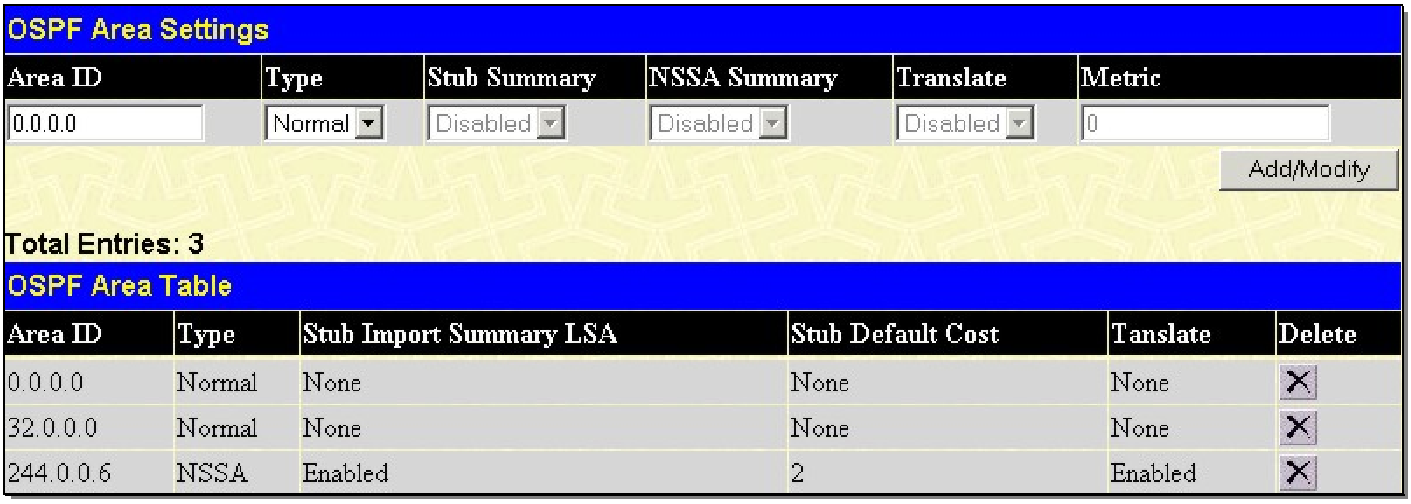
Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Translate	Delete
0.0.0.0	Normal	None	None	None	☒

Figure 4- 53. OSPF Area Settings 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 Summary drop-down menu and determine the Metric. 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.



OSPF Area Settings

Area ID	Type	Stub Summary	NSSA Summary	Translate	Metric
0.0.0.0	Normal	Disabled	Disabled	Disabled	0

Total Entries: 3

OSPF Area Table

Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Tanslate	Delete
0.0.0.0	Normal	None	None	None	☒
32.0.0.0	Normal	None	None	None	☒
244.0.0.6	NSSA	Enabled	2	Enabled	☒

Figure 4- 54. OSPF Area Settings example window

See the parameter descriptions below for information on the **OSPF Area Settings** window. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

The Area ID settings are as follows:

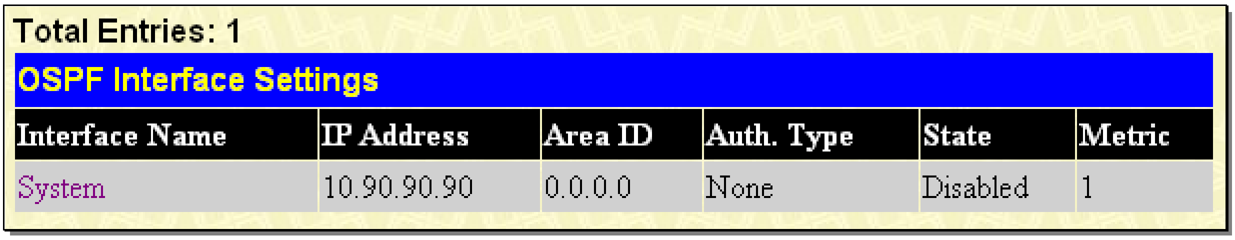
Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	This field can be toggled between *Normal*, *Stub* and *NSSA* using the pull-down menu. When it is toggled to *Stub*, the additional field Stub Summary will then be capable of being configured. Choosing NSSA allows the NSSA Summary field and the Translate field to be configured.

Stub Summary	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
NSSA Summary	Use the pull-down menu to enable or disable the importing of OSPF summary routes into the NSSA as Type-3 summary LSAs. The default is *Disabled*. This field can only be configured if NSSA is chosen in the Type field.
Translate	Use the pull-down menu to enable or disable the translating of Type-7 LSAs into Type-5 LSAs, so that they can be distributed outside of the NSSA. The default is *Disabled*. This field can only be configured if NSSA is chosen in the Type field.
Metric	Displays the default cost for the route to the stub of between *0* and *65,535*. The default is *1*. For NSSA areas, the metric field determines the cost of traffic entering the NSSA area.

OSPF Interface Settings

This window is used to set up OSPF 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 window for that interface.

To view this window, click **L3 Features > OSPF > OSPF > OSPF Interface Settings**, as shown below:



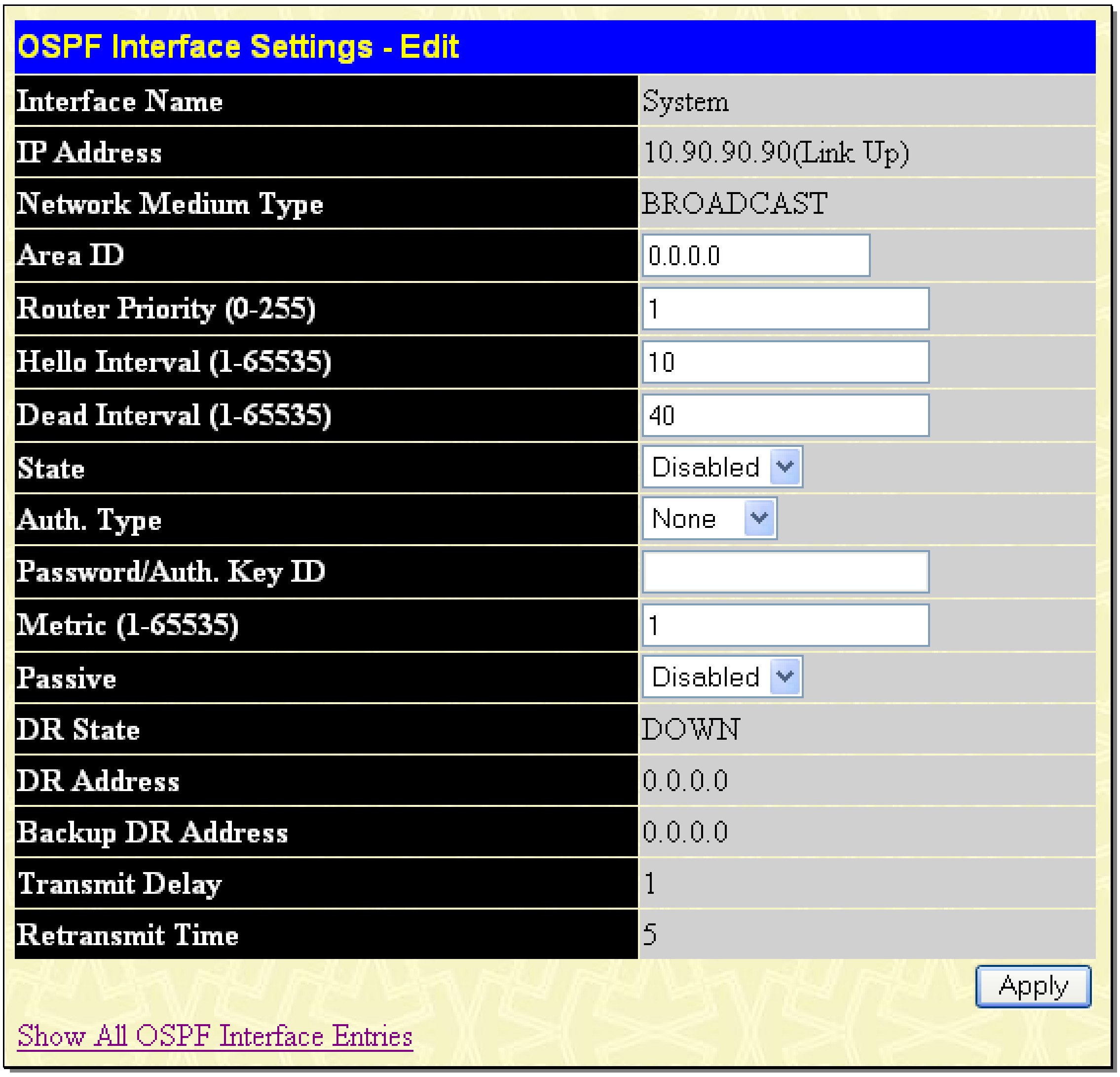
Total Entries: 1

OSPF Interface Settings

Interface Name	IP Address	Area ID	Auth. Type	State	Metric
System	10.90.90.90	0.0.0.0	None	Disabled	1

Figure 4- 55. OSPF Interface Settings window

Click the hyperlinked name of the interface to configure the settings for OSPF, which will give access to the following window:



OSPF Interface Settings - Edit

Interface Name	System
IP Address	10.90.90.90(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
Passive	Disabled
DR State	DOWN
DR Address	0.0.0.0
Backup DR Address	0.0.0.0
Transmit Delay	1
Retransmit Time	5

Figure 4- 56. OSPF Interface Settings - Edit window

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

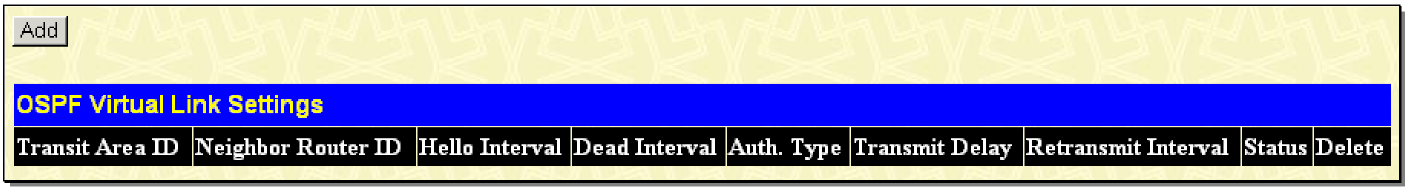
Parameter	Description

Interface Name	Displays the IP interface previously configured on the Switch.
IP Address	Displays the IP address of the IP interface to be edited.
Network Medium Type	Displays the network medium type of the IP interface to be edited.
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 Settings** window. 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 eight 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*.
Passive	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. When this field is disabled, it denotes an active interface.
DR State	DR State is a read-only field describing the Designated Router state of the IP interface. This field may 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.

OSPF Virtual Link Settings

This window shows the current OSPF Virtual Interface Settings. There are no virtual interface settings configured by default, so the first time this table is viewed there will be no interfaces listed. To add a new OSPF virtual interface configuration set to the table, click the **Add** button. A new window appears (see below). To change an existing configuration, click on the hyperlinked Transit Area ID for the set you want to change. The window to modify an existing set is the same as the window used to add a new one.

To view this window, click **L3 Features > OSPF > OSPF > OSPF Virtual Link Settings**, as shown below:

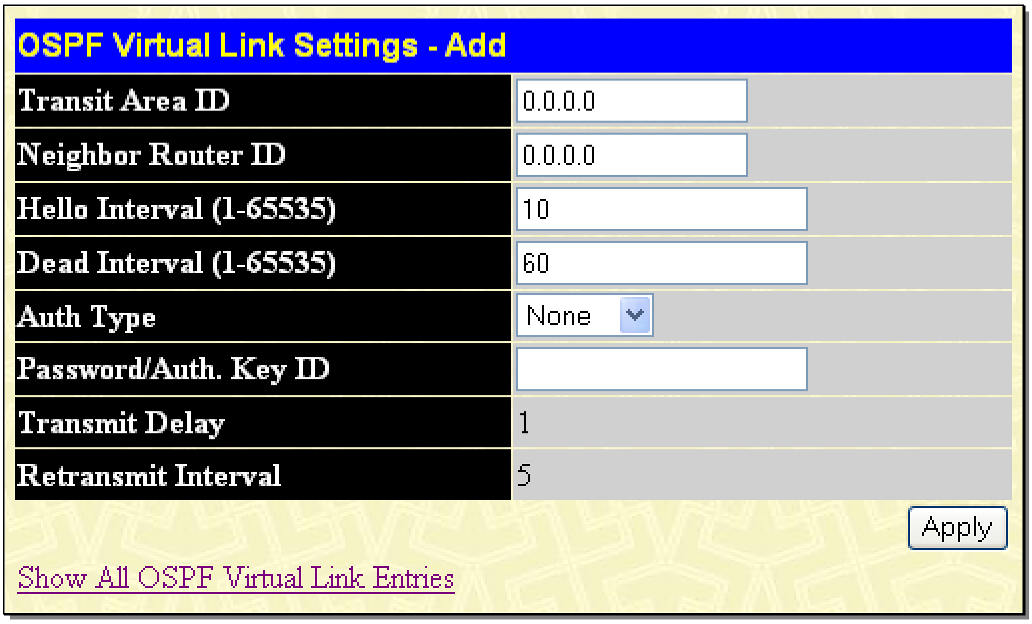


OSPF Virtual Link Settings

Transit Area ID	Neighbor Router ID	Hello Interval	Dead Interval	Auth. Type	Transmit Delay	Retransmit Interval	Status	Delete

Figure 4- 57. OSPF Virtual Link Settings window

To delete an existing configuration, click the corresponding ☒ button in the Delete column. The status of the virtual interface appears in the Status column.


OSPF Virtual Link Settings - Add

Transit Area ID	0.0.0.0
Neighbor Router ID	0.0.0.0
Hello Interval (1-65535)	10
Dead Interval (1-65535)	60
Auth Type	None
Password/Auth. Key ID	
Transmit Delay	1
Retransmit Interval	5

Figure 4- 58. OSPF Virtual Link Settings – Add window

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 ID	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** window.

Password/Auth. Key ID	Enter a case-sensitive password for simple authorization or enter the MD5 key you set in the **MD5 Key Settings** window.
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.
Retransmit Interval	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. This field is fixed at 5 seconds.

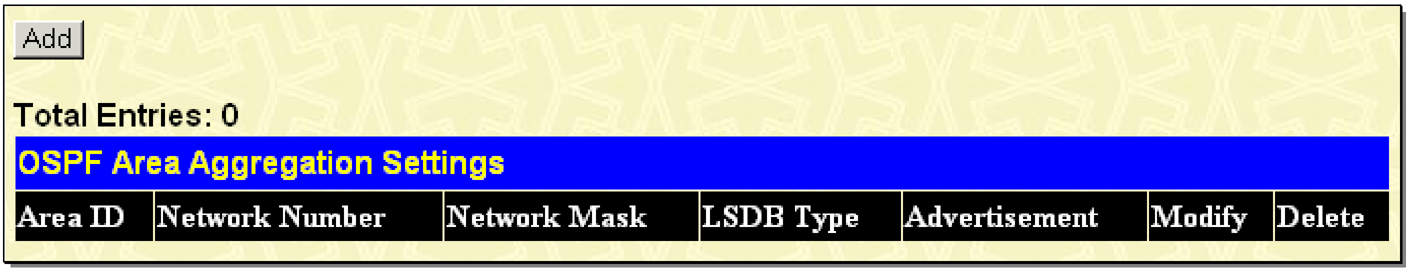
Click **Apply** to implement changes made.

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. There are no aggregation settings configured by default, so there will not be any listed the first accessing the window. To add a new OSPF Area Aggregation setting, click the **Add** button. A new window (pictured below) appears. To change an existing configuration, click on the corresponding **Modify** button for the set you want to change. The window to modify an existing configuration is the same as the window used to add a new one.

To view this window, click **L3 Features** > **OSPF** > **OSPF** > **OSPF Area Aggregation Settings**, as shown below:



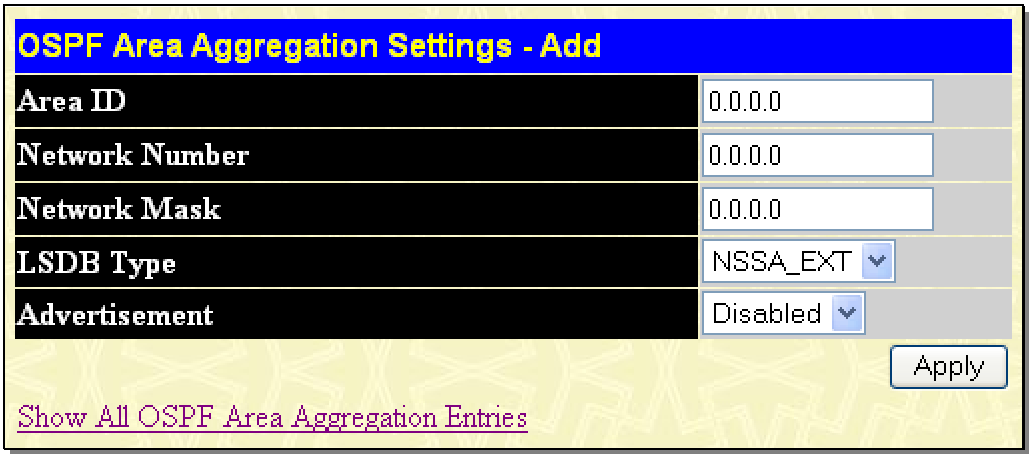
Total Entries: 0

OSPF Area Aggregation Settings

Area ID	Network Number	Network Mask	LSDB Type	Advertisement	Modify	Delete

Figure 4- 59. OSPF Area Aggregation Settings window

Use the window below to change settings or add a new OSPF Area Aggregation setting.



OSPF Area Aggregation Settings - Add

Area ID	0.0.0.0
Network Number	0.0.0.0
Network Mask	0.0.0.0
LSDB Type	NSSA_EXT
Advertisement	Disabled

Figure 4- 60. OSPF Area Aggregation Settings – Add window

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** window. To view the table, click the Show All OSPF Area Aggregation Entries link to return to the previous window.

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

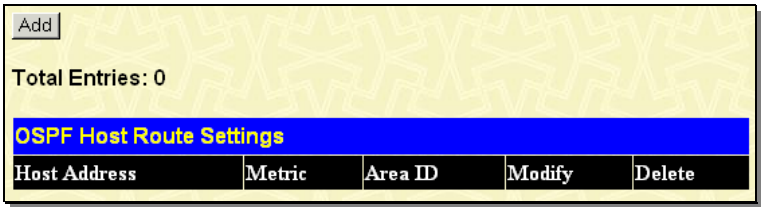
Parameter	Description
Area ID	Allows the entry the OSPF Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the Switch.
Network Number	Sometimes called the Network Address. The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area above.
Network Mask	The corresponding network mask for the Network Number specified above.
LSDB Type	Specifies the type of address aggregation. The user may choose *Summary* or *NSSA-EXT*, depending on the type of aggregation being configured. The default setting is Summary.
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 add a new OSPF Route, click the **Add** button. Configure the setting in the window that appears. The **Add** and **Modify** windows for OSPF host route settings are nearly identical. The difference between them is 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 corresponding Modify button in the list for the configuration to change and proceed to change the metric or area ID.

To configure OSPF host routes, click **L3 Features** > **OSPF**> **OSPF** > **OSPF Host Route Settings**, as shown below:



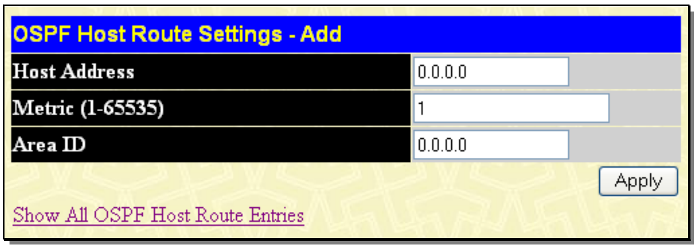
Total Entries: 0

OSPF Host Route Settings

Host Address	Metric	Area ID	Modify	Delete

Figure 4- 61. OSPF Host Route Settings window

Use the window below to add an OSPF host route. To remove an entry from the table, click its corresponding ☒ under the Delete heading.


OSPF Host Route Settings - Add

Host Address	0.0.0.0
Metric (1-65535)	1
Area ID	0.0.0.0

Figure 4- 62. OSPF Host Route Settings – Add window

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** window. 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 (1-65535)	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.

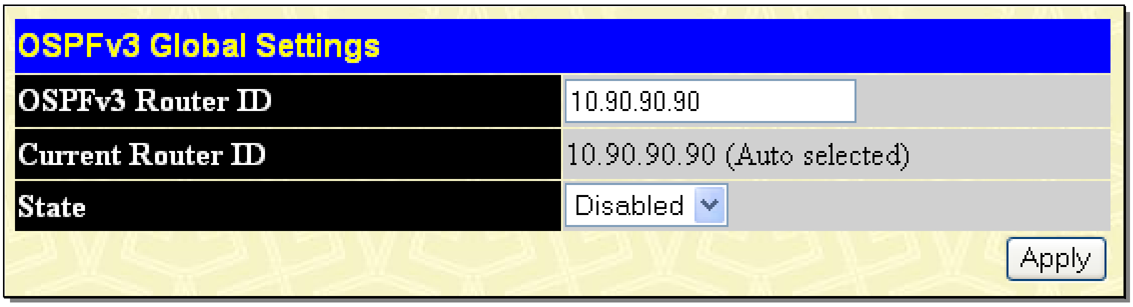
OSPFv3

The Switch supports Open Shortest Path First (OSPF) version 3, a dynamic routing protocol used in Internet Protocol (IP) version 6 networks.

OSPFv3 Global Settings

This window allows OSPFv3 to be enabled or disabled on the Switch – without changing the Switch's OSPFv3 configuration. To enable OSPFv3, first supply an OSPFv3 Router ID (see below), select *Enabled* from the State drop-down menu and click the **Apply** button.

To view the following window, click **L3 Features** > **OSPF** > **OSPFv3** > **OSPFv3 Global Settings**, as shown below:



OSPFv3 Global Settings

OSPFv3 Router ID	10.90.90.90
Current Router ID	10.90.90.90 (Auto selected)
State	Disabled

Figure 4- 63. OSPFv3 Global Settings window

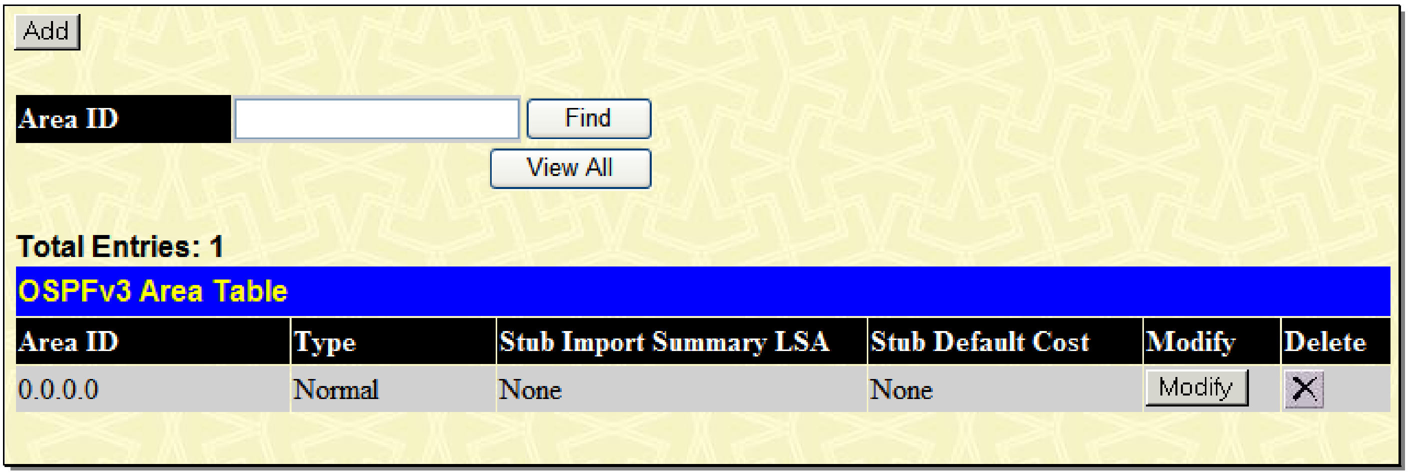
The following parameters are used for general OSPF configuration:

Parameter	Description
OSPFv3 Router ID	User may enter a 32-bit number in the form of an IPv4 address that uniquely identifies the router in the OSPFv3 domain. The setting *0.0.0.0* means auto-selected. The Switch will select the maximum interface's IPv4 address to be the router ID. The default value of OSPFv3 router ID is *0.0.0.0* (auto-selected).
Current Router ID	Displays the OSPFv3 Router ID currently in use by the Switch. This router ID is displayed as a convenience to the user when changing the Switch's OSPFv3 Router ID.
State	Allows OSPFv3 to be enabled or disabled globally on the Switch without changing the OSPFv3 configuration.

OSPFv3 Area Settings

This window allows the configuration of OSPFv3 Area IDs and to designate these areas as Normal or Stub. Normal OSPFv3 areas allow Link-State Database (LSDB) advertisements of routes to networks that are external to the area. Stub areas do not allow the LSDB advertisement of external routes. Stub areas use a default summary external route (0.0.0.0 or Area 0) to reach external destinations.

To view the following window, click **L3 Features** > **OSPF** > **OSPFv3** > **OSPFv3 Area Settings**, as shown below:



Total Entries: 1

OSPFv3 Area Table

Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Modify	Delete
0.0.0.0	Normal	None	None	Modify	☒

Figure 4- 64. OSPFv3 Area Table window

To search for an entry by Area ID, click the **Find** button.

To display all Area entries, click the **View All** button.

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To add an OSPFv3 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 Summary drop-down menu and determine the Metric. Click the **Add** 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.

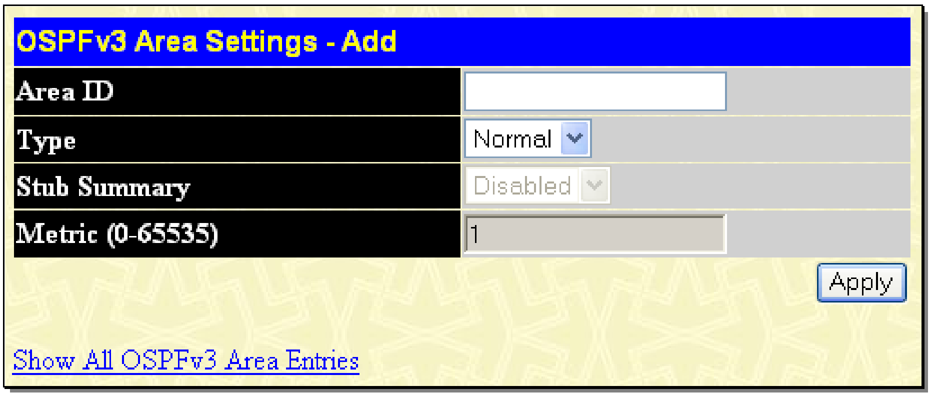
To change an existing set in the list, type the Area ID of the set you want to change, make the changes and click the **Modify** button. The modified OSPFv3 area type will appear in the table.

See the parameter descriptions below for information on the **OSPFv3 Area Tables** window. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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 OSPFv3 area in the OSPFv3 domain.
Type	This field can be toggled between *Normal* and *Stub* using the pull-down menu. When it is toggled to *Stub*, the additional field Stub Summary will then be capable of being configured.
Stub Import Summary LSA	Displays whether or not the selected OSPFv3 Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Stub Default Cost	Displays the default OSPFv3 cost for the route to the stub of between *0* and *65,535*. The default is *1*.

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

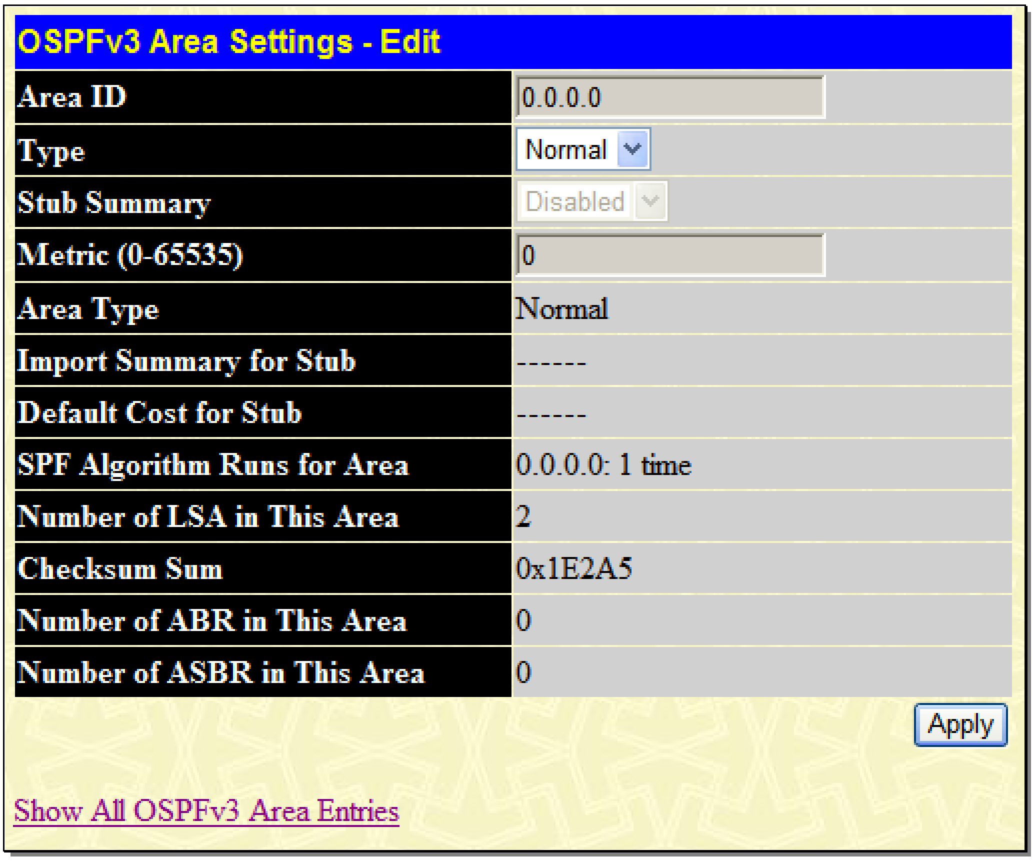


OSPFv3 Area Settings - Add

Area ID	
Type	Normal
Stub Summary	Disabled
Metric (0-65535)	1

Figure 4- 65. OSPFv3 Area Settings - Add window

Clicking the **Modify** button on the **OSPFv3 Area Table** window will reveal the following window to configure:



OSPFv3 Area Settings - Edit

Area ID	0.0.0.0
Type	Normal
Stub Summary	Disabled
Metric (0-65535)	0
Area Type	Normal
Import Summary for Stub	------
Default Cost for Stub	------
SPF Algorithm Runs for Area	0.0.0.0: 1 time
Number of LSA in This Area	2
Checksum Sum	0x1E2A5
Number of ABR in This Area	0
Number of ASBR in This Area	0

Figure 4- 66. OSPFv3 Area Settings - Edit window

The OSPFv3 Area configurable settings are as follows:

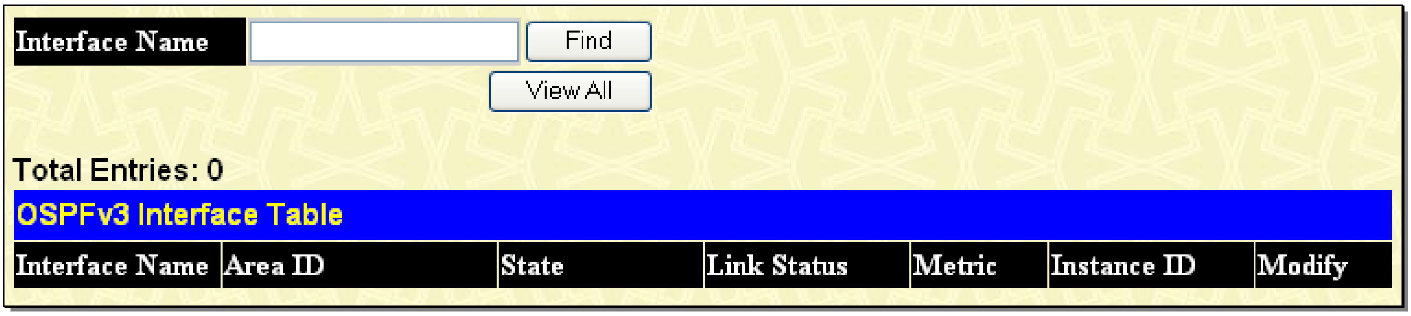
Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPFv3 area in the OSPFv3 domain.
Type	This field can be toggled between *Normal* and *Stub* using the pull-down menu. When it is toggled to *Stub*, the additional field Stub Summary will then be capable of being configured.
Stub Summary	Displays whether or not the selected OSPFv3 Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Metric (0-65535)	Displays the default OSPFv3 cost for the route to the stub of between *0* and *65,535*. The default is *1*.

Click **Apply** to implement changes made.

OSPFv3 Interface Settings

This window is used to set up OSPFv3 interfaces. To change settings for an existing IP interface, click on the hyperlinked name of the interface to see the configuration window for that interface.

To view the following window, click **L3 Features** > **OSPF** > **OSPFv3** > **OSPFv3 Interface Settings**, as shown below:



Interface Name

Total Entries: 0

OSPFv3 Interface Table

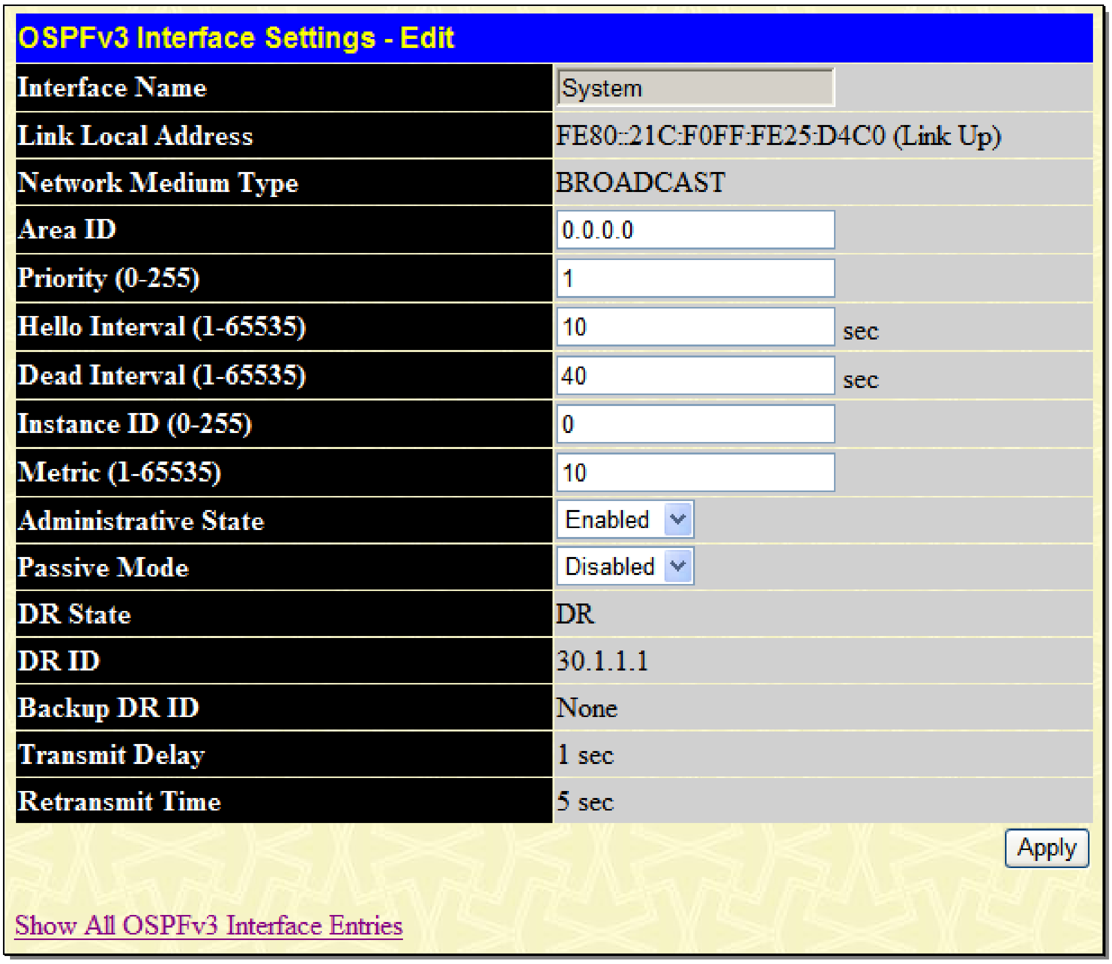
Interface Name	Area ID	State	Link Status	Metric	Instance ID	Modify

Figure 4- 67. OSPFv3 Interface Table window

To search for an entry by interface name, click the **Find** button.

To display all OSPFv3 interface entries, click the **View All** button.

To configure the settings for a specifc entry, click the **Modify** button, which will give access to the following window:



OSPFv3 Interface Settings - Edit

Interface Name	System
Link Local Address	FE80::21C:F0FF:FE25:D4C0 (Link Up)
Network Medium Type	BROADCAST
Area ID	0.0.0.0
Priority (0-255)	1
Hello Interval (1-65535)	10 sec
Dead Interval (1-65535)	40 sec
Instance ID (0-255)	0
Metric (1-65535)	10
Administrative State	Enabled
Passive Mode	Disabled
DR State	DR
DR ID	30.1.1.1
Backup DR ID	None
Transmit Delay	1 sec
Retransmit Time	5 sec

Figure 4- 68. OSPFv3 Interface Settings - Edit window

Configure each IP interface individually using the **OSPFv3 Interface Settings - Edit** window. Click the **Apply** button when you have entered the settings. The new configuration appears listed in the **OSPFv3 Interface Table** window. To return to the **OSPFv3 Interface Table** window, click the Show All OSPFv3 Interface Entries link.

OSPFv3 interface settings are described below. Some OSPFv3 interface settings require previously configured OSPFv3 settings. Read the descriptions below for details.

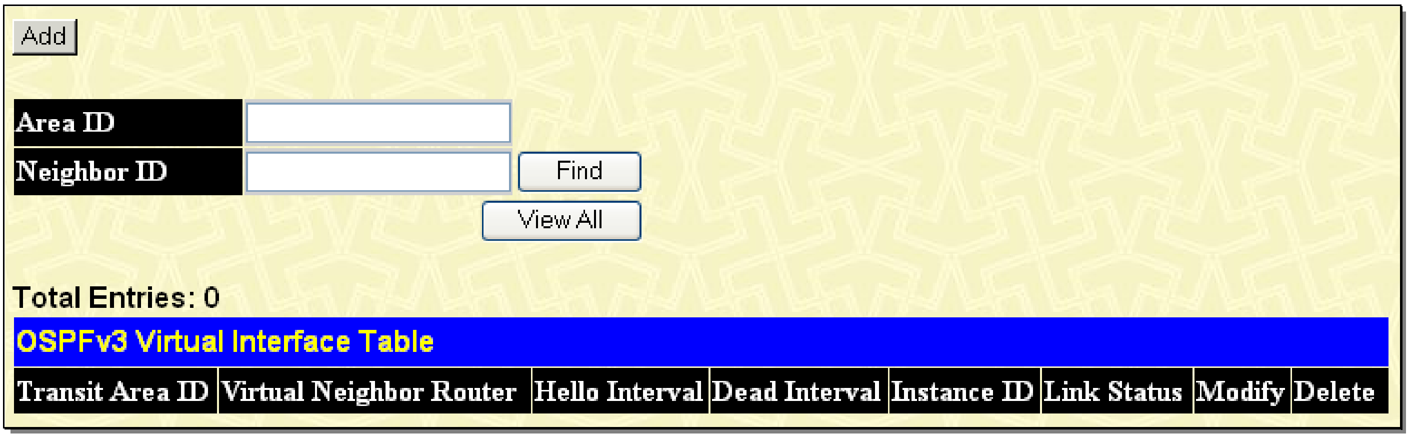
Parameter	Description

Interface Name	Displays the entry of an IP interface previously configured on the Switch.
Area ID	Allows the entry of an OSPFv3 Area ID configured above.
Priority (0-255)	Allows the entry of a number between *0* and *255* representing the OSPFv3 priority of the selected interface. 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 OSPFv3 Hello packets, in seconds. Between *1* and *65535* seconds can be specified. The Hello Interval, Dead Interval, and Instance 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.
Instance ID (0-255)	The instance ID of the interface. Its default value is *0*.
Metric (1-65535)	This field allows the entry of a number between *1* and *65,535* that is representative of the OSPFv3 cost of reaching the selected OSPFv3 interface. The default metric is *1*.
Administrative State	Allows the OSPFv3 interface to be *Enabled* or *Disabled* for the selected area without changing the configuration for that area.
Passive Mode	The user may select Active or Passive for this OSPFv3 interface. Active interfaces actively advertise OSPFv3 to routers on other Intranets that are not part of this specific OSPFv3 group. Passive interface will not advertise to any other routers than those within its OSPFv3 intranet. When this field is disabled, it denotes an active interface.
DR State	DR State is a read-only field describing the Designated Router state of the IP interface. This field may 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 OSPFv3 Hello Protocol of the Switch.
DR ID	The IP address of the aforementioned Designated Router.
Backup DR ID	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.

OSPFv3 Virtual Interface Settings

This window shows the current OSPFv3 Virtual Interface Settings. There are no virtual interface settings configured by default, so the first time this table is viewed there will be no interfaces listed. To add a new OSPFv3 virtual interface configuration set to the table, click the **Add** button. A new window appears (see below). To change an existing configuration, click on the hyperlinked Transit Area ID for the set you want to change. The window to modify an existing set is the same as the window used to add a new one.

To view the following window, click **L3 Features** > **OSPF** > **OSPFv3** > **OSPFv3 Virtual Interface Settings**, as shown below:



Area ID	
Neighbor ID	

Total Entries: 0

OSPFv3 Virtual Interface Table

Transit Area ID	Virtual Neighbor Router	Hello Interval	Dead Interval	Instance ID	Link Status	Modify	Delete

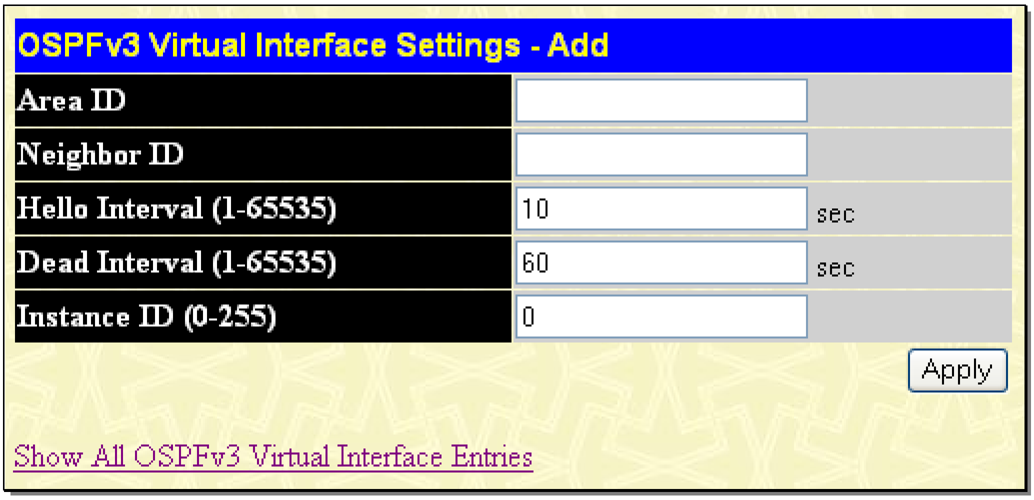
Figure 4- 69. OSPFv3 Virtual Interface Table window

To search for an entry by Area ID and Neighbor ID, click the **Find** button.

To display all virtual interface entries, click the **View All** button.

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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

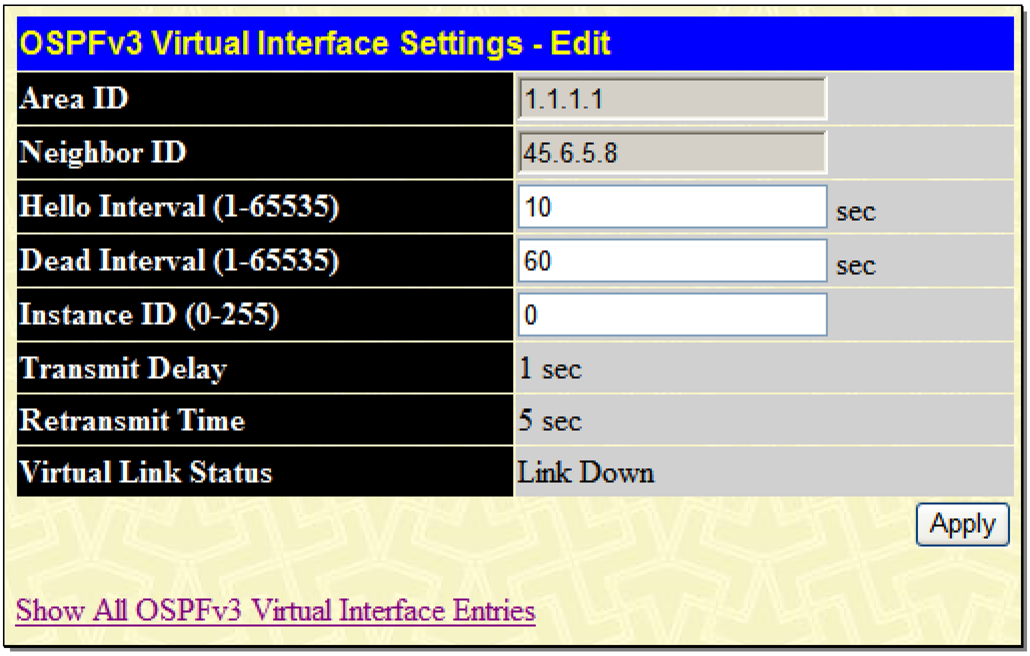


OSPFv3 Virtual Interface Settings - Add

Area ID		
Neighbor ID		
Hello Interval (1-65535)	10	sec
Dead Interval (1-65535)	60	sec
Instance ID (0-255)	0	

Figure 4- 70. OSPFv3 Virtual Interface Settings - Add window

To edit an entry in the OSPFv3 Virtual Interface Table window, click the Modify button.



OSPFv3 Virtual Interface Settings - Edit

Area ID	1.1.1.1	
Neighbor ID	45.6.5.8	
Hello Interval (1-65535)	10	sec
Dead Interval (1-65535)	60	sec
Instance ID (0-255)	0	
Transmit Delay	1 sec	
Retransmit Time	5 sec	
Virtual Link Status	Link Down	

Figure 4- 71. OSPFv3 Virtual Interface Settings - Edit window

Configure the following parameters if you are adding or changing an OSPFv3 Virtual Interface:

Parameter	Description
Area ID	Allows the entry of an OSPFv3 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 ID	The OSPFv3 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 OSPFv3 Hello packets, in seconds. Enter a value between *1* and *65535* seconds. The Hello Interval, Dead Interval, and Instance 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.
Instance ID (0-255)	The instance ID of the interface. Its default value is *0*.
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.
Retransmit Time	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. This field is fixed at 5 seconds.
Virtual Link Status	This displays the state of the current virtual link.

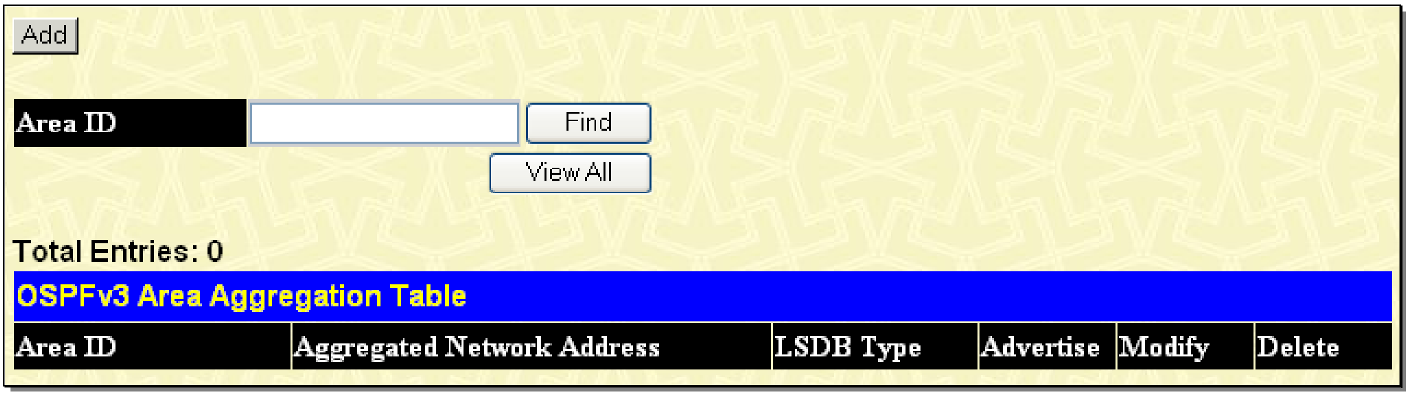
Click **Apply** to implement changes made.

NOTE: For OSPFv3 to function properly, some settings should be identical on all participating OSPFv3 devices. These settings include Hello Interval and Dead Interval.

OSPFv3 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. There are no aggregation settings configured by default, so there will not be any listed the first accessing the window. To add a new OSPFv3 Area Aggregation setting, click the **Add** button. A new window (pictured below) appears. To change an existing configuration, click on the corresponding **Modify** button for the set you want to change. The window to modify an existing configuration is the same as the window used to add a new one.

To view the following window, click **L3 Features** > **OSPF** > **OSPFv3** > **OSPFv3 Area Aggregation Settings**, as shown below:



Total Entries: 0

OSPFv3 Area Aggregation Table

Area ID	Aggregated Network Address	LSDB Type	Advertise	Modify	Delete

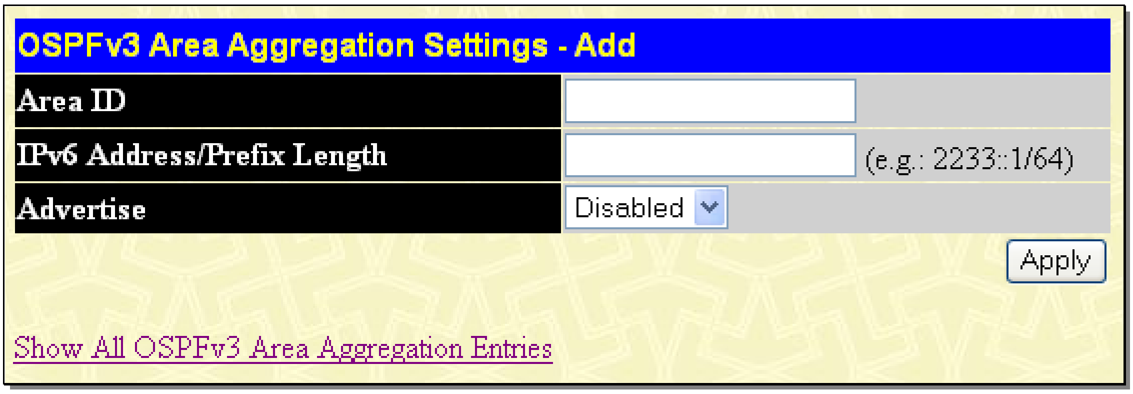
Figure 4- 72. OSPFv3 Area Aggregation Table window

To search for an entry by Area ID, click the **Find** button.

To display all OSPFv3 area aggregation entries, click the **View All** button.

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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

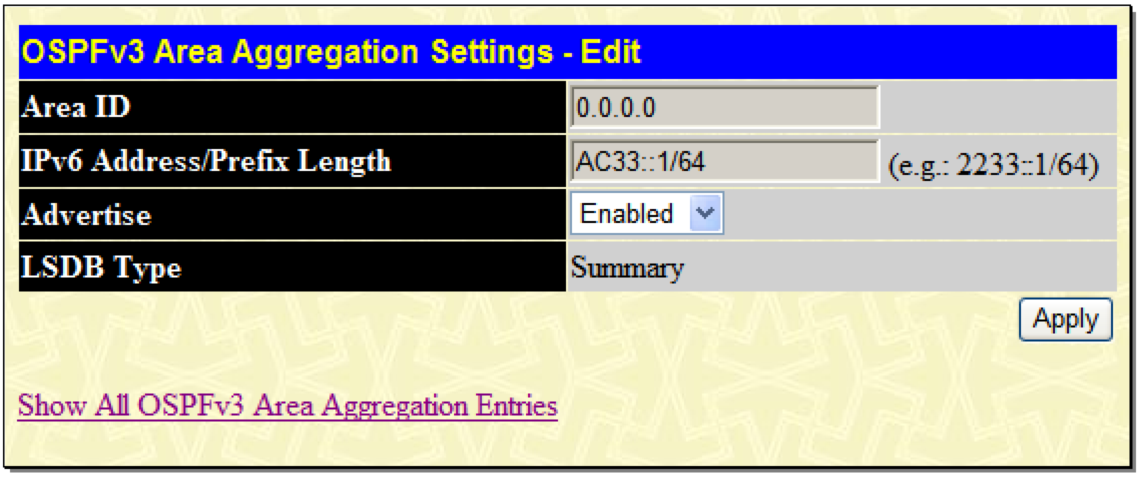


OSPFv3 Area Aggregation Settings - Add

Area ID	
IPv6 Address/Prefix Length	(e.g.: 2233::1/64)
Advertise	Disabled

Figure 4- 73. OSPFv3 Area Aggregation Settings - Add window

To edit an entry in the **OSPFv3 Area Aggregation Table** window, click the **Modify** button.



OSPFv3 Area Aggregation Settings - Edit

Area ID	0.0.0.0
IPv6 Address/Prefix Length	AC33::1/64 (e.g.: 2233::1/64)
Advertise	Enabled
LSDB Type	Summary

Figure 4- 74. OSPFv3 Area Aggregation Settings - Edit window

Specify the OSPFv3 aggregation settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPFv3 Area Aggregation Settings** window. To view the table, click the Show All OSPFv3 Aggregation Entries link to return to the previous window.

Use the following parameters to configure the following settings for OSPFv3 Area Aggregation Settings:

Parameter	Description
Area ID	Allows the entry the OSPFv3 Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the Switch.
IPv6 Address/Prefix Length	Specify the IPv6 network address of the aggregation.
Advertise	Select *Enabled* or *Disabled* to determine whether the selected OSPFv3 Area will advertise its summary LSDB.
LSDB Type	The LSDB type is Summary.

Click **Apply** to implement changes made.

DHCP Server

For this release, the Switch now has the capability to act as a DHCP server to devices within its locally attached network. 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.

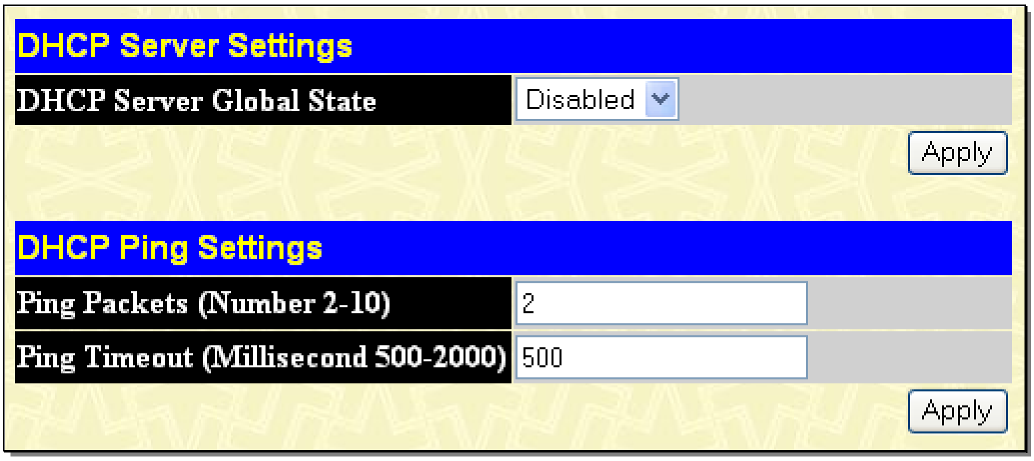
Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address. The Switch supports 1024 DHCP pool entries along with eight pools.

To begin configuring the Switch as a DHCP Server, open the **L3 Features** folder, then the **DHCP Server** folder, which will display five 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**, as shown below:



DHCP Server Settings

DHCP Server Global State: Disabled

DHCP Ping Settings

Ping Packets (Number 2-10): 2

Ping Timeout (Millisecond 500-2000): 500

Figure 4- 75. DHCP Server Settings window

The following parameters may be configured.

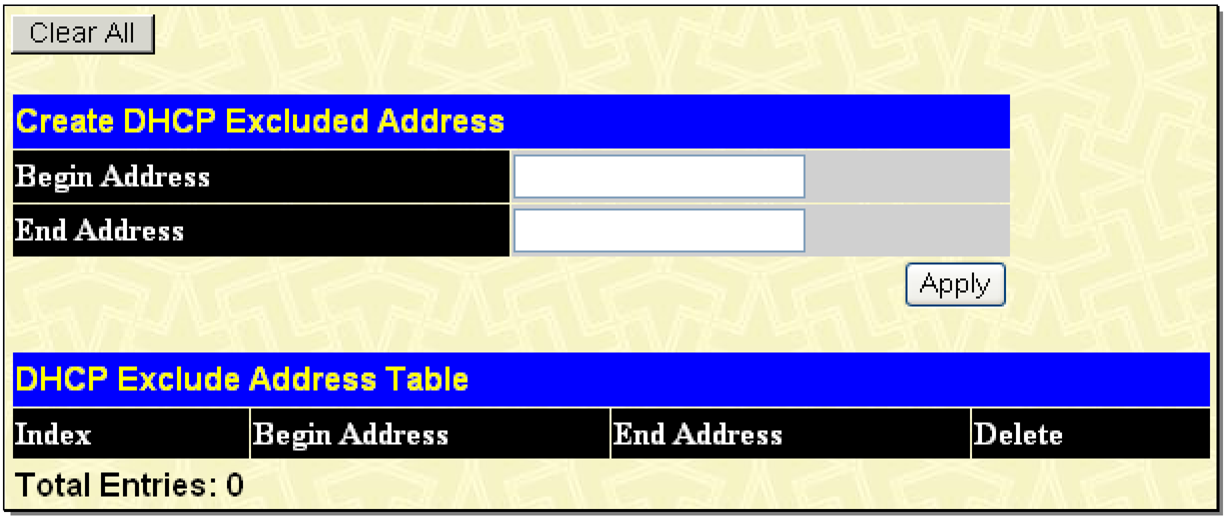
Parameter	Description
DHCP Server Global State	Use the pull-down menu to globally enable or disable the switch as a DHCP server.
Ping Packets (Numbers 2-10)	Enter a number between *2* and *10* to denote the number of ping packets that the Switch will send out on the network containing the IP address 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 (Millisecond 500-2000)	The user may set a time between *500* and *2000* milliseconds that the Switch will wait before timing out a ping packet. The default setting is *500* milliseconds.

Click **Apply** to implement changes made.

DHCP Server Exclude 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 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 Exclude Address Table in the bottom half of the window, as shown below:

To view this window, click **L3 features > DHCP Server > DHCP Server Exclude Address Settings**, as shown below:



Clear All

Create DHCP Excluded Address

Begin Address	
End Address	

Apply

DHCP Exclude Address Table

Index	Begin Address	End Address	Delete

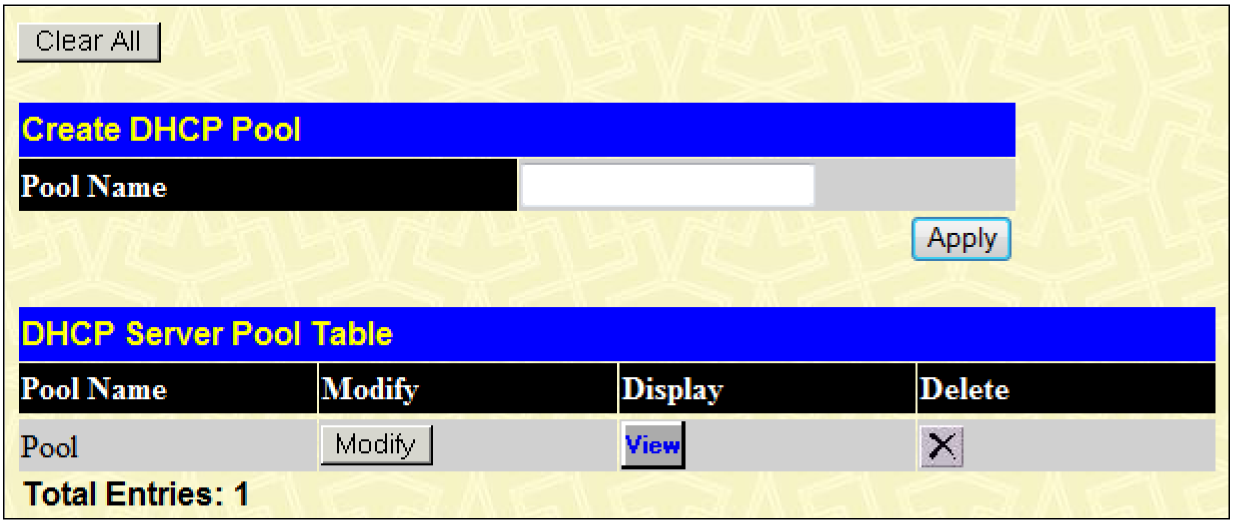
Total Entries: 0

Figure 4- 76. Create DHCP Excluded Address window

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 pool by clicking its corresponding **Modify** button.

To view the following window, click **L3 features > DHCP Server > DHCP Server Pool Settings**, as shown below:



Clear All

Create DHCP Pool

Pool Name	

Apply

DHCP Server Pool Table

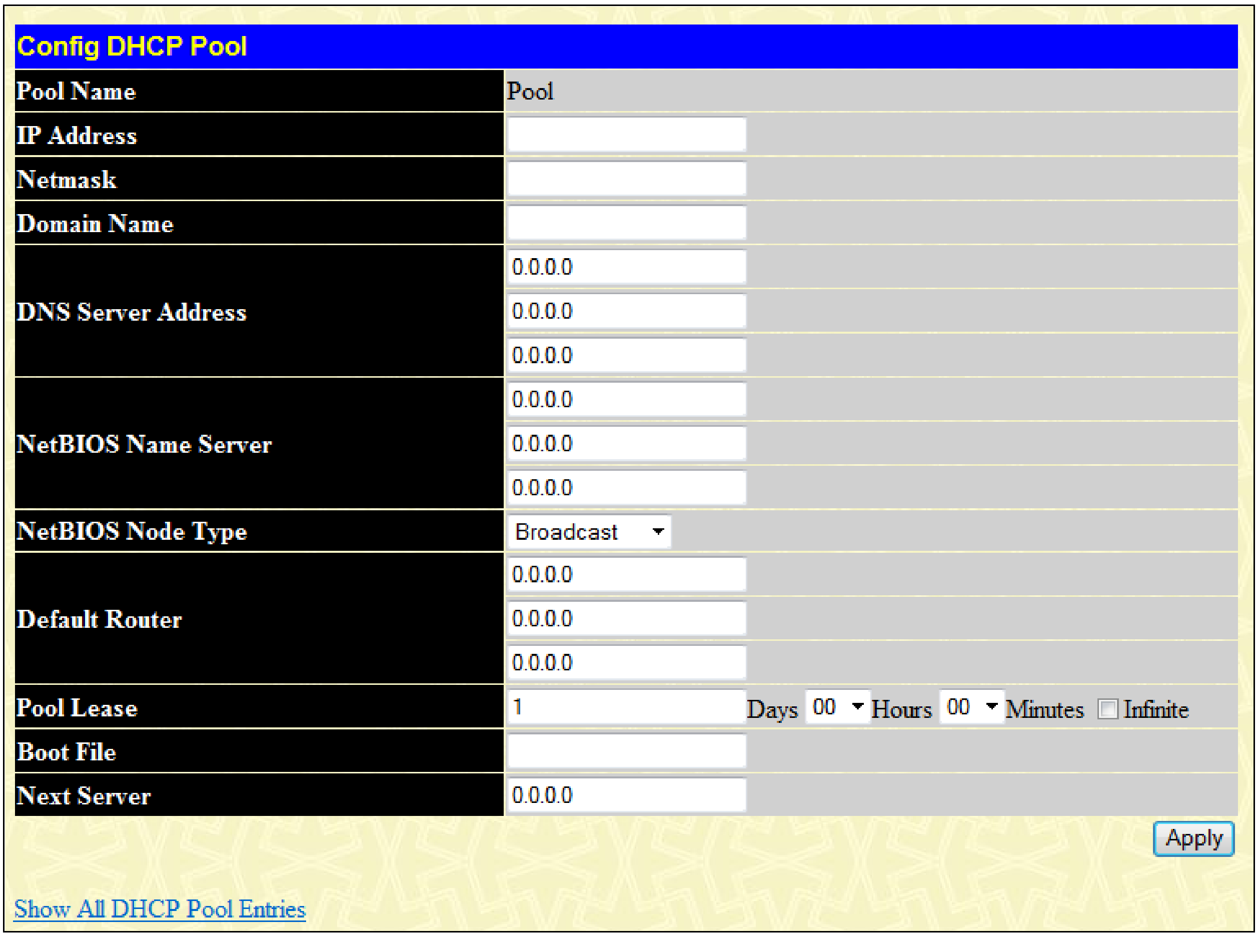
Pool Name	Modify	Display	Delete
Pool	Modify	View	☒

Total Entries: 1

Figure 4- 77. Create DHCP Pool window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

Clicking the **Modify** button of a corresponding DHCP Pool will lead to the following window in which users can adjust the settings for the specific DHCP pool table.



Config DHCP Pool

Pool Name	Pool
IP Address	
Netmask	
Domain Name	
DNS Server Address	0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Name Server	0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Node Type	Broadcast
Default Router	0.0.0.0 0.0.0.0 0.0.0.0
Pool Lease	1 Days 00 Hours 00 Minutes □ Infinite
Boot File	
Next Server	0.0.0.0

Figure 4- 78. Config DHCP Pool window

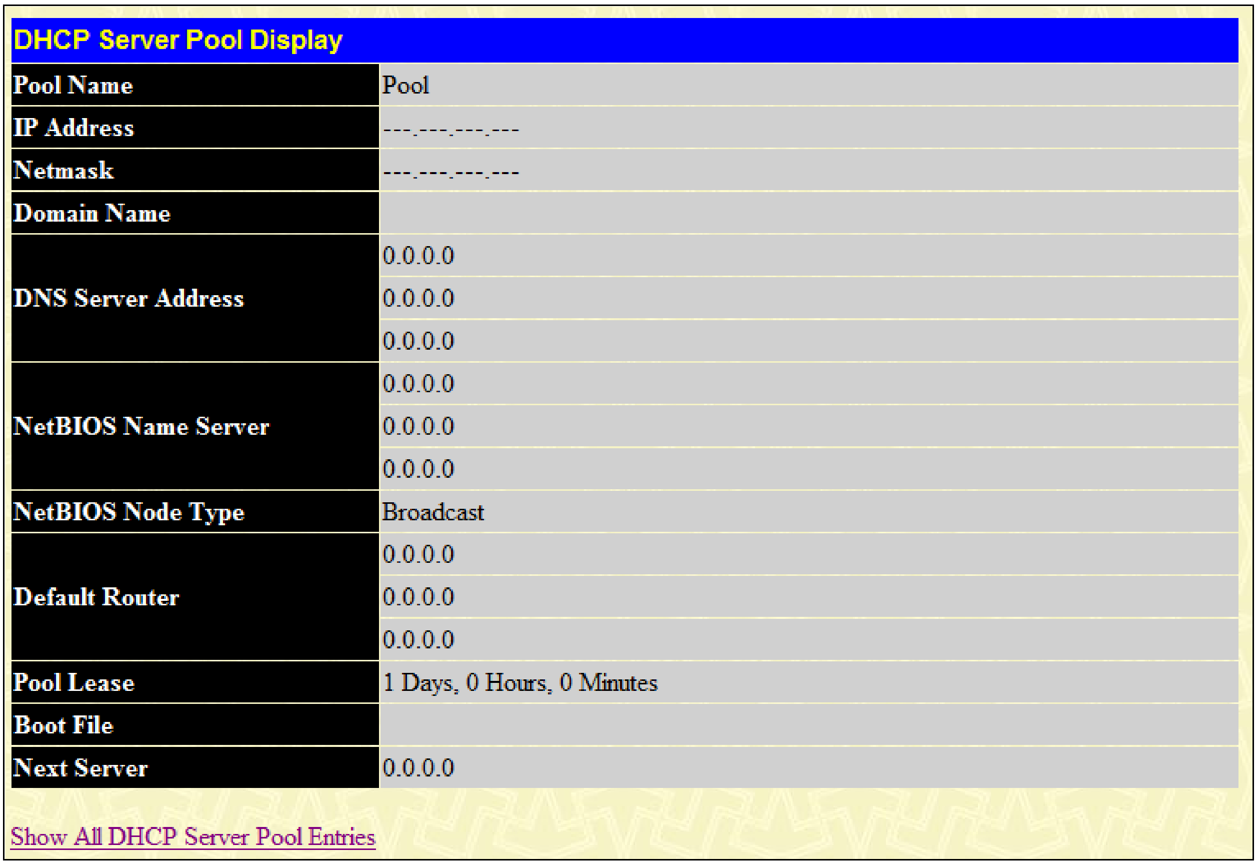
The following parameters may be configured or viewed.

Parameter	Description
Pool Name	Denotes the name of the DHCP pool for which you are currently adjusting the parameters.
IP Address	Enter the IP address to be assigned to requesting DHCP Clients. This address will not be chosen but the first three sets of numbers in the IP address will be used for the IP address of requesting DHCP Clients. (ex. If this entry is given the IP address 10.10.10.2, then assigned addresses to DHCP Clients will resemble 10.10.10.x, where x is a number between 1 and 255 but does not include the assigned 10.10.10.2)
Netmask	Enter the corresponding Netmask 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 Address	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 three 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 three 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 four node type choices: *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.

To view the set parameters for configured DHCP Pool, click the **View** button of a configured entry in the DHCP Server Pool Table in the **Create DHCP Pool** window, which will produce the following window:



DHCP Server Pool Display

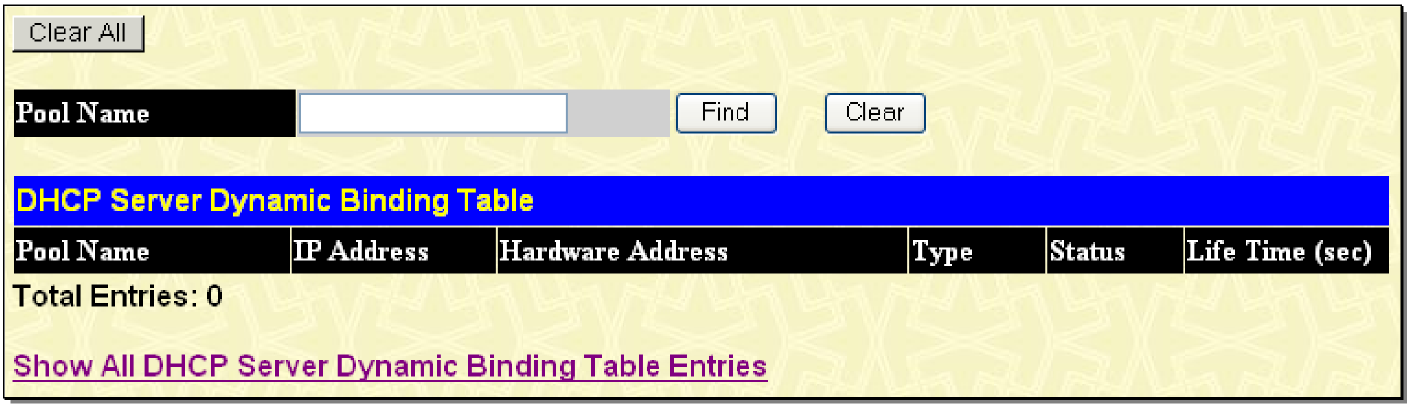
Pool Name	Pool
IP Address	---.---.---.---
Netmask	---.---.---.---
Domain Name	
DNS Server Address	0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Name Server	0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Node Type	Broadcast
Default Router	0.0.0.0 0.0.0.0 0.0.0.0
Pool Lease	1 Days, 0 Hours, 0 Minutes
Boot File	
Next Server	0.0.0.0

Figure 4- 79. DHCP Server Pool Display window

DHCP Server Dynamic Binding

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 Dynamic Binding**, as shown below:



DHCP Server Dynamic Binding Table

Pool Name	IP Address	Hardware Address	Type	Status	Life Time (sec)

Total Entries: 0

Show All DHCP Server Dynamic Binding Table Entries

Figure 4- 80. DHCP Server Dynamic Binding Table window

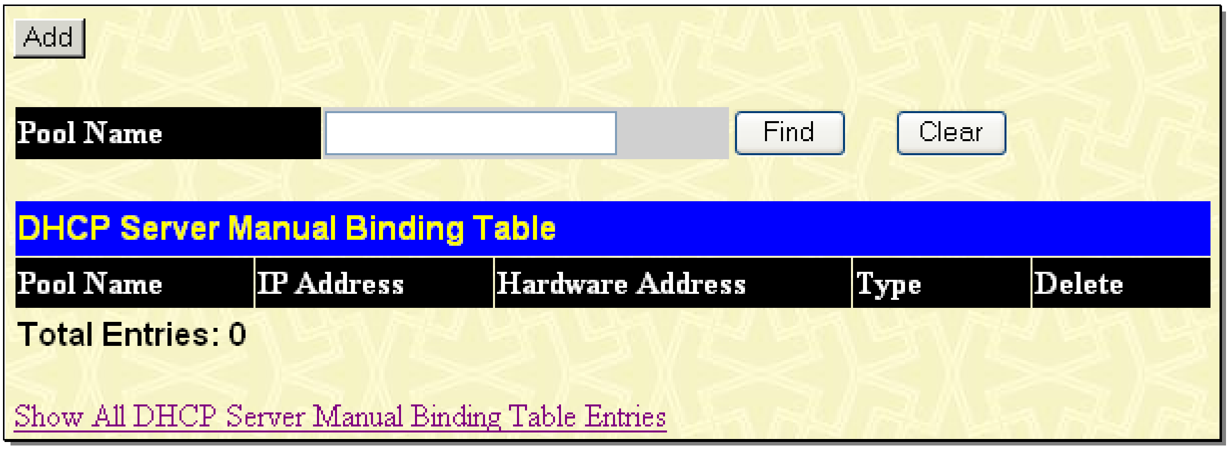
The following parameters may be configured or viewed.

Parameter	Description
Pool Name	To find the dynamically bound entries of a specific pool, enter the Pool Name into the field and click **Find**. Dynamically bound entries of this pool will be displayed in the table. To clear the corresponding Pool Name entries of this table, click **Clear**. To clear all entries, click **Clear All**.
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 (sec)	This field will display, in seconds, the time remaining on the lease for this IP address.

DHCP Server Manual Binding

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 client within a DHCP pool. These entries are necessary for special devices on the local network that will always require a static IP address that cannot be changed.

To view this window, click **L3 Features > DHCP Server > DHCP Server Manual Binding**, as shown below:

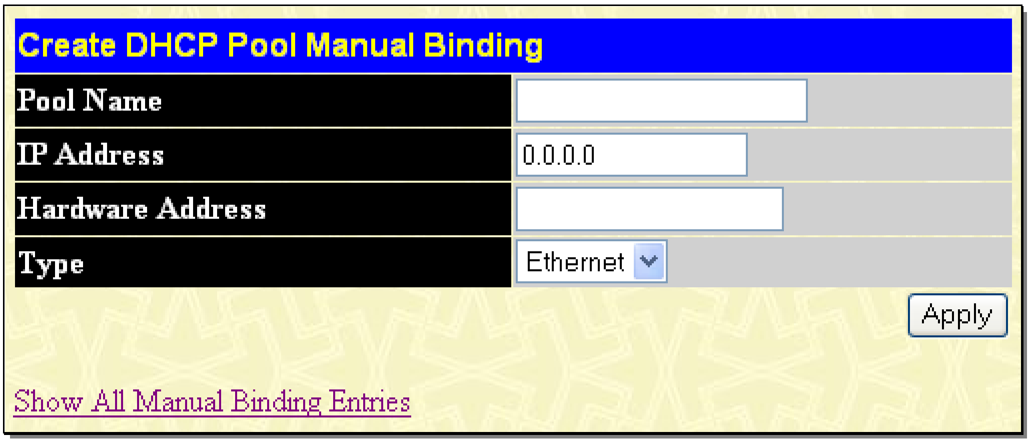

Add
Pool Name
Find
Clear
DHCP Server Manual Binding Table
Pool Name
IP Address
Hardware Address
Type
Delete
Show All DHCP Server Manual Binding Table Entries

Total Entries: 0

Figure 4- 81. DHCP Server Manual Binding Table window

Users may view statically bound DHCP entries within a DHCP pool by entering the Pool Name and clicking **Find**. Results will be displayed in the window above. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To set a manual DHCP Binding entry, click the **Add** window, which will produce the following window to configure.


Create DHCP Pool Manual Binding
Apply
Show All Manual Binding Entries

Pool Name	
IP Address	0.0.0.0
Hardware Address	
Type	Ethernet

Figure 4- 82. Create DHCP Pool Manual Binding window

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 client 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.

DHCPv6 Server

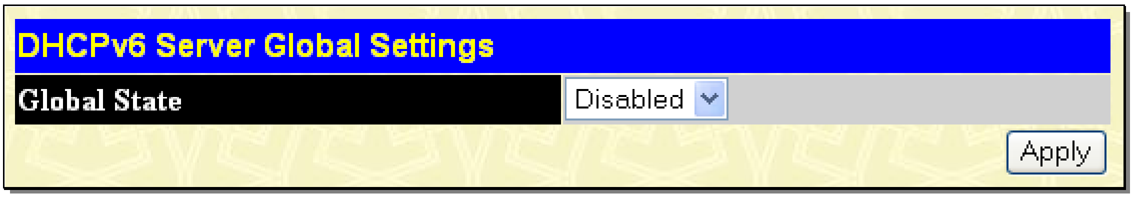
DHCPv6 Server Global Settings

This window is used to configure DHCPv6 server global settings, including specifying the range of IPv6 network addresses for the DHCPv6 pool. The IPv6 addresses in the range are free to be assigned to the DHCPv6 client. When the DHCPv6 server receives a request from the client, the server will automatically find an available pool to allocate an IPv6 address. This window also allows the user to specify the preferred-lifetime and valid-lifetime of IPv6 address within a DHCPv6 pool. The valid lifetime must be greater than or equal to the preferred lifetime.

The beginning network address and ending network address must observe some rules:

1. The prefix of the beginning network address and ending network address must be consistent. Otherwise, the switch will display an error message. (e.g.: beginning network address is 2000::1/64, and the ending network address is 3000::100/64)
2. The beginning IPv6 address must be lower than or equal to the ending IPv6 address.(e.g.: the beginning network address is 2000::200/64, and the ending network address is 2000::100/64)
3. There must not be an intersection between the IPv6 address ranges of two pools. Otherwise, the Switch will display an error message. (e.g.: pool1: 2000::1/64 --- 2000::100/64, pool2: 2000::50/64 --- 2000::200/64)
4. The IPv6 network address cannot be either a link-local address or a multicast address. Otherwise, the Switch will display an error message. (e.g.:: pool1: FE80::1/64 --- FE80::100/64, pool2: FE80::200/64 --- FE80::300/64)

To view this window, click **L3 Features > DHCPv6 Server > DHCPv6 Server Global Settings**, as shown below:



DHCPv6 Server Global Settings

Global State	Disabled

Figure 4- 83. DHCPv6 Server Global Settings window

The following parameters may be configured or viewed.

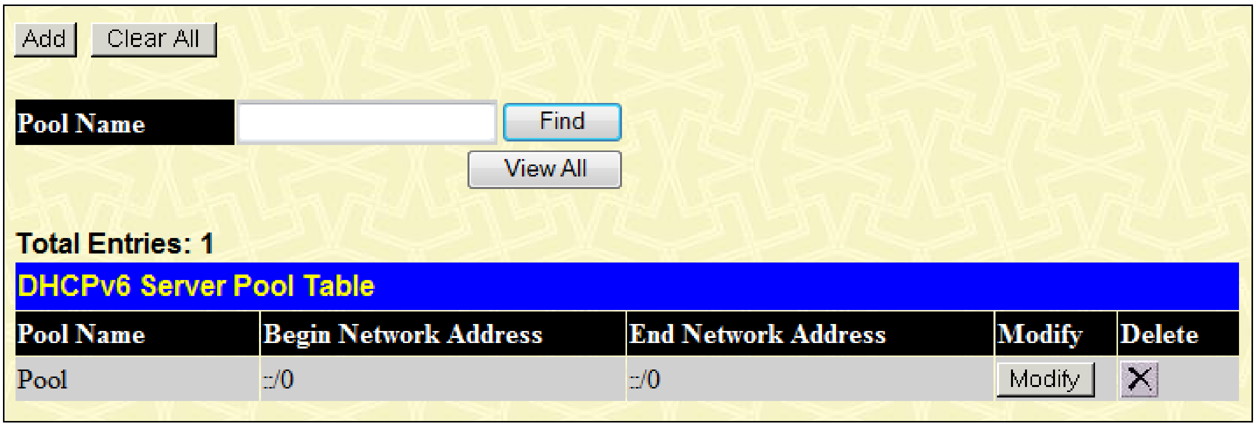
Parameter	Description
Global State	Use the pull-down menu to globally enable or disable the switch as a DHCPv6 server.

Click **Apply** to set the entry.

DHCPv6 Server Pool Settings

This window is used to configure DHCPv6 server pool settings.

To view this window, click **L3 Features > DHCPv6 Server > DHCPv6 Server Pool Settings**, as shown below:



Total Entries: 1

DHCPv6 Server Pool Table

Pool Name	Begin Network Address	End Network Address	Modify	Delete
Pool	::/0	::/0	Modify	☒

Figure 4- 84. DHCPv6 Server Pool Table window

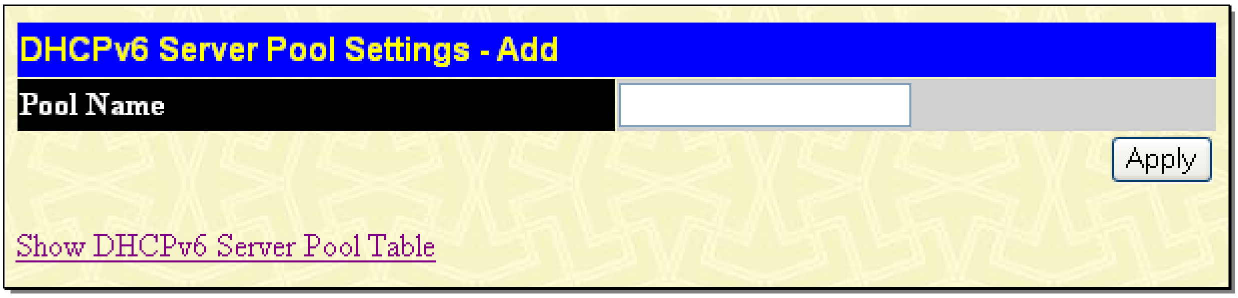
The following parameter may be configured:

Parameter	Description

Pool Name	Enter the pool name.

Click **Apply** to set the entry. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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



DHCPv6 Server Pool Settings - Add

Pool Name	

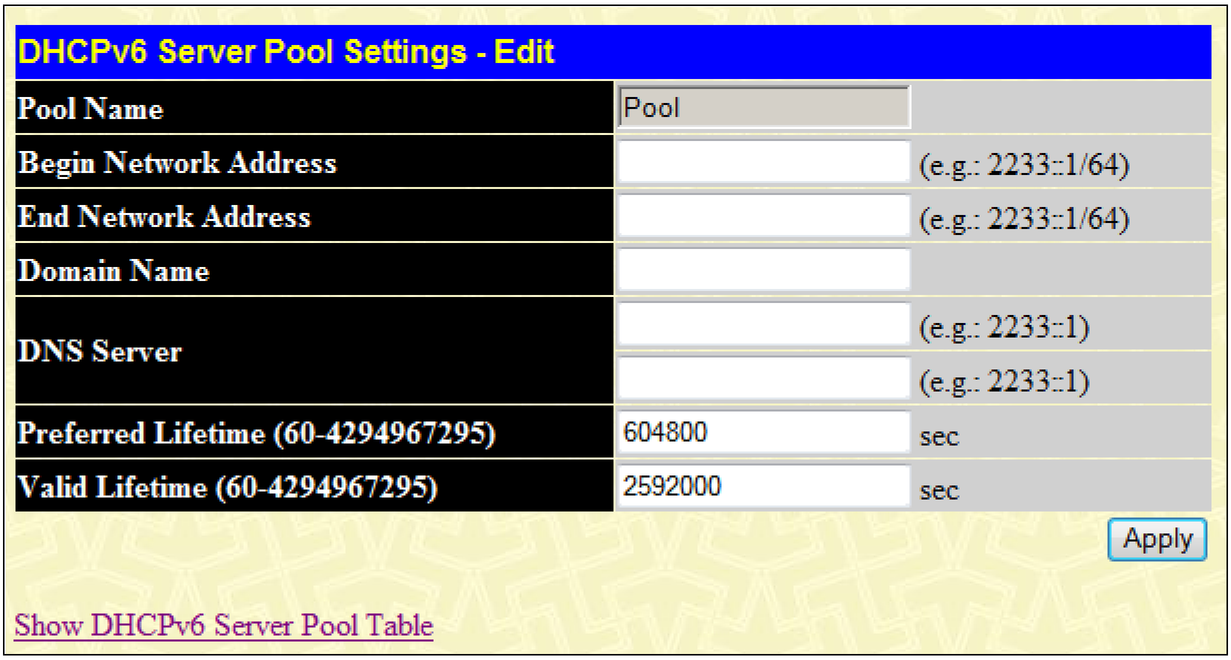
Figure 4- 85. DHCPv6 Server Pool Settings - Add window

The following parameter may be configured:

Parameter	Description
Pool Name	Enter a name of up to 12 alphanumeric characters to identify the pool to be created.

Click **Apply** to set the entry.

Clicking the **Modify** button on an entry on the DHCPv6 Server Pool Table will reveal the following window to configure:



DHCPv6 Server Pool Settings - Edit

Pool Name	Pool	
Begin Network Address		(e.g.: 2233::1/64)
End Network Address		(e.g.: 2233::1/64)
Domain Name		
DNS Server		(e.g.: 2233::1)
		(e.g.: 2233::1)
Preferred Lifetime (60-4294967295)	604800	sec
Valid Lifetime (60-4294967295)	2592000	sec

Figure 4- 86. DHCPv6 Server Pool Settings - Edit window

The following parameter may be configured:

Parameter	Description
Pool Name	Enter the pool name for which to set the network address.
Begin Network Address	The beginning IPv6network address of the DHCPv6 pool.
End Network Address	The ending IPv6 network address of the DHCPv6 pool.

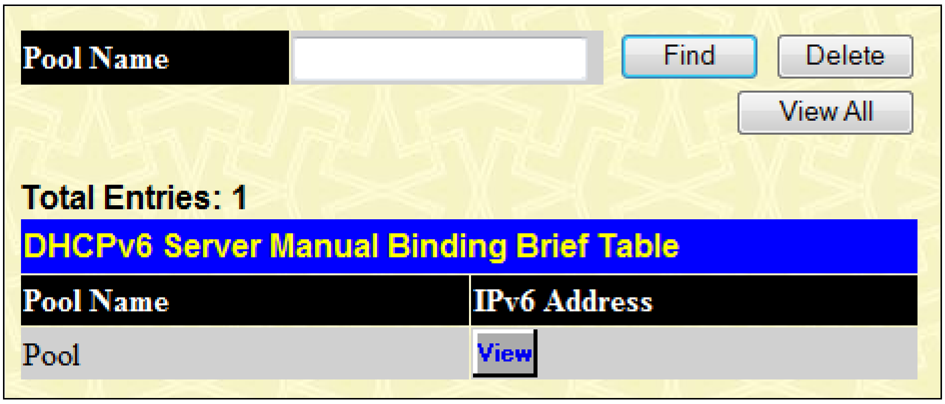
Domain Name	Enter the domain name. The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If domain name is empty, the domain name information will not be provided to the client.
DNS Server	Enter the DNS server IPv6 address for this pool. Users may specify up to two DNS server addresses.
Preferred Lifetime (60-4294967295)	Enter the length of time that a valid address is preferred (i.e., the time until depreciation). When the preferred lifetime expires, the address becomes depreciated.
Valid Lifetime (60-4294967295)	Enter the length of time an address remains in the valid state (i.e., the time until invalidation). When the valid lifetime expires, the address becomes invalid. The valid lifetime must be greater than or equal to the preferred lifetime.

Click **Apply** to implement changes made.

DHCPv6 Server Manual Binding Settings

This window is used to configure DHCPv6 server manual binding settings. An address binding is a mapping between the IPv6 address and DUID (A DHCPv6 Unique Identifier for a DHCPv6 participant) of a client. The IPv6 address specified in the manual binding entry must be in the range of the DHCPv6 pool. If the user specifies a conflict IPv6 address, an error message will be returned.

To view this window, click **L3 Features > DHCPv6 Server > DHCPv6 Server Manual Binding Settings**, as shown below:



Pool Name

Total Entries: 1

DHCPv6 Server Manual Binding Brief Table

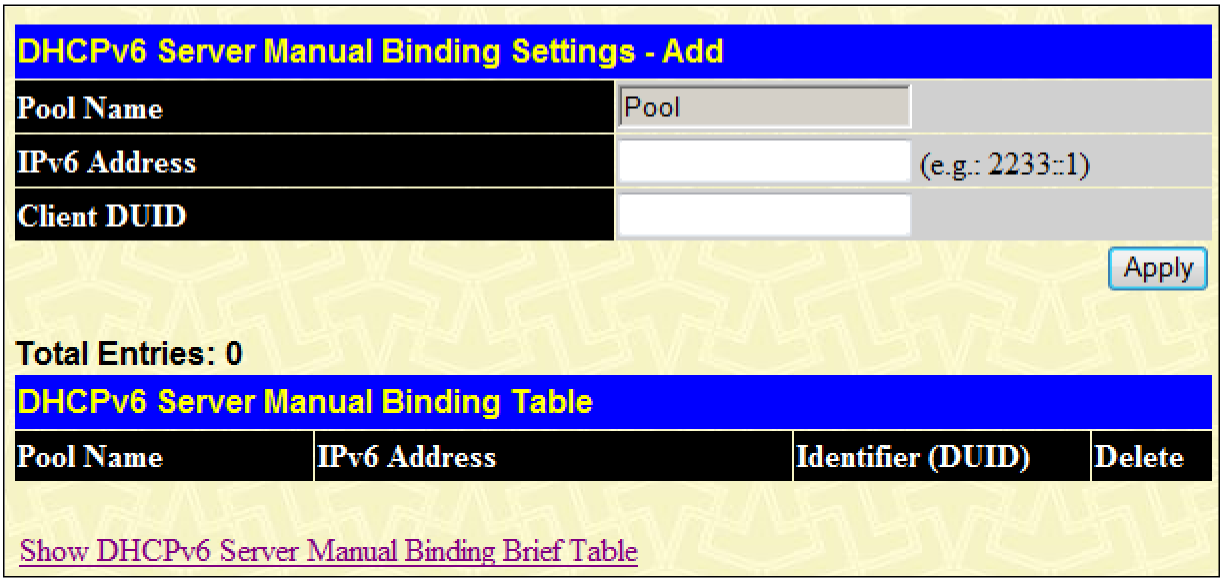
Pool Name	IPv6 Address
Pool	View

Figure 4- 87. DHCPv6 Server Manual Binding Brief Table window

The following parameter may be configured:

Parameter	Description
Pool Name	Enter the pool name.

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



DHCPv6 Server Manual Binding Settings - Add

Pool Name	Pool
IPv6 Address	(e.g.: 2233::1)
Client DUID	

Total Entries: 0

DHCPv6 Server Manual Binding Table

Pool Name	IPv6 Address	Identifier (DUID)	Delete

Figure 4- 88. DHCPv6 Server Manual Binding Settings - Add window

The following parameter may be configured:

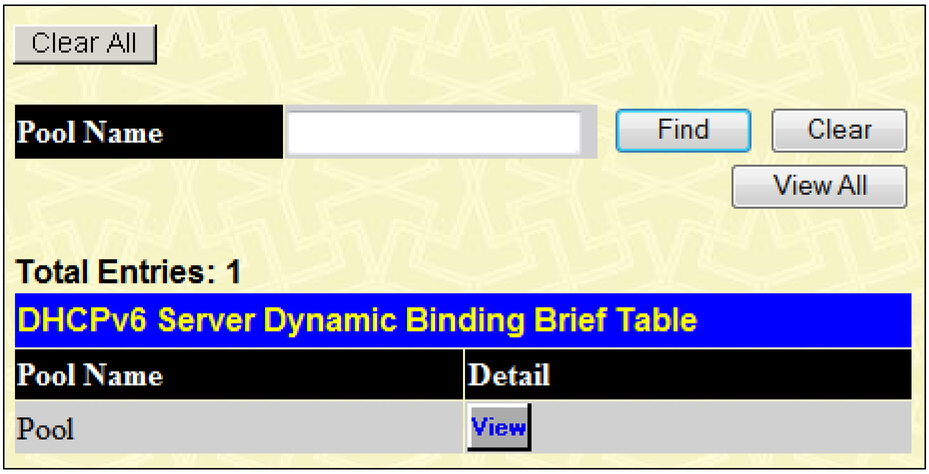
Parameter	Description
Pool Name	Enter the name of the previously created pool that will contain the manual binding entry.
IPv6 Address	Enter the IPv6 address to be statically bound to a device.
Client DUID	Enter the DHCPv6 Unique Identifie (DUID) of the device to be statically bound to the IPv6 address entered in the previous field. The DUID string must be '0--9', 'a--f' or ' A--F'.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

DHCPv6 Server Dynamic Binding Settings

This window is used to display the DHCPv6 dynamic binding information. Entering the command without the pool name will display all information regarding DHCPv6 dynamic binding on the switch. This command only displays the dynamic binding information, not including manual binding information.

To view this window, click **L3 Features > DHCPv6 Server > DHCPv6 Server Dynamic Binding Settings**, as shown below:



Total Entries: 1

DHCPv6 Server Dynamic Binding Brief Table

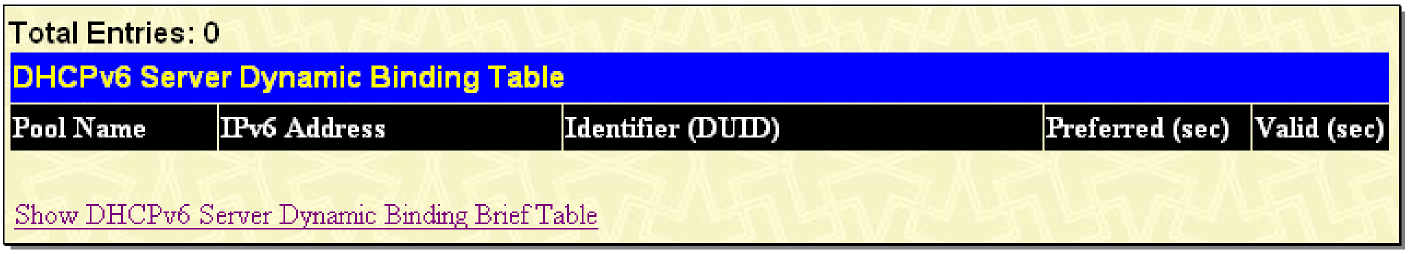
Pool Name	Detail
Pool	View

Figure 4- 89. DHCPv6 Server Dynamic Binding Brief Table window

The following parameter may be configured:

Parameter	Description
Pool Name	Enter the pool name.

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



Total Entries: 0

DHCPv6 Server Dynamic Binding Table

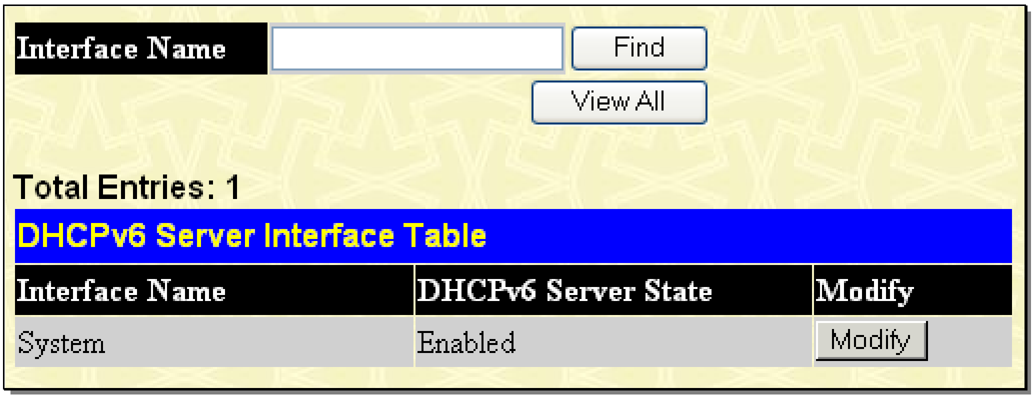
Pool Name	IPv6 Address	Identifier (DUID)	Preferred (sec)	Valid (sec)

Figure 4- 90. DHCPv6 Server Dynamic Binding Table window

DHCPv6 Server Interface Settings

This window is used to enable the DHCPv6 server global state on the Switch.

To view this window, click **L3 Features > DHCPv6 Server > DHCPv6 Server Interface Settings**, as shown below:



Interface Name

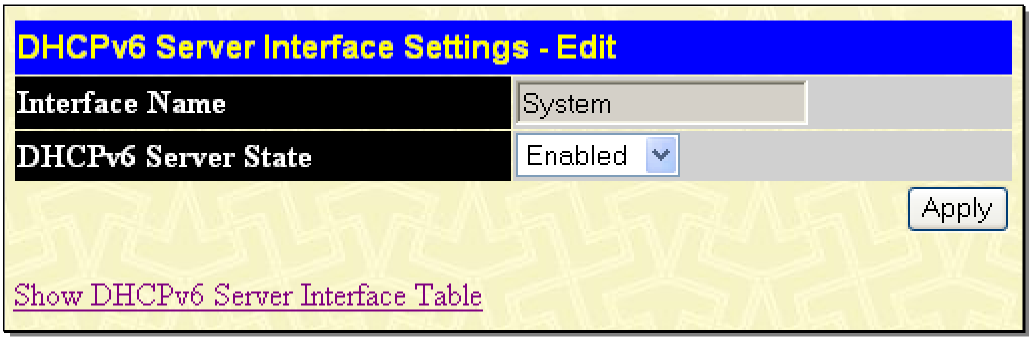
Total Entries: 1

DHCPv6 Server Interface Table

Interface Name	DHCPv6 Server State	Modify
System	Enabled	Modify

Figure 4- 91. DHCPv6 Server Interface Table window

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



DHCPv6 Server Interface Settings - Edit

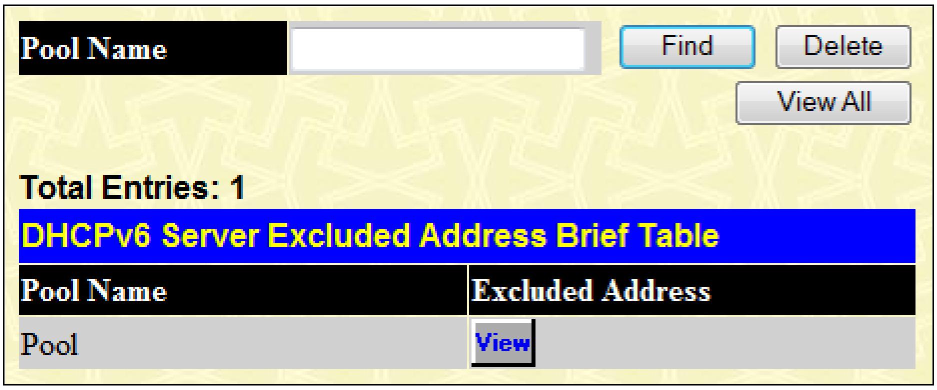
Interface Name	System
DHCPv6 Server State	Enabled

Figure 4- 92. DHCPv6 Server Interface Settings - Edit window

DHCPv6 Server Excluded Address Settings

This window is used to configure the reserved IPv6 addresses on the DHCPv6 server.

To view this window, click **L3 Features > DHCPv6 Server > DHCPv6 Server Excluded Address Settings**, as shown below:



Pool Name

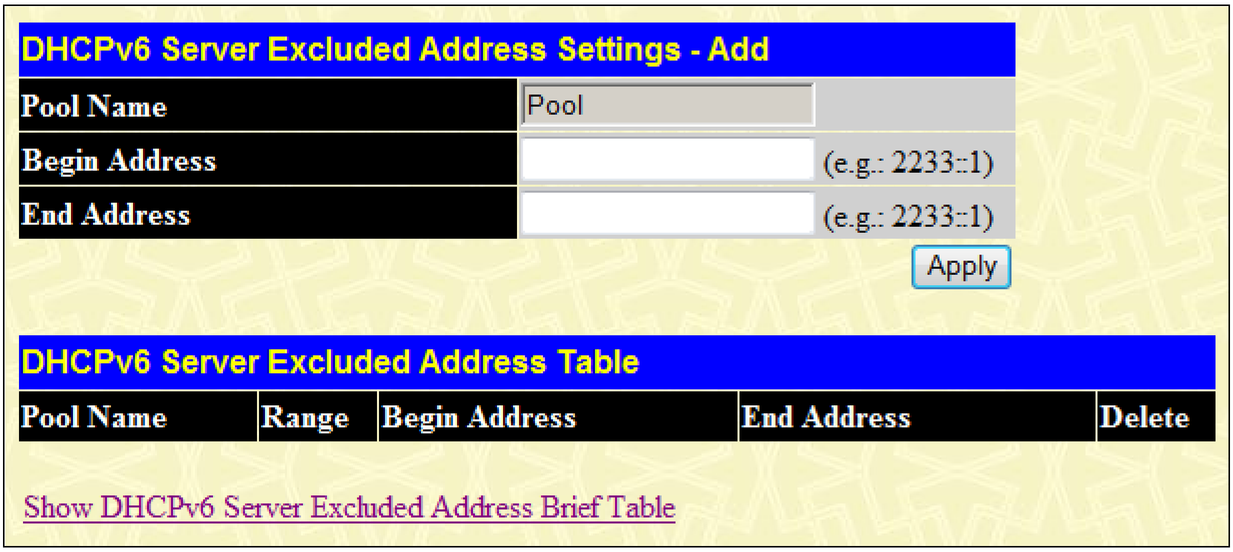
Total Entries: 1

DHCPv6 Server Excluded Address Brief Table

Pool Name	Excluded Address
Pool	View

Figure 4- 93. DHCPv6 Server Excluded Address Brief Table window

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



DHCPv6 Server Excluded Address Settings - Add

Pool Name	Pool	
Begin Address		(e.g.: 2233::1)
End Address		(e.g.: 2233::1)

DHCPv6 Server Excluded Address Table

Pool Name	Range	Begin Address	End Address	Delete

Show DHCPv6 Server Excluded Address Brief Table

Figure 4- 94. DHCPv6 Server Excluded Address Settings - Add window

The following parameter may be configured:

Parameter	Description
Pool Name	Enter the name of the DHCPv6 pool for which to add or delete the excluded address information.
Begin Address	Enter the beginning IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.
End Address	Enter the ending IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

Filter DHCP Server

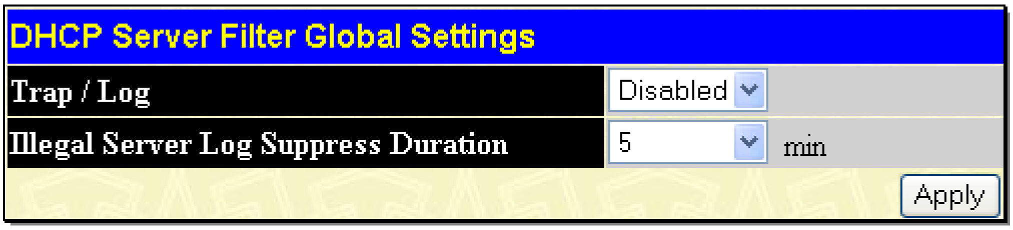
The Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses, subnet masks, default routers, and other IP parameters. The assignment usually occurs when the DHCP configured machine boots up or regains connectivity to the network. The DHCP client sends out a query requesting a response from a DHCP server on the locally attached network. The DHCP server then replies to the client with its assigned IP address, subnet mask, DNS server and default gateway information.

This function allows DHCP server packets except those that have been IP/client MAC bound to be filtered. The Filter DHCP Server is used to configure the state of the function for filtering of DHCP server packets and to add or delete the DHCP server/client binding entry. This command has two purposes firstly to filter all DHCP server packets on the specified port(s) and secondly to allow some DHCP server packets to be forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on a network.

Filter DHCP Server Global Settings

This window is used to enable the settings for the Filter DHCP Server Global Settings on the Switch.

To view this table, click **L3 Features > Filter DHCP Server > Filter DHCP Server Global Settings**, as shown below:



DHCP Server Filter Global Settings

Trap / Log: Disabled

Illegal Server Log Suppress Duration: 5 min

Figure 4- 95. DHCP Server Filter Global Settings window

The following parameters may be configured.

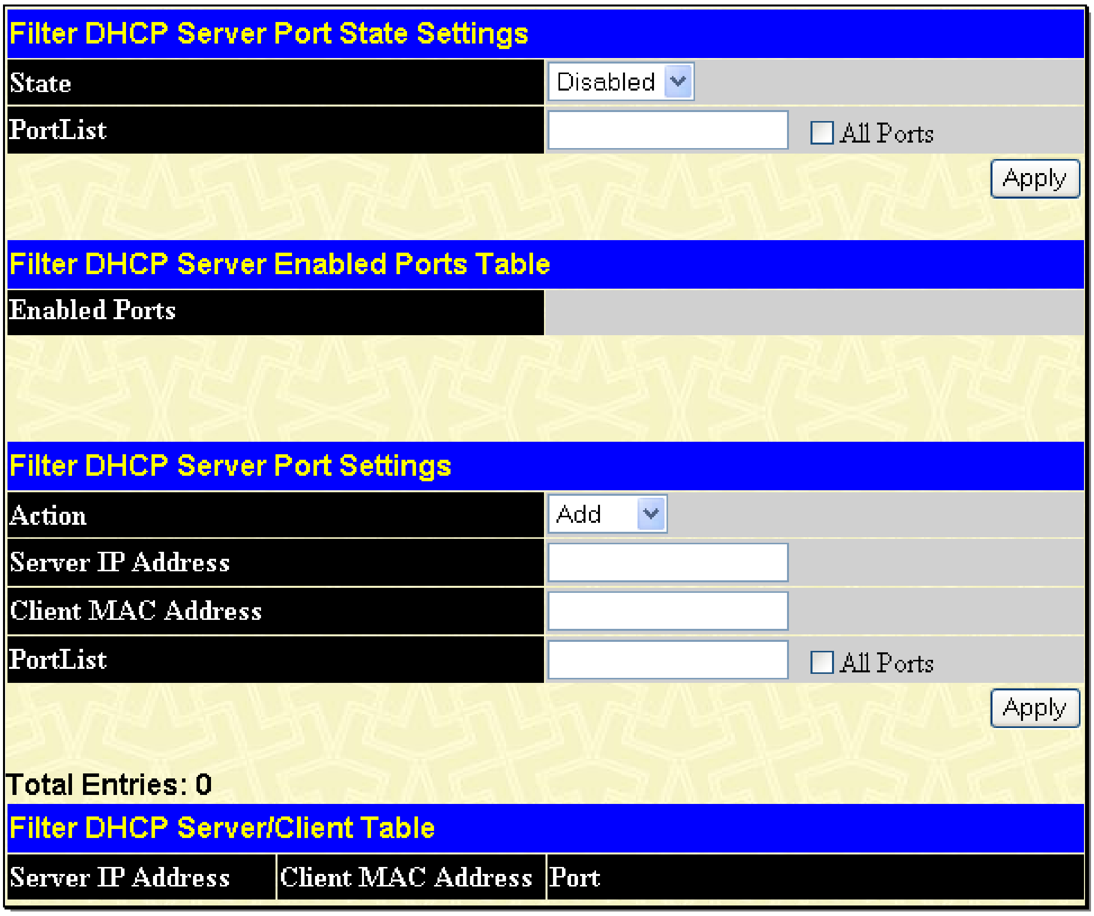
Parameter	Description
Trap/Log	To enable or disable the function for filtering DHCP server packets.
Illegal Server Log Suppress Duration	The DHCP server filtering function filters any illegal DHCP server packets. The DHCP server which sends the illegal packets will be logged. This command is used to suppress the logging of DHCP servers that continue to send illegal DHCP packets. The same illegal DHCP server IP address that is detected will be logged only once regardless of how many illegal packets are sent. The log can be suppressed by *1*, *5* or *30* minutes. The default value is *5* minutes.

Click **Apply** to implement the changes.

Filter DHCP Server Port Settings

This window is used to enable the settings for the Filter DHCP Server Port Settings.

To view this window, click **L3 Features > Filter DHCP Server > Filter DHCP Server Port Settings**, as shown below:



Filter DHCP Server Port State Settings

State	Disabled
PortList	□ All Ports

Filter DHCP Server Enabled Ports Table

Enabled Ports	

Filter DHCP Server Port Settings

Action	Add
Server IP Address	
Client MAC Address	
PortList	□ All Ports

Total Entries: 0

Filter DHCP Server/Client Table

Server IP Address	Client MAC Address	Port

Figure 4- 96. Filter DHCP Server Port State Settings window

The following parameters may be configured.

Parameter	Description
State	Enable or disable the Filter DHCP Server Port State Settings.
PortList	Enter the ports that will enable filter DHCP server.
	Filter DHCP Server Port Settings
Action	Select *Add* or *Delete* to add or delete a filter DHCP server entry.
Server IP Address	Enter the IP address of the DHCP server that specifies an allotted server ipaddress to the client.
Client MAC Address	Enter the MAC address of the client which allowed the requested IP address from the DHCP server.
PortList	Enter the list of ports to use the given filter DHCP server entry or tick the All Ports check box.

Click **Apply** to implement the changes

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.

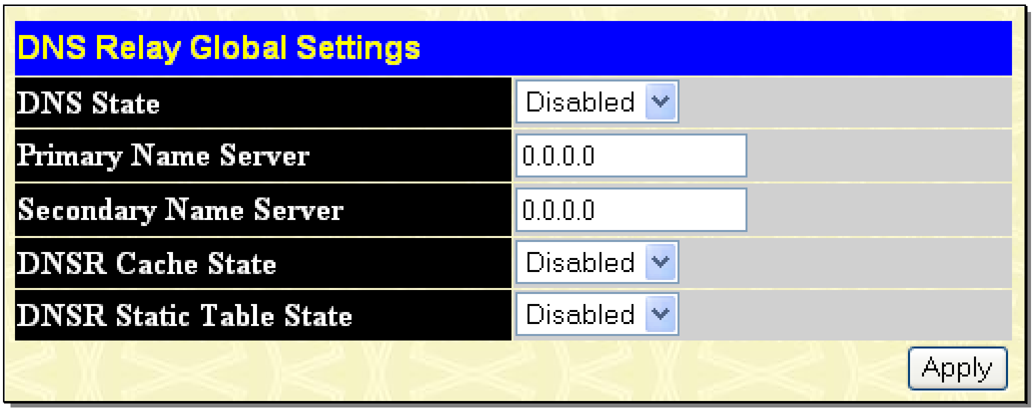
Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

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

This window is used to configure the DNS function on the Switch.

To view the **DNS Relay Global Settings**, click **L3 Features** > **DNS Relay** > **DNS Relay Global Settings**, as shown below:



DNS Relay Global Settings

DNS State	Disabled
Primary Name Server	0.0.0.0
Secondary Name Server	0.0.0.0
DNSR Cache State	Disabled
DNSR Static Table State	Disabled

Figure 4- 97. 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

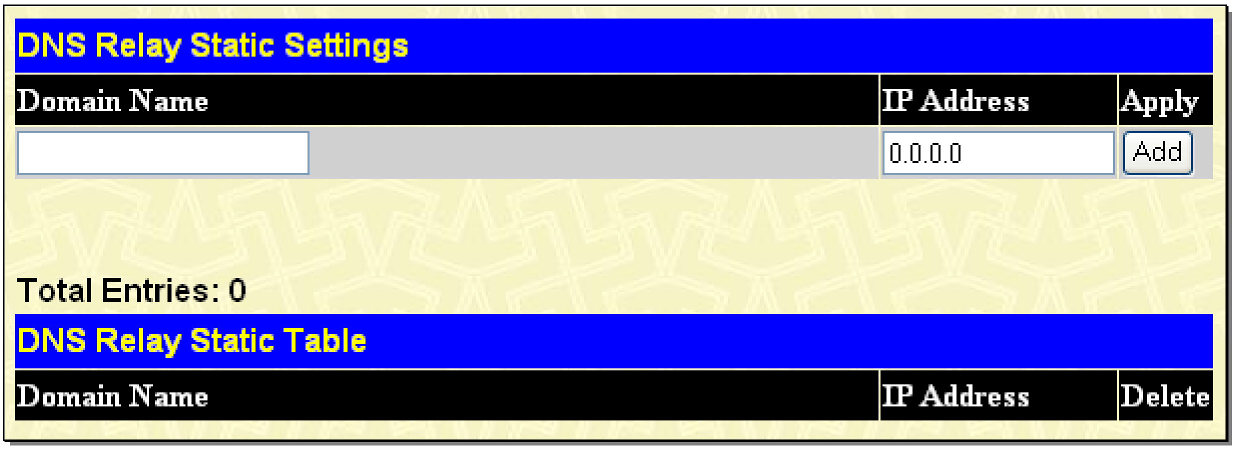
	enabled on the Switch.
DNSR Static Table State	This field can be toggled using the pull-down menu between *Disabled* and *Enabled.* This determines if the static DNS table will be used or not.

Click **Apply** to implement changes made.

DNS Relay Static Settings

This window is used to set the DNS Relay Static Settings on the Switch.

To view this window, click **L3 Features > DNS Relay > DNS Relay Static Settings**, as shown below:



DNS Relay Static Settings

Domain Name	IP Address	Apply
	0.0.0.0	Add

Total Entries: 0

DNS Relay Static Table

Domain Name	IP Address	Delete

Figure 4- 98. DNS Relay Static Settings window

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.

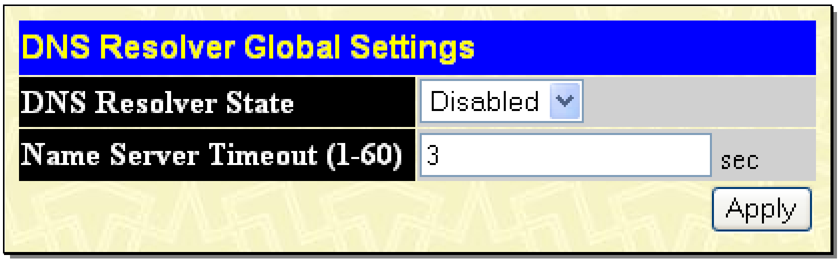
DNS Resolver

The DNS Resolver provides a solution to translate the domain name to an IP address for application on the switch itself.

DNS Resolver Global Settings

This window is used to configure the DNS resolver state and name server timeout.

To view this window, click **L3 Features > DNS Resolver > DNS Resolver Global Settings**, as shown below:



DNS Resolver Global Settings

DNS Resolver State: Disabled

Name Server Timeout (1-60): 3 sec

Figure 4- 99. DNS Resolver Global Settings window

The following fields can be set:

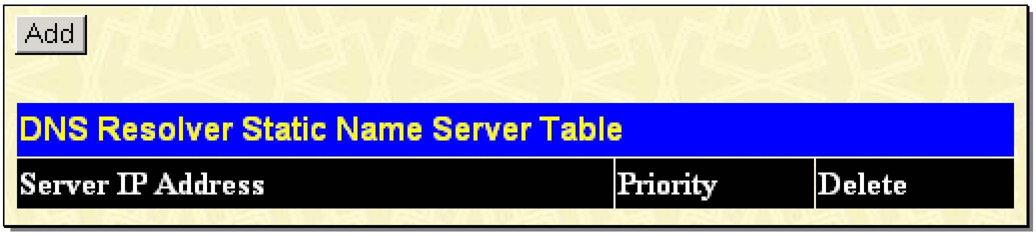
Parameter	Description
DNS Resolver State	Use the pull-down menu to enable or disable the DNS resolver on the Switch. The default is *Disabled*.
Name Server Timeout (1-60)	Enter the maximum time waiting for a response from a specified name server. The range is *1* to *60* seconds. The default value is *3*.

Click **Apply** to implement changes made.

DNS Resolver Static Name Server Settings

When adding a name server, if one primary name server exists in the static name server table and a new primary name server is added, the existing primary name server will be changed to a normal name server. If the added primary name server's IP address is the same as an existing normal name server's IP address, the existing normal name server will be changed to a primary name server, but won't add new name server. When no primary name server is specified, the first configured name server will automatically change to become the primary name server. If the deleted name server's IP address is the same as one of the existing name servers' IP addresses, regardless of whether a normal name server or primary name server, the name server will be deleted.

To view this read-only window, click **L3 Features > DNS Resolver > DNS Resolver Static Name Server Settings**, as shown below:



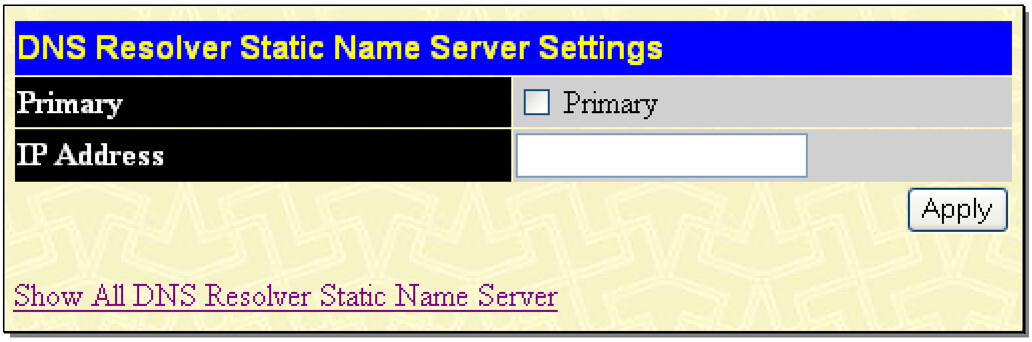
DNS Resolver Static Name Server Table

Server IP Address	Priority	Delete

Figure 4- 100. DNS Resolver Static Name Server Table window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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



DNS Resolver Static Name Server Settings

Primary	□ Primary
IP Address	

Figure 4- 101. DNS Resolver Static Name Server Settings window

The following fields can be set:

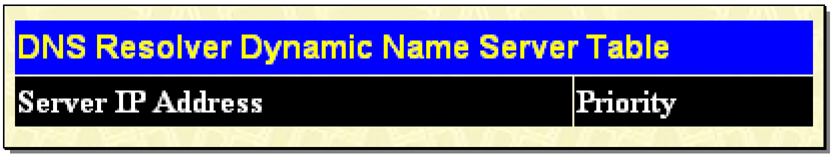
Parameter	Description
Primary	Tick the check box to indicate the name server is a primary name server.
IP Address	Enter the DNS resolver name server IP address.

Click **Apply** to implement changes made.

DNS Resolver Dynamic Name Server Table

This read-only window is used to display the DNS resolver dynamic name server table.

To view this window, click **L3 Features > DNS Resolver > DNS Resolver Dynamic Server Settings**, as shown below:



DNS Resolver Dynamic Name Server Table

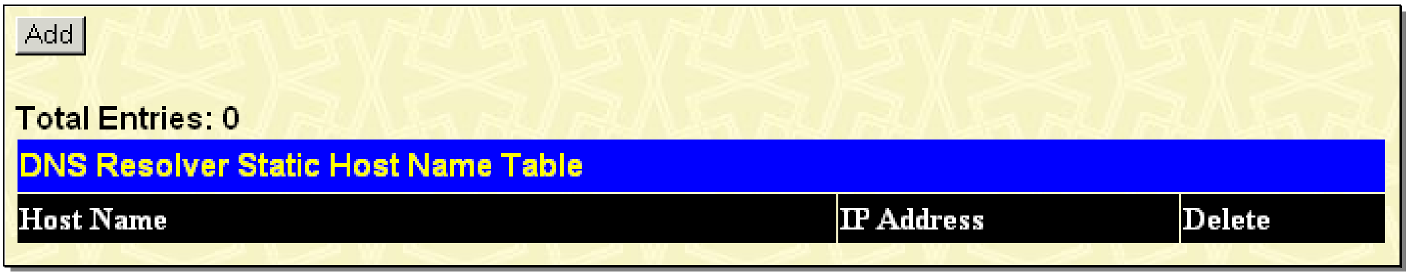
Server IP Address	Priority

Figure 4- 102. DNS Resolver Dynamic Server Table window

DNS Resolver Static Host Name Settings

This window is used to create or delete a static host name entry of the Switch. If the created host name entry exists in the dynamic host name table, the existing dynamic host name entry will be deleted, and the created host name entry is then added into the static host name table and a log for a duplicate is recorded.

To view this window, click **L3 Features > DNS Resolver > DNS Resolver Static Host Name Settings**, as shown below:



Total Entries: 0

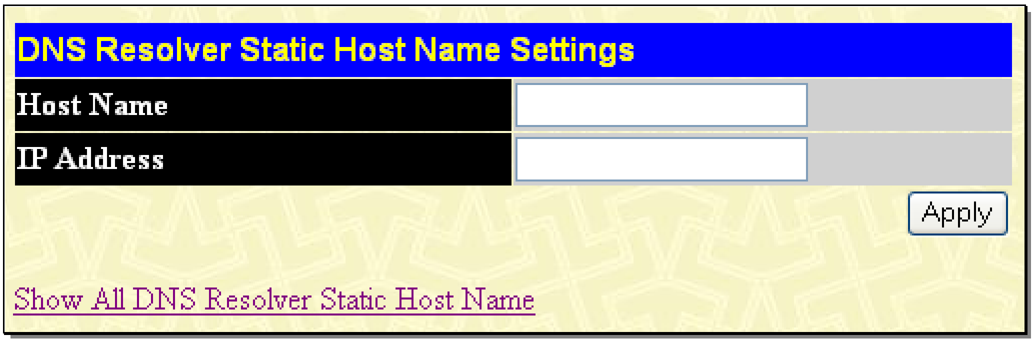
DNS Resolver Static Host Name Table

Host Name	IP Address	Delete

Figure 4- 103. DNS Resolver Static Host Name Table window

To remove an entry from the table, click its corresponding ☒ under the Delete heading.

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



DNS Resolver Static Host Name Settings

Host Name	
IP Address	

Figure 4- 104. DNS Resolver Static Host Name Settings window

The following fields can be set:

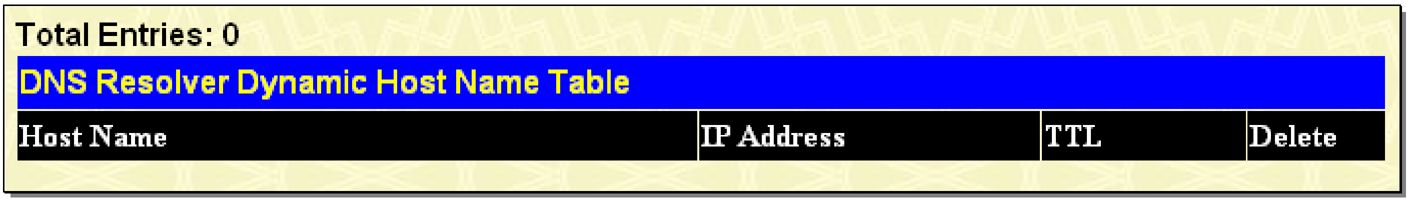
Parameter	Description
Host Name	Enter the host's host name.
IP Address	Enter the host's IP address.

Click **Apply** to implement changes made.

DNS Resolver Dynamic Host Name Table

This window is used to display or delete entries on the DNS Resolver Dynamic Host Name Table.

To view this window, click **L3 Features > DNS Resolver > DNS Resolver Dynamic Host Name Table**, as shown below:



Total Entries: 0

DNS Resolver Dynamic Host Name Table

Host Name	IP Address	TTL	Delete

Figure 4- 105. DNS Resolver Dynamic Host Name Table window

To remove 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.

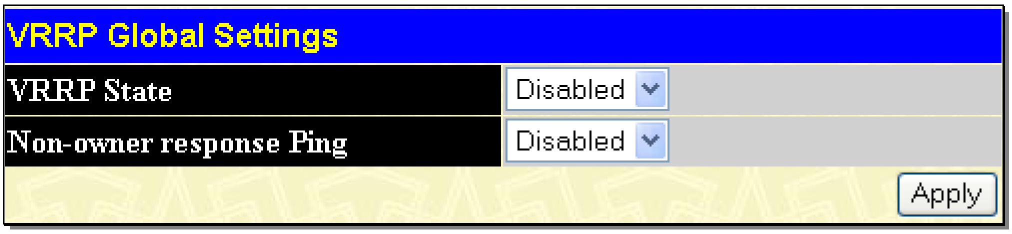
Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election 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

This window is used to enable VRRP globally on the Switch.

To view this window, click **L3 Features > VRRP > VRRP Global Settings**, as shown below:



VRRP Global Settings

VRRP State	Disabled
Non-owner response Ping	Disabled

Figure 4- 106. VRRP Global Settings window

The following fields can be set:

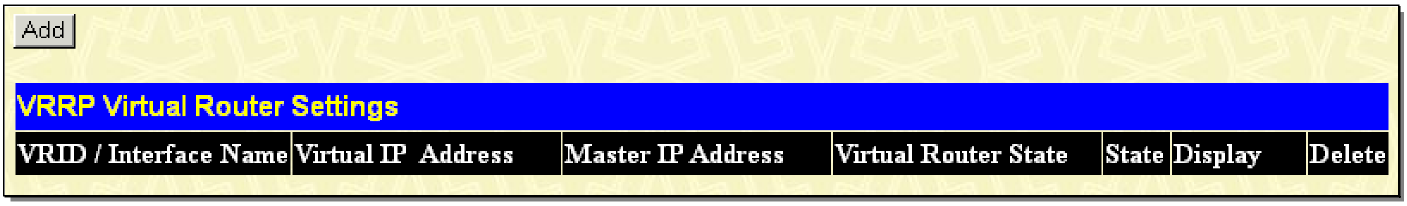
Parameter	Description
VRRP State	Use the pull-down menu to enable or disable VRRP globally on the Switch. The default is *Disabled*.
Non-owner response Ping	Enabling this parameter will allow the virtual IP address to be pinged from other host end nodes to verify connectivity. This will only enable the 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**, as shown below:



VRRP Virtual Router Settings

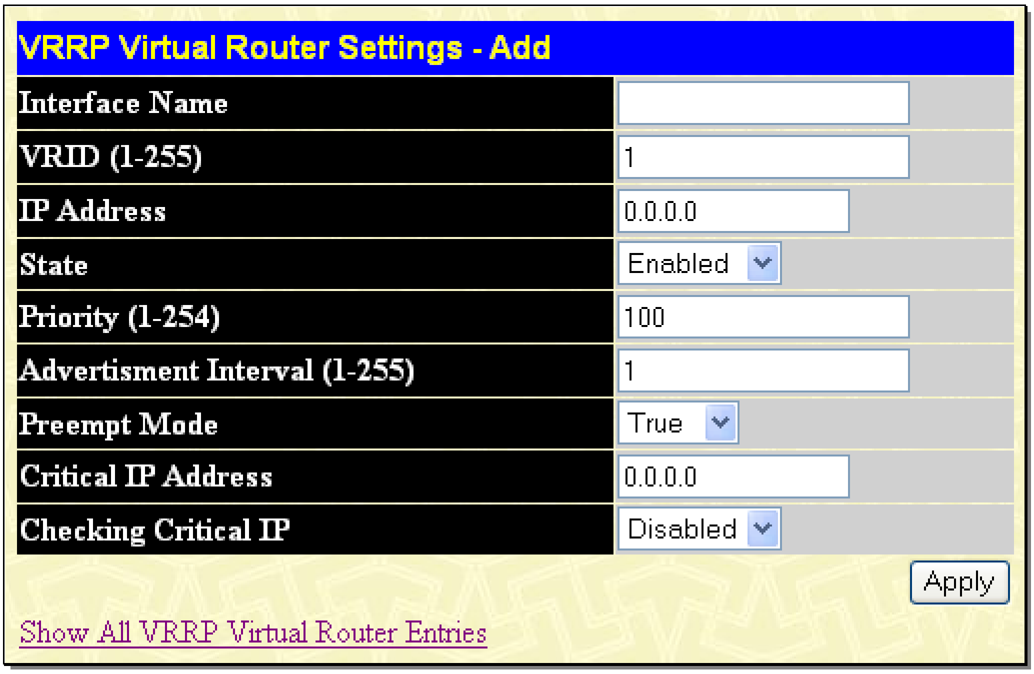
VRID / Interface Name	Virtual IP Address	Master IP Address	Virtual Router State	State	Display	Delete

Figure 4- 107. 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.



VRRP Virtual Router Settings - Add

Interface Name	
VRID (1-255)	1
IP Address	0.0.0.0
State	Enabled
Priority (1-254)	100
Advertisment Interval (1-255)	1
Preempt Mode	True
Critical IP Address	0.0.0.0
Checking Critical IP	Disabled

Figure 4- 108. VRRP Virtual Router Settings – Add window

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

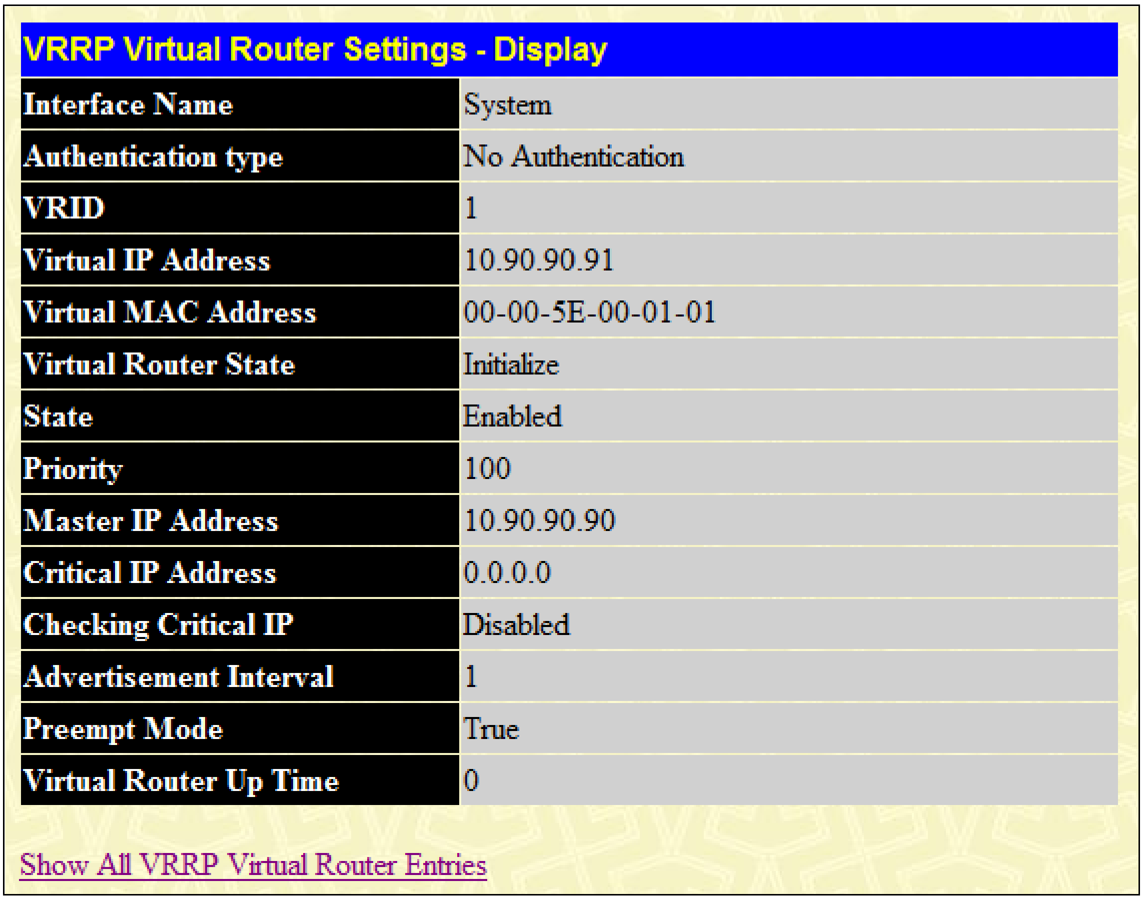
The following parameters may be set to configure an existing or new VRRP interface.

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 and disable 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:



VRRP Virtual Router Settings - Display

Interface Name	System
Authentication type	No Authentication
VRID	1
Virtual IP Address	10.90.90.91
Virtual MAC Address	00-00-5E-00-01-01
Virtual Router State	Initialize
State	Enabled
Priority	100
Master IP Address	10.90.90.90
Critical IP Address	0.0.0.0
Checking Critical IP	Disabled
Advertisement Interval	1
Preempt Mode	True
Virtual Router Up Time	0

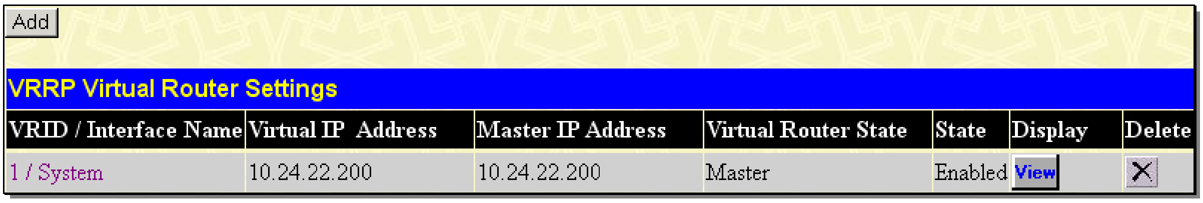
Figure 4- 109. VRRP Virtual Router Settings - Display window

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.
State	Displays the current state of the router.
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

To edit the settings for a particular VRRP setting, click **L3 Features** > **VRRP** > **VRRP Virtual Router Settings**, which will display the following window:

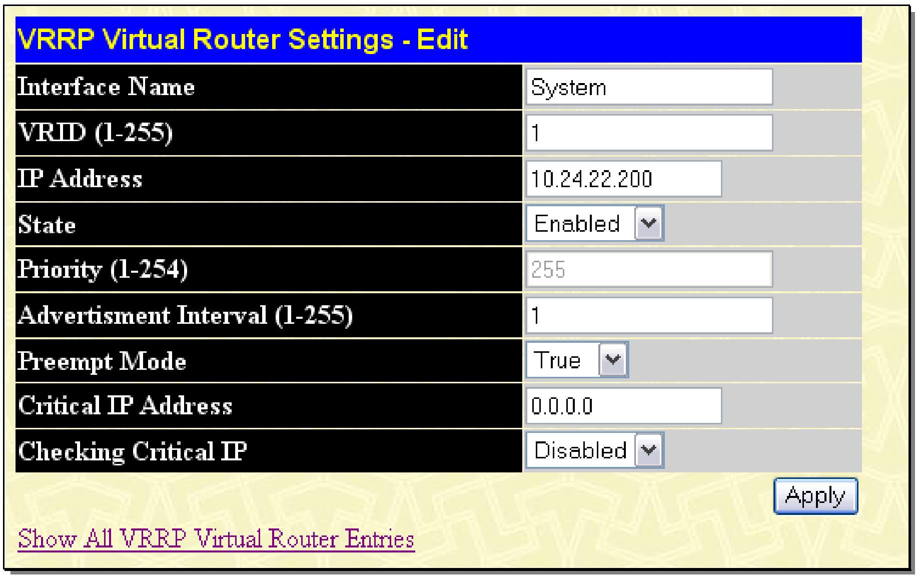


VRRP Virtual Router Settings

VRID / Interface Name	Virtual IP Address	Master IP Address	Virtual Router State	State	Display	Delete
1 / System	10.24.22.200	10.24.22.200	Master	Enabled	View	☒

Figure 4- 110. VRRP Virtual Router Settings window

Click the hyperlink VRID / Interface Name that you want to edit to display the following window:



VRRP Virtual Router Settings - Edit

Interface Name	System
VRID (1-255)	1
IP Address	10.24.22.200
State	Enabled
Priority (1-254)	255
Advertisment Interval (1-255)	1
Preempt Mode	True
Critical IP Address	0.0.0.0
Checking Critical IP	Disabled

Figure 4- 111. VRRP Virtual Router Settings - Edit window

This window displays the following information:

Parameter	Description
Interface Name	The name of a previously configured IP interface used to create a VRRP entry is displayed. This IP interface must have been assigned to a VLAN on the Switch.
VRID (1-255)	The value displayed between *1* and *255* to uniquely identify this VRRP group on the Switch. All routers participating in this group must have been 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 and disable 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

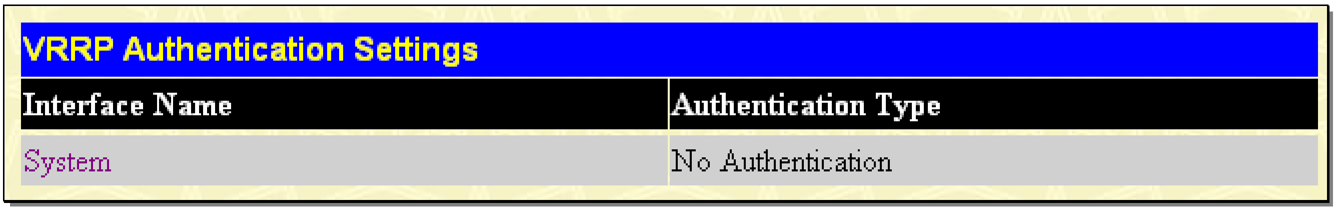
	multiple routes to the Internet or other critical network connections.
Checking Critical IP	Use the pull-down menu to enable or disable the Critical IP address entered above.

Click **Apply** to implement changes made.

VRRP Authentication Settings

This 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**, as shown below:

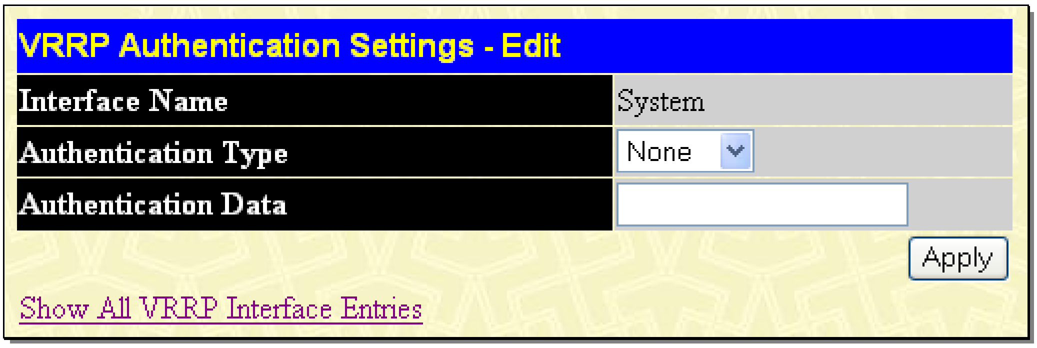


VRRP Authentication Settings

Interface Name	Authentication Type
System	No Authentication

Figure 4- 112. VRRP Authentication Settings window

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



VRRP Authentication Settings - Edit

Interface Name	System
Authentication Type	None
Authentication Data	

Figure 4- 113. 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 drop-down menu. *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 found in **L3 Features > IP Multicast Routing Protocol**. IGMP, DVMRP, and PIM-DM/SM/SM-DM can be enabled or disabled on the Switch without changing the individual protocol's configuration by using the **DGS-3600 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 subnetwork, 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 subnetwork or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnetwork. If there are no members on a subnetwork, packets will not be forwarded to that subnetwork.

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:

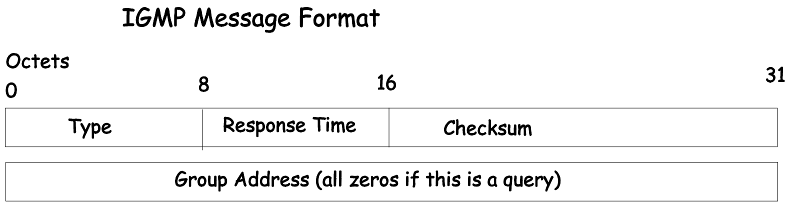


Figure 4- 114. IGMP Message Format

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 4- 1. IGMP Type Codes

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective subnetworks. 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 subnetworks. 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 subnetworks.

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:

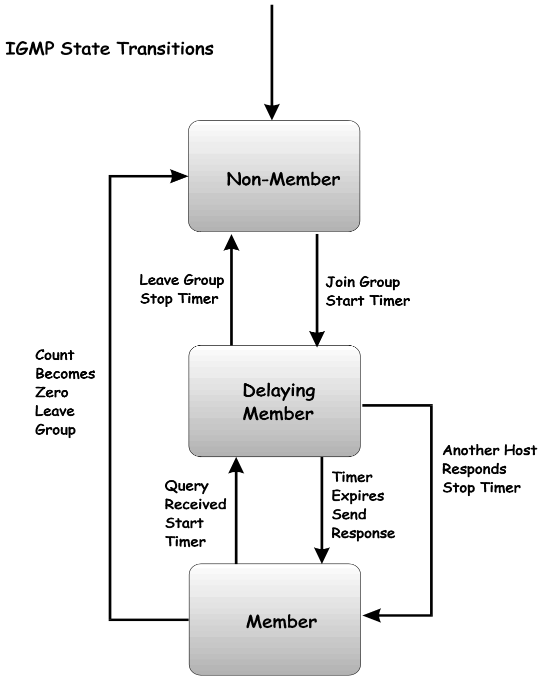

IGMP State Transitions
Non-Member
Leave Group Stop Timer
Join Group Start Timer
Count Becomes Zero Leave Group
Delaying Member
Another Host Responds Stop Timer
Query Received Start Timer
Timer Expires Send Response
Member

Figure 4- 115. IGMP State Transitions

IGMP Version 3

The current release of the Switch 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 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.

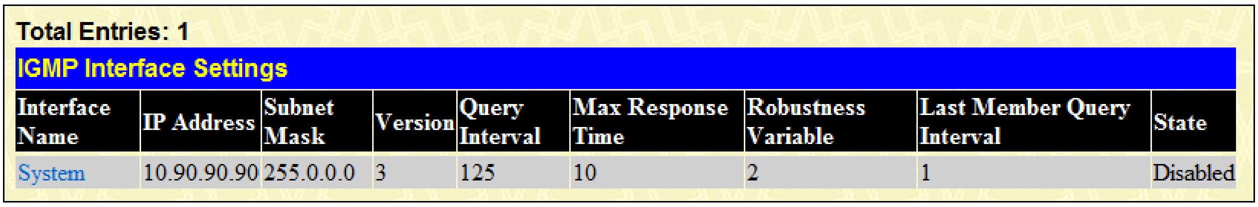
NOTE: The length of time for all timers utilized in IGMPv3 can be determined using IGMP configurations to perform the following calculation:

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

IGMP Interface Settings

The Internet Group Management Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. Each IP interface configured on the Switch is displayed in the below **IGMP Interface Settings** window. To configure IGMP for a particular interface, click the corresponding hyperlink for that IP interface.

To view this Table, click **L3 Features > IP Multicast Routing Protocol** > **IGMP Interface Settings**, as shown below:

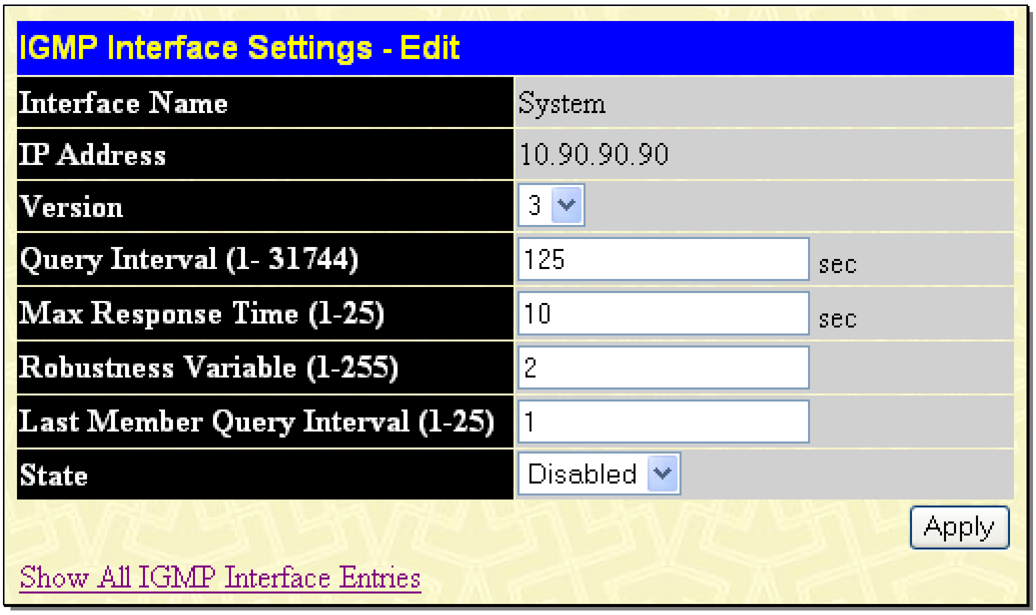


Total Entries: 1

IGMP Interface Settings

Interface Name	IP Address	Subnet Mask	Version	Query Interval	Max Response Time	Robustness Variable	Last Member Query Interval	State
System	10.90.90.90	255.0.0.0	3	125	10	2	1	Disabled

Figure 4- 116. IGMP Interface Settings window



IGMP Interface Settings - Edit

Interface Name	System
IP Address	10.90.90.90
Version	3
Query Interval (1- 31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Variable (1-255)	2
Last Member Query Interval (1-25)	1
State	Disabled

Figure 4- 117. 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:

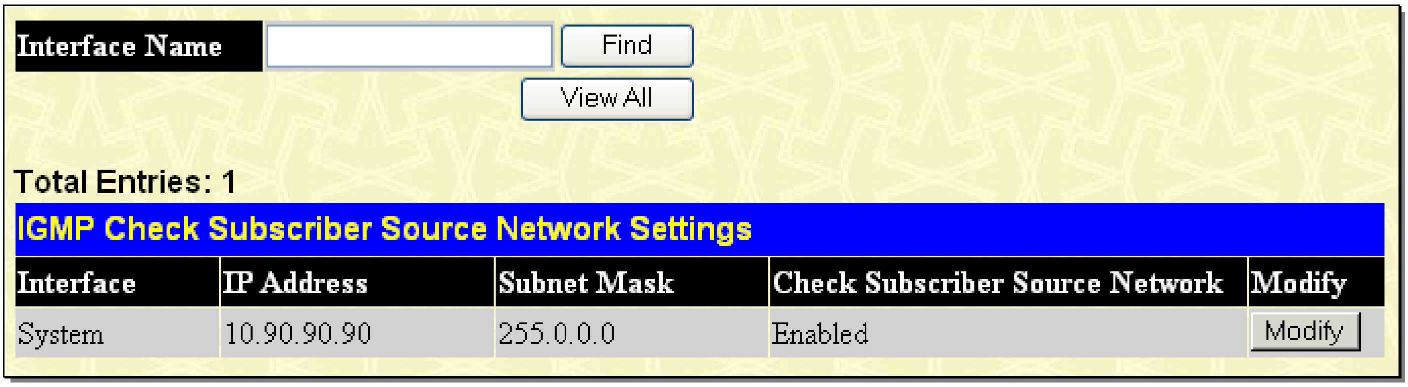
Parameter	Description
Interface Name	Displays the name of the IP interface that is to be configured for IGMP. This must be a previously configured IP interface.
IP Address	Displays the IP address corresponding to the IP interface name above.
Version	Enter the IGMP version (*1*, *2* or *3*) that will 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 subnetworks 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 subnetworks that are expected to lose larger numbers of packets. The default setting is 2.
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.

IGMP Check Subscriber Source Network Settings

This window allows users to configure IGMP check subscriber source network settings. When Check Subscriber Source Network is enabled on an interface, every IGMP report/leave message received by the interface will be checked to see whether its source IP is in the same network as the interface. If the check is disabled, an IGMP report/leave message with any source IP can be processed by IGMP protocol.

To view this Table, click **L3 Features > IP Multicast Routing Protocol** > **IGMP Check Subscriber Source Network Settings**, as shown below:

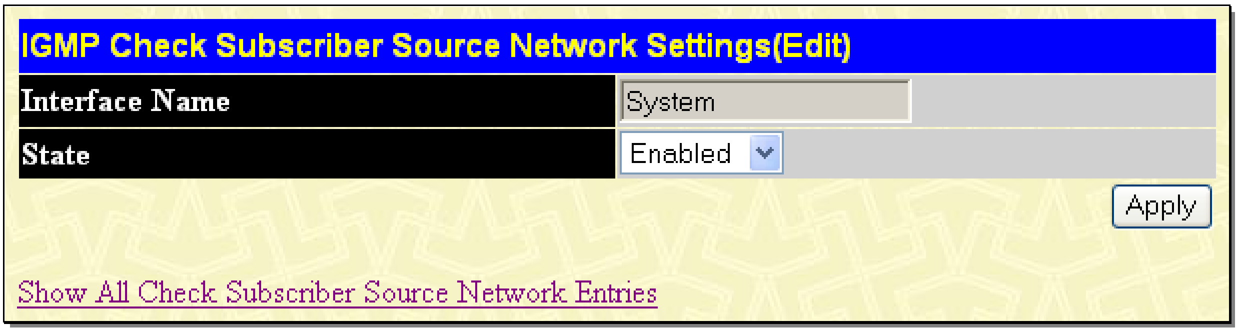


Total Entries: 1

IGMP Check Subscriber Source Network Settings

Interface	IP Address	Subnet Mask	Check Subscriber Source Network	Modify
System	10.90.90.90	255.0.0.0	Enabled	Modify

Figure 4- 118. IGMP Check Subscriber Source Network Settings window



IGMP Check Subscriber Source Network Settings(Edit)

Interface Name	System
State	Enabled

Figure 4- 119. IGMP Check Subscriber Source Network Settings (Edit) window

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 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.

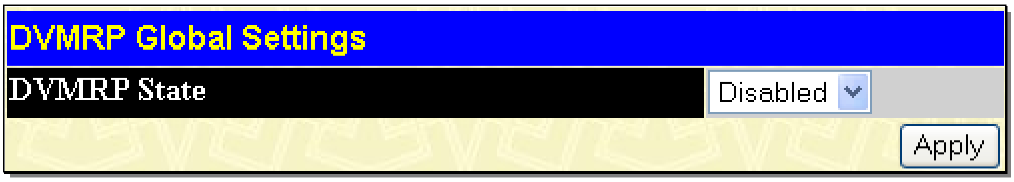
Route cost is a relative number that is used by DVMRP to calculate which branches of a multicast delivery tree should be ‘pruned’. The ‘cost’ is relative to other costs assigned to other DVMRP routes throughout the network.

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

This window is used to enable DVMRP globally on the Switch.

To view this window, click **L3 Features > IP Multicast Routing Protocol > DVMRP Global Settings**, as shown below:



DVMRP Global Settings

DVMRP State: Disabled

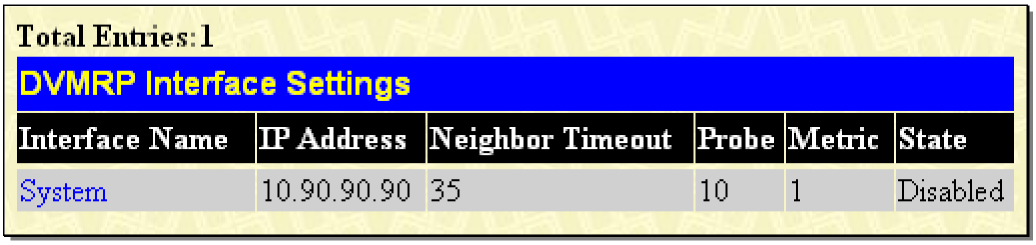
Figure 4- 120. DVMRP Global Settings window

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

DVMRP Interface Settings

This window 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 Settings** window. To configure DVMRP for a particular interface, click the corresponding hyperlink for that IP interface.

To view this Table, click **L3 Features > IP Multicast Routing Protocol > DVMRP Interface Settings**, as shown below:

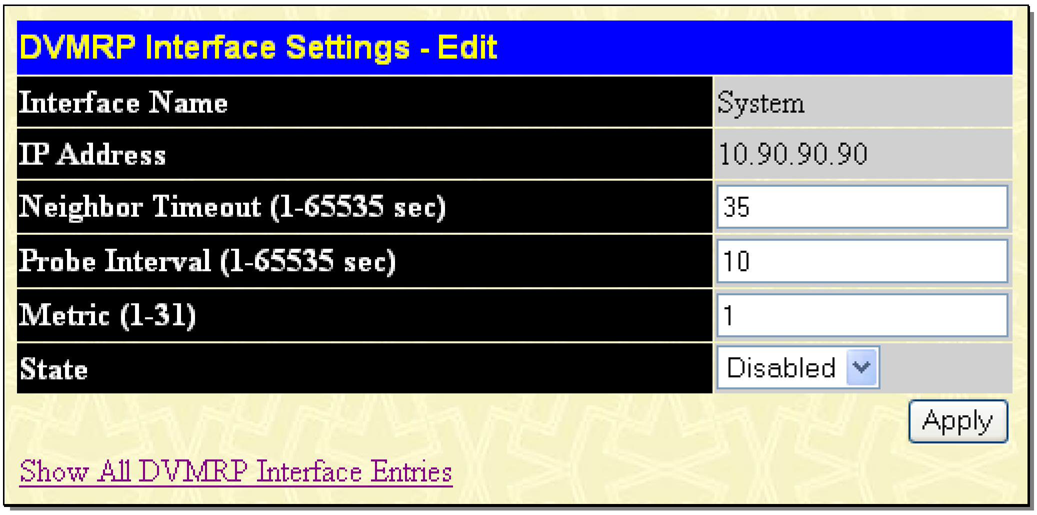


Total Entries: 1

DVMRP Interface Settings

Interface Name	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.90.90.90	35	10	1	Disabled

Figure 4- 121. DVMRP Interface Settings window



DVMRP Interface Settings - Edit

Interface Name	System
IP Address	10.90.90.90
Neighbor Timeout (1-65535 sec)	35
Probe Interval (1-65535 sec)	10
Metric (1-31)	1
State	Disabled

Figure 4- 122. 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 (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* seconds.
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

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 Switch supports three types of PIM, Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Sparse-Dense Mode (PIM-DM-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 routers are 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

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.

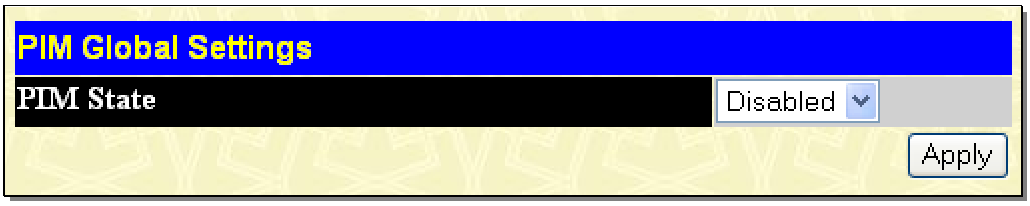
PIM-SM-DM

In the PIM-SM, RP is a key point for the first hop of the sender. If the first hop does not have RP information when the sender sends data out, it will drop the packet and do nothing. Sparse-Dense mode will be useful in this condition. In Sparse-Dense mode, the packets can be flooded to all the outgoing interfaces and pruning/joining (prune/graft) can be used to control the outgoing interface list if RP is not found. In other words, the PIM Sparse-Dense mode is treated in either the sparse mode or dense mode of the operation; it depends on which mode the multicast group operates. When an interface receives multicast traffic, if there is a known RP for the group, then the current operation mode on the interface is sparse mode, otherwise the current operation mode on the interface will be dense mode.

PIM Global Settings

This window is used to enable PIM globally on the Switch.

To view this window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM Global Settings**, as shown below:



PIM Global Settings

PIM State: Disabled

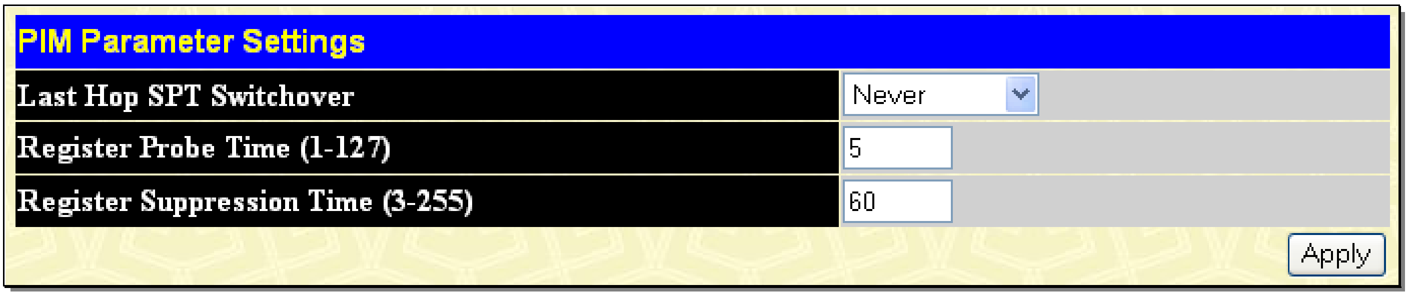
Figure 4- 123. PIM Global Settings window

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

PIM Parameter Settings

The following window will configure the parameter settings for the PIM distribution tree.

To view this window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM Parameter Settings**, as shown below:



PIM Parameter Settings

Last Hop SPT Switchover	Never
Register Probe Time (1-127)	5
Register Suppression Time (3-255)	60

Figure 4- 124. PIM Parameter Settings window

The following fields can be viewed or set:

Parameter	Description
Last Hop SPT Switchover	This field is used by the last hop router to decide whether to receive multicast data from the shared tree or switch over to the shortest path tree. When the switchover mode is set to never, the last hope router will always receive multicast data from the shared tree. When the mode is set to immediately, the last hop router will always receive data from the shortest path tree.
Register Probe Time (1-127)	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 *1* and *127* seconds with a default setting of *5* seconds.
Register Suppression Time (3-255)	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 *3* and *255* with a default setting of *60* seconds.

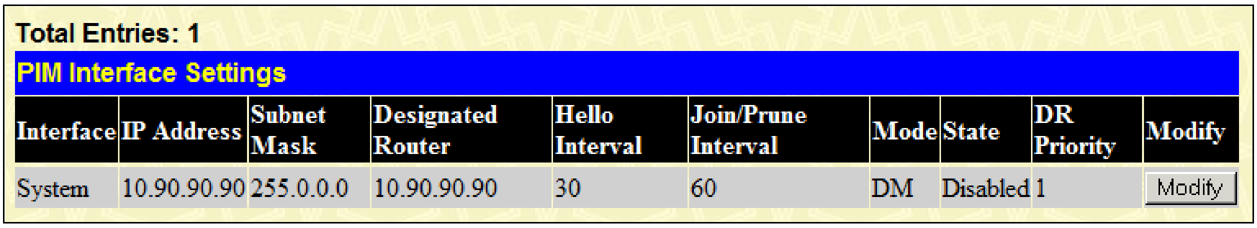
Click **Apply** to implement changes made.

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 Interface Settings

This window is used to configure the settings for the PIM Protocol per IP interface.

To view this window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM Interface Settings**, as shown below:



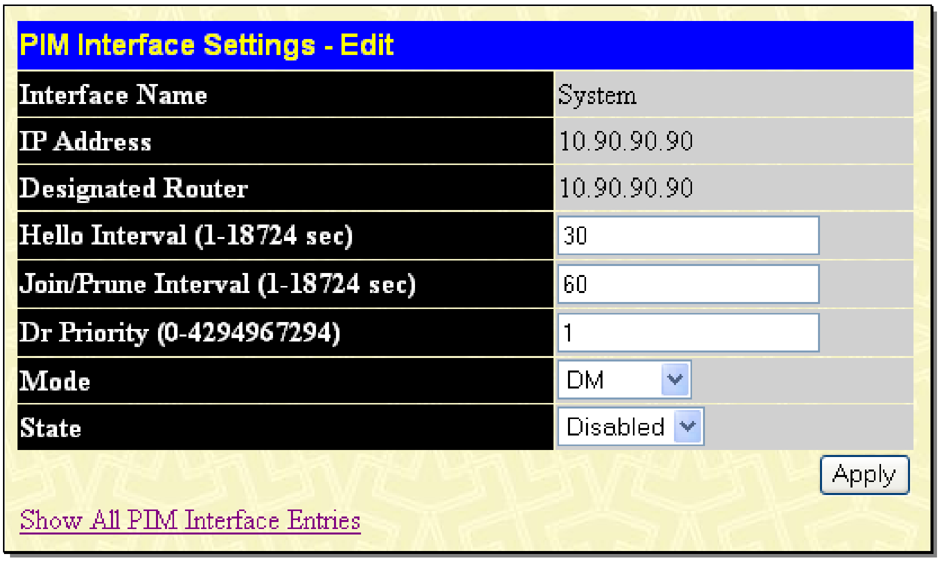
Total Entries: 1

PIM Interface Settings

Interface	IP Address	Subnet Mask	Designated Router	Hello Interval	Join/Prune Interval	Mode	State	DR Priority	Modify
System	10.90.90.90	255.0.0.0	10.90.90.90	30	60	DM	Disabled	1	Modify

Figure 4- 125. PIM Interface Settings window

To configure an IP interface for PIM, click its corresponding **Modify** button, which will lead you to the following window:



PIM Interface Settings - Edit

Interface Name	System
IP Address	10.90.90.90
Designated Router	10.90.90.90
Hello Interval (1-18724 sec)	30
Join/Prune Interval (1-18724 sec)	60
Dr Priority (0-4294967294)	1
Mode	DM
State	Disabled

Figure 4- 126. PIM Interface Settings – Edit window

The following fields can be set:

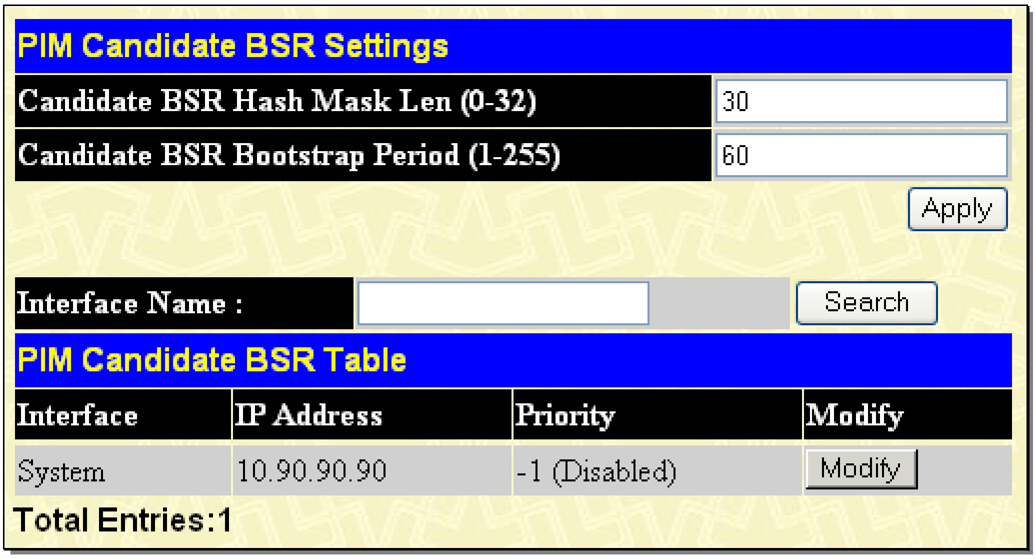
Parameter	Description
Interface Name	This read-only field denotes the IP interface selected to be configured for PIM.
IP Address	This read-only field denotes the IP address of the IP interface selected to be configured for PIM.
Designated Router	This read-only field denotes the IP address of the Designated 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* and *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* and *18724* seconds with a default interval time of *60* seconds.
DR Priority (0-4294967294)	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*.
Mode	Use the pull-down menu to select the type of PIM protocol to use, Sparse Mode (*SM*), Dense Mode (*DM*), or Sparse-Dense Mode (*SM-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*.

Click **Apply** to implement changes made.

PIM Candidate BSR Settings

The following windows are used to configure the Candidate Boot Strap Router 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 this window, click **L3 Features** > **IP Multicast Routing Protocol** > **PIM** > **PIM Candidate BSR Settings**, as shown below:



PIM Candidate BSR Settings

Candidate BSR Hash Mask Len (0-32)	30
Candidate BSR Bootstrap Period (1-255)	60

Interface Name :

PIM Candidate BSR Table

Interface	IP Address	Priority	Modify
System	10.90.90.90	-1 (Disabled)	Modify

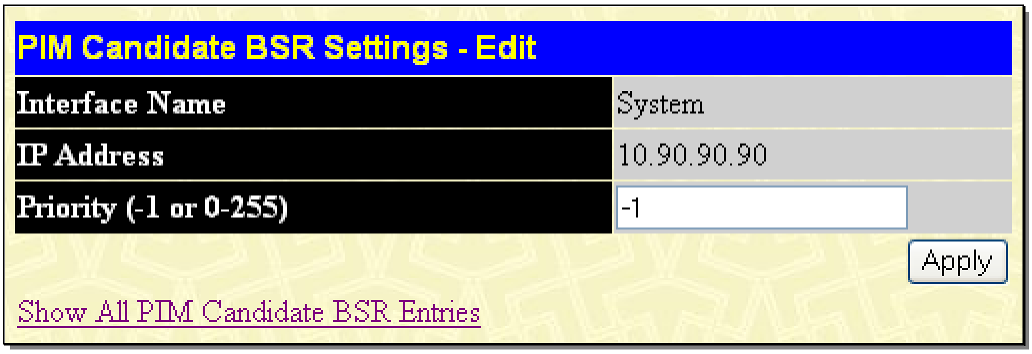
Total Entries:1

Figure 4- 127. PIM Candidate BSR Settings window

The following fields can be set:

Parameter	Description
Candidate BSR Hash Mask Len (0-32)	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* and *32* with a default setting of *30*.
Candidate BSR Bootstrap Period (1-255)	Enter a time period between *1* and *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 **Search**. 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 corresponding **Modify** button, which will lead you to the following window.



PIM Candidate BSR Settings - Edit

Interface Name	System
IP Address	10.90.90.90
Priority (-1 or 0-255)	-1

Figure 4- 128. PIM Candidate BSR Settings – Edit window

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 (-1 or 0-255)	Used to state the Priority of this IP Interface to become the BSR. The user may select a priority between *-1* and *0* to *255*. An entry of *-1* states that the interface will be disabled to be

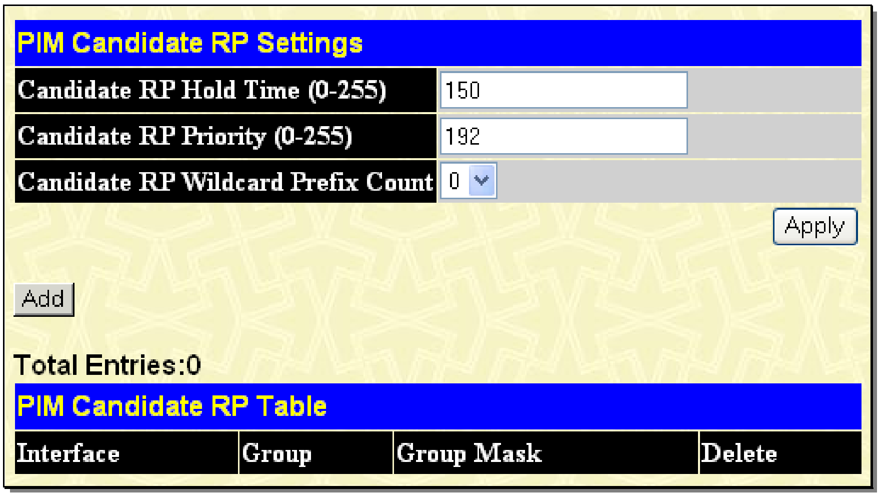
	the BSR.

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

PIM Candidate RP Settings

The following window is used to set the Parameters for this Switch to become a candidate RP.

To view this window, click **L3 Features** > **IP Multicast Routing Protocol** > **PIM** > **PIM Candidate RP Settings**, as shown below:



PIM Candidate RP Settings

Candidate RP Hold Time (0-255)	150
Candidate RP Priority (0-255)	192
Candidate RP Wildcard Prefix Count	0

Total Entries:0

PIM Candidate RP Table

Interface	Group	Group Mask	Delete

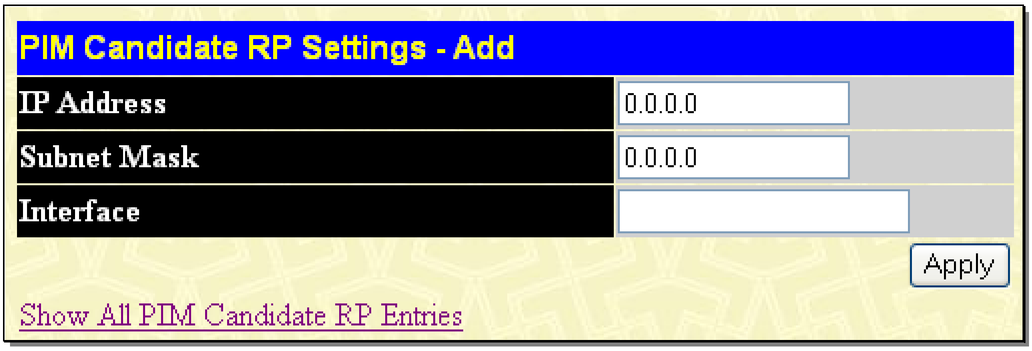
Figure 4- 129. PIM Candidate RP Settings window

The following fields can be viewed or set:

Parameter	Description
Candidate RP Hold Time (0-255)	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* and *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.
Candidate RP 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* and *255* with a default setting of *192*.
Candidate RP Wildcard Prefix Count	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. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To add a PIM Candidate RP, click the **Add** button in the previous window, which will display the following window for the user to configure.



PIM Candidate RP Settings - Add

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Interface	

Figure 4- 130. PIM Candidate RP Settings – Add window

The following fields can be set:

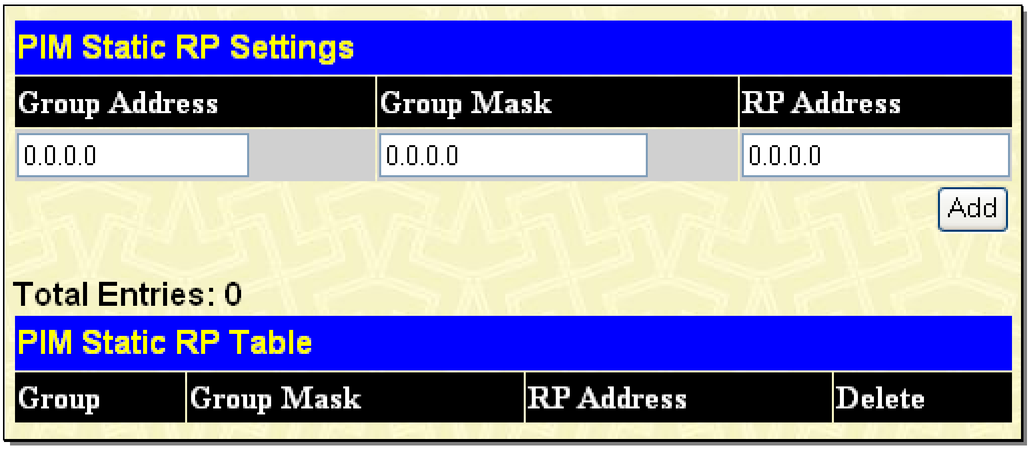
Parameter	Description
IP Address	Enter the IP address of the device to be added as a Candidate RP.
Subnet Mask	Enter the corresponding subnet mask of the device to be added as a Candidate RP.
Interface	Enter the IP interface where this device is located.

Click Apply to add the device as a Candidate RP.

PIM Static RP Settings

The following window will display the parameters for the switch to become a static RP.

To view this window, click **L3 Features** > **IP Multicast Routing Protocol** > **PIM** > **PIM Static RP Settings**, as shown below:



PIM Static RP Settings

Group Address	Group Mask	RP Address
0.0.0.0	0.0.0.0	0.0.0.0

Total Entries: 0

PIM Static RP Table

Group	Group Mask	RP Address	Delete

Figure 4- 131. PIM Static RP Settings window

The following fields can be viewed or set:

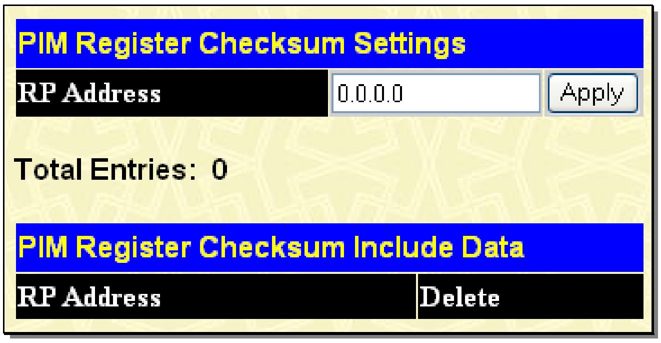
Parameter	Description
Group Address	Enter the multicast group address for this Static RP. This address must be a class D address.
Group Mask	Enter the mask for the multicast group address stated above.
RP Address	Enter the IP address of the rendezvous Point.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

PIM Register Checksum Settings

This window is used to configure RP addresses. The data part is included when calculating the checksum for a PIM register message to the RP on the first hop router.

To view this window, click **L3 Features** > **IP Multicast Routing Protocol** > **PIM** > **PIM Register Checksum Settings**, as shown below:



PIM Register Checksum Settings

RP Address: 0.0.0.0

Total Entries: 0

PIM Register Checksum Include Data

RP Address	Delete

Figure 4- 132. PIM Register Checksum Settings window

The following fields can be set:

Parameter	Description
RP Address	Enter the IP address of the RP for which the data part will be included when calculating checksum for registering packets to the RP.

Click **Apply** to add the RP into the checksum including the data list. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

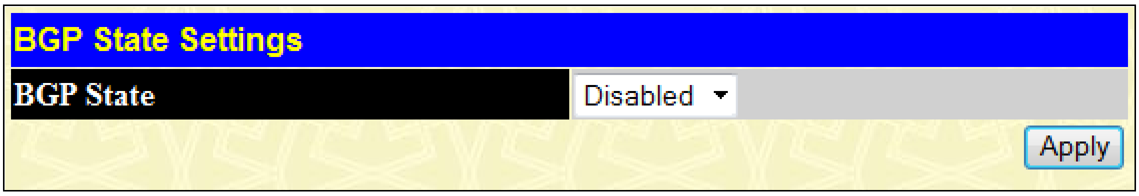
BGP

The Switch supports Border Gateway Protocol (BGP), a layer 3 Unicast routing protocol that maintains a table of IP networks or “prefixes” which designate network reachability among autonomous systems. BGP makes routing decisions based on path, network policies, and/or rule sets.

BGP Global Settings

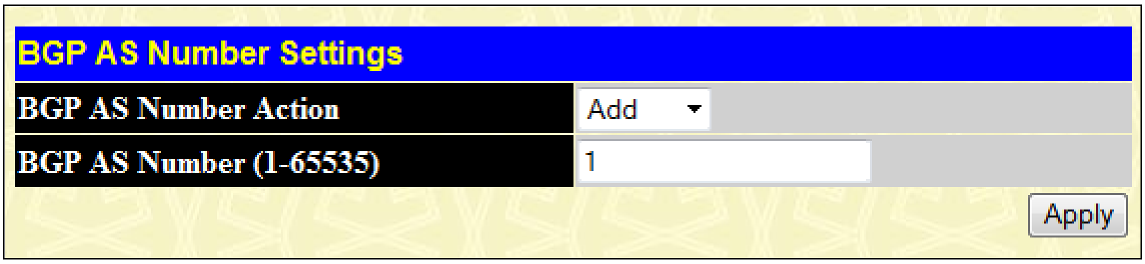
This window is used to configure BGP state, AS number, and global settings.

To view this window, click **L3 Features** > **BGP** > **BGP Global Settings**, as shown below:



BGP State Settings

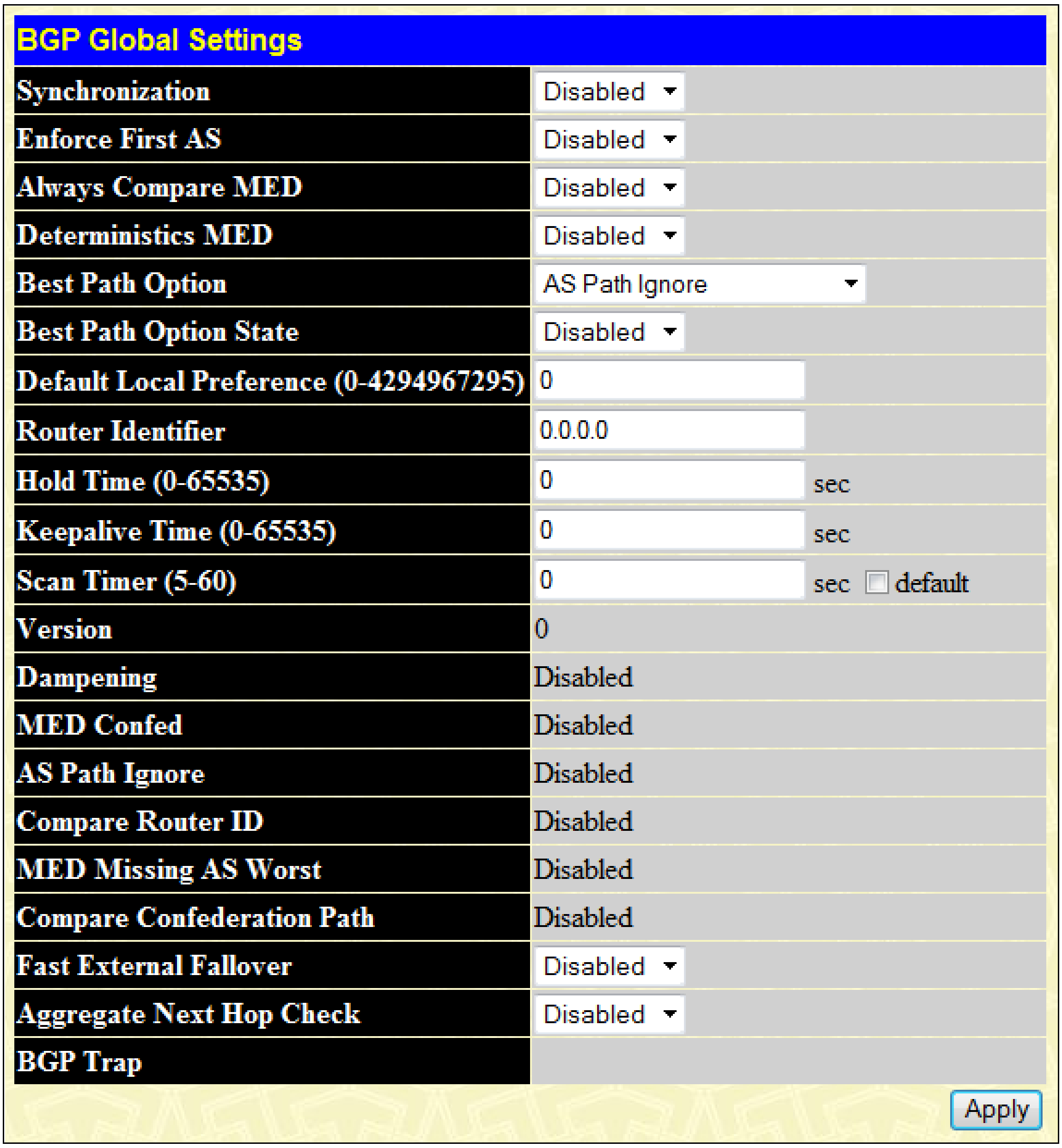
BGP State: Disabled



BGP AS Number Settings

BGP AS Number Action: Add

BGP AS Number (1-65535): 1



BGP Global Settings

Synchronization	Disabled
Enforce First AS	Disabled
Always Compare MED	Disabled
Deterministics MED	Disabled
Best Path Option	AS Path Ignore
Best Path Option State	Disabled
Default Local Preference (0-4294967295)	0
Router Identifier	0.0.0.0
Hold Time (0-65535)	0 sec
Keepalive Time (0-65535)	0 sec
Scan Timer (5-60)	0 sec □ default
Version	0
Dampening	Disabled
MED Confed	Disabled
AS Path Ignore	Disabled
Compare Router ID	Disabled
MED Missing AS Worst	Disabled
Compare Confederation Path	Disabled
Fast External Fallover	Disabled
Aggregate Next Hop Check	Disabled
BGP Trap	

Figure 4- 133. BGP State Settings window

To configure BGP state settings on the Switch, complete the following fields:

Parameter	Description
BGP State Settings	
BGP State	Use the drop-down menu to enable or disable the Border Gateway Protocol state. By disabling the BGP protocol, all peers will be disconnected and dynamic routes will be deleted. All the static configurations however will be reserved. If BGP is enabled again, the previous configurations can be re-applied.
BGP AS Number Settings	
BGP AS Number Action	Toggle to *Add* or *Delete* the BGP AS number. When the BGP protocol starts, it must belong to a single AS. The user must set the AS number before configuring any of the other attributes. When the BGP process is deleted, all peer and route information from BGP will be deleted. Route entries redistributed from BGP must also be canceled.
BGP AS Number (1-65535)	Enter a BGP AS number between 1 and 65535.

BGP Global Settings	
Synchronization	Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the BGP to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an Autonomous System to have the route before BGP makes it available to other autonomous systems.
Enforce First AS	This command is used to enforce the neighbor's AS as the first AS in the AS list. When the setting is *Enabled*, any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update, will be denied and the neighbor will be closed. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.
Always Compare MED	Enable or disable the comparison of the Multi Exit Discriminator (MED) for paths from the neighbors in different Autonomous Systems. By default this setting is *Disabled*.
Deterministics MED	Enable or disable to enforce the deterministic comparison of the Multi Exit Discriminator (MED) for paths received from the neighbors within the same Autonomous System. By default this setting is *Disabled*.
Best Path Option	Choose from *AS Path Ignore*, *Compare Router ID*, *Med Confed*, *MED Missing As Worst*, and *Compare Confed Aspath*. *AS Path Ignore* – If selected, the BGP process will ignore the AS path in the path selection process. *Compare Router ID* – If selected, the BGP process will include the router ID in the path selection process. Similar routes are compared and the route with the lowest router ID is selected. *Med Confed* – If selected, the BGP process will compare the MED for the routes that are received from confederation peers. For routes that have an external AS in the path, the comparison does not occur. *MED Missing As Worst* – If selecteded, the BGP process will assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute. If disabled, the BGP process will assign a value of zero to routes that are missing the Multi Exit Discriminator (MED) attribute, causing this route to be chosen as the best path. *Compare Confed Aspath* - If selected, the BGP process will compare the confederation AS path length of the routes received. The shorter the confederation AS path length, the better the route is.
Best Path Option State	Used to enable or disable AS Path Ignore, Compare Router ID, Med Confed, MED Missing As Worst, and Compare Confed Aspath. The default is *Disabled*.
Default Local Preference (0-4294967295)	Enter a default local preference between *0* and *4294967295*. The default value is *100*.
Route Identifier	This field is used to set BGP router ID. An ID to identify a BGP router. If it is set to zero the router ID will be automatically determined. User must specify a unique router ID within the network.
Hold Time (0-65535)	The valid values are from *0* to *65535*. The system will declare a peer as dead if a keepalive message is received that is more than the hold time. The default value is *180* seconds. If the holdtime is set to zero, then the holdtime will never expire. If the two routers that build a BGP connection have a different hold time, then the smaller hold time will be used. If the timer is specified for specific neighbors, then the neighbor specific timer will take effect. The hold time needs to be at least three times that of the keepalive timer.
Keepalive Time (0-65535)	The valid values are from *0* to *65535*. This specifies the interval at which keepalive messages are sent to its peer. If the keepalive value is set to zero, then the keepalive message will not be sent out. The default value is *60* seconds. If the two routers that build a BGP connection

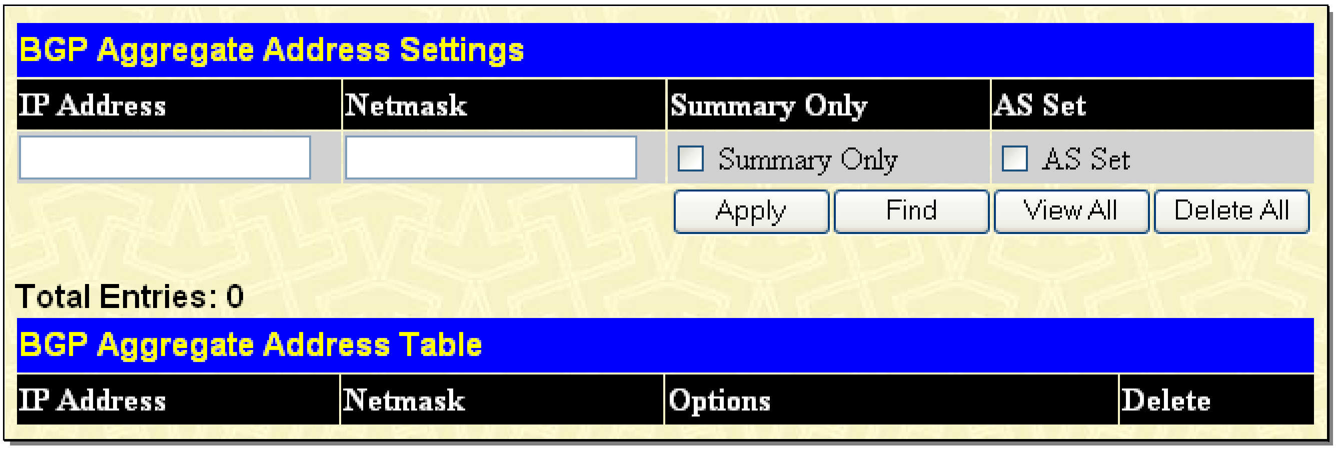
	have a different keepalive timer, then the smaller keepalive timer will be used. If the timer is specified for specific neighbors, then the neighbor specific timer will take effect.
Scan Timer (5-60)	Enter the BGP scan timer value from *5* to *60* seconds or tick the Default check box. The default value is *60* seconds.
Fast External Fallover	Enable or disable fast external fallover. This configures a Border Gateway Protocol (BGP) routing process to immediately reset its external BGP peer sessions if the link used to reach these peers goes down. The default state is *Enabled*.
Aggregate Next Hop Check	Enable or disable aggregate next hop check. This is used to configure the BGP aggregated routes' next hop check. Only the routes with the same next hop attribute can be aggregated if the BGP aggregate next hop check is *Enabled*. The default state is *Disabled*.

Click **Apply** to implement changes made.

BGP Aggregate Address Settings

This window is used to create an aggregate entry in the Border Gateway Protocol (BGP) database.

To view this window, click **L3 Features > BGP > BGP Aggregate Address Settings**, as shown below:



BGP Aggregate Address Settings

IP Address	Netmask	Summary Only	AS Set
		□ Summary Only	□ AS Set

Total Entries: 0

BGP Aggregate Address Table

IP Address	Netmask	Options	Delete

Figure 4- 134. BGP Aggregate Address Settings window

To configure BGP aggregate address settings on the Switch, complete the following fields:

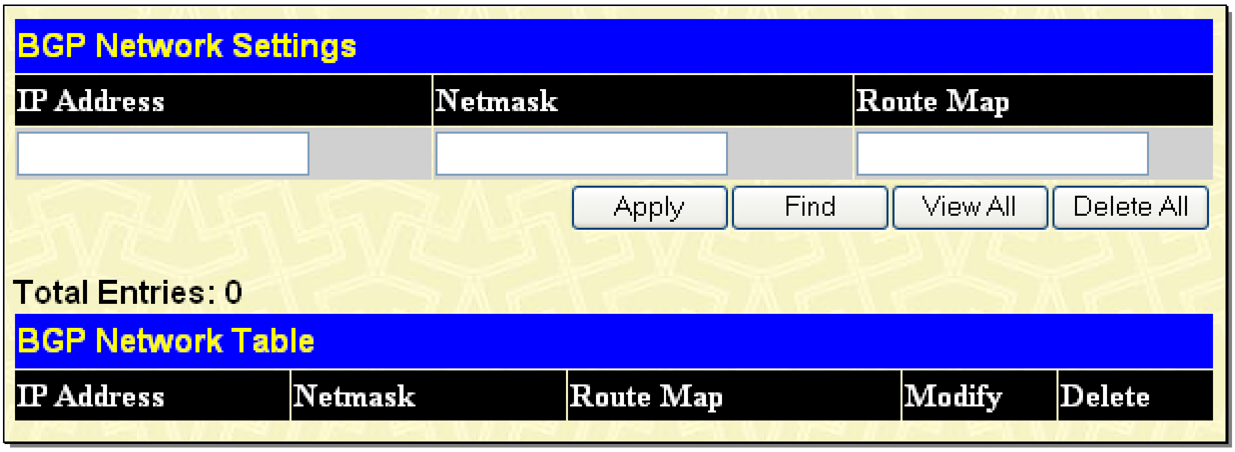
Parameter	Description
IP Address	Enter the IP network address to be aggregated.
Netmask	Enter the netmask of the IP network address to be aggregated.
Summary Only	Tick this check box to stop more specific routes from being advertised. The default setting is unticked.
AS Set	Tick this check box to generate Autonomous System set path information. The default setting is unticked.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

BGP Network Settings

This window is used to specify the network advertised by the Border Gateway Protocol (BGP).

To view this window, click **L3 Features > BGP > BGP Network Settings**, as shown below:



BGP Network Settings

IP Address	Netmask	Route Map

Total Entries: 0

BGP Network Table

IP Address	Netmask	Route Map	Modify	Delete

Figure 4- 135. BGP Network Settings window

To configure BGP network settings on the Switch, complete the following fields:

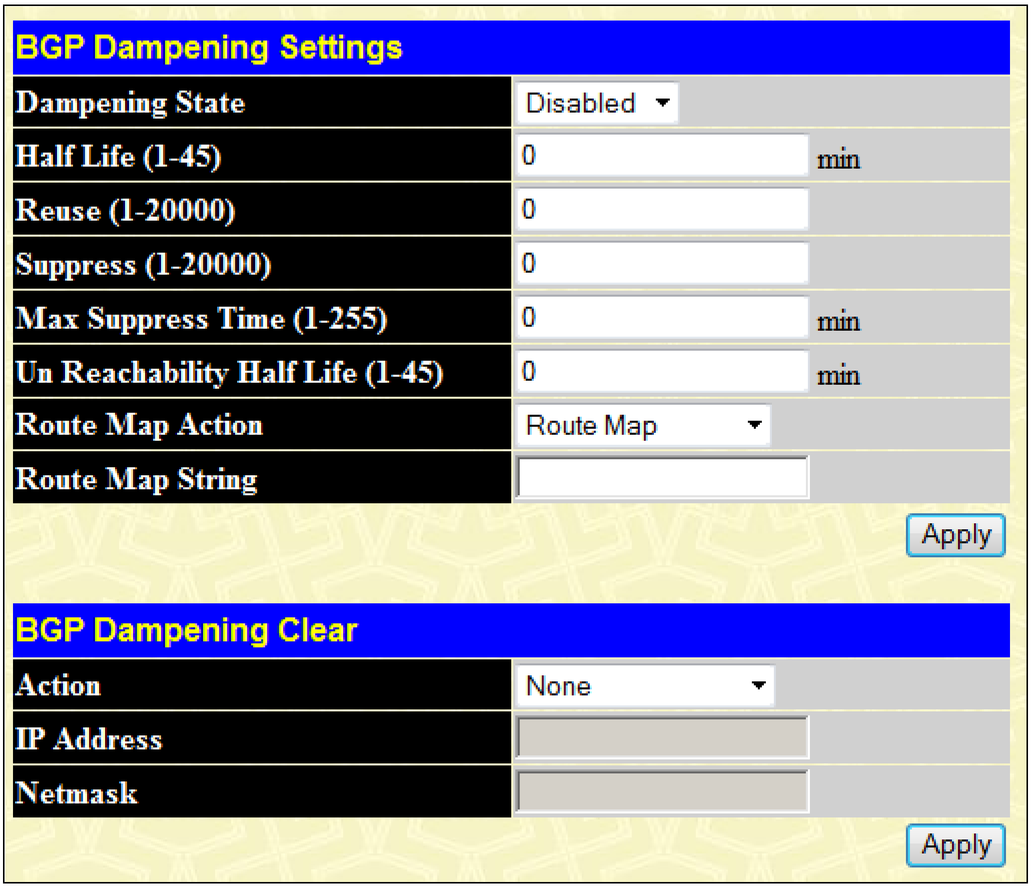
Parameter	Description
IP Address	Enter the IP address of the local network that BGP will advertise.
Netmask	Enter the netmask of the local network that BGP will advertise.
Route Map	Enter the route map to be applied to the advertised networks. If not specified, all networks are advertised.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

BGP Dampening Settings

This window is used to configure the Border Gateway Protocol (BGP) process's dampening settings. The purpose of this feature is to eliminate the dampening of routes and thus to avoid unstable networks caused by flapping routes.

To view this window, click **L3 Features > BGP > BGP Dampening Settings**, as shown below:



BGP Dampening Settings

Dampening State	Disabled
Half Life (1-45)	0 min
Reuse (1-20000)	0
Suppress (1-20000)	0
Max Suppress Time (1-255)	0 min
Un Reachability Half Life (1-45)	0 min
Route Map Action	Route Map
Route Map String	

BGP Dampening Clear

Action	None
IP Address	
Netmask	

Figure 4- 136. BGP Dampening Settings window

To configure BGP dampening settings on the Switch, complete the following fields:

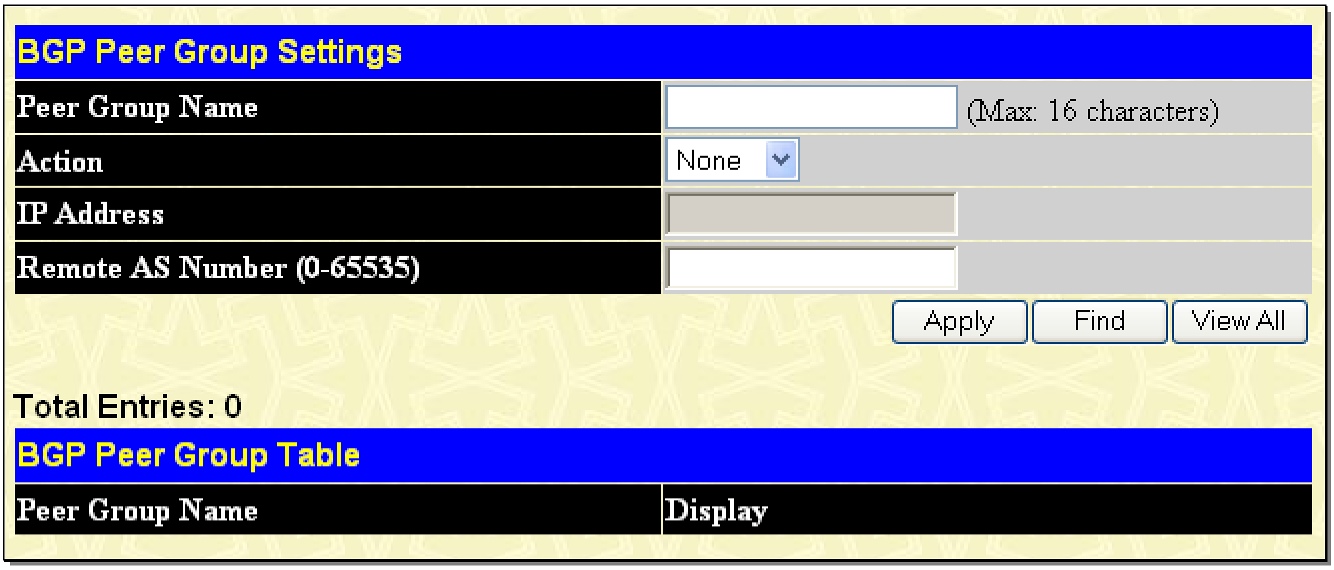
Parameter	Description
Dampening State	Select the BGP dampening function's state, *Enabled* or *Disabled*.
Half Life (1-45)	Enter the time (in minutes) after which the penalty of the reachable routes will be down, by half. The default setting is *15* minutes.
Reuse (1-20000)	Enter a reuse value. If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The default setting is *750*.
Suppress (1-20000)	Enter a suppress value. A route is suppressed when its penalty exceeds this limit. The default setting is *2000*.
Max Suppress Time (1-255)	Enter the maximum time (in minutes) a route can be suppressed. The default setting is *60* minutes.
Un Reachability Half Life (1-45)	Enter the time (in minutes) after which the penalty of the unreachable routes will be down, by half. The default setting is *15* minutes.
Route Map Action	Toggle between *Route Map* and *Clear Route Map*. *Route Map* sets the dampening running configuration while *Clear Route Map* withdraws the route map configuration.
Route Map String	Enter a route map name to be set or withdrawn. The default value is null.

Click **Apply** to implement changes made.

BGP Peer Group Settings

This window is used to create or delete a Border Gateway Protocol (BGP) neighbor.

To view this window, click **L3 Features > BGP > BGP Peer Group Settings**, as shown below:



BGP Peer Group Settings

Peer Group Name (Max: 16 characters)

Action None

IP Address

Remote AS Number (0-65535)

Total Entries: 0

BGP Peer Group Table

Peer Group Name	Display

Figure 4- 137. BGP Peer Group Settings window

To configure BGP peer group settings on the Switch, complete the following fields:

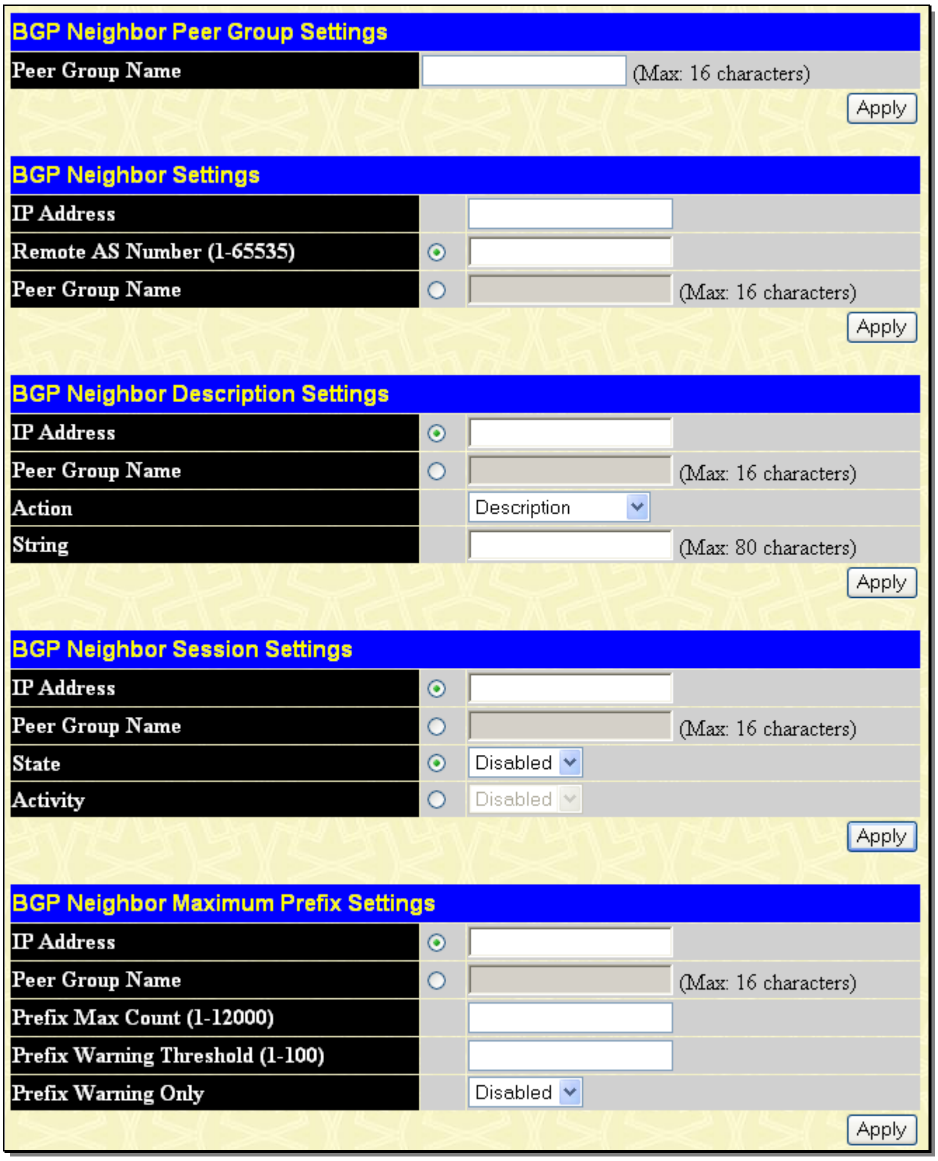
Parameter	Description
Peer Group Name	Enter the name of the BGP peer group.
Action	Choose among *None*, *Add*, or *Delete*. *None* is the default.
IP Address	Enter the IP address to be added or deleted.
Remote AS Number (0-65535)	Enter the number of the autonomous system to which the peer group belongs to. The range is from *0* to *65535*.

Click **Apply** to implement changes made.

BGP Neighbor Settings

This window is used to configure a Border Gateway Protocol (BGP) neighbor.

To view this window, click **L3 Features > BGP > BGP Neighbor Settings**, as shown below:



BGP Neighbor Peer Group Settings

Peer Group Name (Max: 16 characters)

Apply

BGP Neighbor Settings

IP Address

Remote AS Number (1-65535) ●

Peer Group Name ○ (Max: 16 characters)

Apply

BGP Neighbor Description Settings

IP Address ●

Peer Group Name ○ (Max: 16 characters)

Action: Description

String (Max: 80 characters)

Apply

BGP Neighbor Session Settings

IP Address ●

Peer Group Name ○ (Max: 16 characters)

State ● Disabled

Activity ○ Disabled

Apply

BGP Neighbor Maximum Prefix Settings

IP Address ●

Peer Group Name ○ (Max: 16 characters)

Prefix Max Count (1-12000)

Prefix Warning Threshold (1-100)

Prefix Warning Only: Disabled

Apply

Figure 4- 138. BGP Neighbor Peer Group Settings window

To configure BGP neighbor peer group settings on the Switch, complete the following fields:

Parameter	Description
BGP Neighbor Peer Group Settings	
Peer Group Name	Enter the name of the BGP peer group.
BGP Neighbor Settings	
IP Address	Enter the IP address of the BGP speaking neighbor.
Remote AS Number (1-65535)	Enter the number of autonomous systems to which the peer group belongs to. The range is from *1* to *65535*.
Peer Group Name	Enter the name of the BGP peer group.
BGP Neighbor Description Settings	

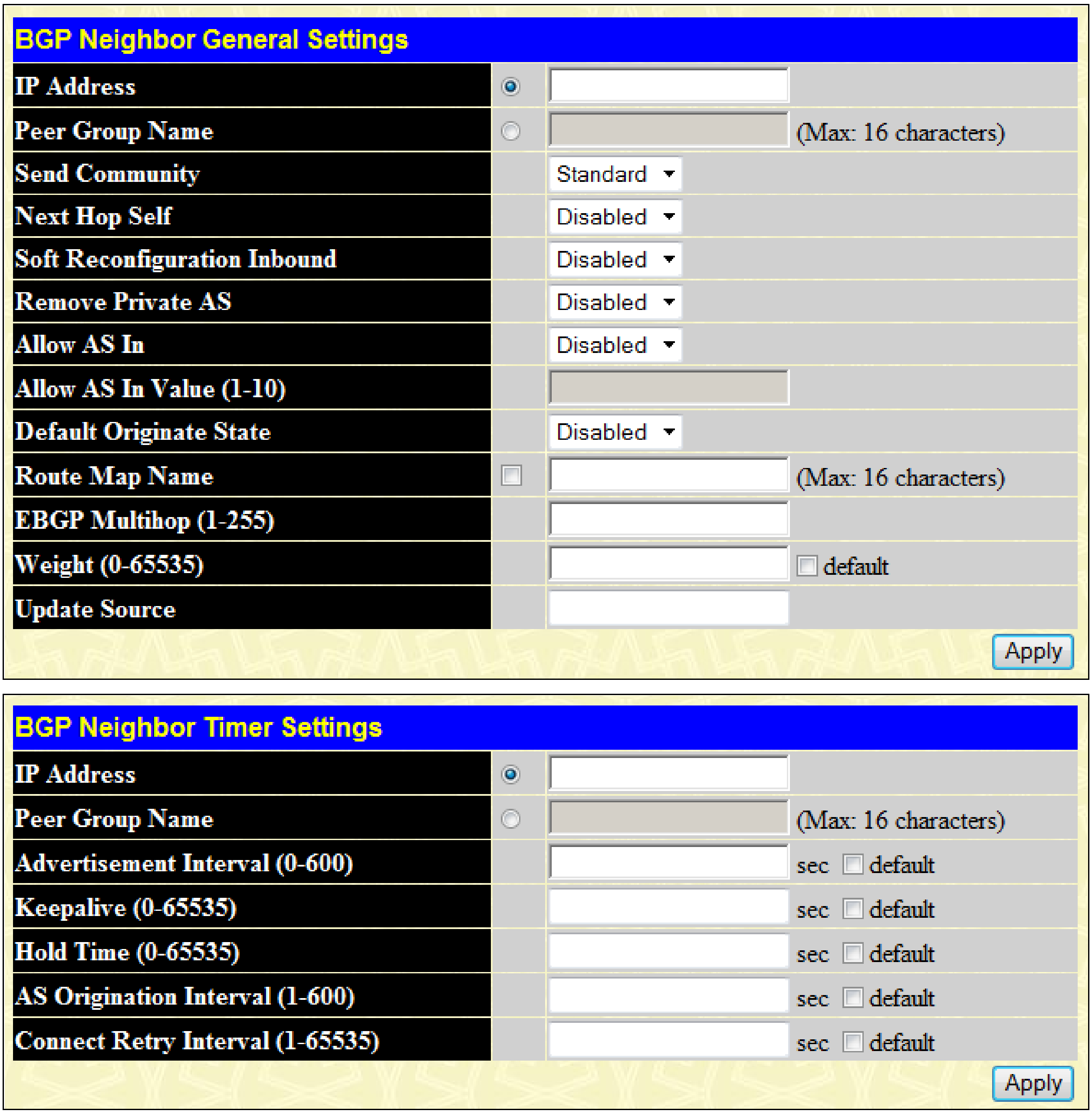
IP Address	Enter the IP address of the BGP speaking neighbor.
Peer Group Name	Enter the name of the BGP peer group.
Action	Toggle between *Description* and *Clear Description*. *Description* associates a description with a neighbor. By default, the description is not specified. *Clear Description* removes the neighbor's description.
String	Associate a description with a neighbor. By default, the description is not specified.
BGP Neighbor Session Settings	
IP Address	Enter the IP address of the BGP speaking neighbor.
Peer Group Name	Enter the name of the BGP peer group.
State	If state is changed from *Enabled* to *Disabled*, the session with the neighbor peer will be terminated.
Activity	Toggle to enable or disable the state for an individual address family. By default, the setting is enabled for IPv4 address families.
BGP Neighbor Maximum Prefix Settings	
IP Address	Enter the IP address of the BGP speaking neighbor.
Peer Group Name	Enter the name of the BGP peer group.
Prefix Max Count (1-12000)	Enter the maximum number of prefixes allowed from the specified neighbor. The default is *12000*.
Prefix Warning Threshold (1-100)	Enter the percentage the maximum prefix limit on the router starts to generate a warning message. The range is from *1* to *100*. The default is *75*.
Prefix Warning Only	Enable or disable prefix warning only. This allows the router to generate a log message when the maximum prefix limit is exceeded, instead of terminating the peering session.

Click **Apply** to implement changes made.

BGP Neighbor General & Timer Settings

This window is used to configure the BGP neighbor’s general and timer settings.

To view this window, click **L3 Features > BGP > BGP Neighbor General & Timer Settings**, as shown below:



BGP Neighbor General Settings

IP Address	●		
Peer Group Name	○		(Max: 16 characters)
Send Community		Standard	
Next Hop Self		Disabled	
Soft Reconfiguration Inbound		Disabled	
Remove Private AS		Disabled	
Allow AS In		Disabled	
Allow AS In Value (1-10)			
Default Originate State		Disabled	
Route Map Name	□		(Max: 16 characters)
EBGP Multihop (1-255)			
Weight (0-65535)			□ default
Update Source			

BGP Neighbor Timer Settings

IP Address	●		
Peer Group Name	○		(Max: 16 characters)
Advertisement Interval (0-600)			sec □ default
Keepalive (0-65535)			sec □ default
Hold Time (0-65535)			sec □ default
AS Origination Interval (1-600)			sec □ default
Connect Retry Interval (1-65535)			sec □ default

Figure 4- 139. BGP Neighbor General Settings window

To configure BGP neighbor general settings on the Switch, complete the following fields:

Parameter	Description
	BGP Neighbor General Settings
IP Address	Enter the IP address of the neighbor to be configured.
Peer Group Name	Enter the peer group to be configured.
Send Community	Toggle between *Standard* and *None*. This specifies the communities attribute to be sent to the BGP neighbor. *Standard* means only standard communities will be sent and *None* means no communities will be sent. The default value is *None*.

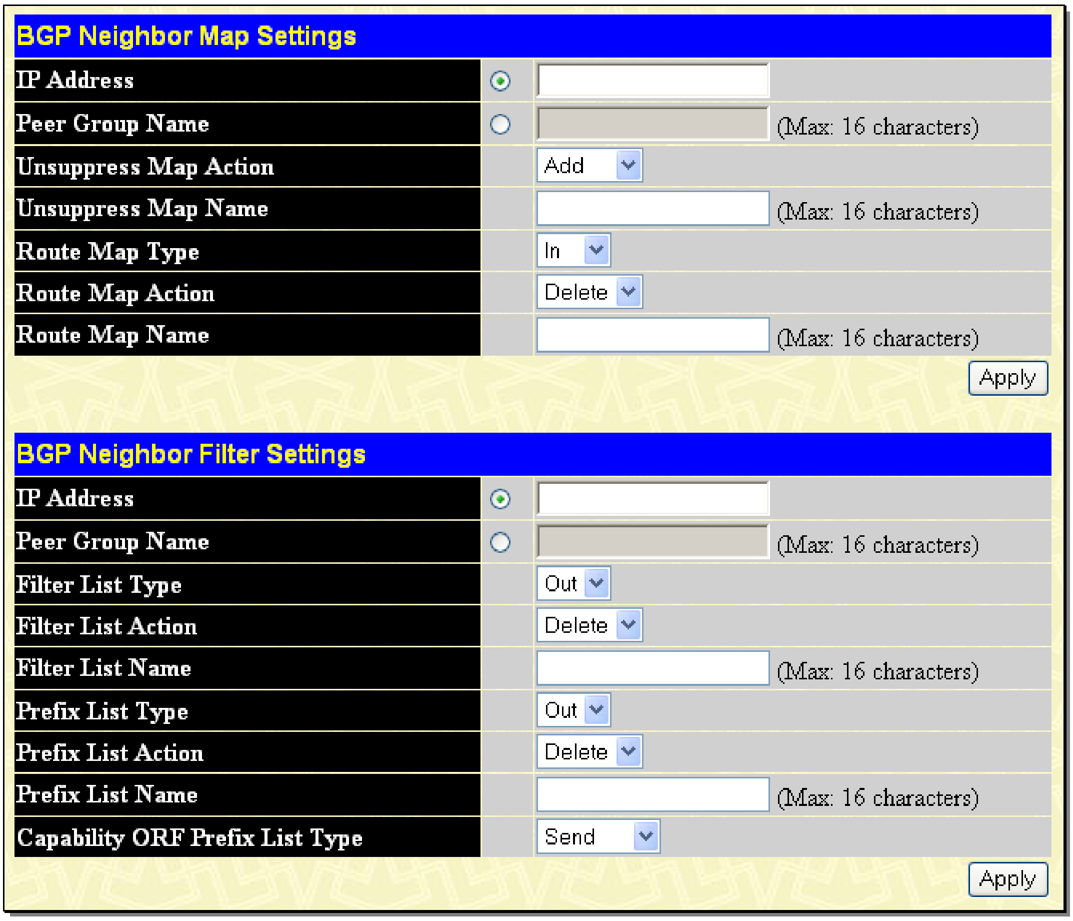
Next Hop Self	Enable or disable the next hop self attribute. By default, this setting is *Disabled*
Soft Reconfiguration Inbound	Enable or disable the inbound soft reconfiguration function. By default, this setting is *Disabled*.
Remove Private AS	If this setting is set to *Enabled*, the private AS number in the AS path attribute of the BGP update packets will be dropped. By default, the setting is *Disabled*.
Allow As In	If this is *Enabled,* the BGP router's self AS is allowed in the AS path list. By default, this setting is *Disabled*. If no number is supplied, the default value of three times is used.
Allow As In Value (1-10)	Enter an Allowas In Value between *1* and *10*.
Default Originate State	Enable or disable the default originate function. By default, this setting is *Disabled*.
Route Map Name	Enter a Route Map Name of a maximum of 16 characters.
EBGP Multihop (1-255)	Enter the TTL of the BGP packet sent to the neighbor. For an EBGP neighbor the default setting is 1. This means only direct connected neighbors are allowed.
Weight (0-65535)	Enter a value for weight. The valid range is from *0* to *65535*. If this is not specified, the routes learned through another BGP peer will have a default weight of 0. Routes sourced by the local router have a weight of 3768. It cannot be changed.
Update Source	Enter an interface to be used by BGP sessions for TCP connection. By default, this parameter is not set.
BGP Neighbor Timer Settings	
IP Address	Enter the IP address of the neighbor to be configured.
Peer Group Name	Enter the peer group to be configured.
Advertisement Interval (0-600)	Enter the interval at which the BGP process sends update messages to its peer. The valid value is from *0* to *600*. If this value is set to zero, the update or withdrawn message will be sent immediately. The default value for IBGP peers is 5 seconds and for EBGP peers it is 30 seconds. When the default check box is ticked, the neighbor specific advertisement interval setting will be returned to the default setting.
Keepalive (0-65535)	Enter the interval at which a keepalive message is sent to its peers. If the two routers, that build a BGP connection, have different keepalive timers, the smaller keepalive timer will be unset. The valid value is from *0* to *65535*. If the keepalive is set to zero, then the keepalive message will not be sent out. By default, the timer is not specified. This neighbor specific setting will follow the global setting.
Hold Time (0-65535)	The system will declare a peer as dead if not receiving a keepalive message until the hold time. If two routers, that built a BGP connection, have different hold times, the smaller hold time will be used. The valid value is from *0* to *65535*. If the holdtime is zero, then the holdtime will never expire. It is recommended that the holdtime value is three times that of the keepalive timer. By default, the timer is not specified. This neighbor specific setting will follow the global setting.
AS Origination Interval (1-600)	Enter the minimum interval between the sending AS origination routing updates. The valid value is from *1* to *600*. The default setting is *15* seconds.
Connect Retry Interval (1-65535)	Enter the minimum interval BGP sends TCP connect requests to the peer after a TCP connection fail happens. The valid value is from *1* to *65535*. The default setting is *120* seconds.

Click **Apply** to implement changes made.

BGP Neighbor Map & Filter Settings

This window is used to configure BGP neighbor map and filter settings.

To view this window, click **L3 Features > BGP > BGP Neighbor Map & FilterSettings**, as shown below:



BGP Neighbor Map Settings

IP Address	●	
Peer Group Name	○	(Max: 16 characters)
Unsuppress Map Action		Add
Unsuppress Map Name		(Max: 16 characters)
Route Map Type		In
Route Map Action		Delete
Route Map Name		(Max: 16 characters)

BGP Neighbor Filter Settings

IP Address	●	
Peer Group Name	○	(Max: 16 characters)
Filter List Type		Out
Filter List Action		Delete
Filter List Name		(Max: 16 characters)
Prefix List Type		Out
Prefix List Action		Delete
Prefix List Name		(Max: 16 characters)
Capability ORF Prefix List Type		Send

Figure 4- 140. BGP Neighbor Map & Filter Settings window

To configure BGP neighbor map & filter settings on the Switch, complete the following fields:

Parameter	Description
BGP Neighbor Map Settings	
IP Address	Enter the IP address of the neighbor to be configured.
Peer Group Name	Enter the peer group to be configured.
Unsuppress Map Action	Toggle between *Add* and *Delete*.
Unsuppress Map Name	Enter the name of a route map used to selectively advertise routes previously suppressed by the aggregate address command.
Route Map Type	Toggle between *In* and *Out*. *In* specifies the incoming routes from the neighbor and *Out* specifies the outgoing routes sent to the peer.
Route Map Action	Toggle between *Add* and *Delete*.
Route Map Name	Enter the route map to be applied to the incoming or outgoing routes.
BGP Neighbor Filter Settings	

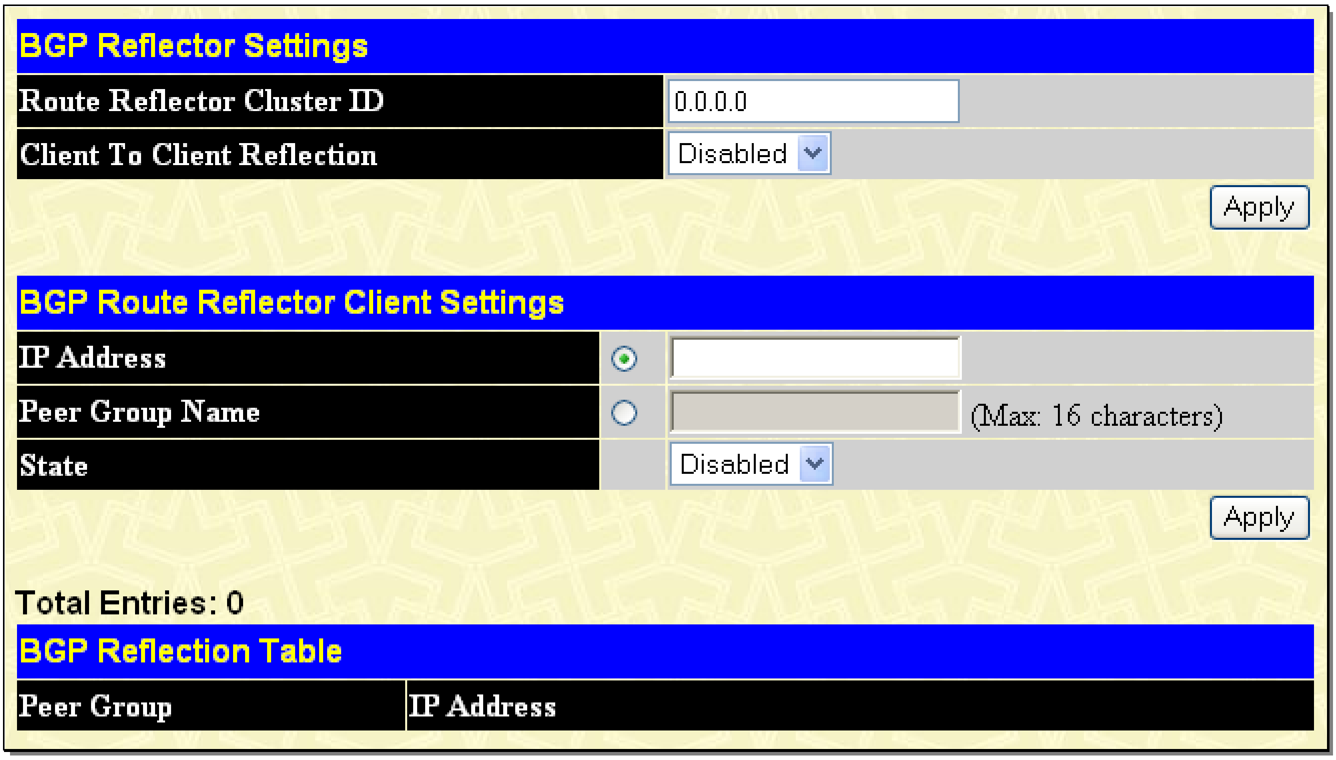
IP Address	Enter the IP address of the neighbor to be configured.
Peer Group Name	Enter the peer group to be configured.
Filter List Type	Toggle between *In* and *Out* to apply to either inbound or outbound traffic.
Filter List Action	Toggle between *Add* and *Delete*.
Filter List Name	Enter the name of an AS path access list to be applied as a filter. The filtering can be applied to incoming routes or outgoing routes.
Prefix List Type	Toggle between *In* and *Out* to apply to either inbound or outbound traffic.
Prefix List Action	Toggle between *Add* and *Delete*.
Prefix List Name	Enter the name of a prefix list to be applied as a filter. The filtering can be applied to incoming routes or outgoing routes.
Capability ORF Prefix List Type	Use to configure an outbound route filter prefix list capability. It can be sent with the following values: *Receive*: Enable the ORF prefix list capability in the receiving direction. The local router will install the prefix filter list notified by the remote router. *Send*: Enable the ORF prefix list capability in the sending direction. The local router will notify the remote router for the ORF prefix list capability. *Both*: Enable the ORF prefix list capability in both received and send directions. *None*: Disable the ORF prefix list capability in both received and send directions

Click **Apply** to implement changes made.

BGP Reflector Settings

This window is used to configure the BGP's neighbor of the route reflector client.

To view this window, click **L3 Features > BGP > BGP Reflector Settings**, as shown below:



BGP Reflector Settings

Route Reflector Cluster ID	0.0.0.0
Client To Client Reflection	Disabled

BGP Route Reflector Client Settings

IP Address	●	
Peer Group Name	○	(Max: 16 characters)
State		Disabled

Total Entries: 0

BGP Reflection Table

Peer Group	IP Address

Figure 4- 141. BGP Reflector Settings window

To configure BGP reflector settings on the Switch, complete the following fields:

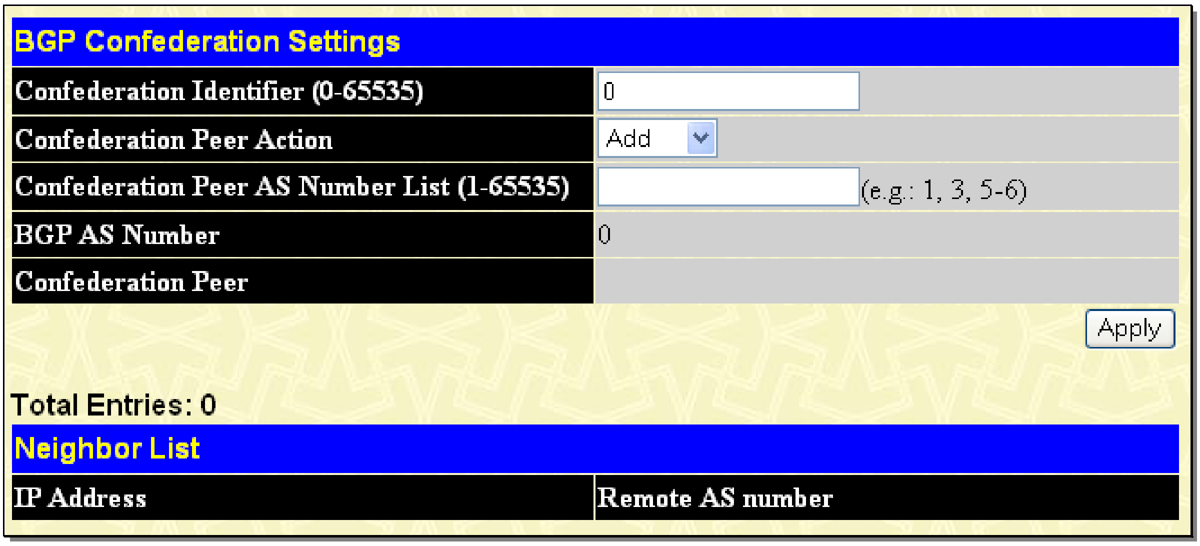
Parameter	Description
BGP Reflector Settings	
Route Reflector Cluster ID	Enter the IP address of the cluster ID. The route reflector and its clients together form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector. The BGP cluster ID command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and to avoid a single point of failure. When multiple route reflectors are configured in a cluster, they must be configured with the same cluster ID. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that needs to be stored in BGP routing tables. Setting the cluster ID to 0.0.0.0 will remove specifications of the cluster ID. The default value is *0.0.0.0*.
Client To Client Reflection	Enable or disable client-to-client reflection. When *Enabled*, the reflector operates in reflector mode. When *Disabled*, the reflector operates in non-reflector mode. This means the router will not reflect routes from the route reflect client to other route reflect clients, but it will still send routes received from a non-reflecting client to a reflecting client.
BGP Route Reflector Client Settings	
IP Address	Enter the IP address of the neighbor to be configured.
Peer Group Name	Enter the peer group to be configured.
State	When *Enabled*, the specified neighbor will become the router reflector client. By default, this state is *Disabled*.

Click **Apply** to implement changes made.

BGP Confederation Settings

This window is used to configure BGP confederation. A confederation, which is represented by an AS, is a group of the sub AS. A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single AS into multihop sub AS. External peers interact with the confederation as if it is a single AS. Each sub AS is fully meshed within itself and it has connections to other sub ASes within the confederation. The next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing users to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

To view this window, click **L3 Features > BGP > BGP Confederation Settings**, as shown below:



BGP Confederation Settings

Confederation Identifier (0-65535)	0
Confederation Peer Action	Add
Confederation Peer AS Number List (1-65535)	(e.g.: 1, 3, 5-6)
BGP AS Number	0
Confederation Peer	

Total Entries: 0

Neighbor List

IP Address	Remote AS number

Figure 4- 142. BGP Confederation Settings window

To configure BGP confederation settings on the Switch, complete the following fields:

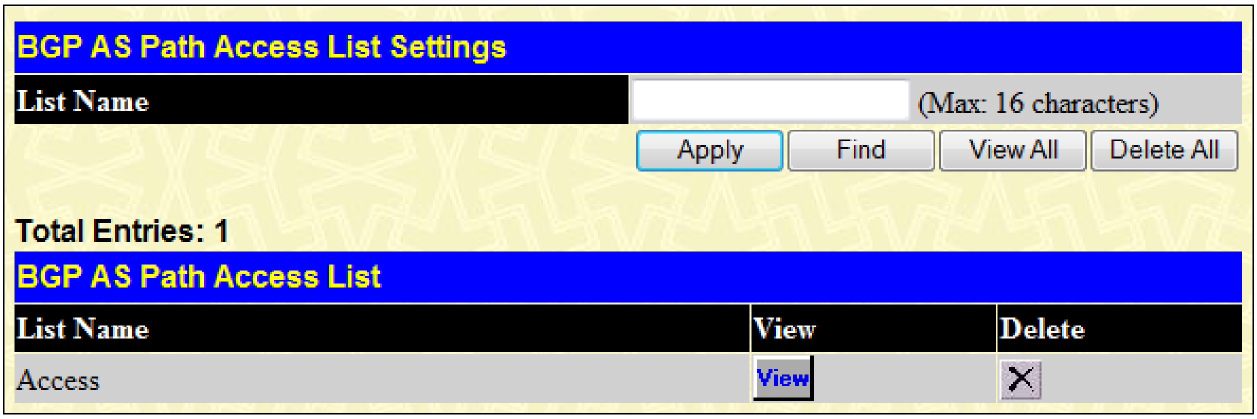
Parameter	Description
Confederation Identifier (0-65535)	Enter an Autonomous System number which is used to specify a BGP confederation. If it is set to zero, the BGP confederation number is deleted. By default, this setting is zero.
Confederation Peer Action	Toggle between *Add* and *Delete*.
Confederation Peer AS Number List (1-65535)	Enter one or multiple AS number partitions, each separated by a comma. These are the Autonomous System numbers for BGP peers that will belong to the confederation.

Click **Apply** to implement changes made.

BGP AS Path Access List Settings

This window is used to configure an Autonomous System path access list.

To view this window, click **L3 Features > BGP > BGP AS Path Access List Settings**, as shown below:



BGP AS Path Access List Settings

List Name (Max: 16 characters)

Total Entries: 1

BGP AS Path Access List

List Name	View	Delete
Access	View	☒

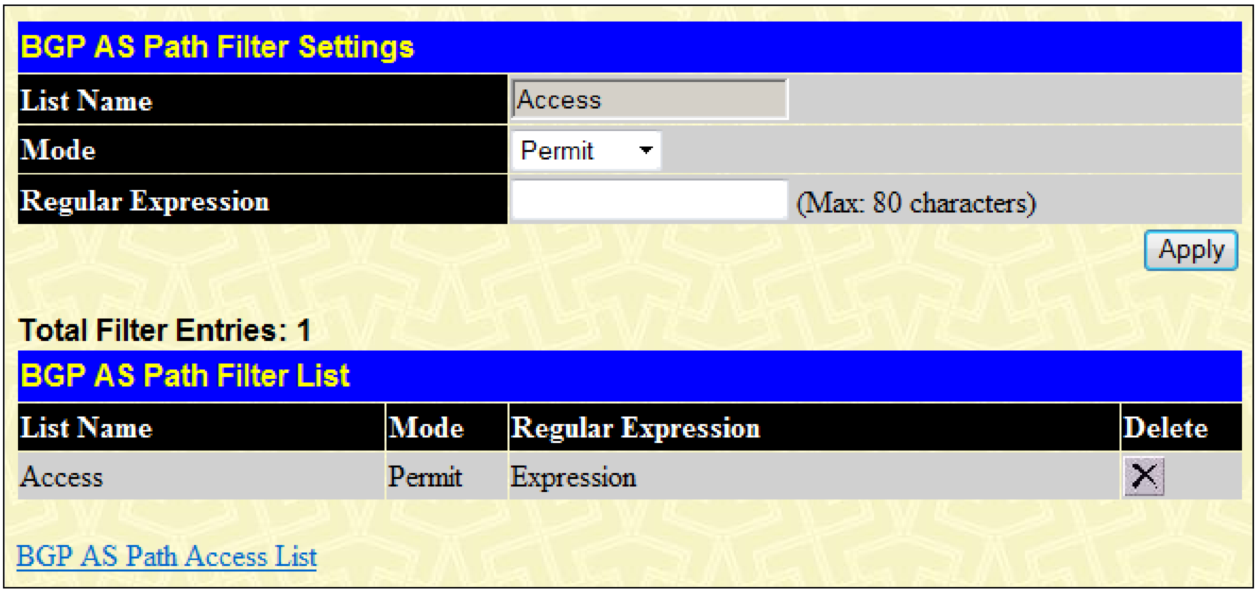
Figure 4- 143. BGP AS Path Access List Settings window

To configure BGP AS path access list settings on the Switch, complete the following fields:

Parameter	Description
List Name	Enter an Autonomous System path access list name.

Click **Apply** to implement changes made.

Click **View** to view the BGP AS Path Filter Settings for the specified entry, as shown below:



BGP AS Path Filter Settings

List Name	Access
Mode	Permit
Regular Expression	(Max: 80 characters)

Total Filter Entries: 1

BGP AS Path Filter List

List Name	Mode	Regular Expression	Delete
Access	Permit	Expression	☒

Figure 4- 144. BGP AS Path Filter Settings window

To configure BGP AS Path Filter Settings on the Switch, complete the following fields:

Parameter	Description
Mode	Select the mode option here. Options to choose from are *Permit* and *Deny*.
Regular Expression	Enter the regular expression string here.

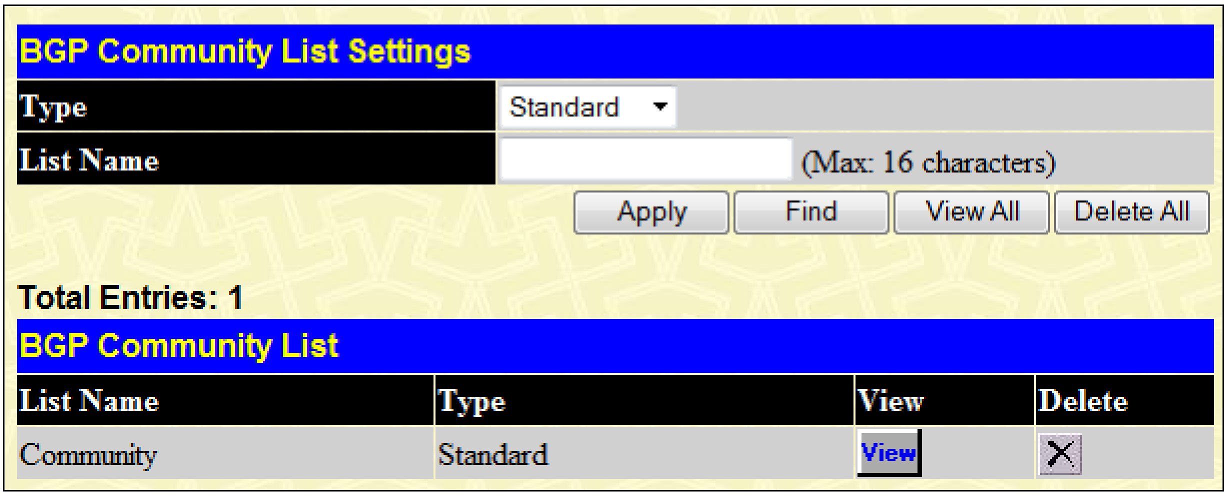
Click **Apply** to implement changes made.

Click the ☒ button to delete the specified entry.

BGP Community List Settings

This window is used to configure the matching rules for a BGP community list.

To view this window, click **L3 Features > BGP > BGP Community List Settings**, as shown below:



BGP Community List Settings

Type	Standard
List Name	(Max: 16 characters)

Total Entries: 1

BGP Community List

List Name	Type	View	Delete
Community	Standard	View	☒

Figure 4- 145. BGP Community List Settings window

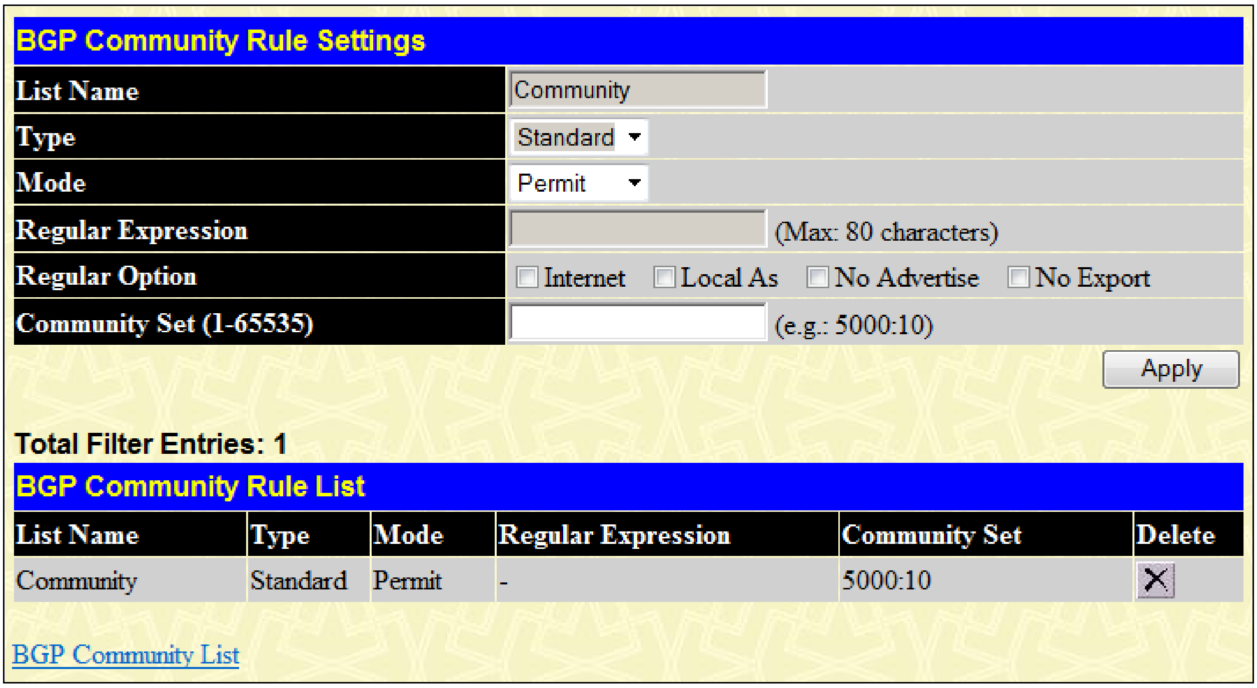
To configure BGP AS community list settings on the Switch, complete the following fields:

Parameter	Description
Type	Toggle between *Standard* and *Expanded*. *Standard* configures a standard community list and *Expanded* configures an expanded community list.

List Name	Enter the name of community list to be configured.

Click **Apply** to implement changes made.

Click **View** to access the BGP Community Rule Settings page for the specified entry, as shown below:



BGP Community Rule Settings

List Name	Community
Type	Standard
Mode	Permit
Regular Expression	(Max: 80 characters)
Regular Option	□ Internet □ Local As □ No Advertise □ No Export
Community Set (1-65535)	(e.g.: 5000:10)

Total Filter Entries: 1

BGP Community Rule List

List Name	Type	Mode	Regular Expression	Community Set	Delete
Community	Standard	Permit	-	5000:10	☒

Figure 4- 146. BGP Community Rule Settings window

To configure BGP Community Rule Settings on the Switch, complete the following fields:

Parameter	Description
Type	Select the type option here. Options to choose from are *Standard* and *Expanded*.
Mode	Select the mode option here. Options to choose from are *Permit* and *Deny*.
Regular Expression	When the *Expanded* type option is selected, enter the regular expression string here.
Regular Option	When the *Standard* type option is selected, select the regular option parameters listed here. Parameters available for selection are *Internet*, *Local As*, *No Advertise*, and *No Export*.
Community Set (1-65535)	When the *Standard* type option is selected, enter the community set value here.

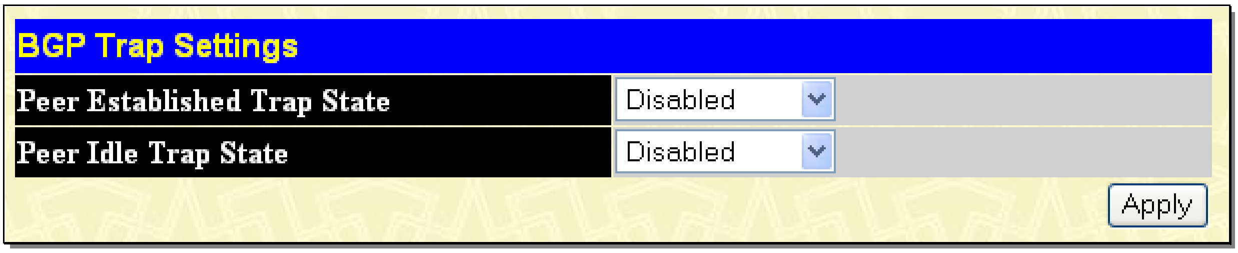
Click **Apply** to implement changes made.

Click the ☒ button to delete the specified entry.

BGP Trap Settings

This window is used to configure the BGP trap state.

To view this window, click **L3 Features > BGP > BGP Trap Settings**, as shown below:



BGP Trap Settings

Peer Established Trap State	Disabled
Peer Idle Trap State	Disabled

Figure 4- 147. BGP Trap Settings window

To configure BGP trap settings on the Switch, complete the following fields:

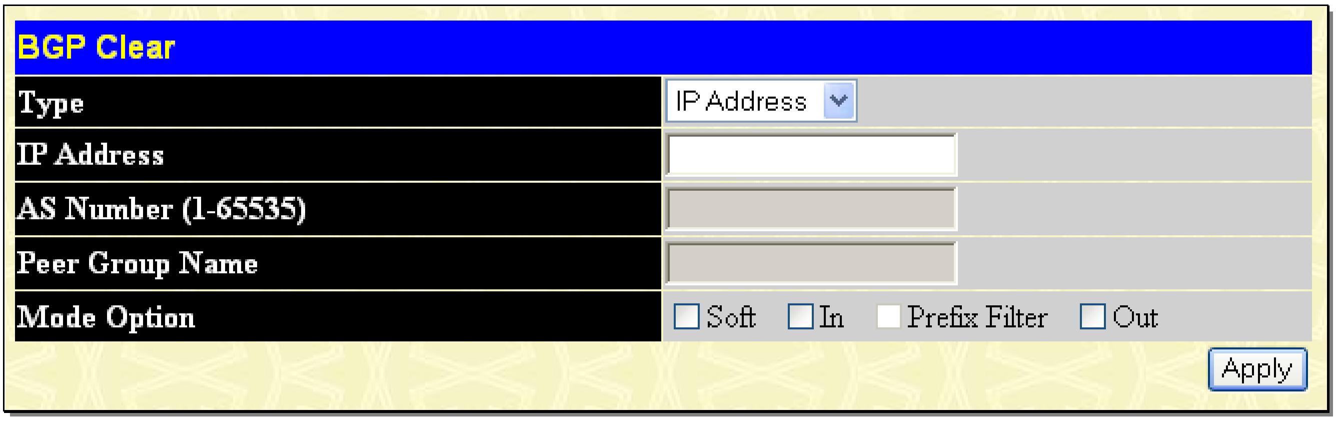
Parameter	Description
Peer Established Trap State	Enable or disable the sending of the peer established trap.The default value is *Disabled*.
Peer Idle Trap State	Enable or disable the sending of the peer idle trap. The default value is *Disabled*.

Click **Apply** to implement changes made.

BGP Clear

This window is used to reset the Border Gateway Protocol (BGP) connections using hard or soft reconfigurations.

To view this window, click **L3 Features > BGP > BGP Clear**, as shown below:



BGP Clear

Type	IP Address
IP Address	
AS Number (1-65535)	
Peer Group Name	
Mode Option	□ Soft □ In □ Prefix Filter □ Out

Figure 4- 148. BGP Clear window

To configure BGP clear on the Switch, complete the following fields:

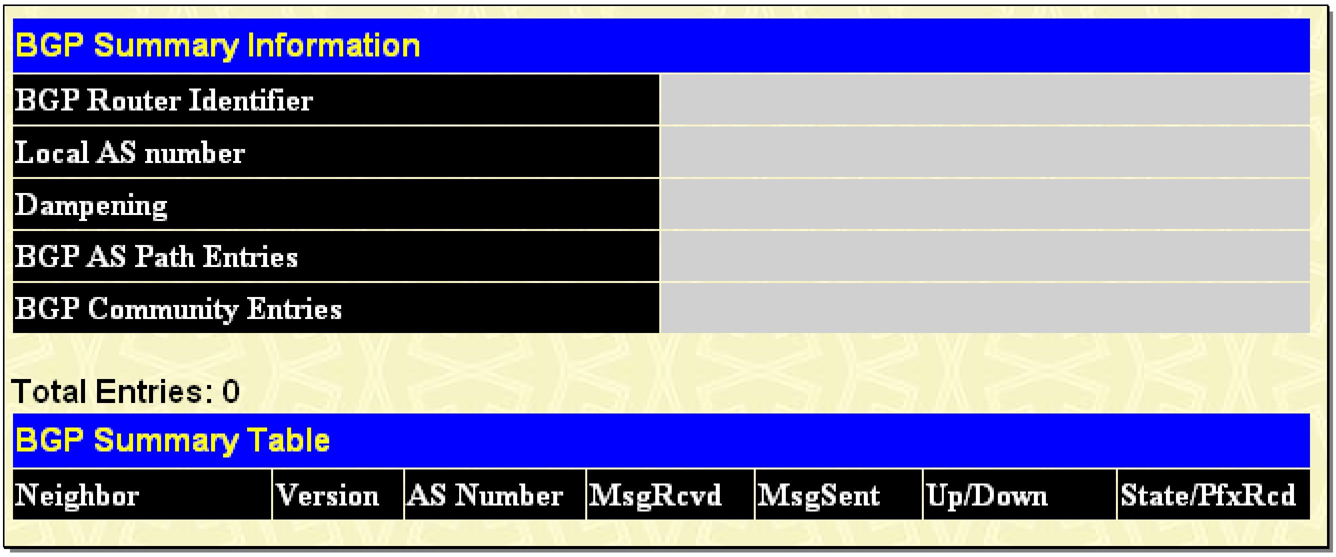
Parameter	Description
Type	Choose among *IP Address*, *AS*, *Peer Group*, *External*, or *All*. *IP Address* - Specify to reset the session with the specified neighbor. *AS* - Specify to reset sessions with BGP peers in the specified Autonomous System. *Peer Group* - Specify to reset a peer group. *External* - Specify all eBGP sessions will be reset. *All* - Specify that all current BGP sessions will be reset.
IP Address	If IP Address is specified in the Type above, enter an IP address.
AS Number (1-65535)	If AS is specified in the Type above, enter an Autonomous System number.
Peer Group Name	If Peer Group is specified in the Type above, enter a peer group name.

Mode Option	Tick the desired mode option: Soft, In, Prefix Filter, or Out. Soft – This initiates a soft reset. It does not tear down the session. In – This iInitiates inbound reconfiguration. If neither in nor out keywords are specified, both inbound and outbound sessions are reset. Prefix Filter – The local site configured prefix filter will be notified to the remote neighbor when inbound soft reset is applied. Out – This initiates outbound reconfiguration.

Click **Apply** to implement changes made.

BGP Summary Table

To view this read-only window, click **L3 Features > BGP > BGP Summary Tables**, as shown below:



BGP Summary Information

BGP Router Identifier	
Local AS number	
Dampening	
BGP AS Path Entries	
BGP Community Entries	

Total Entries: 0

BGP Summary Table

Neighbor	Version	AS Number	MsgRcvd	MsgSent	Up/Down	State/PfxRcd

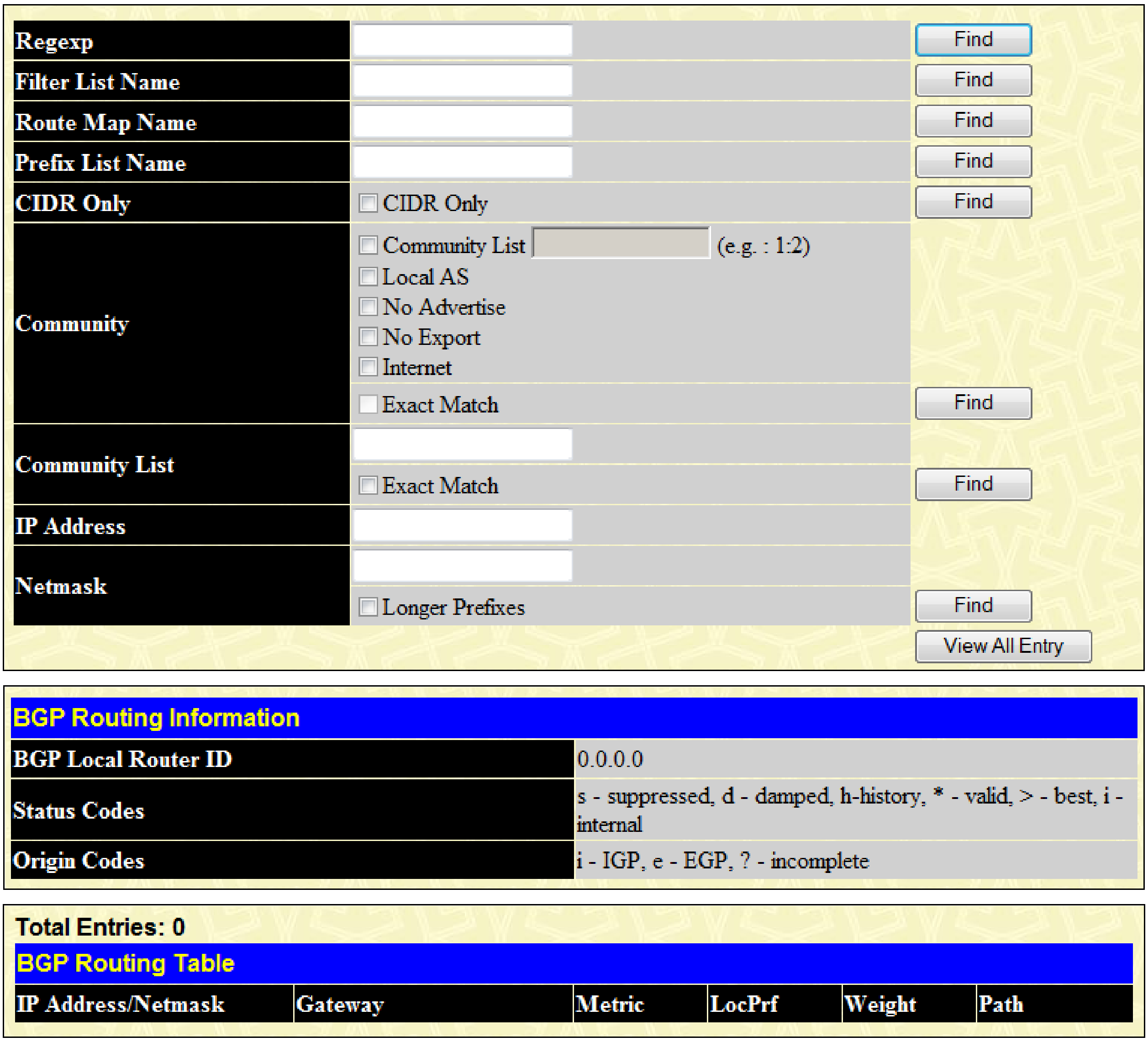
Figure 4- 149. BGP Summary Information window

The BGP summary information parameters are described below:

Parameter	Description
BGP Summary Information	
BGP Router Identifier	This field is used to display the local BGP router identifier previously configured.
Local AS Number	This field is used to display the local AS Number previously configured.
Dampening	This field is used to display the BGP dampending state: enabled or disabled.
BGP AS Path Entries	This field is used to display the total number of BGP AS path entries.
BGP Community Entries	This field is used to display the total number of BGP community entries.
BGP Summary Table	
Neighbor	This field is used to display the IP address of the BGP neighbor.
Version	This field is used to display the BGP version of the BGP neighbor.
AS Number	This field is used to display the remote AS number of the BGP neighbor.
MsgRcvd	This field is used to display the number of all BGP packets received from the BGP neighbor.
MsgSent	This field is used to display the number of all BGP packets sent to the BGP neighbor.
Up/Down	This field is used to display the connecting state or connecting time of the BGP neighbor.
State/PfxRcd	This field is used to display the establishing state or the number of BGP prefixes received from the BGP neighbor.

BGP Routing Table

To view this window, click **L3 Features > BGP > BGP Routing Table**, as shown below:



Regexp	
Filter List Name	
Route Map Name	
Prefix List Name	
CIDR Only	□ CIDR Only
Community	□ Community List (e.g. : 1:2) □ Local AS □ No Advertise □ No Export □ Internet □ Exact Match
Community List	 □ Exact Match
IP Address	
Netmask	 □ Longer Prefixes

BGP Routing Information	
BGP Local Router ID	0.0.0.0
Status Codes	s - suppressed, d - damped, h-history, * - valid, > - best, i - internal
Origin Codes	i - IGP, e - EGP, ? - incomplete

Total Entries: 0

BGP Routing Table

IP Address/Netmask	Gateway	Metric	LocPrf	Weight	Path

Figure 4- 150. BGP Route Information window

The BGP route information parameters are described below:

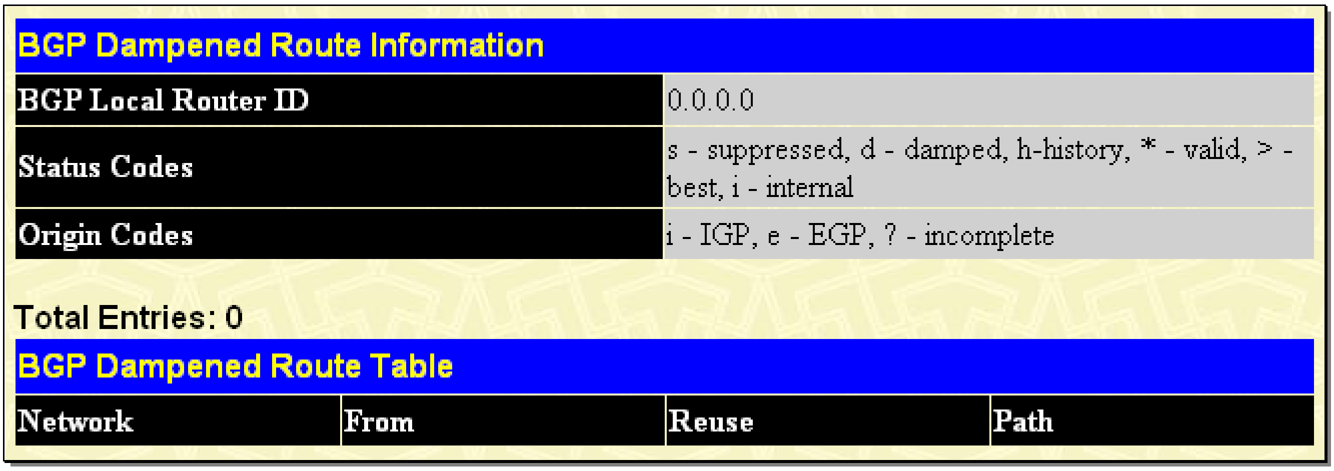
Parameter	Description
Regexp	Enter the regular expression that defines the AS path filter.
Filter List Name	Enter the filter list name that was previously created by bgp as_path access_list. This is used to display routes conforming to the filter list.
Route Map Name	Enter the filter list name that was previously created by route map. This is used to display routes matching the route map.
Prefix List Name	Enter the filter list name that was previously created by ip prefix list. This is used to display routes conforming to the prefix list.
CIDR Only	Tick Classless Inter-Domain Routing (CIDR) Only to just display routes with custom masks.
Community	This is used to display routes matching the communities.
Community List	Enter the community list or tick the Exact Match check box.

IP Address	This is used to display the host route that matches the specified IP address.
Netmask	This field works with the above IP address and is used to display the route that matches the specified network address. If specified, more specific routes will also be displayed.
BGP Route Information	
BGP Local Router ID	This field is used to display the BGP local router ID.
Status Codes	This field is used to show the meaning of some characters.
Origin Codes	This field is used to show the meaning of some characters.
BGP Route Table	
IP Address/Netmask	This field is used to display the IP address/netmask and status code of a specified route.
Gateway	This field is used to display the gateway of a specified route.
Metric	This field is used to display the metric of a specified route.
LocPrf	This field is used to display the local preference of a specified route.
Weight	This field is used to display the weight of a specified route.
Path	This field is used to display the AS path and origin code of a specified route.

BGP Dampened Route Table

This read-only window displays BGP dampened route information.

To view this window, click **L3 Features > BGP > BGP Dampened Route Table**, as shown below:



BGP Dampened Route Information

BGP Local Router ID	0.0.0.0
Status Codes	s - suppressed, d - damped, h-history, * - valid, > - best, i - internal
Origin Codes	i - IGP, e - EGP, ? - incomplete

Total Entries: 0

BGP Dampened Route Table

Network	From	Reuse	Path

Figure 4- 151. BGP Dampened Route Information window

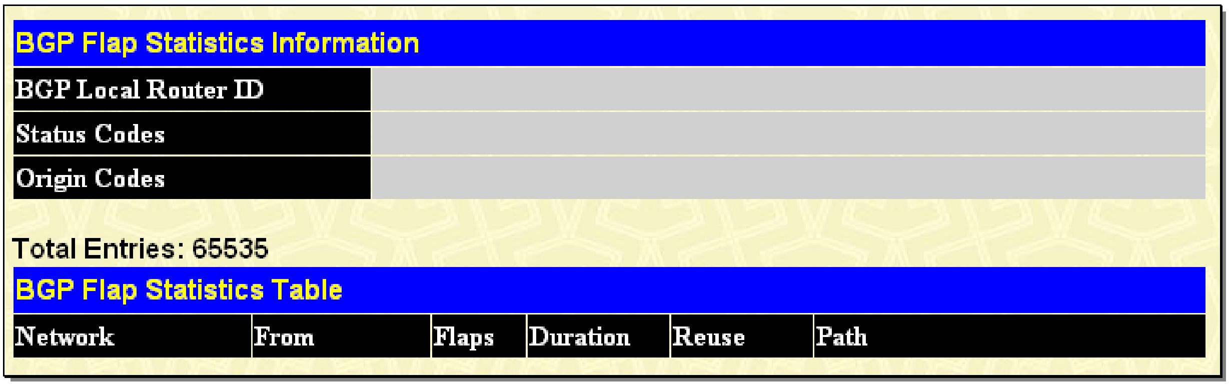
The BGP dampened route information parameters are described below:

Parameter	Description
BGP Local Router ID	This field is used to display the BGP local router ID.
Status Codes	This field is used to show the meaning of the characters and symbols used on this window.
Origin Codes	This field is used to show the meaning of the characters and symbols used on this window.
Network	This field is used to display the network and status code of a specified route.
From	This field is used to display where a specified route is from.
Reuse	The field is used to disaplay the reused time of a specified route.
Path	This field is used to display the AS path and origin code of a specified route.

BGP Flap Statistics Table

This read-only window displays BGP flap statistics information.

To view this window, click **L3 Features > BGP > BGP Flap Statistics Table**, as shown below:



BGP Flap Statistics Information

BGP Local Router ID	
Status Codes	
Origin Codes	

Total Entries: 65535

BGP Flap Statistics Table

Network	From	Flaps	Duration	Reuse	Path

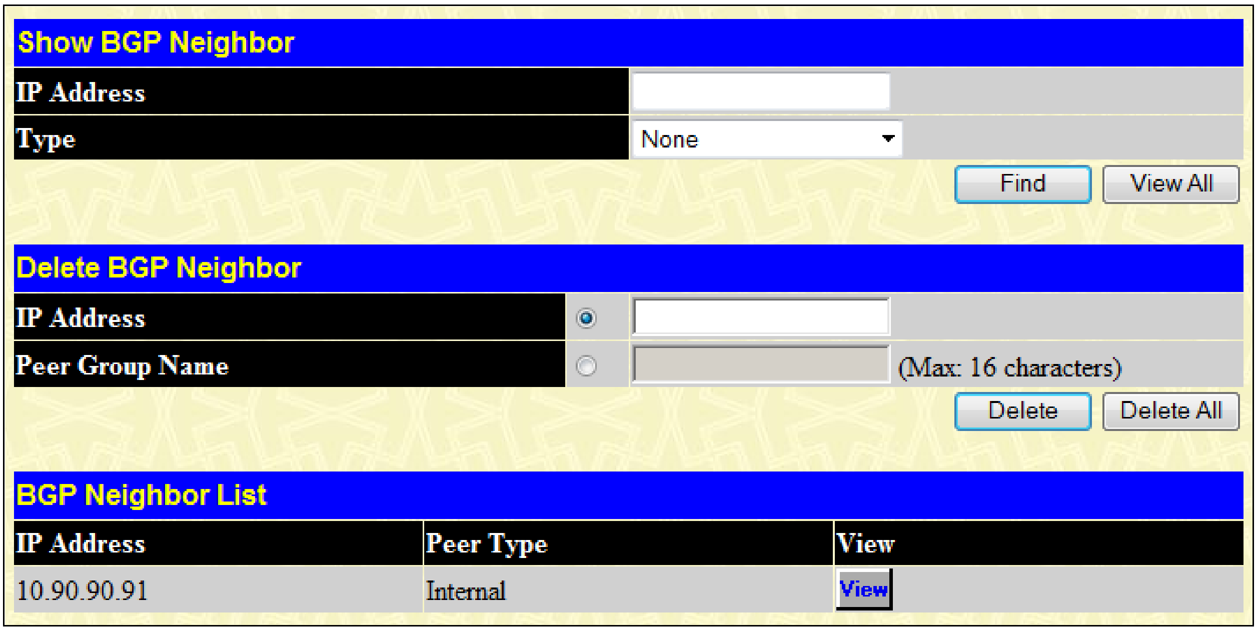
Figure 4- 152. BGP Flap Statistics Information window

The BGP flap statistics table information parameters are described below:

Parameter	Description
BGP Local Router ID	This field is used to display the BGP local router ID.
Status Codes	This field is used to show the meaning of the characters and symbols used on this window.
Origin Codes	This field is used to show the meaning of the characters and symbols used on this window.
Network	This field is used to display the network and status code of a specified route.
From	This field is used to display where a specified route is from.
Flaps	The field is used to display the flapped count of a specified route.
Duration	The field is used to display the duration of dampened time of a specified route.
Reuse	The field is used to disaplay the reused time of a specified route.
Path	This field is used to display the AS path and origin code of a specified route.

BGP Neighbors List

To view this window, click **L3 Features > BGP > BGP Neighbors List**, as shown below:



Show BGP Neighbor

IP Address	
Type	None

Delete BGP Neighbor

IP Address	●	
Peer Group Name	○	(Max: 16 characters)

BGP Neighbor List

IP Address	Peer Type	View
10.90.90.91	Internal	View

Figure 4- 153. Show BGP Neighbor window

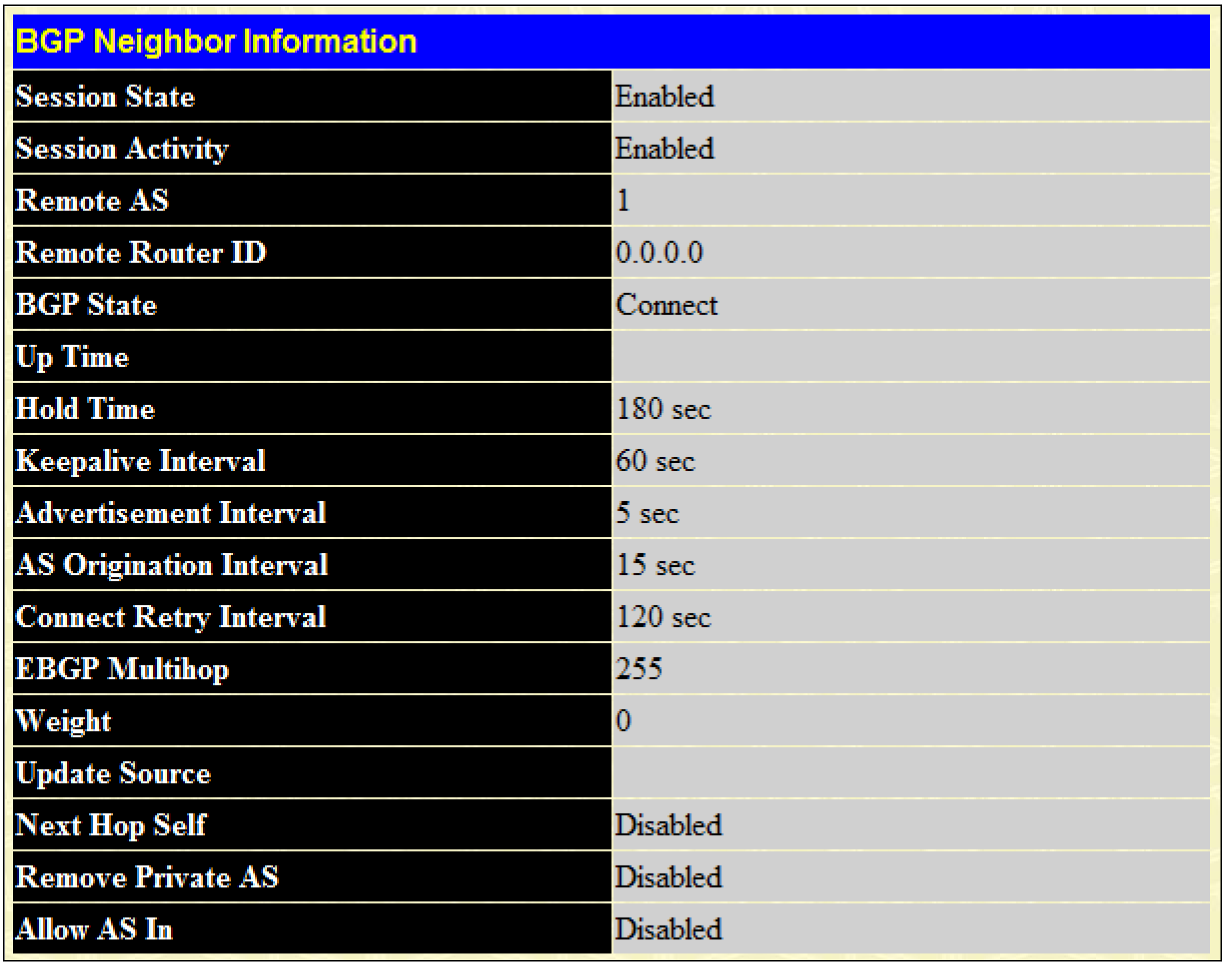
The BGP neighbor list parameters are described below:

Parameter	Description
Show BGP Neighbor	
IP Address	Enter the IP address of the BGP neighbor to be displayed.
Type	Choose among: *None*, *Advertised Routes*, *Received Routes*, *Routes*, *Received Prefix Filter*, and *Statistics*.
Delete BGP Neighbor	
IP Address	Click the radio button and enter the IP address of the BGP neighbor to be deleted.
Peer Group Name	Click the radio button and enter the peer group name of the BGP neighbor to be deleted.

Click **Find** to display a specific BGP neighbor or click **View All** to display all configured BGP neighbors.

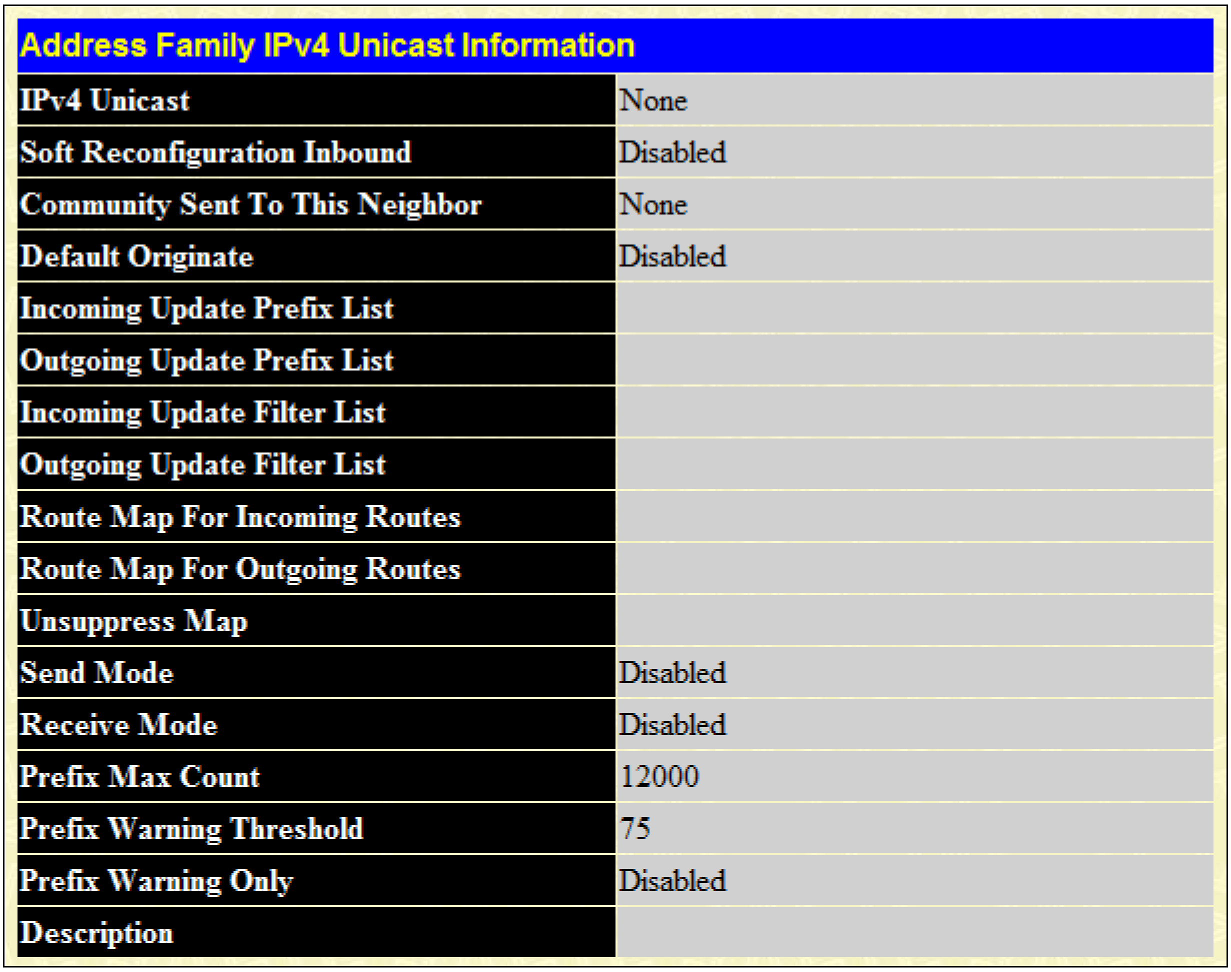
Click **Delete** to remove a specific BGP neighbor or click **Delete All** to remove all configured BGP neighbors.

Click **View** to access the BGP Neighbor Information page for the specified entry, as shown below:



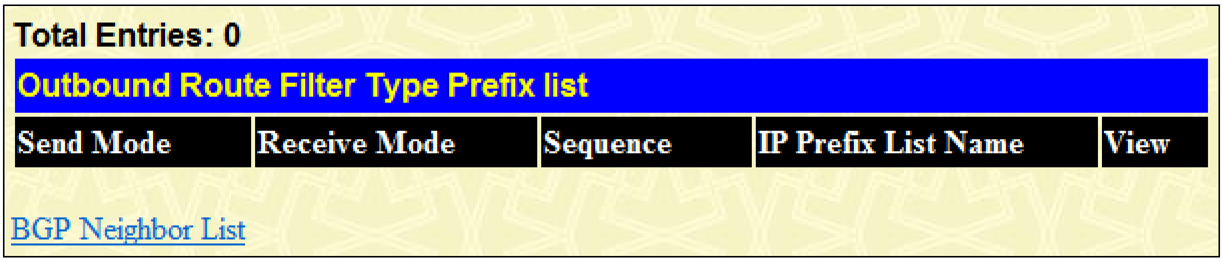
BGP Neighbor Information

Session State	Enabled
Session Activity	Enabled
Remote AS	1
Remote Router ID	0.0.0.0
BGP State	Connect
Up Time	
Hold Time	180 sec
Keepalive Interval	60 sec
Advertisement Interval	5 sec
AS Origination Interval	15 sec
Connect Retry Interval	120 sec
EBGP Multihop	255
Weight	0
Update Source	
Next Hop Self	Disabled
Remove Private AS	Disabled
Allow AS In	Disabled



Address Family IPv4 Unicast Information

IPv4 Unicast	None
Soft Reconfiguration Inbound	Disabled
Community Sent To This Neighbor	None
Default Originate	Disabled
Incoming Update Prefix List	
Outgoing Update Prefix List	
Incoming Update Filter List	
Outgoing Update Filter List	
Route Map For Incoming Routes	
Route Map For Outgoing Routes	
Unsuppress Map	
Send Mode	Disabled
Receive Mode	Disabled
Prefix Max Count	12000
Prefix Warning Threshold	75
Prefix Warning Only	Disabled
Description	



Total Entries: 0

Outbound Route Filter Type Prefix list

Send Mode	Receive Mode	Sequence	IP Prefix List Name	View

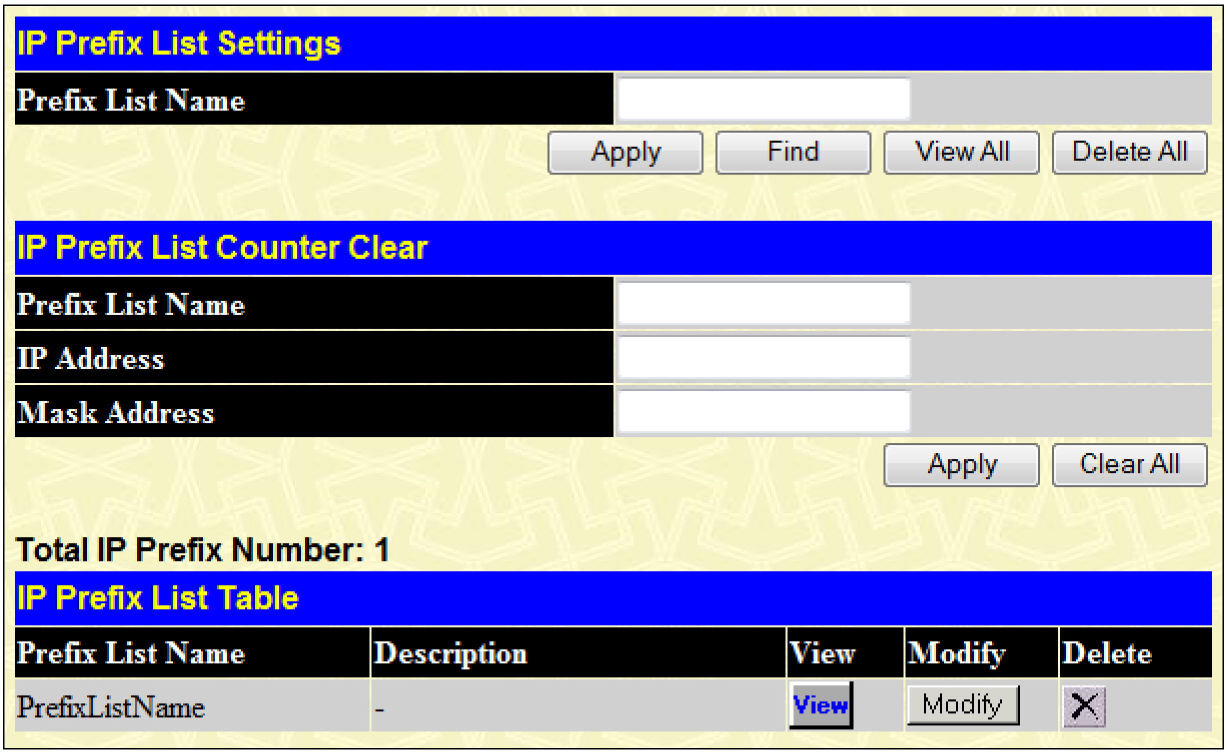
Figure 4- 154. BGP Neighbor Information window

IP Route Filter

IP Prefix List Settings

This window is used to create and configure an IP prefix list.

To view this window, click **L3 Features > IP Route Filter > IP Prefix List Settings**, as shown below:



IP Prefix List Settings

Prefix List Name

IP Prefix List Counter Clear

Prefix List Name

IP Address

Mask Address

Total IP Prefix Number: 1

IP Prefix List Table

Prefix List Name	Description	View	Modify	Delete
PrefixListName	-	View	Modify	☒

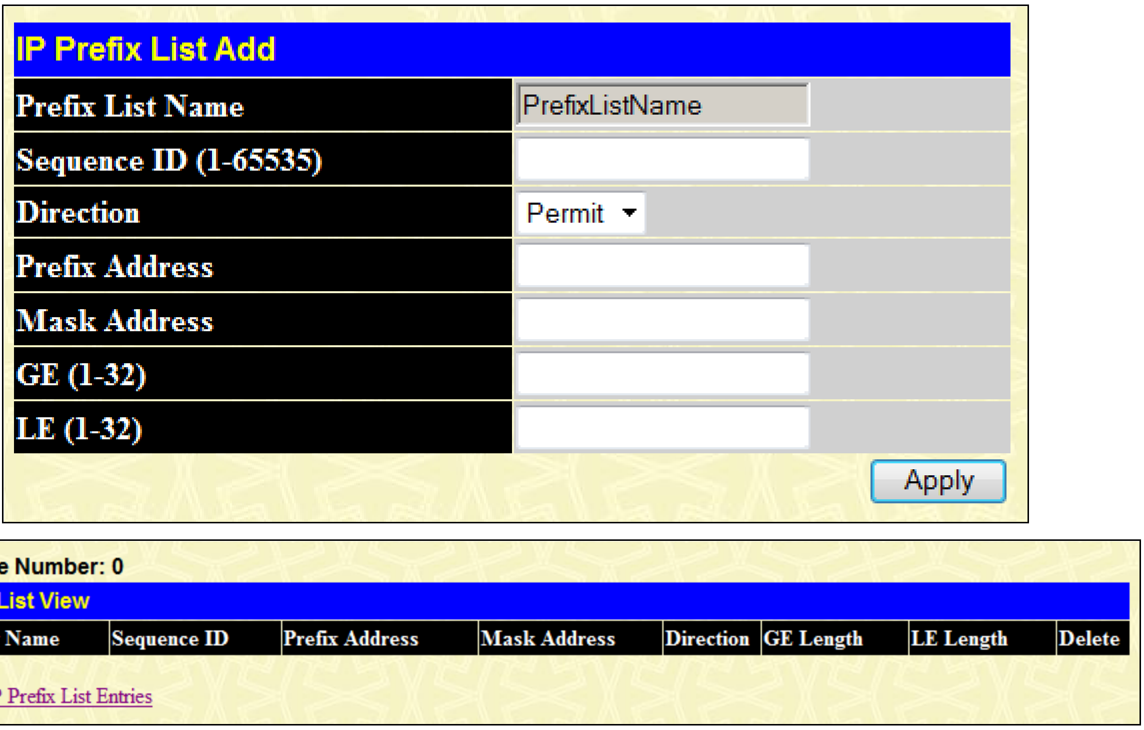
Figure 4- 155. IP Prefix List Settings window

The IP prefix list table parameters are described below:

Parameter	Description
IP Prefix List Settings	
Prefix List Name	Enter the name to identify the prefix list.
IP Prefix List Counter Clear	
Prefix List Name	Enter the name of the prefix list that will be cleared.
IP Address	Enter the IP address to be cleared.
Mask Address	Enter the mask address to be cleared.

Click **Apply** to implement changes made.

Click **View** to access the IP Prefix List Add page for the specified entry, as shown below:



IP Prefix List Add

Prefix List Name	PrefixListName
Sequence ID (1-65535)	
Direction	Permit
Prefix Address	
Mask Address	
GE (1-32)	
LE (1-32)	

Total Rule Number: 0

IP Prefix List View

Prefix List Name	Sequence ID	Prefix Address	Mask Address	Direction	GE Length	LE Length	Delete

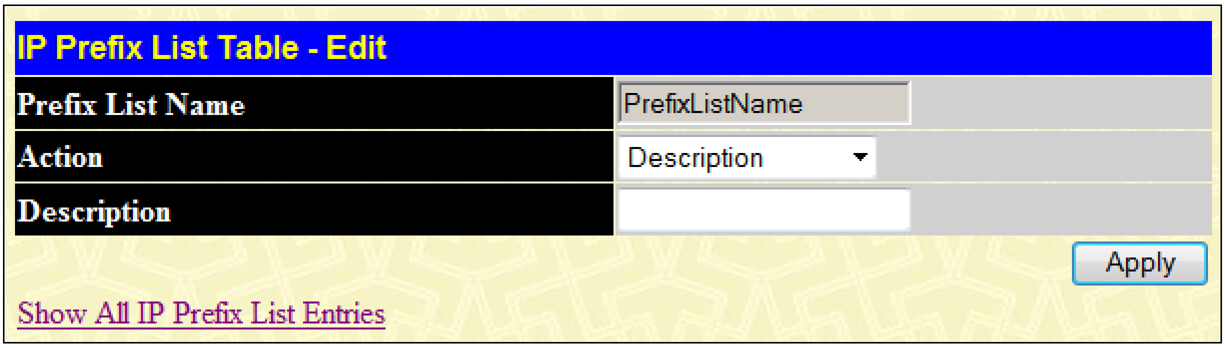
Figure 4- 156. IP Prefix List Add window

The following parameters are described below:

Parameter	Description
IP Prefix List Settings	
Sequence ID (1-65535)	Enter the sequence ID number here.
Direction	Select the direction option here. Options to choose from are *Permit* and *Deny*.
Prefix Address	Enter the prefix address here.
Mask Address	Enter the mask address here.
GE (1-32)	Enter the minimum prefix length to be matched.
LE (1-32)	Enter the maximum prefix length to be matched.

Click **Apply** to implement changes made.

Click **Modify** to access the IP Prefix List Edit page for the specified entry, as shown below:



IP Prefix List Table - Edit

Prefix List Name	PrefixListName
Action	Description
Description	

Figure 4- 157. IP Prefix List Edit window

The following parameters are described below:

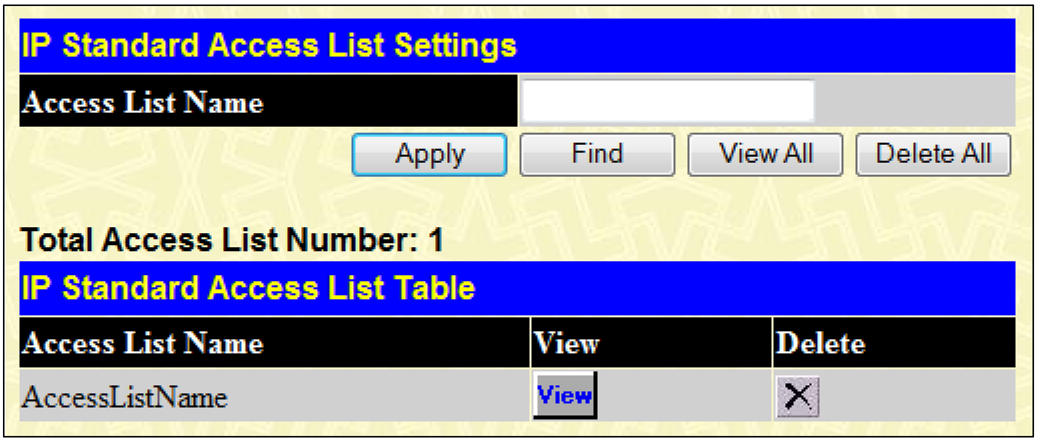
Parameter	Description
IP Prefix List Settings	
Action	Select the action here. Options to choose from are *Description* and *Clear Description*.
Description	Enter the description here.

Click **Apply** to implement changes made.

IP Standard Access List Settings

This window is used to create an access list used to filter routes.

To view this window, click **L3 Features > IP Route Filter > IP Standard Access List Settings**, as shown below:



IP Standard Access List Settings

Access List Name:

Total Access List Number: 1

IP Standard Access List Table

Access List Name	View	Delete
AccessListName	View	☒

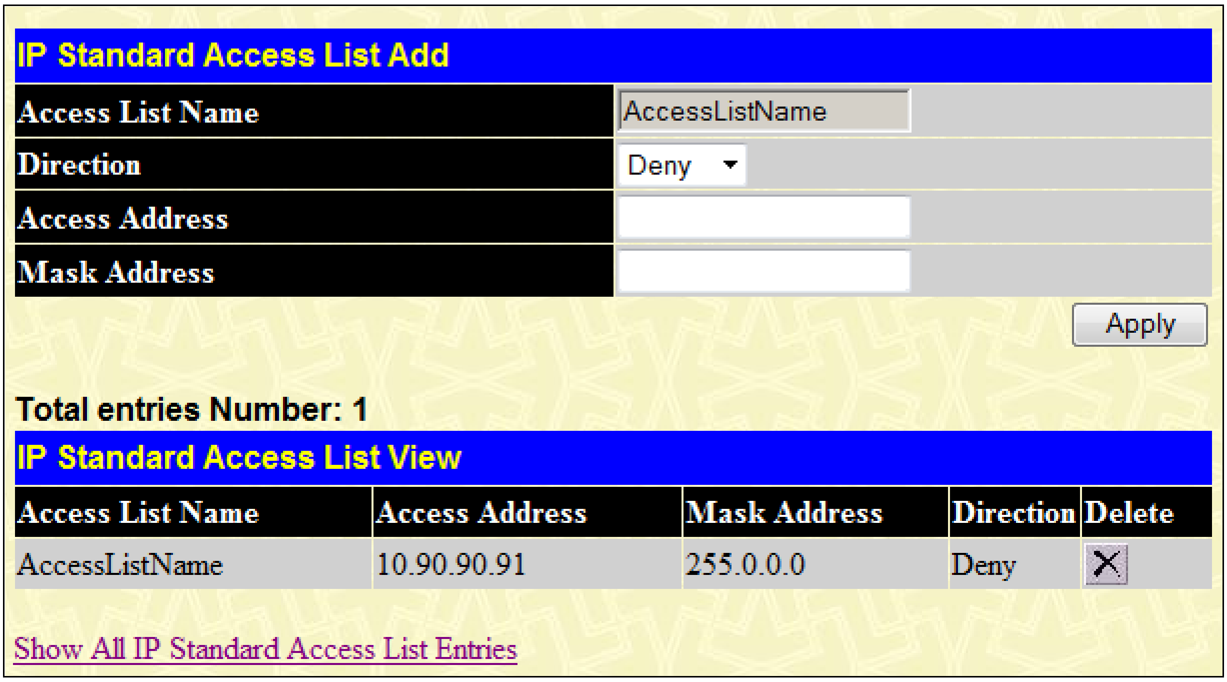
Figure 4- 158. IP Standard Access List Settings window

The IP standard access list parameters are described below:

Parameter	Description
Access List Name	Enter the name of the access list.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

Click **View** to access the IP Standard Access List Add page for the specified entry, as shown below:



IP Standard Access List Add

Access List Name	AccessListName
Direction	Deny
Access Address	
Mask Address	

Total entries Number: 1

IP Standard Access List View

Access List Name	Access Address	Mask Address	Direction	Delete
AccessListName	10.90.90.91	255.0.0.0	Deny	☒

Figure 4- 159. IP Standard Access List Add window

The IP standard access list parameters are described below:

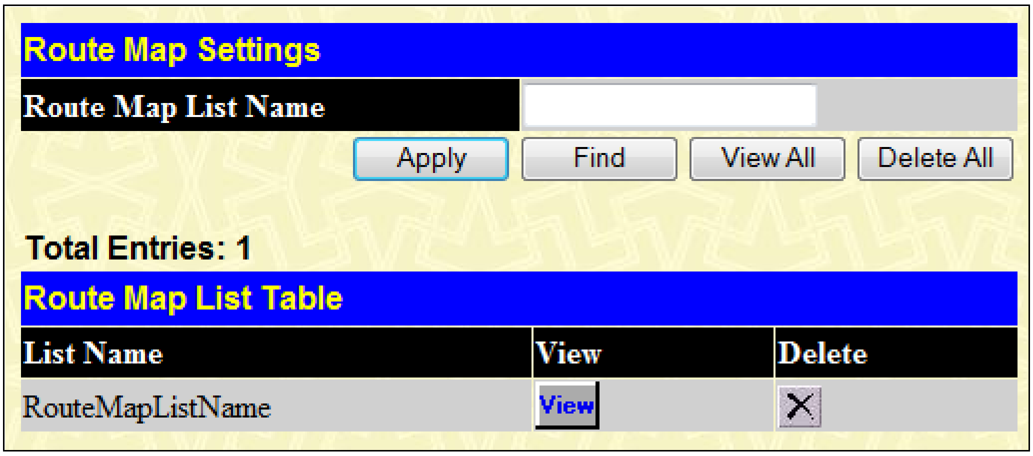
Parameter	Description
Direction	Use the drop-down menu to Permit or Deny the specified network.
Access Address	Enter the network address.
Mask Address	Enter the mask address of the network address.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

Route Map Settings

This window is used to create a route map or add/delete sequences to a route map.

To view this window, click **L3 Features > IP Route Filter > Route Map Settings**, as shown below:



Route Map Settings

Route Map List Name	

Total Entries: 1

Route Map List Table

List Name	View	Delete
RouteMapListName	View	☒

Figure 4- 160. Route Map Settings window

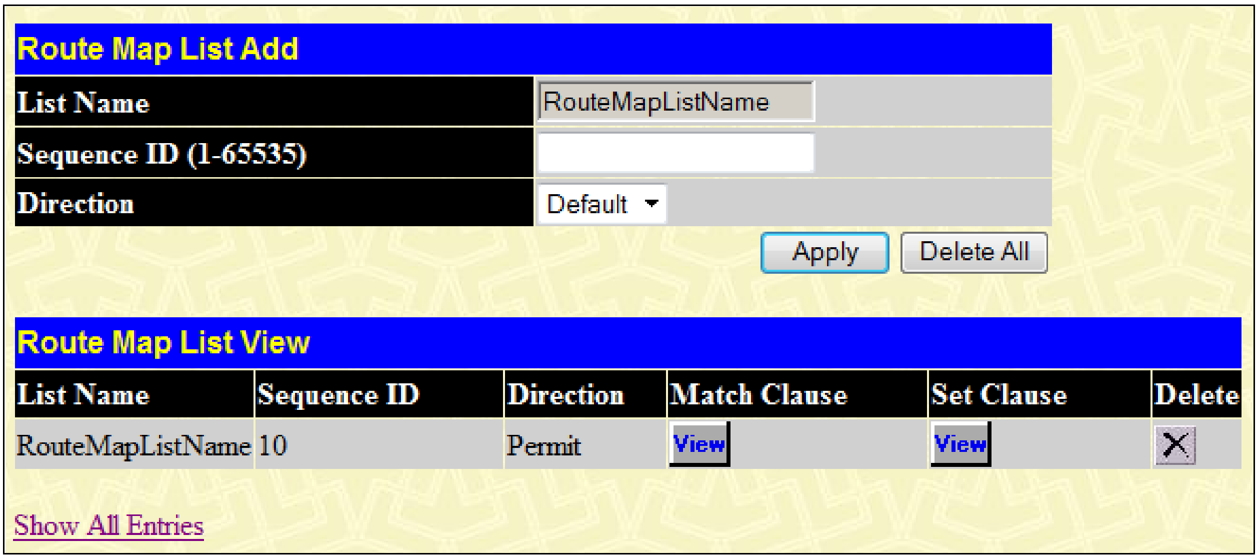
The route map parameters are described below:

Parameter	Description

Route Map List Name	Enter the route map name.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

Click **View** to access the Route Map List Add page for the specified entry, as shown below:



Route Map List Add

List Name	RouteMapListName
Sequence ID (1-65535)	
Direction	Default

Route Map List View

List Name	Sequence ID	Direction	Match Clause	Set Clause	Delete
RouteMapListName	10	Permit	View	View	☒

Figure 4- 161. Route Map List Add Settings window

The route map parameters are described below:

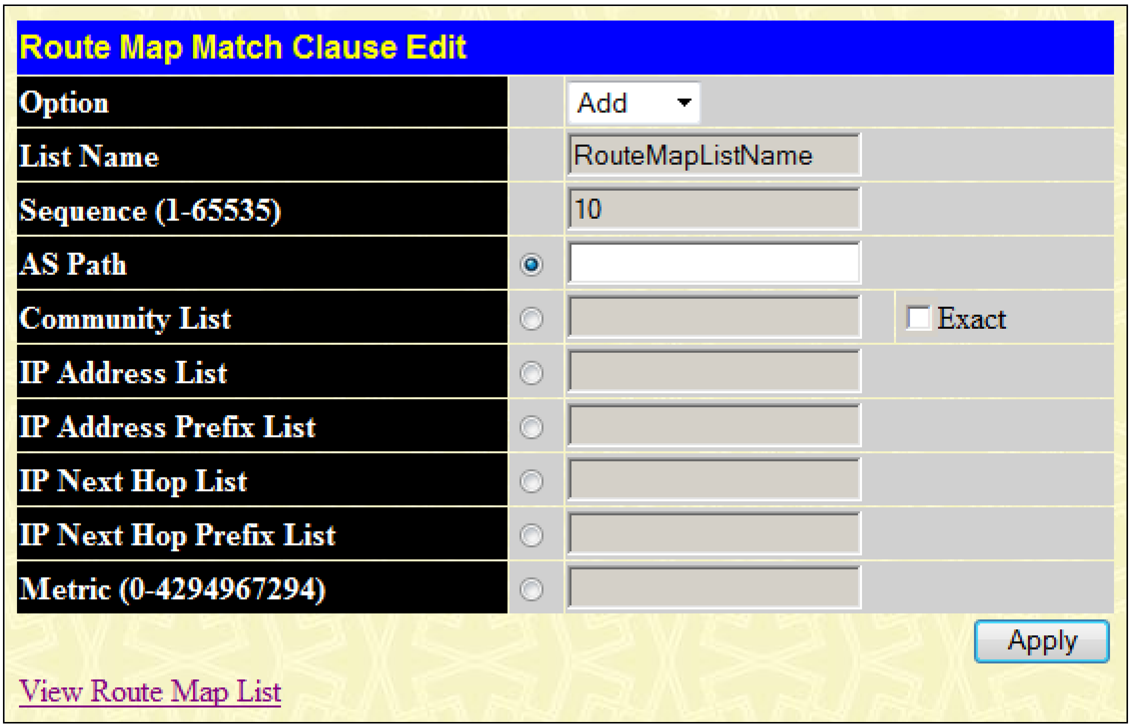
Parameter	**Description**
List Name	Display the route map list name.
Sequence ID (1-65535)	Enter the sequence number for the rule.
Direction	Use the drop-down menu to *Permit* or *Deny* the matched rule.

Click **Apply** to implement changes made. To remove an entry from the table, click its corresponding ☒ under the Delete heading.

To view more information about the **Match Clause**, click on the **View** button it the related column.

To view more information about the **Set Clause**, click on the **View** button it the related column.

After clicking the **View** button, in the **Match Clause** column, the following window will be displayed:



Route Map Match Clause Edit

Option		Add	
List Name		RouteMapListName	
Sequence (1-65535)		10	
AS Path	●		
Community List	○		□ Exact
IP Address List	○		
IP Address Prefix List	○		
IP Next Hop List	○		
IP Next Hop Prefix List	○		
Metric (0-4294967294)	○		

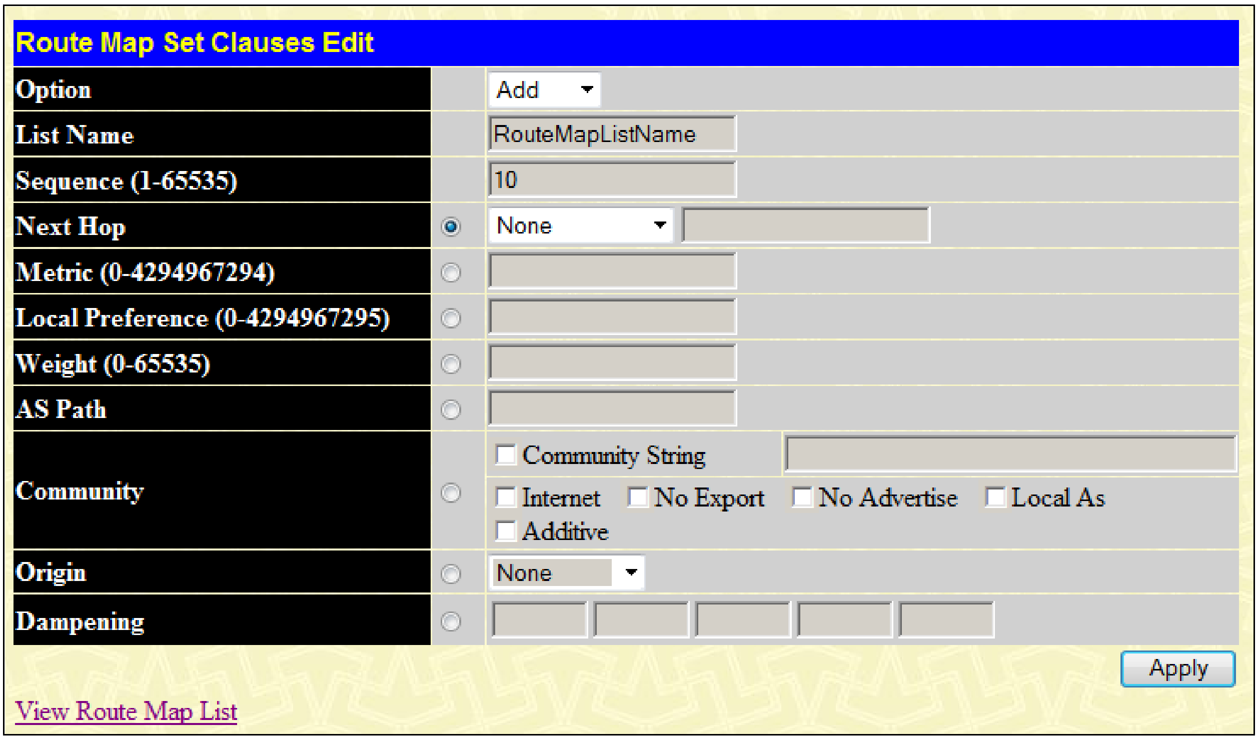
Figure 4- 162. Route Map Match Clause Edit Settings window

The route map parameters are described below:

Parameter	Description
Option	Use the drop-down menu to *Add* or *Delete* a sequence entry.
List Name	Displays the route map list name.
Sequence	Displays the route map sequence number.
AS Path	Click the radio button and specify to match the AS path of the route against the AS path list. The AS path list specified here needs to be a sub-list of the AS path list associated with the route.
Community List	Click the radio button and specify to match the community of the route against the community string. Tick the **Exact** check box to present all the specified communities.
IP Address List	Click the radio button and specify to match the route according to the access list.
IP Address Prefix List	Click the radio button and specify to match the route according to the prefix list.
IP Next Hop List	Click the radio button and specify to match the next hop of the route according to the prefix list.
IP Next Hop Prefix List	Click the radio button and specify to match the next hop of the route according to the prefix list.
Metric (0-4294967294)	Click the radio button and specify to match the metric of the route.

Click **Apply** to implement changes made.

After clicking the **View** button, in the **Set Clause** column, the following window will be displayed:



Route Map Set Clauses Edit

Option		Add
List Name		RouteMapListName
Sequence (1-65535)		10
Next Hop	●	None
Metric (0-4294967294)	○	
Local Preference (0-4294967295)	○	
Weight (0-65535)	○	
AS Path	○	
Community	○	□ Community String □ Internet □ No Export □ No Advertise □ Local As □ Additive
Origin	○	None
Dampening	○	

Figure 4- 163. Route Map Set Clause Edit Settings window

The route map parameters are described below:

Parameter	Description
Option	Use the drop-down menu to *Add* or *Delete* a sequence entry.
List Name	Displays the route map list name.
Sequence (1-65535)	Displays the route map sequence number.
Next Hop	Click the radio button to set the next hop attribute. Use the drop-down menu to select between *IP Address* and *Peer Address*. *IP Address* - IP address to set. *Peer Address* - This will take effect for both the ingress and egress directions. For ingress direction, the next hop will be set to the neighbor peer address. For egress direction, the next hop associated with the route in the packet will be the local router ID address.
Metric (0-4294967294)	Click the radio button to enter the metric. The BGP router will not send metrics associated with a route by default unless the metric is egress set in the route map. If the BGP route receives a route with a metric, then this metric will be used in best path selection. This can be overwritten by the metric that is ingress set for the route. If the received route has neither metric attribute nor metric ingress metric set, then the default metric (0) will be associated with the route for the best path selection. If med-missing-as-worst is enabled for the router, then a value of infinite will be associated with the route. This will take effect for both ingress and egress directions.
Local Preference (0-4294967295)	Click the radio button to enter the local preference for the matched route. By default, the BGP router will send the default local preference with the routes. It can be overwritten by the local preference set by the route map. For the received route, the local preference sent with the route will be used in the best path selection. This local preference will be overwritten if the local preference is ingress set by the route map. For the local routes, the default local preference will be used for them in the best path

	selection. This will take effect for both ingress and egress directions.
Weight (0-65535)	Click the radio button to enter the weight for the matched routes. It will overwrite the weight specified by the neighbor weight command for the routes received from the neighbor. If weight is neither specified by the neighbor weight command nor set by the route map, then routes learned through another BGP peer have a default weight of 0. The weight of local routes is always 32768. This will only take effect for ingress direction.
AS Path	Click the radio button to enter an AS path list which is used to prepend the AS list.
Community	Click the radio button to configure a community to be used or to be appended to the original communities of the route. *Community String* - A community is 4 bytes long, including the 2 byte's autonomous system number and 2 bytes' network number This value is configured with two 2-byte numbers separated by a colon. The valid range of both numbers is from 1 to 65535. A community set can be formed by multiple communities, separated by a comma. An example of a community set is 200:1024, 300:1025, 400:1026. *Internet* – Routes with this community will be sent to all peers either internal or external. *No Export* – Routes with this community will be sent to peers in the same AS or in other sub autonomous systems within a confederation, but will not be sent to an external BGP (eBGP) peer. *No Advertise* – Routes with this community will not be advertised to any peer either internal or external. *Local AS* – Routes with this community will be sent to peers in the same AS, but will not be sent to peers in other sub ASes in the same confederation and to the external peers. *Additive* - If this keyword is specified, the specified community string will be appended to the original community string. If not specified, the specified community string will replace the original community string.
Origin	Click the radio button to enter the origin for the route. It can be one of the following three values, *EGP*, *IGP*, or *Incomplete*.
Dampening	Click the radio button to enter the dampening timer and parameter.

Click **Apply** to implement changes made.

Section 5

QoS

802.1p Settings
Bandwidth Control
HOL Prevention Settings
Schedule Settings

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

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements 802.1p priority queuing.

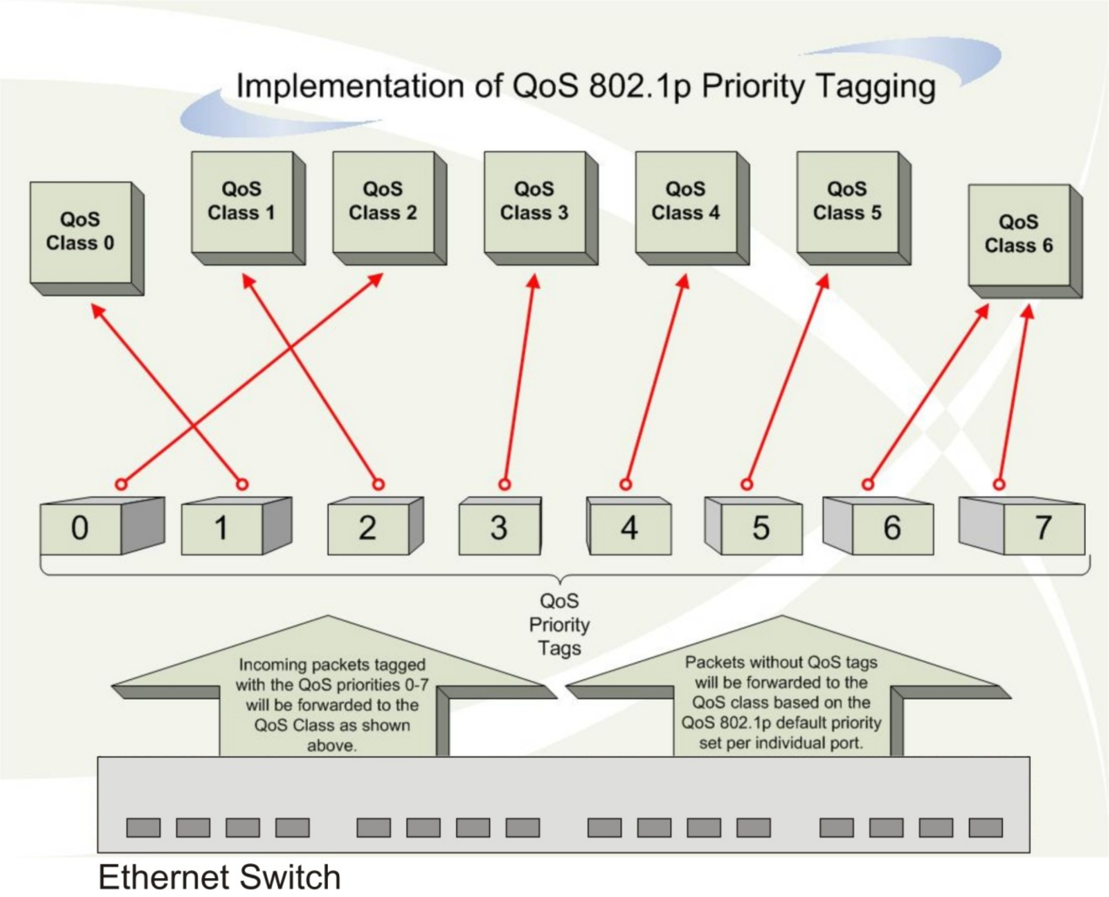

Implementation of QoS 802.1p Priority Tagging
QoS Class 0
QoS Class 1
QoS Class 2
QoS Class 3
QoS Class 4
QoS Class 5
QoS Class 6
0
1
2
3
4
5
6
7
QoS Priority Tags
Incoming packets tagged with the QoS priorities 0-7 will be forwarded to the QoS Class as shown above.
Packets without QoS tags will be forwarded to the QoS class based on the QoS 802.1p default priority set per individual port.
Ethernet Switch

Figure 5- 1. Mapping QoS on the Switch

The previous picture shows the default priority setting for the Switch. Class-6 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 video conference 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, one of which is internal and unconfigurable. These priority queues are labeled as 6, 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 Q6 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 Switch has seven configurable priority queues (and seven Classes of Service) for each port on the Switch.

NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and therefore is not configurable. All references in the following section regarding classes of service will refer to only the seven classes of service that may be used and configured by the Switch’s Administrator.

802.1p Settings

The 802.1p Settings section includes 802.1p Default Priority Settings and 802.1p User Priority Settings.

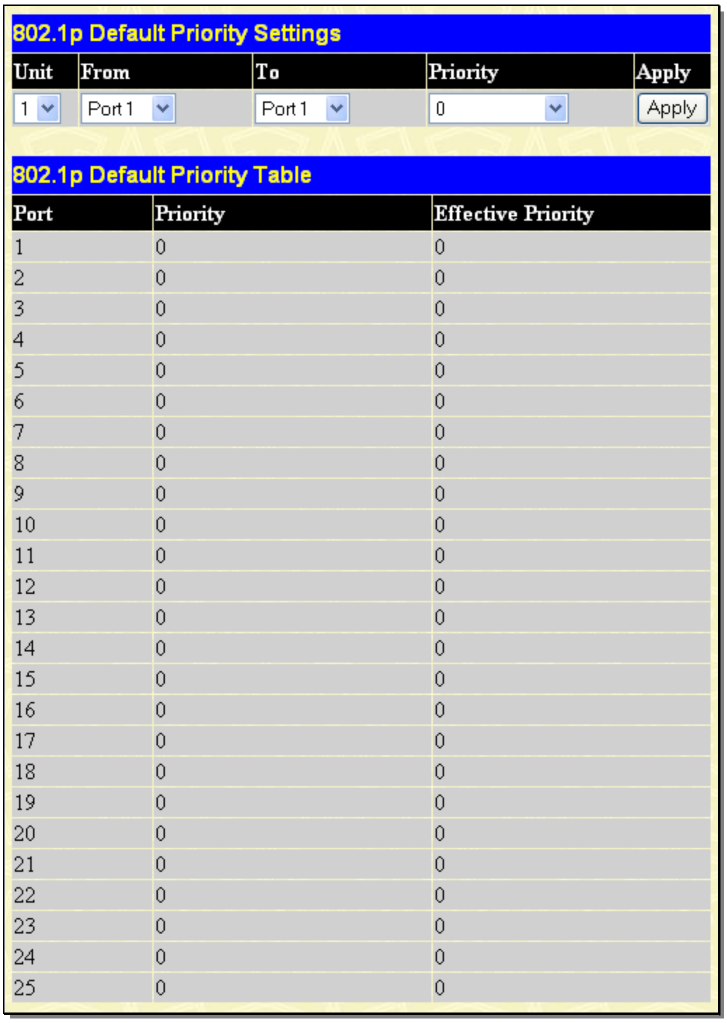
802.1p Default Priority Settings

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

This window allows users 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 changes made.

To view this window, click **QoS** > **802.1p Settings** > **802.1p Default Priority Settings**, as shown on the right.

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



802.1p Default Priority Settings

Unit	From	To	Priority	Apply
1	Port 1	Port 1	0	Apply

802.1p Default Priority Table

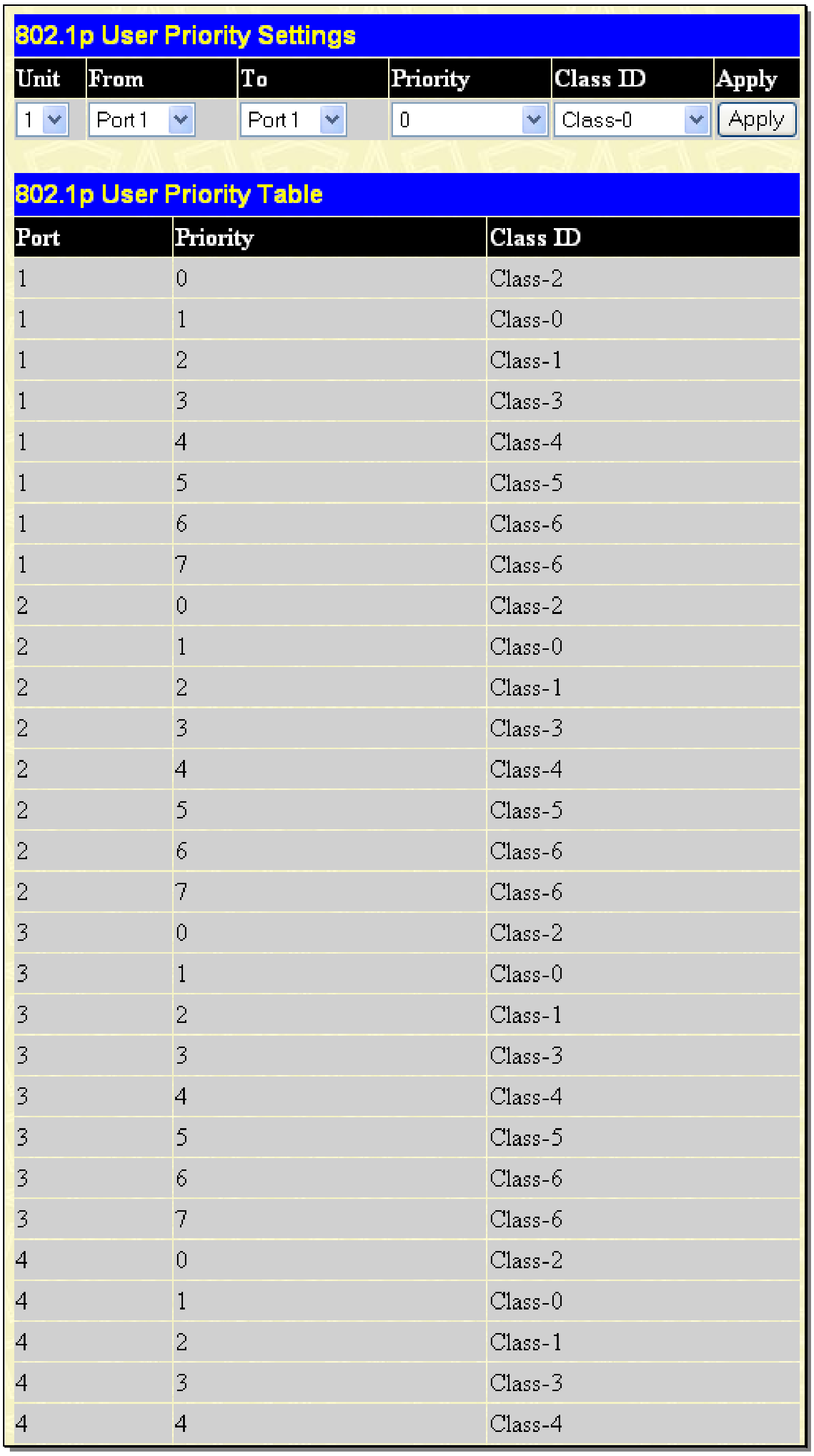
Port	Priority	Effective Priority
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0

Figure 5- 2. 802.1p Default Priority Settings window

802.1p User Priority Settings

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

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



802.1p User Priority Settings

Unit	From	To	Priority	Class ID	Apply
1	Port 1	Port 1	0	Class-0	Apply

802.1p User Priority Table

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

Figure 5- 3. 802.1p User Priority Settings window

Once a priority to the port groups on the Switch has been assigned, users can then assign this Class to each of the eight levels of 802.1p priorities. Click **Apply** to set changes made.

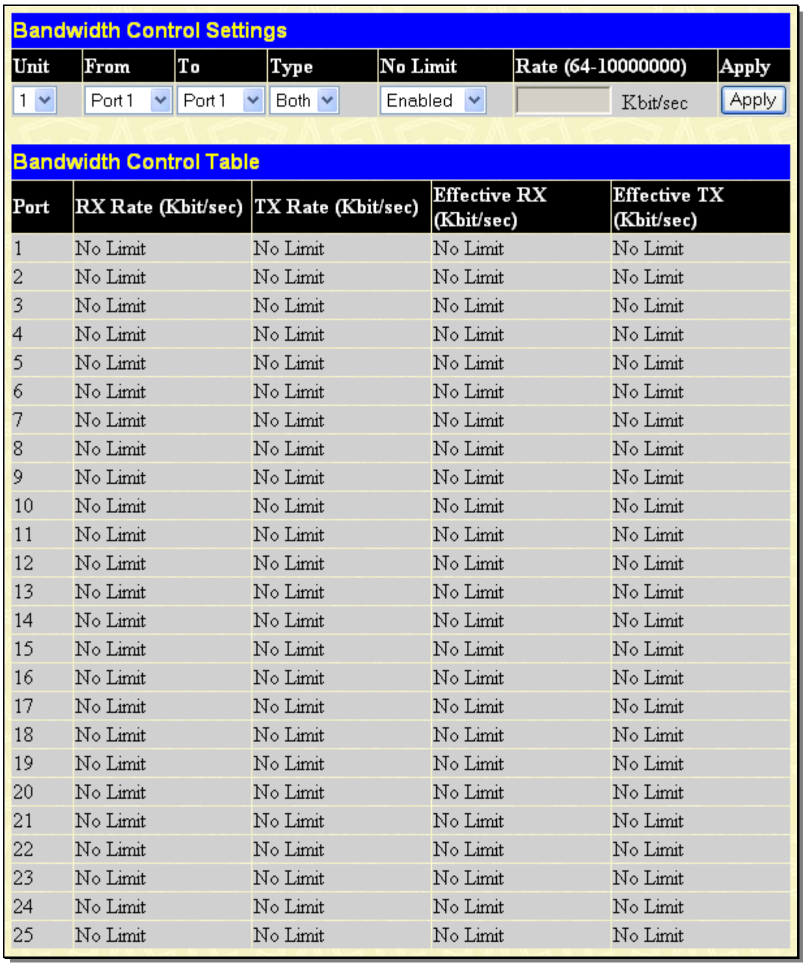
Bandwidth Control

The Bandwidth Control section includes Bandwidth Control Settings and Per Queue Bandwith Control Settings.

Bandwidth Control Settings

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

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



Bandwidth Control Settings

Unit	From	To	Type	No Limit	Rate (64-10000000)	Apply
1	Port 1	Port 1	Both	Enabled	Kbit/sec	Apply

Bandwidth Control Table

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

Figure 5- 4. Bandwidth Control Settings window

The following parameters can be set or are displayed:

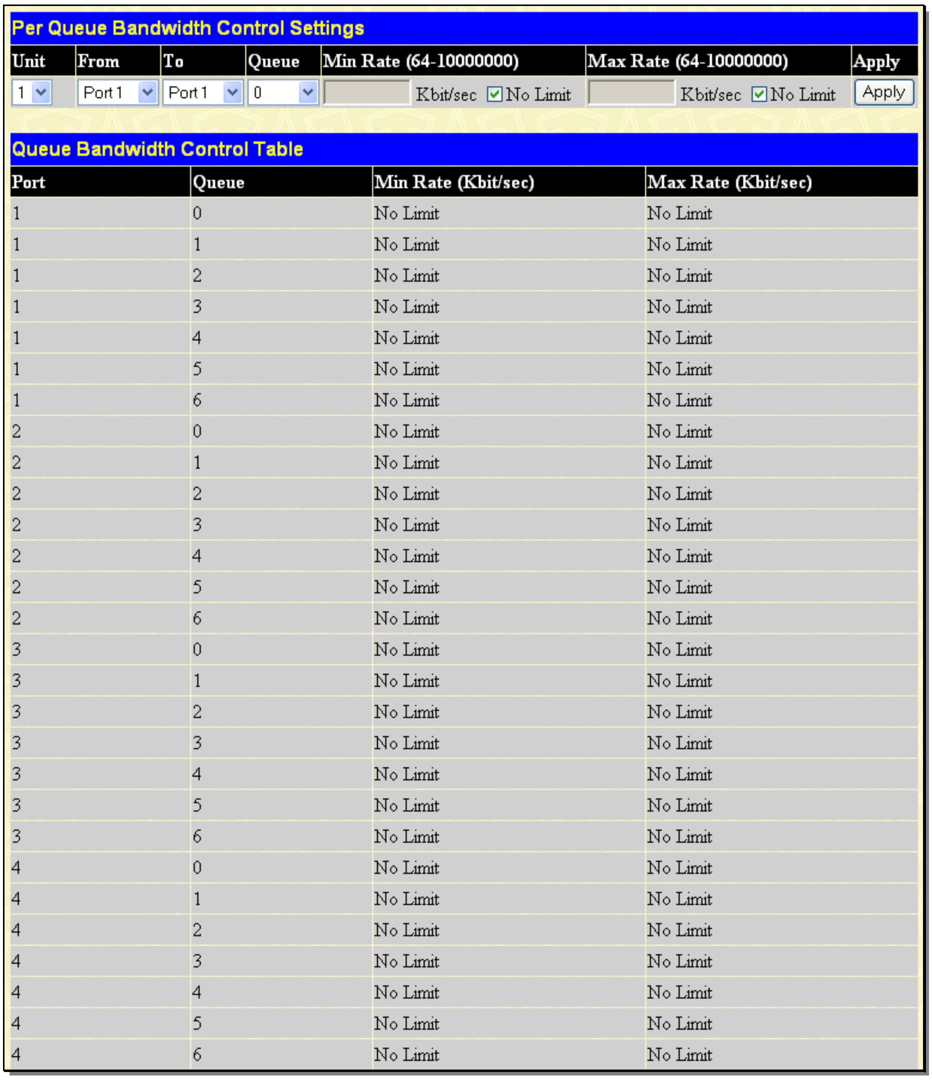
Parameter	Description
Unit	Select the unit to configure.
From/To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling 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 or limits the bandwidth on a given port.
Rate (64-10000000)	This field allows the user to enter the data rate that will be the limit for the selected port. A rate can only be entered if the No Limit feature is *Disabled*.

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

Per Queue Bandwidth Control Settings

This window is used to sets the bandwidth control for each specific queue on specified ports.

To view the **Per Queue Bandwidth Control Settings** window, click **QoS** > **Bandwidth Control > Per Queue Bandwidth Control Settings**, as shown below:



Per Queue Bandwidth Control Settings

Unit	From	To	Queue	Min Rate (64-10000000)	Max Rate (64-10000000)	Apply
1	Port 1	Port 1	0	Kbit/sec ☑ No Limit	Kbit/sec ☑ No Limit	Apply

Queue Bandwidth Control Table

Port	Queue	Min Rate (Kbit/sec)	Max Rate (Kbit/sec)
1	0	No Limit	No Limit
1	1	No Limit	No Limit
1	2	No Limit	No Limit
1	3	No Limit	No Limit
1	4	No Limit	No Limit
1	5	No Limit	No Limit
1	6	No Limit	No Limit
2	0	No Limit	No Limit
2	1	No Limit	No Limit
2	2	No Limit	No Limit
2	3	No Limit	No Limit
2	4	No Limit	No Limit
2	5	No Limit	No Limit
2	6	No Limit	No Limit
3	0	No Limit	No Limit
3	1	No Limit	No Limit
3	2	No Limit	No Limit
3	3	No Limit	No Limit
3	4	No Limit	No Limit
3	5	No Limit	No Limit
3	6	No Limit	No Limit
4	0	No Limit	No Limit
4	1	No Limit	No Limit
4	2	No Limit	No Limit
4	3	No Limit	No Limit
4	4	No Limit	No Limit
4	5	No Limit	No Limit
4	6	No Limit	No Limit

Figure 5- 5. Per Queue Bandwidth Control Settings window

The following parameters can be set or are displayed:

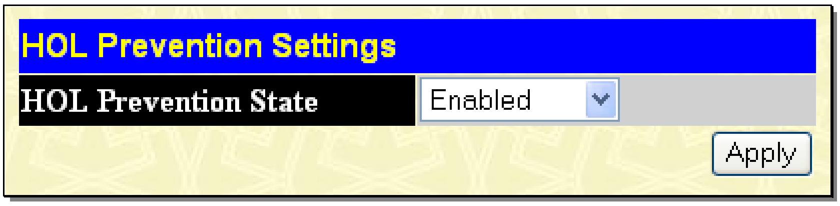
Parameter	Description
Unit	Select the unit to configure.
From/To	A consecutive group of ports may be configured starting with the selected port.
Queue	Use the drop-down menu to select the desired priority queue. Please note Queue 7 is reserved for stacking.
Min Rate (64-10000000)	This field allows the user to enter a minimum guaranteed bandwidth. Ticking the no limit check box means there will be no limit on the rate of packets received.
Max Rate (64-10000000)	This field allows the user to limit the bandwidth. When specified, packets transmitted from the queue will not exceed the specified limit even if extra bandwidth is available.Ticking the no limit check box means there will be no limit on the rate of packets received.

Click **Apply** to set the per queue bandwidth control for the selected ports. Results of configured per queue bandwidth settings will be displayed in the Queue Bandwidth Table.

HOL Prevention Settings

This window is used to enable or disable Head of Line (HOL) prevention.

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



HOL Prevention Settings

HOL Prevention State	Enabled

Apply

Figure 5- 6. HOL Prevention Settings window

Toggle to enable or disable head of line prevention. The default is *Enabled*.

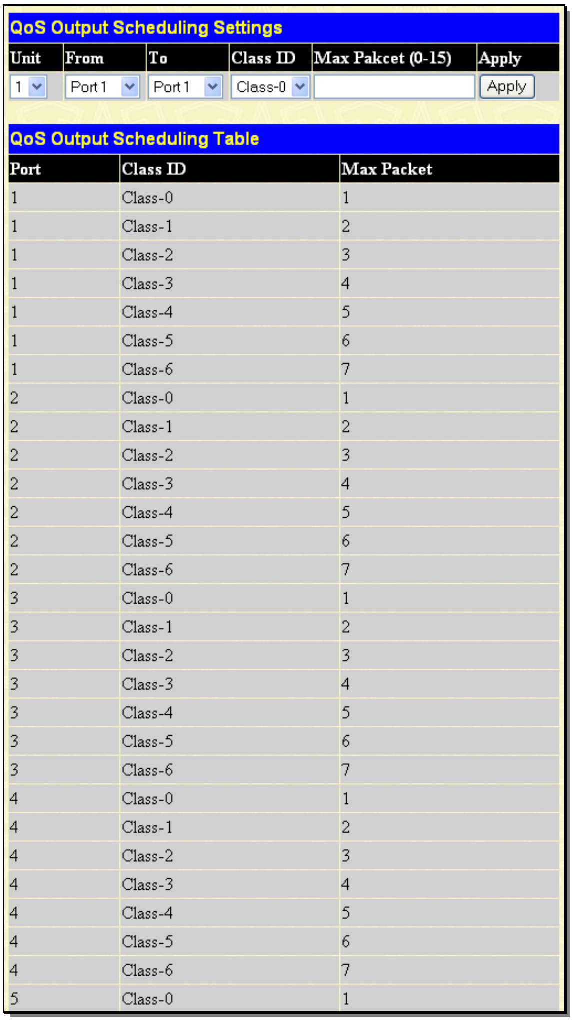
Schedule Settings

The Schedule Settings section includes QoS Output Scheduling Settings and QoS Scheduling Mechanism Settings.

QoS Output Scheduling Settings

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 table, click **QoS > Schedule Settings** > **QoS Output Scheduling Settings**, as shown below:



QoS Output Scheduling Settings

Unit	From	To	Class ID	Max Pakcet (0-15)	Apply
1	Port 1	Port 1	Class-0		Apply

QoS Output Scheduling Table

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

Figure 5- 7. QoS Output Scheduling Settings window

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

Parameter	Description

Unit	Select the unit to configure.
From/To	A consecutive group of ports may be configured starting with the selected port.
Class ID	Select the class ID from *Class-0* through *Class-6*.
Max. Packet (0-15)	Specify 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.

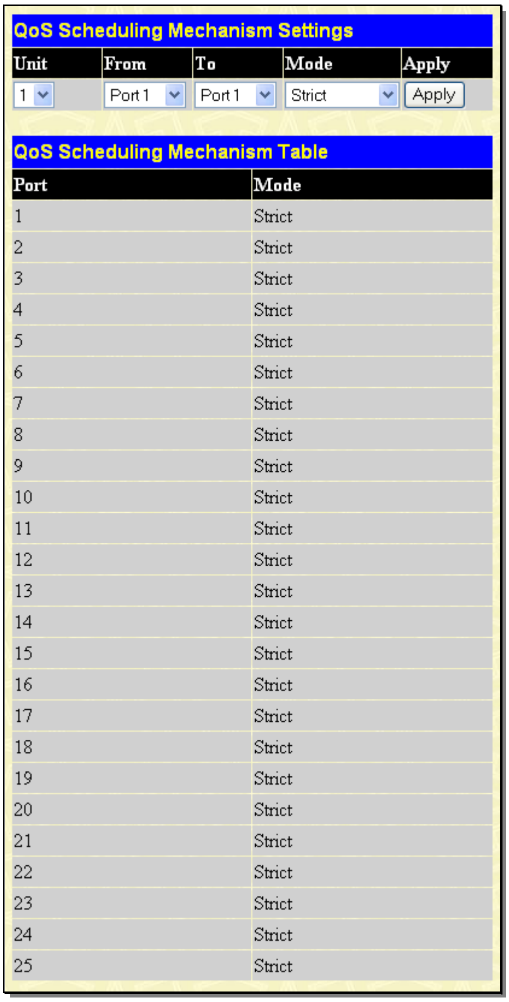
Configuring the Combination Queue

Utilizing the **QoS Output Scheduling Settings** window shown above, the Switch can implement a combination queue for forwarding packets. This combination queue allows for a combination of strict and weight-fair (weighted round-robin "WRR") scheduling for emptying given classes of service. To set the combination queue, enter a 0 for the Max Packets entry of the corresponding priority classes of service listed in the window above. Priority classes of service that have a 0 in the Max Packet field will forward packets with strict priority scheduling. The remaining classes of service, that do not have a 0 in their Max Packet field, will follow a weighted round-robin (WRR) method of forwarding packets — as long as the priority classes of service with a 0 in their Max Packet field are empty. When a packet arrives in a priority class with a 0 in its Max Packet field, this class of service will automatically begin forwarding packets until it is empty. Once a priority class of service with a 0 in its Max Packet field is empty, the remaining priority classes of service will reset the weighted round-robin (WRR) cycle of forwarding packets, starting with the highest available priority class of service. Priority classes of service with an equal level of priority and equal entries in their Max Packet field will empty their fields based on hardware priority scheduling. The Max Packet parameter allows the maximum number of packets a given priority class of service can transmit per weighted round-robin (WRR) scheduling cycle to be selected. This provides for a controllable CoS behavior while allowing other classes to empty as well. A value between 0 and 15 packets can be specified per priority class of service to create the combination queue.

QoS Scheduling Mechanism Settings

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If the user chooses 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** > **Schedule Settings** > **QoS Scheduling Mechanism Settings**, as shown below:



QoS Scheduling Mechanism Settings

Unit	From	To	Mode	Apply
1	Port 1	Port 1	Strict	Apply

QoS Scheduling Mechanism Table

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

Figure 5- 8. QoS Scheduling Mechanism Settings window

The Scheduling Mechanism has the following parameters.

Parameter	Description
Unit	Select the unit to configure.
From/To	A consecutive group of ports may be configured starting with the selected port.
Mode: 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. *Strict* is the default setting.
Mode: Weight Fair	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.

Section 6

Access Control List (ACL)

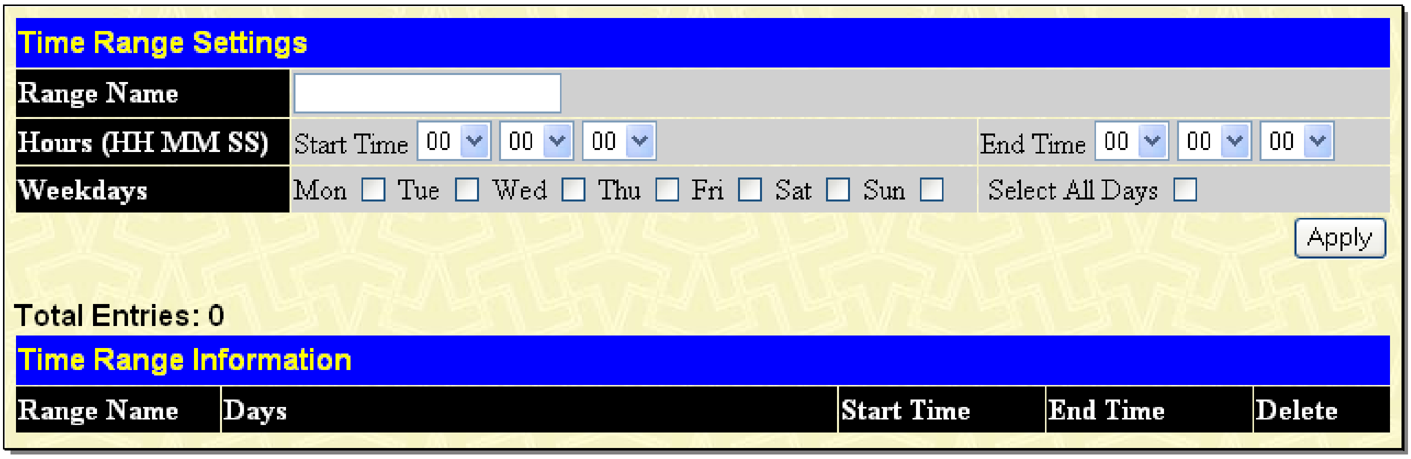
__Time Range__
__Access Profile Table__
__ACL Flow Meter__
__CPU Interface Filtering__

Time Range

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

NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the following chapter, Time and SNTP Commands.

To open the **Time Range Settings** window, click **ACL** > **Time Range**, as shown below:



Time Range Settings

Range Name		
Hours (HH MM SS)	Start Time 00 00 00	End Time 00 00 00
Weekdays	Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun □	Select All Days □

Total Entries: 0

Time Range Information

Range Name	Days	Start Time	End Time	Delete

Figure 6- 1. Time Range Settings window

The user may adjust the following parameters to configure a time range on the Switch:

Parameter	Description
Range Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the Access Profile table to identify the access profile and associated rule to be enabled during this time range.
Hours (HH MM SS)	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: Start Time <time hh:mm:ss> - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system.

	End Time <time hh:mm:ss> - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.
Weekdays	Use the check boxes to tick the corresponding days of the week that this time range is to be enabled.

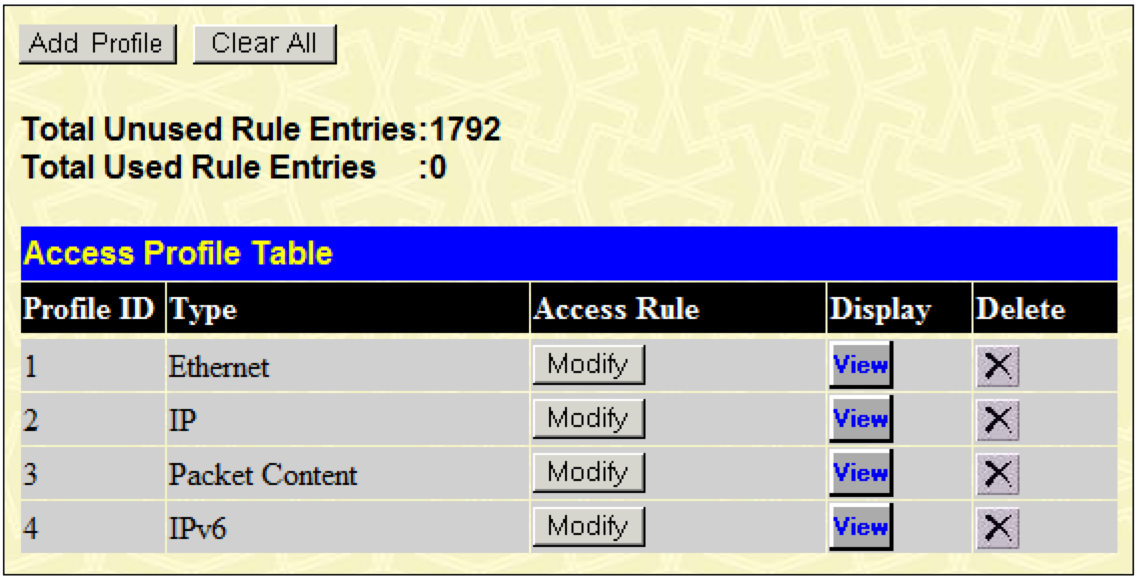
Click **Apply** to implement changes made. Currently configured entries will be displayed in the Time Range Information table in the bottom half of the window shown above.

Access profiles allow users 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.

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



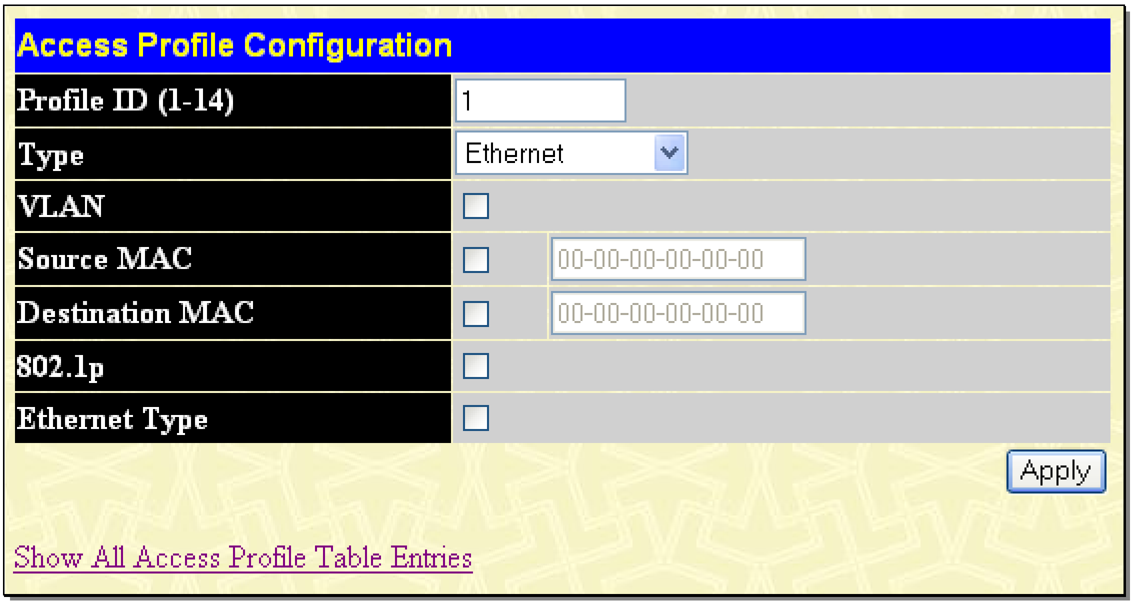
Total Unused Rule Entries:1792
Total Used Rule Entries :0

Access Profile Table

Profile ID	Type	Access Rule	Display	Delete
1	Ethernet	Modify	View	☒
2	IP	Modify	View	☒
3	Packet Content	Modify	View	☒
4	IPv6	Modify	View	☒

Figure 6- 2. Access Profile Table window

To add an entry to the Access Profile Table, click the **Add Profile** button. This will open the **Access Profile Configuration** window, as shown below: There are four **Access Profile Configuration** windows; one for Ethernet (or MAC address-based) profile configuration, one for IP address-based profile configuration, one for Packet Content and one for IPv6 addresses. Users can switch between the four **Access Profile Configuration** windows by using the Type drop-down menu. The window shown below is the **Access Profile Configuration** window for Ethernet. To remove all access profiles from this table, click **Clear All**.



Access Profile Configuration

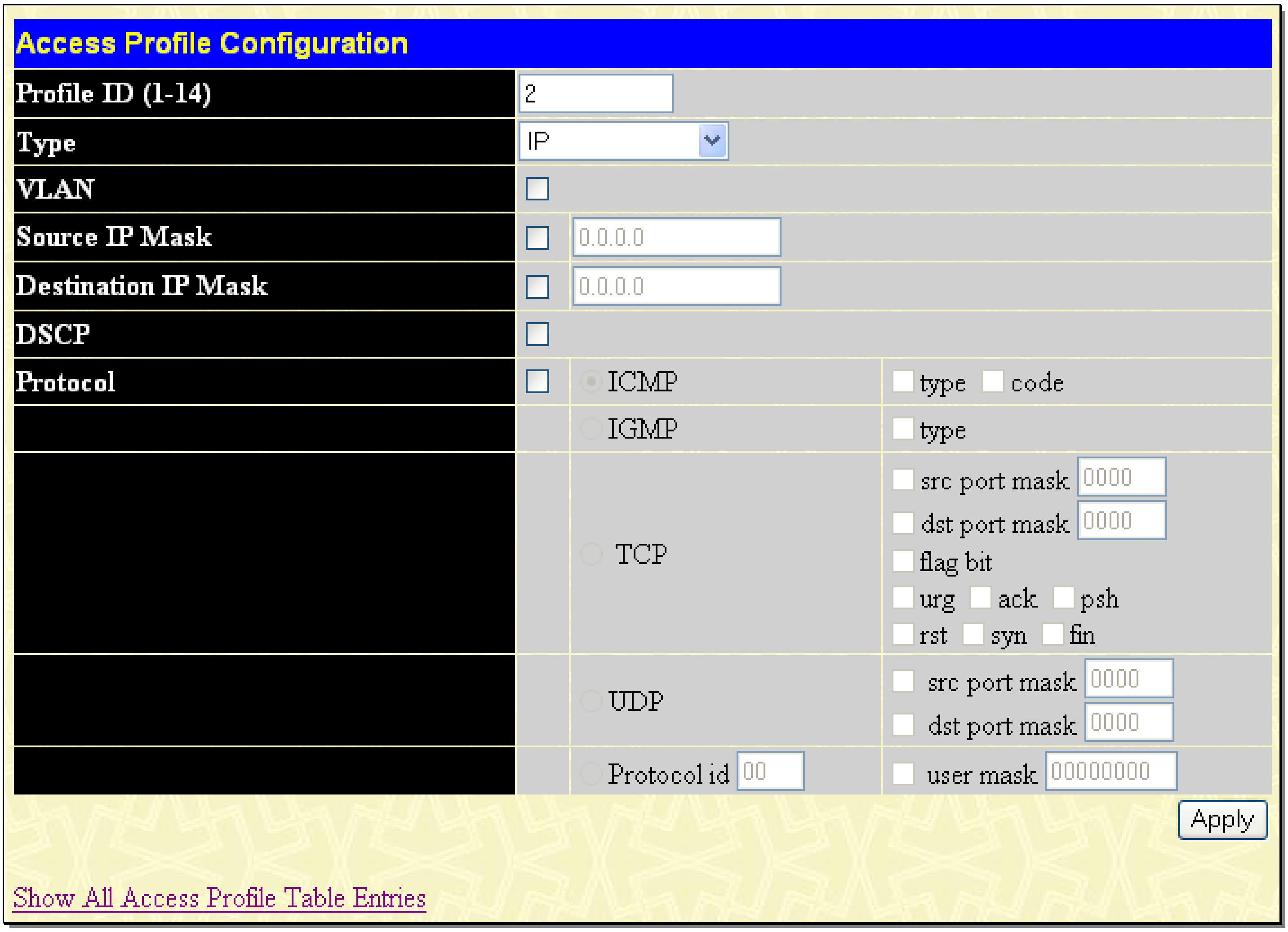
Profile ID (1-14)	1	
Type	Ethernet	
VLAN	□	
Source MAC	□	00-00-00-00-00-00
Destination MAC	□	00-00-00-00-00-00
802.1p	□	
Ethernet Type	□	

Figure 6- 3. Access Profile Configuration window (Ethernet)

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

Parameter	**Description**
Profile ID (1-14)	Type in a unique identifier number for this profile set. This value can be set from *1* to *14*.
Type	Select profile based on *Ethernet* (MAC Address), *IP* address, *Packet Content*, or *IPv6* address. This will change the window 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.

The window shown below is the **Access Profile Configuration** window for IP.



Access Profile Configuration

Profile ID (1-14)	2		
Type	IP		
VLAN	□		
Source IP Mask	□	0.0.0.0	
Destination IP Mask	□	0.0.0.0	
DSCP	□		
Protocol	□	● ICMP	□ type □ code
		○ IGMP	□ type
		○ TCP	□ src port mask 0000 □ dst port mask 0000 □ flag bit □ urg □ ack □ psh □ rst □ syn □ fin
		○ UDP	□ src port mask 0000 □ dst port mask 0000
		○ Protocol id 00	□ user mask 00000000

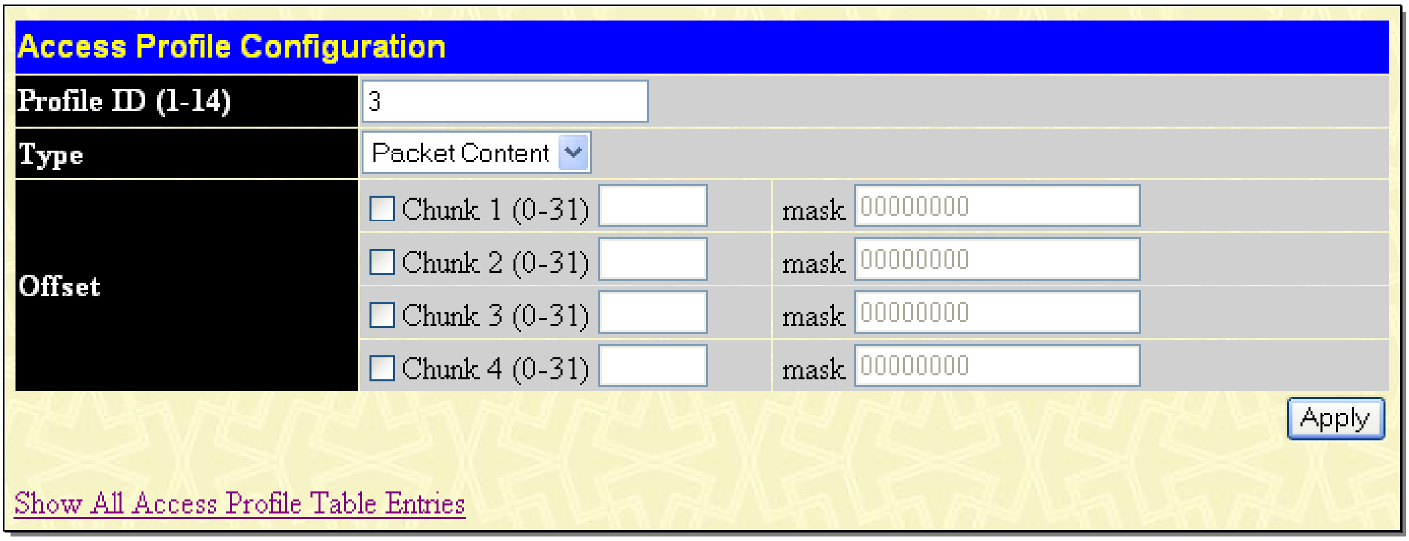
Figure 6- 4. Access Profile Configuration window (IP)

The following parameters can be set, for IP:

Parameter	Description
Profile ID (1-14)	Type in a unique identifier number for this profile set. This value can be set from *1* to *14*.
Type	Select profile based on *Ethernet* (MAC Address), *IP* address, *Packet Content Mask*, or *IPv6* address. This will change the window 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. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). *protocol id* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff) or a user value.

Click **Apply** to implement changes made. The window shown below is the **Access Profile Configuration** window for Packet Content Mask.



Access Profile Configuration

Profile ID (1-14)	3		
Type	Packet Content		
Offset	□ Chunk 1 (0-31)	mask	00000000
	□ Chunk 2 (0-31)	mask	00000000
	□ Chunk 3 (0-31)	mask	00000000
	□ Chunk 4 (0-31)	mask	00000000

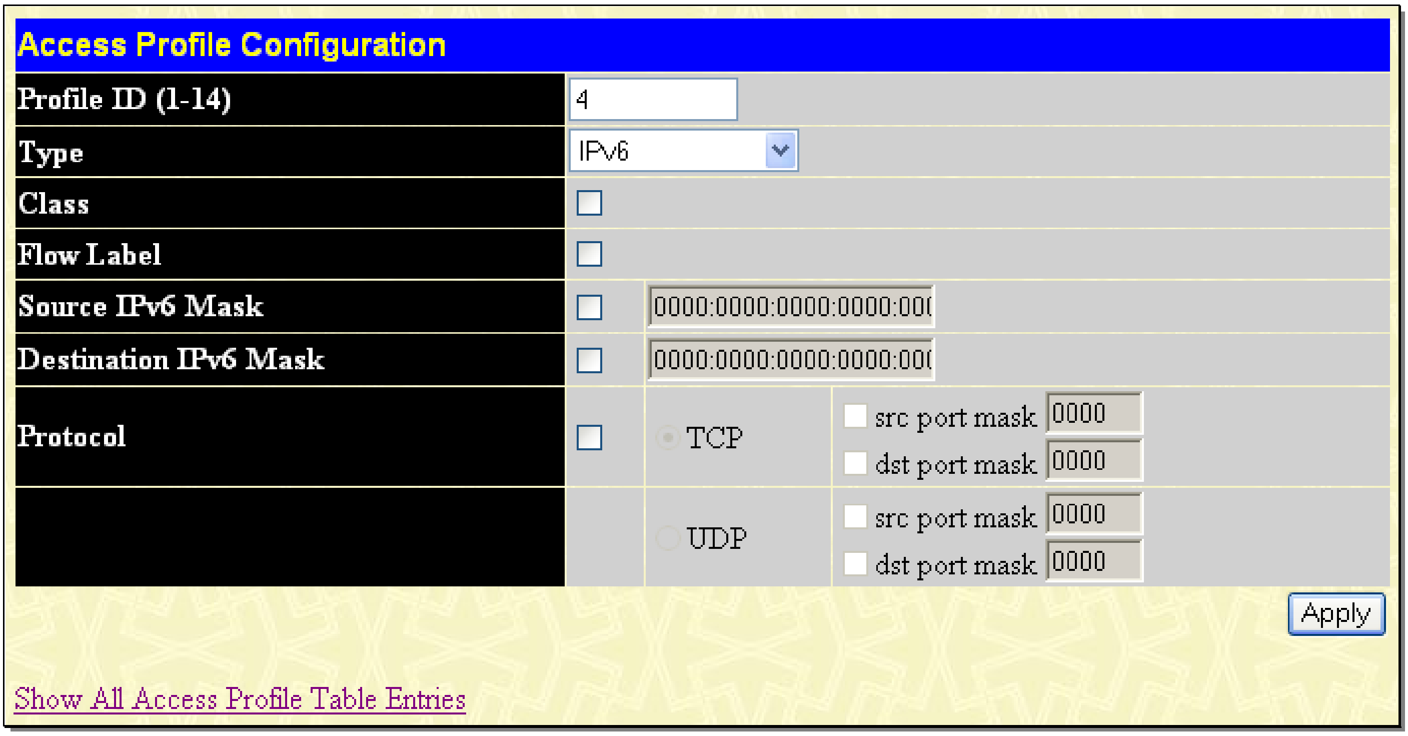
Figure 6- 5. Access Profile Configuration window (Packet Content Mask)

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 (1-14)	Type in a unique identifier number for this profile set. This value can be set from *1* to *14*.
Type	Select profile based on Ethernet (MAC Address), IP address, packet content mask or IPv6. 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 part of each packet header.
Offset	The offset field is used to examine the packet header which is divided up into four “chunks” where each chunk represents 4 bytes. Values within the packet header chunk to be identified are to be marked in hexadecimal form in the “mask” field. The following table will help you identify the bytes in the respective chunks. chunk0 chunk1 chunk2…….. chunk29 chunk30 chunk31 b126 b2 b6 b114 b118 b122 b127 b3 b7 b115 b119 b123 b0 b4 b8 b116 b120 b124 b1 b5 b9 b117 b121 b125 Tick the check box of the chunk, from 1 to 4, you wish to examine and then enter the hexadecimal value in the mask field.

Click **Apply** to implement changes made.

The window shown below is the **Access Profile Configuration** window for IPv6.



Access Profile Configuration

Profile ID (1-14)	4		
Type	IPv6		
Class	□		
Flow Label	□		
Source IPv6 Mask	□	0000:0000:0000:0000:00(	
Destination IPv6 Mask	□	0000:0000:0000:0000:00(	
Protocol	□	● TCP	□ src port mask 0000 □ dst port mask 0000
		○ UDP	□ src port mask 0000 □ dst port mask 0000

Figure 6- 6. Access Profile Configuration window (IPv6)

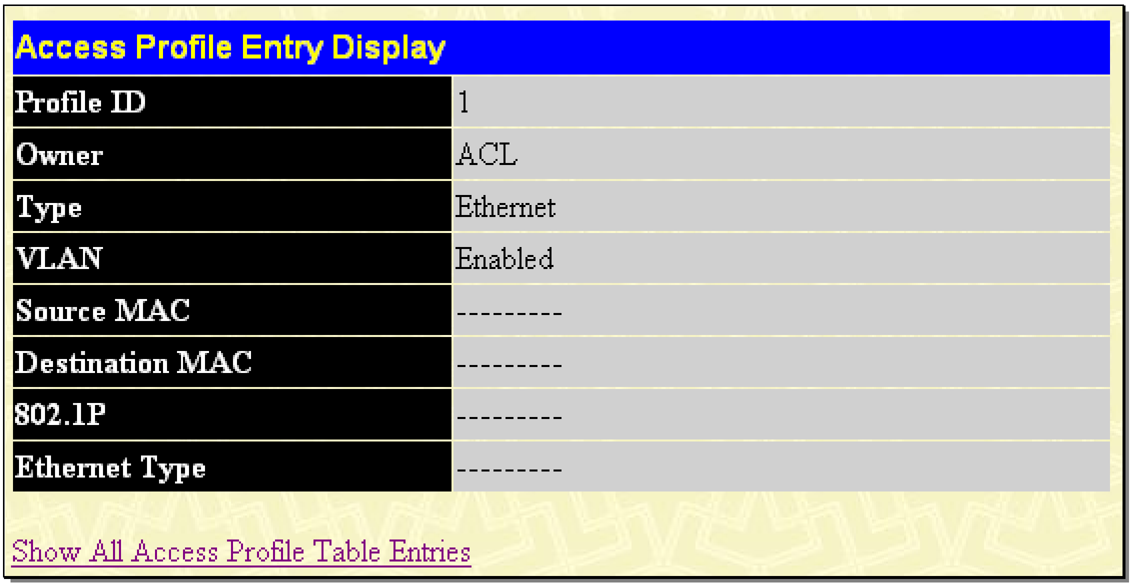
This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the IPv6:

Parameter	Description
Profile ID (1-14)	Type in a unique identifier number for this profile set. This value can be set from *1* to *14*.
Type	Select profile based on *Ethernet* (MAC Address), *IP Address, Packet Content* or *IPv6* address. This will change the window 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	Ticking this check box will instruct the Switch to examine the class field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flow Label	Ticking this check box will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Mask	The user may specify an IP address mask for the source IPv6 address by ticking 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 ticking the corresponding box and entering the IP address mask.
Protocol	Select TCP to use the IPv6 TCP port number contained in an incoming packet as the forwarding criterion. Selecting IPv6 TCP requires that you specify a source port mask and/or a destination port mask. src port mask - Specify a IPv6 TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. dst port mask - Specify a IPv6 TCP port mask for the destination port in hex form (hex

	0x0-0xffff) which you wish to filter. Select UDP to use the IPv6 UDP port number contained in an incoming packet as the forwarding criterion. Selecting IPv6 UDP requires that you specify a source port mask and/or a destination port mask. src port mask - Specify a IPv6 UDP port mask for the source port in hex form (hex 0x0-0xffff). dst port mask - Specify a IPv6 UDP port mask for the destination port in hex form (hex 0x0-0xffff)

Click **Apply** to implement changes made.

To view the configurations set for a previously created access profile, return to the **Access Profile Table** and click the View button under the Display heading, corresponding to the access profile for which to view configurations. A window similar to the one below will be displayed.



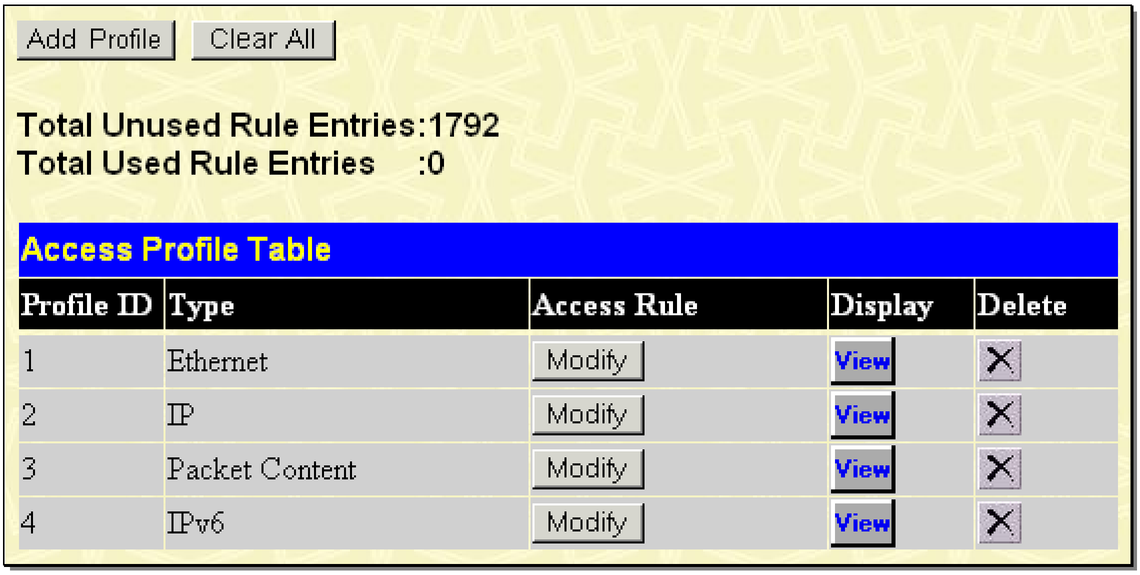
Access Profile Entry Display

Profile ID	1
Owner	ACL
Type	Ethernet
VLAN	Enabled
Source MAC	---------
Destination MAC	---------
802.1P	---------
Ethernet Type	---------

Figure 6- 7. Access Profile Entry Display window (Ethernet)

To establish the rule for a previously created Access Profile:

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



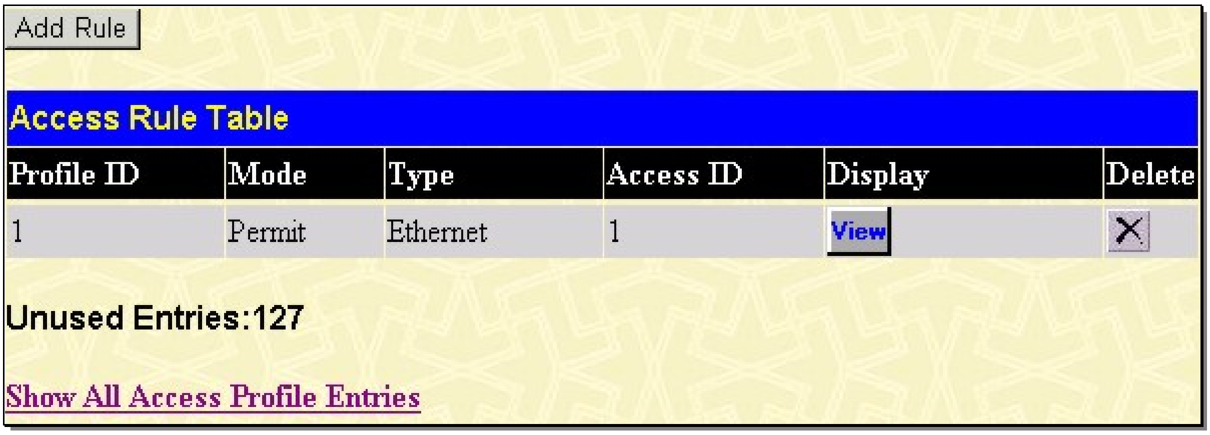
Total Unused Rule Entries:1792
Total Used Rule Entries :0

Access Profile Table

Profile ID	Type	Access Rule	Display	Delete
1	Ethernet	Modify	View	☒
2	IP	Modify	View	☒
3	Packet Content	Modify	View	☒
4	IPv6	Modify	View	☒

Figure 6- 8. Access Profile Table window

To create a new rule set for an access profile click the **Modify** button located under the **Access Rule** heading. The window shown below (**Access Profile Rule**) will be displayed. To remove a previously created rule, click the corresponding ☒ button.



Add Rule

Access Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Ethernet	1	View	☒

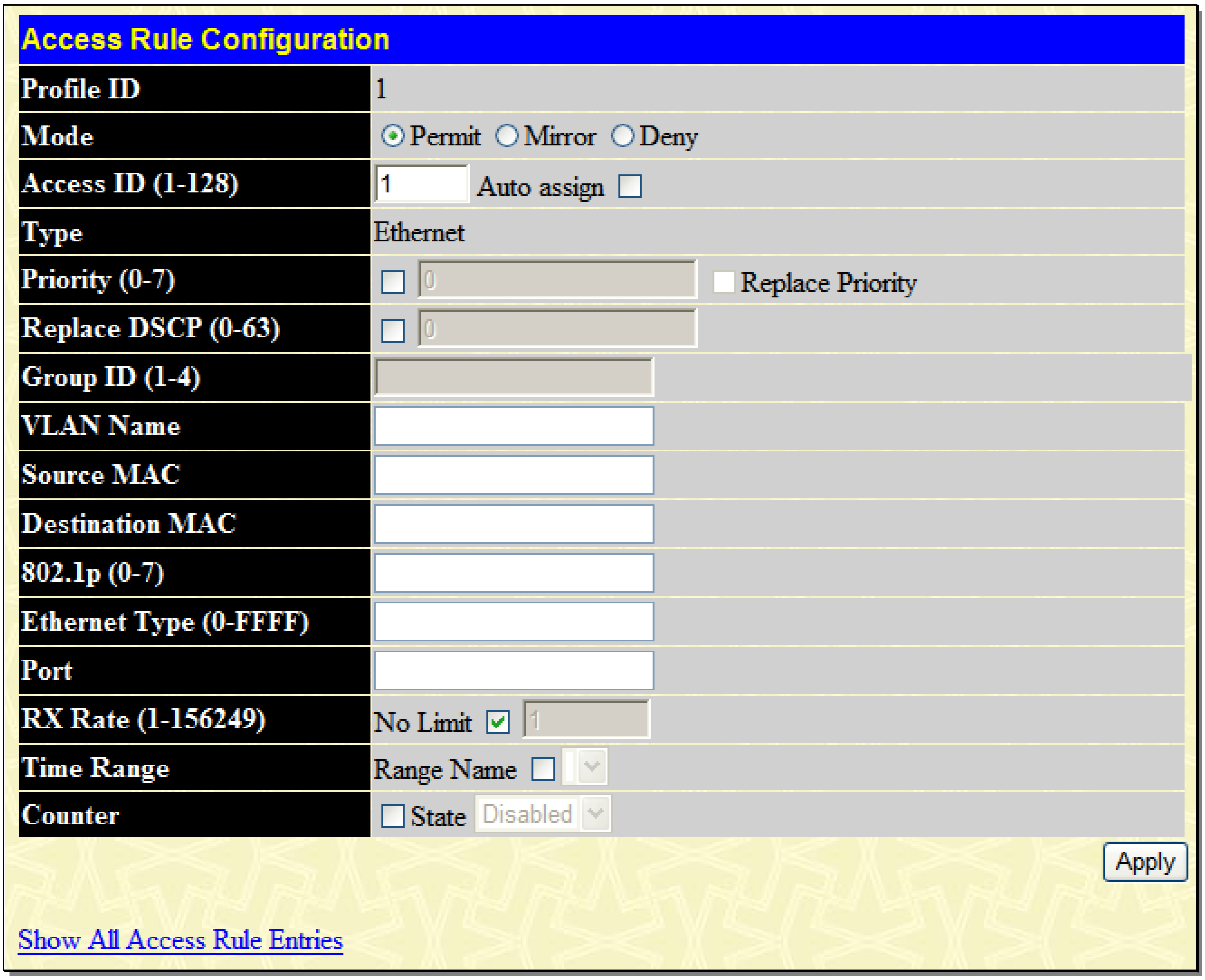
Unused Entries:127

Show All Access Profile Entries

Figure 6- 9. Access Rule Table window

Click **Add Rule** to add a new Rule for an existing profile. The **Access Rule Configuration** window will appear.

To remove a previously created rule, select it and click the ☒ button. To add a new Access Rule, click the **Add Rule** button, and the **Access Rule Configuration** window will appear:



Access Rule Configuration

Profile ID	1
Mode	● Permit ○ Mirror ○ Deny
Access ID (1-128)	1 Auto assign □
Type	Ethernet
Priority (0-7)	□ 0 □ Replace Priority
Replace DSCP (0-63)	□ 0
Group ID (1-4)	
VLAN Name	
Source MAC	
Destination MAC	
802.1p (0-7)	
Ethernet Type (0-FFFF)	
Port	
RX Rate (1-156249)	No Limit ☑ 1
Time Range	Range Name □
Counter	□ State Disabled

Apply

Show All Access Rule Entries

Figure 6- 10. Access Rule Configuration window (Ethernet)

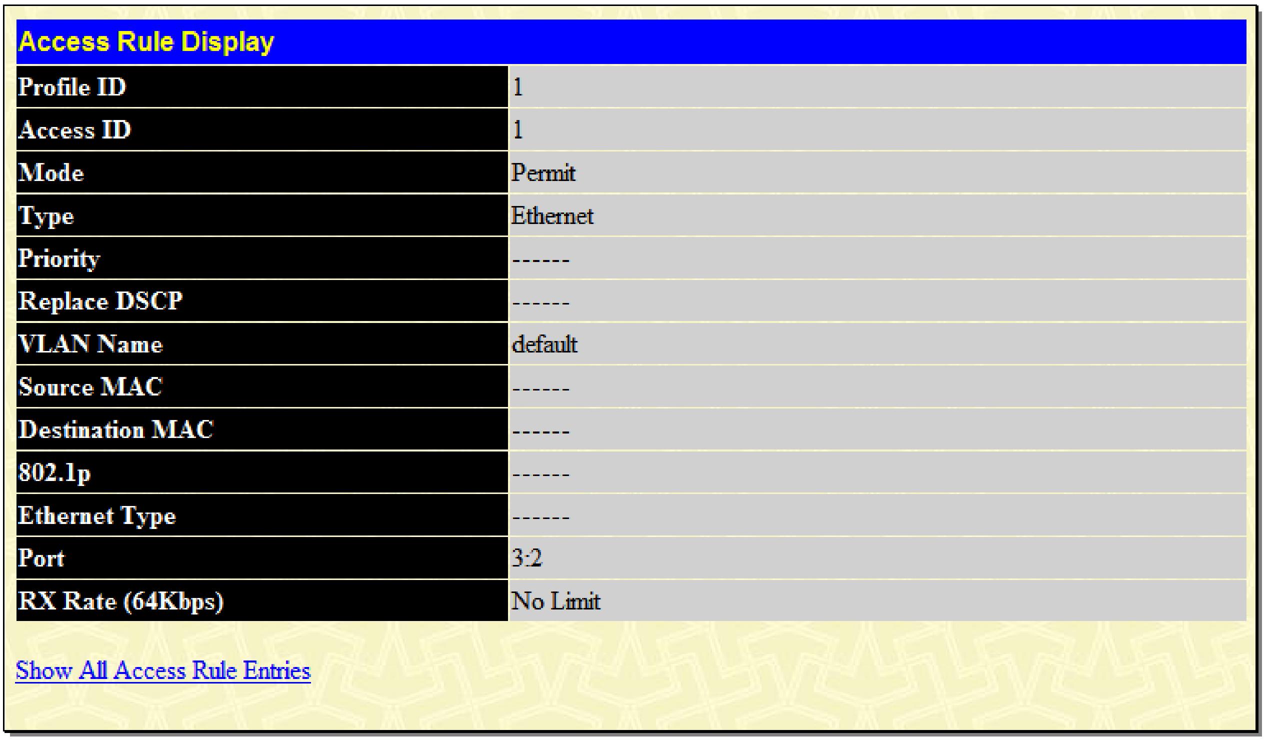
To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).

	Select *Deny* to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content, IPv6 address. 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 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. 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 – Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the *Priority* field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the **QoS** section of this manual.
Replace DSCP (0-63)	This feature allows the user to specify a value to be written to the DSCP field of an incoming packet. This value will over-write the value in the DSCP field of the packet. Enter a value between 0-63.
Group ID (1-4)	This field displays the mirror group's identity.
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 (0-FFFF)	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 0-9.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the *Auto Assign check* box MUST be clicked in the *Access ID* field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. 2 - 4 specifies the range of ports from 2 to 4.
RX Rate (1-156249)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *156249* or *No Limit*. The default setting is *No Limit*.
Time Range	Tick the check box and enter the name of the Time Range settings that has been previously

	configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.

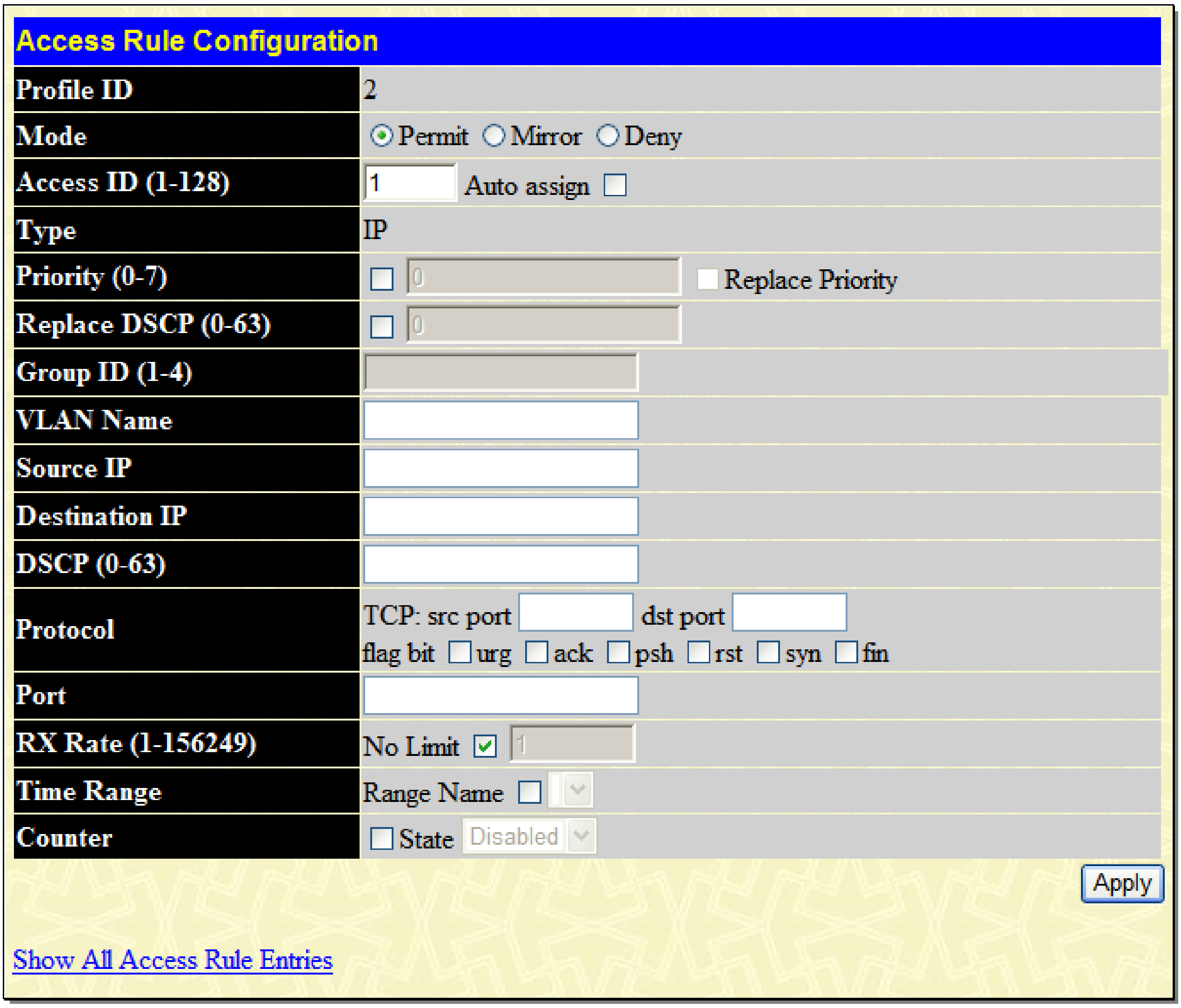
To view the settings of a previously, correctly configured rule, click View in the **Access Rule Table** to view the window shown below.



Access Rule Display

Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
Priority	------
Replace DSCP	------
VLAN Name	default
Source MAC	------
Destination MAC	------
802.1p	------
Ethernet Type	------
Port	3:2
RX Rate (64Kbps)	No Limit

Figure 6- 11. Access Rule Display window (Ethernet)



Access Rule Configuration

Profile ID	2
Mode	● Permit ○ Mirror ○ Deny
Access ID (1-128)	1 Auto assign □
Type	IP
Priority (0-7)	□ 0 □ Replace Priority
Replace DSCP (0-63)	□ 0
Group ID (1-4)	
VLAN Name	
Source IP	
Destination IP	
DSCP (0-63)	
Protocol	TCP: src port dst port flag bit □urg □ack □psh □rst □syn □fin
Port	
RX Rate (1-156249)	No Limit ☑ 1
Time Range	Range Name □
Counter	□State Disabled

Show All Access Rule Entries

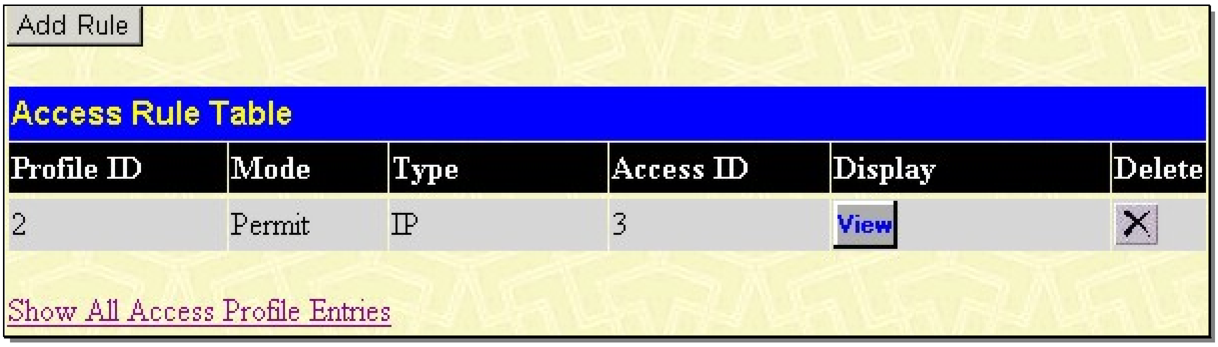
Figure 6- 12. Access Rule Configuration window (IP)

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 do not match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. • Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content, or IPv6 address. 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 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 – Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the *Priority* field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace 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.
Group ID (1-4)	This field displays the mirror group's identity.
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 Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. 2-4 specifies the range of ports from 2 to 4.
RX Rate (1-156249)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *156249* or *No Limit*. The default setting is *No Limit*.
Time Range	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table**.

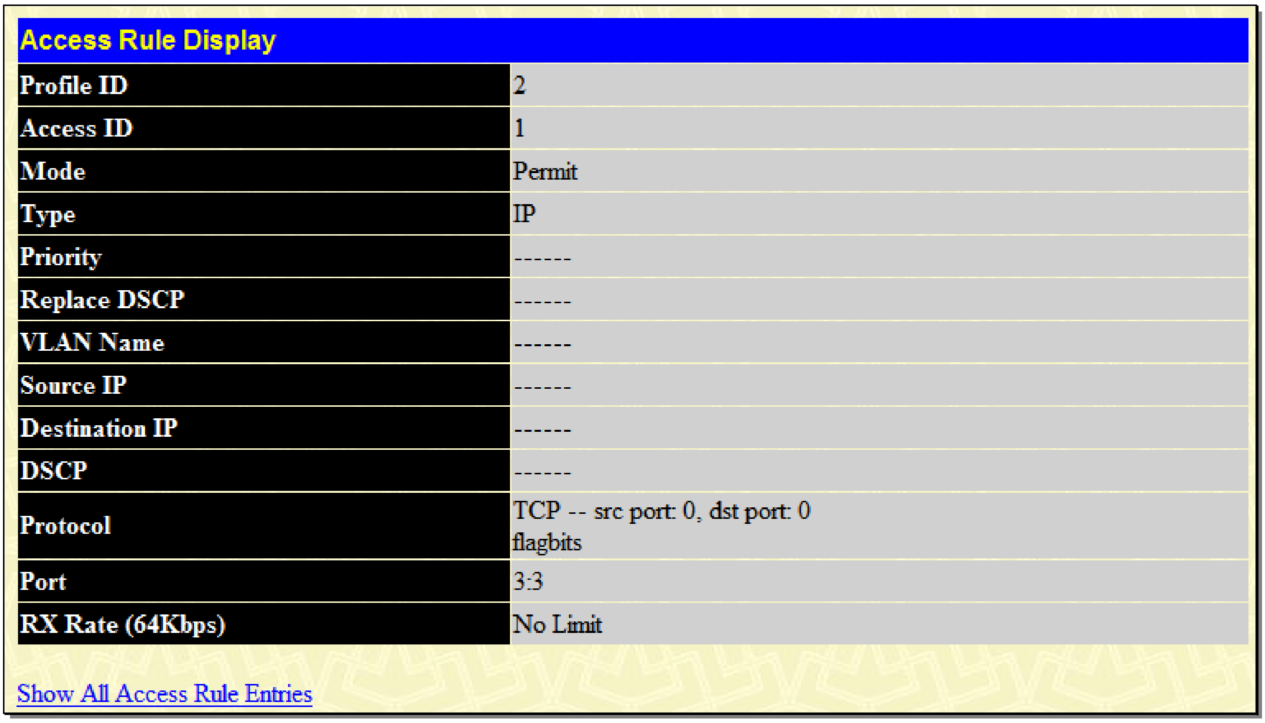


Access Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	IP	3	View	☒

Figure 6- 13. Access Rule Table window

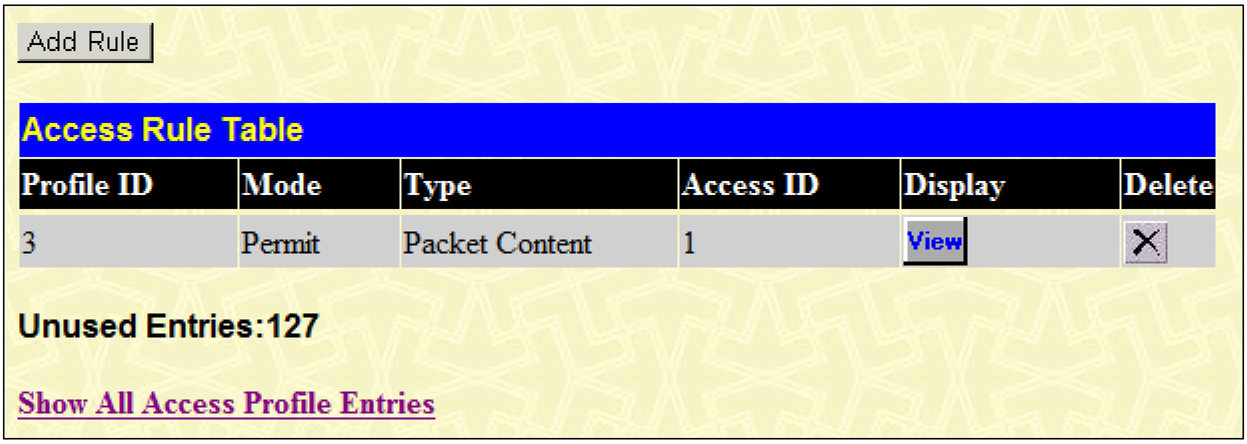
The window shown below will appear.



Access Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	IP
Priority	------
Replace DSCP	------
VLAN Name	------
Source IP	------
Destination IP	------
DSCP	------
Protocol	TCP -- src port: 0, dst port: 0 flagbits
Port	3:3
RX Rate (64Kbps)	No Limit

Figure 6- 14. Access Rule Display window (IP)

The following window is the Access Rule table for Packet Content.



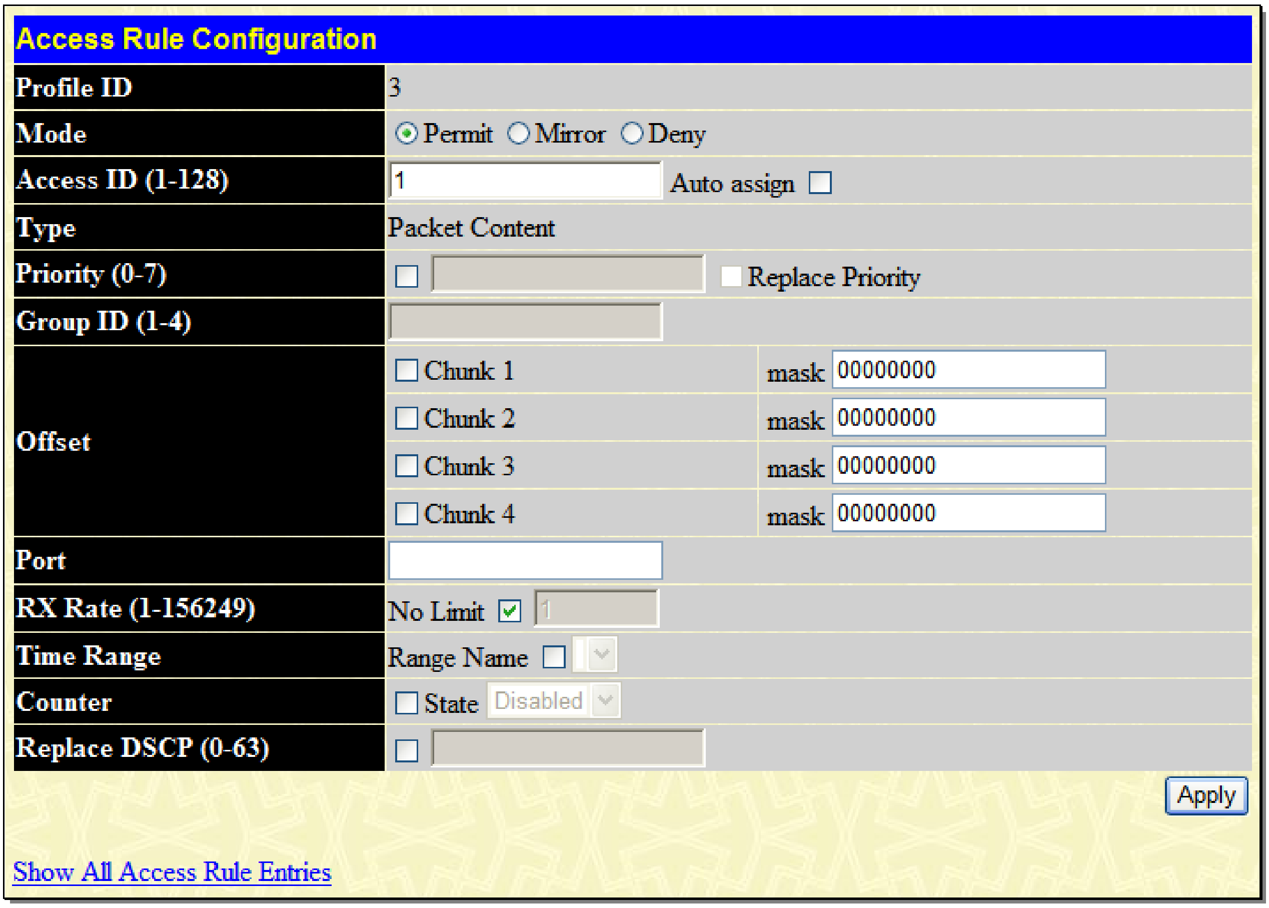
Access Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
3	Permit	Packet Content	1	View	☒

Unused Entries:127

Figure 6- 15. Access Rule Table window (Packet Content Mask)

To remove a previously created rule, select it and click the ☒ button. To add a new Access Rule, click the **Add Rule** button:



Access Rule Configuration

Profile ID	3	
Mode	● Permit ○ Mirror ○ Deny	
Access ID (1-128)	1 Auto assign □	
Type	Packet Content	
Priority (0-7)	□ □ Replace Priority	
Group ID (1-4)		
Offset	□ Chunk 1	mask 00000000
	□ Chunk 2	mask 00000000
	□ Chunk 3	mask 00000000
	□ Chunk 4	mask 00000000
Port		
RX Rate (1-156249)	No Limit ☑ 1	
Time Range	Range Name □	
Counter	□ State Disabled	
Replace DSCP (0-63)	□	

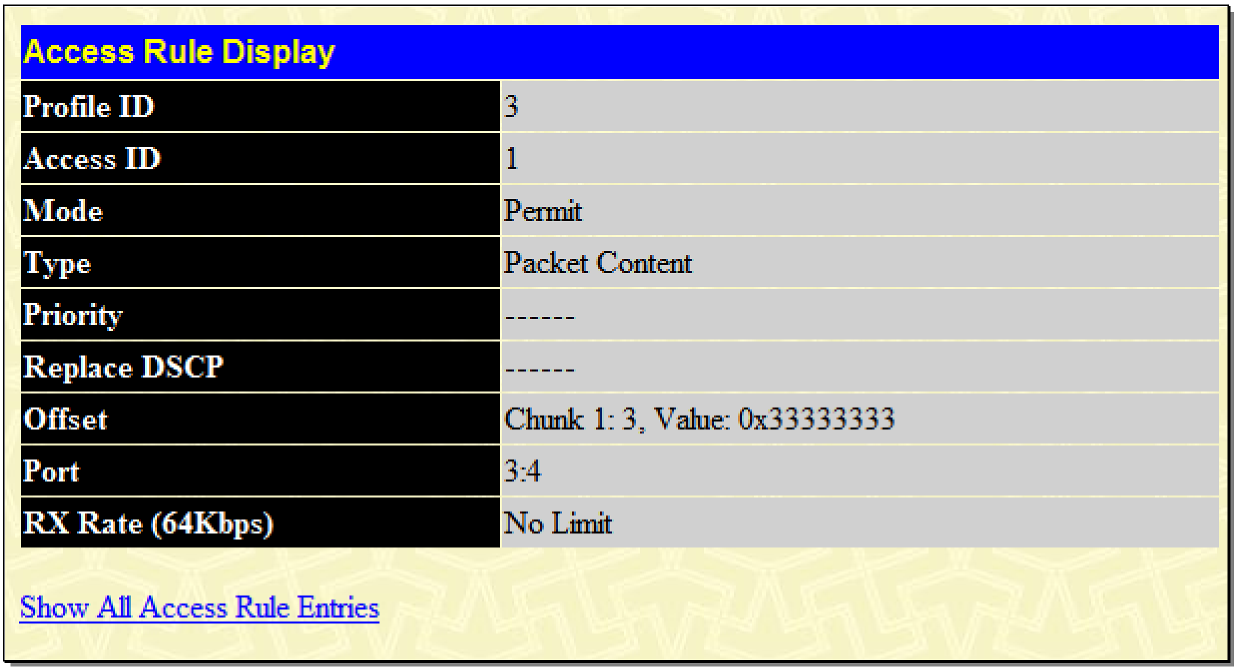
Figure 6- 16. Access Rule Configuration window (Packet Content Mask)

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 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. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
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 part of each packet header.

Priority (0-7)	This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. Replace priority with – Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Group ID (1-4)	This field displays the mirror group's identity.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: Chunk 1 - Enter a value in hex form to mask the packet from the beginning of the packet to the first chunk. Chunk 2 - Enter a value in hex form to mask the packet from the end of the first chunk to the end of the second chunk. Chunk 3- Enter a value in hex form to mask the packet from the end of the second chunk to the end of the third chunk. Chunk 4 - Enter a value in hex form to mask the packet from the end of the third chunk to the end of the fourth chunk.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The beginning and end of the port list range are separated by a dash. Entering *all* will denote all ports on the Switch.
Rx Rate (1-156249)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *156249* or *No Limit*. The default setting is *No Limit*.
Time Range	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.
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.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following window:



Access Rule Display

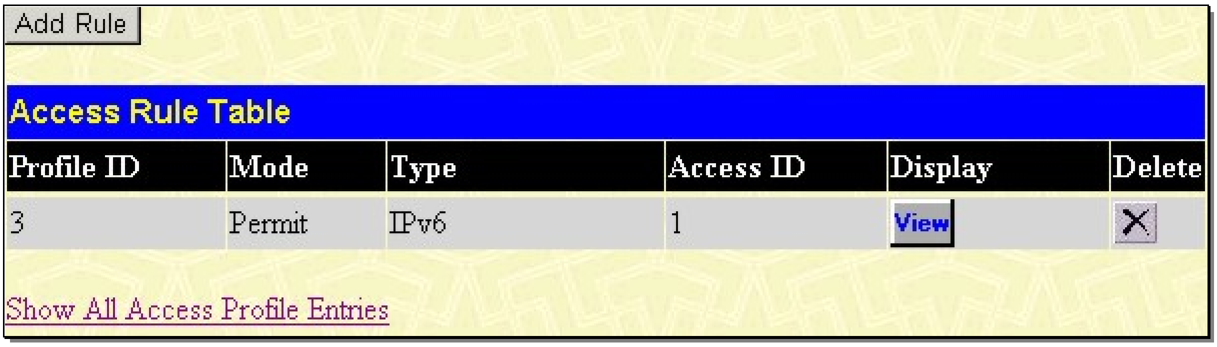
Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
Priority	------
Replace DSCP	------
Offset	Chunk 1: 3, Value: 0x33333333
Port	3:4
RX Rate (64Kbps)	No Limit

Show All Access Rule Entries

Figure 6- 17. Access Rule Display window (Packet Content Mask)

NOTE: When using the ACL Mirror function, ensure that the Port Mirroring function is enabled and a target mirror port is set.

To configure the Access Rule for IPv6, open the **Access Profile Table** window and click **Modify** for an IPv6 entry. This will open the following window:



Add Rule

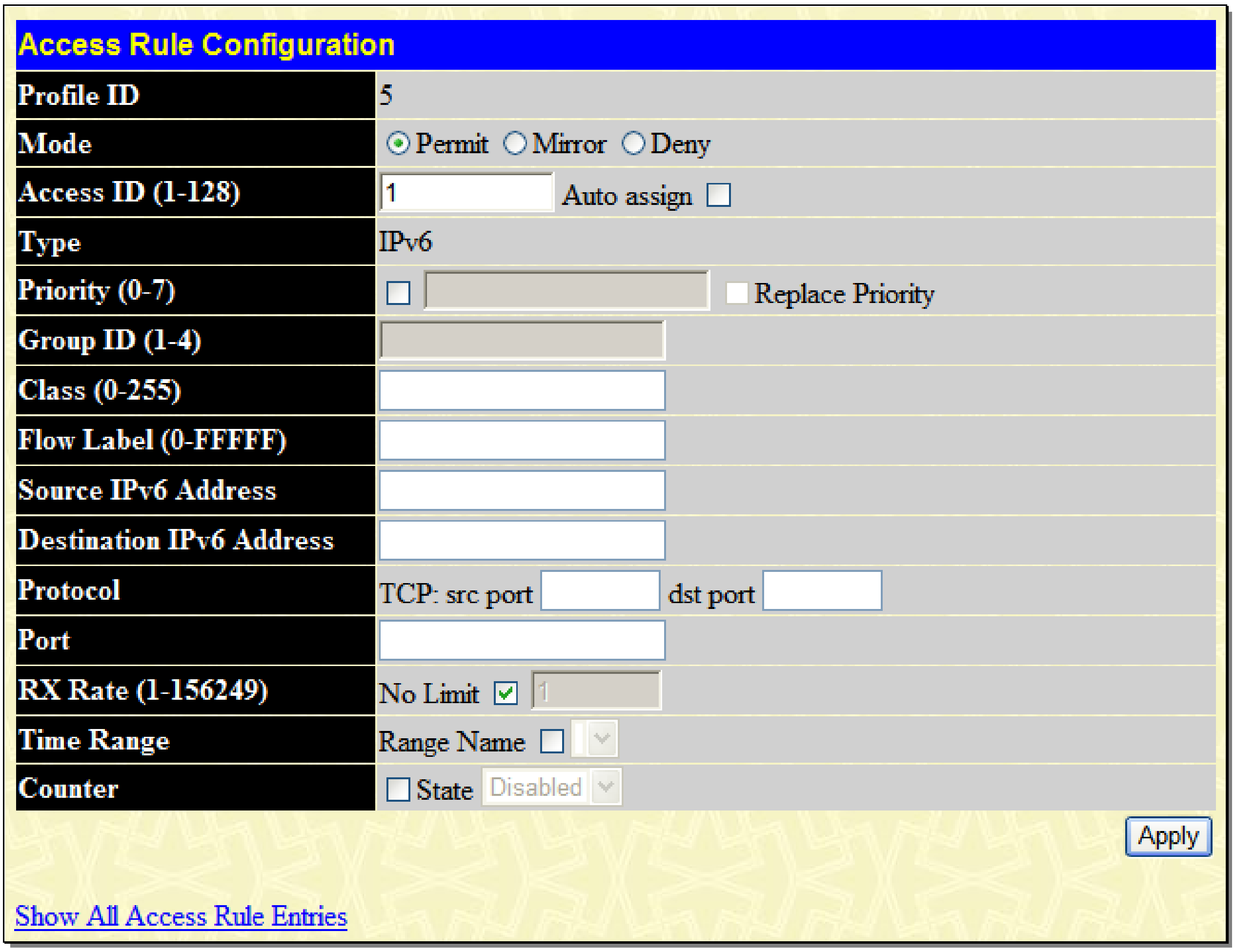
Access Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
3	Permit	IPv6	1	View	☒

Show All Access Profile Entries

Figure 6- 18. Access Rule Table window (IPv6)

To remove a previously created rule, click its corresponding ☒ button. To add a new Access Rule, click the **Add Rule** button:



Access Rule Configuration

Profile ID	5
Mode	● Permit ○ Mirror ○ Deny
Access ID (1-128)	1 Auto assign □
Type	IPv6
Priority (0-7)	□ □ Replace Priority
Group ID (1-4)	
Class (0-255)	
Flow Label (0-FFFFF)	
Source IPv6 Address	
Destination IPv6 Address	
Protocol	TCP: src port dst port
Port	
RX Rate (1-156249)	No Limit ☑ 1
Time Range	Range Name □
Counter	□ State Disabled

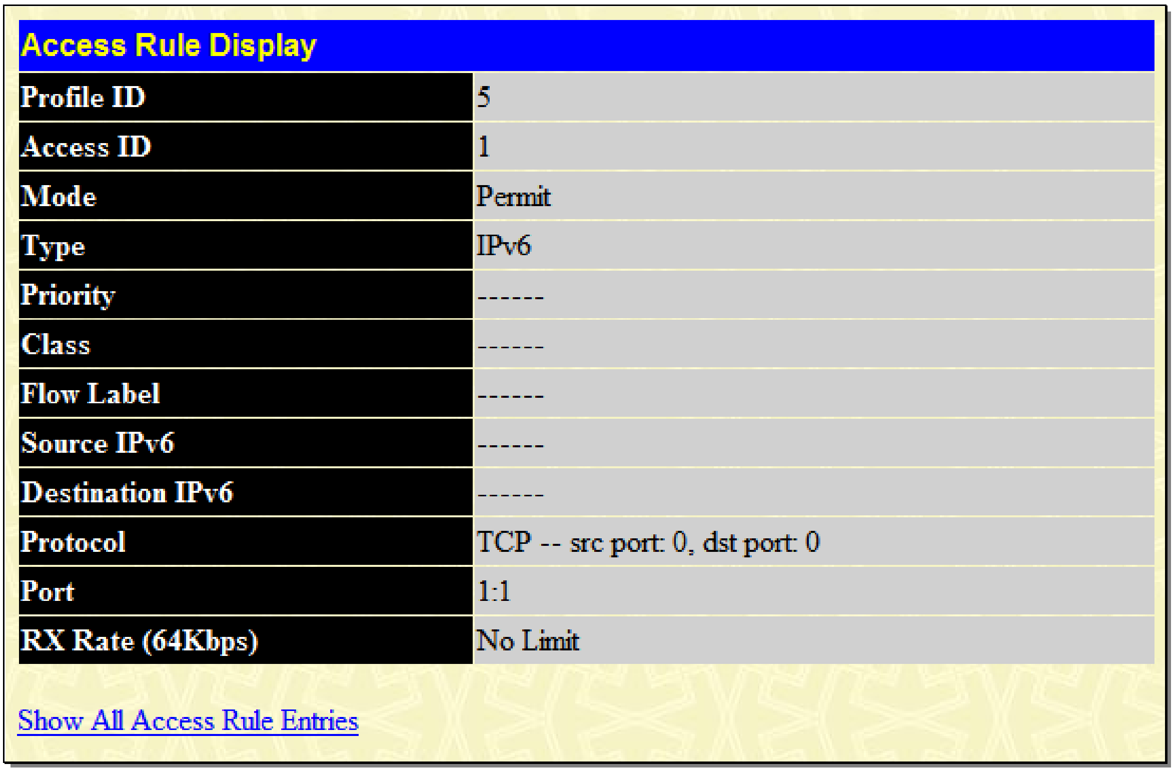
Figure 6- 19. Access Rule Configuration window (IPv6)

To set the Access Rule for the IPv6, 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 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. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access rule. This value can be set from *1* to *128*. • Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content, or IPv6 address. • 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 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 – Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its

	incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Group ID (1-4)	This field displays the mirror group's identity.
Class (0-255)	Entering a value between *0* and *255* 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 of IPv4.
Flow Label (0-FFFFF)	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the Switch.
Rx Rate (1-156249)	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between *1* and *156249* or *No Limit*. The default setting is *No Limit*.
Time Range	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** window to view the following:



Access Rule Display

Profile ID	5
Access ID	1
Mode	Permit
Type	IPv6
Priority	------
Class	------
Flow Label	------
Source IPv6	------
Destination IPv6	------
Protocol	TCP -- src port: 0, dst port: 0
Port	1:1
RX Rate (64Kbps)	No Limit

Figure 6- 20. Access Rule Display window (IPv6)

ACL Flow Meter

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

trTCM – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow's surpassing of two rates, the CIR and the PIR.

> **CIR** – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn't exceed the CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.
>
> **CBS** – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.
>
> **PIR** – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.
>
> **PBS** – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.

srTCM – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.

> **CBS** – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.
>
> **EBS** – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.

DSCP – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.

The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.

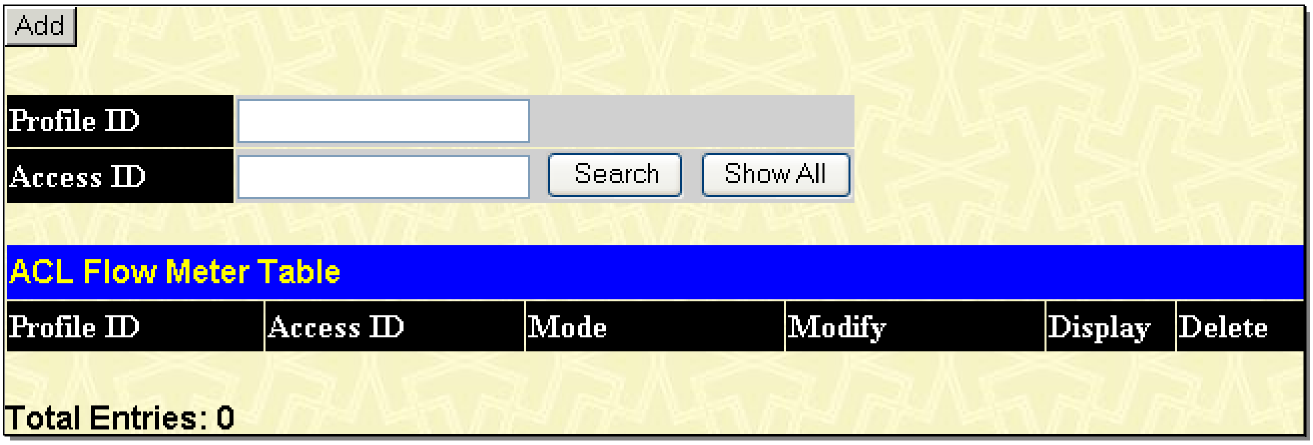
Green – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.

Yellow – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Red – When an IP flow is in the red mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the **Counter** check box. If the counter is enabled, the counter setting in the access profile will be disabled. Users may only enable two counters for one flow meter at any given time.

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



Add

Profile ID			
Access ID		Search	Show All

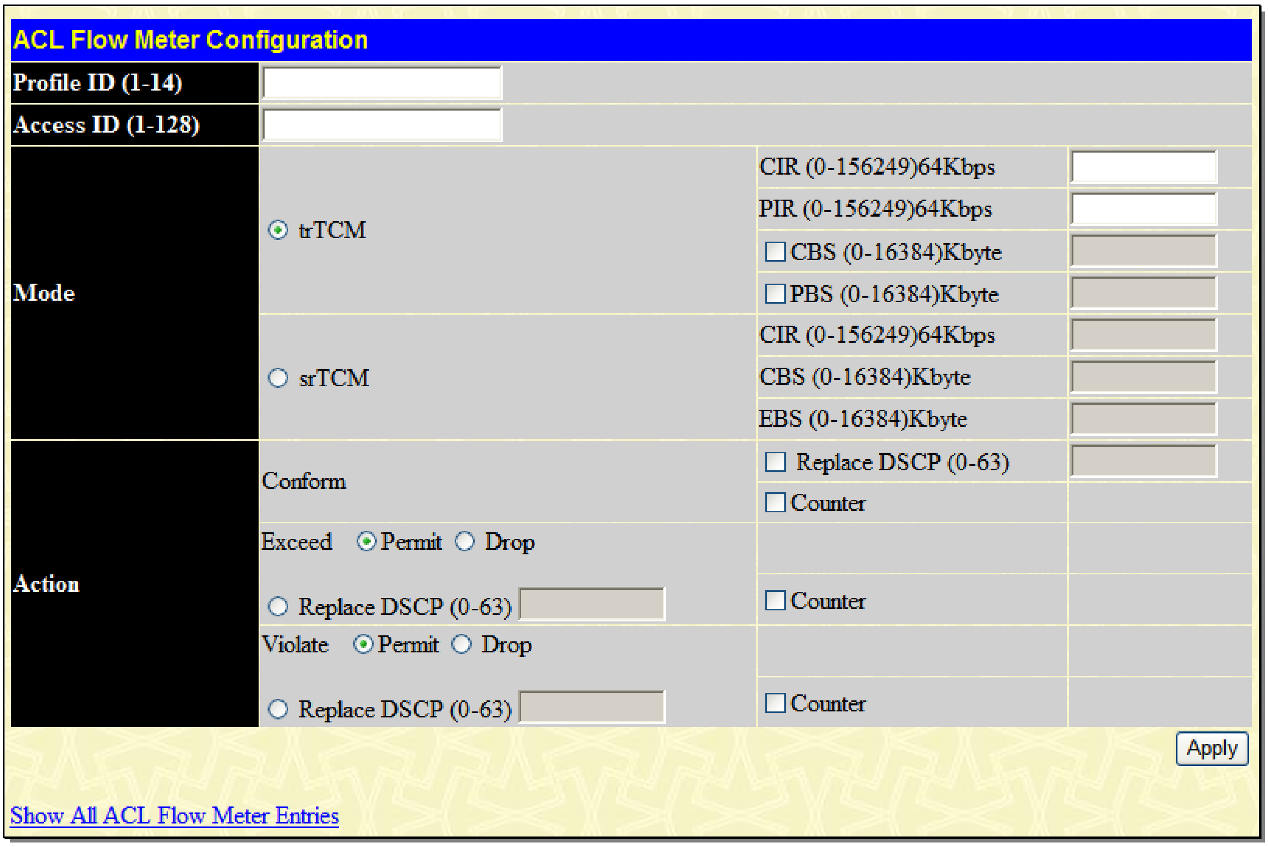
ACL Flow Meter Table

Profile ID	Access ID	Mode	Modify	Display	Delete

Total Entries: 0

Figure 6- 21. ACL Flow Meter Table window

The previous window allows users to view the ACL profile and rule that is utilizing the ACL Flow Meter function, and the mode associated with that profile and rule. Users may search a particular Profile ID or Access ID by entering that value into one of the available fields and clicking Search. The result should be displayed in the table. Click **Show All** to show all ACL Profiles and Access IDs that are utilizing the ACL Flow Metering function. To add an ACL Flow Meter configuration for an Access Profile and Rule, click the **Add** button, which will display the following window for users to configure.



ACL Flow Meter Configuration

Profile ID (1-14)			
Access ID (1-128)			
Mode	● trTCM	CIR (0-156249)64Kbps	
		PIR (0-156249)64Kbps	
		□ CBS (0-16384)Kbyte	
		□ PBS (0-16384)Kbyte	
	○ srTCM	CIR (0-156249)64Kbps	
		CBS (0-16384)Kbyte	
		EBS (0-16384)Kbyte	
Action	Conform	□ Replace DSCP (0-63)	
		□ Counter	
	Exceed ● Permit ○ Drop		
	○ Replace DSCP (0-63)	□ Counter	
	Violate ● Permit ○ Drop		
	○ Replace DSCP (0-63)	□ Counter	

Apply

Show All ACL Flow Meter Entries

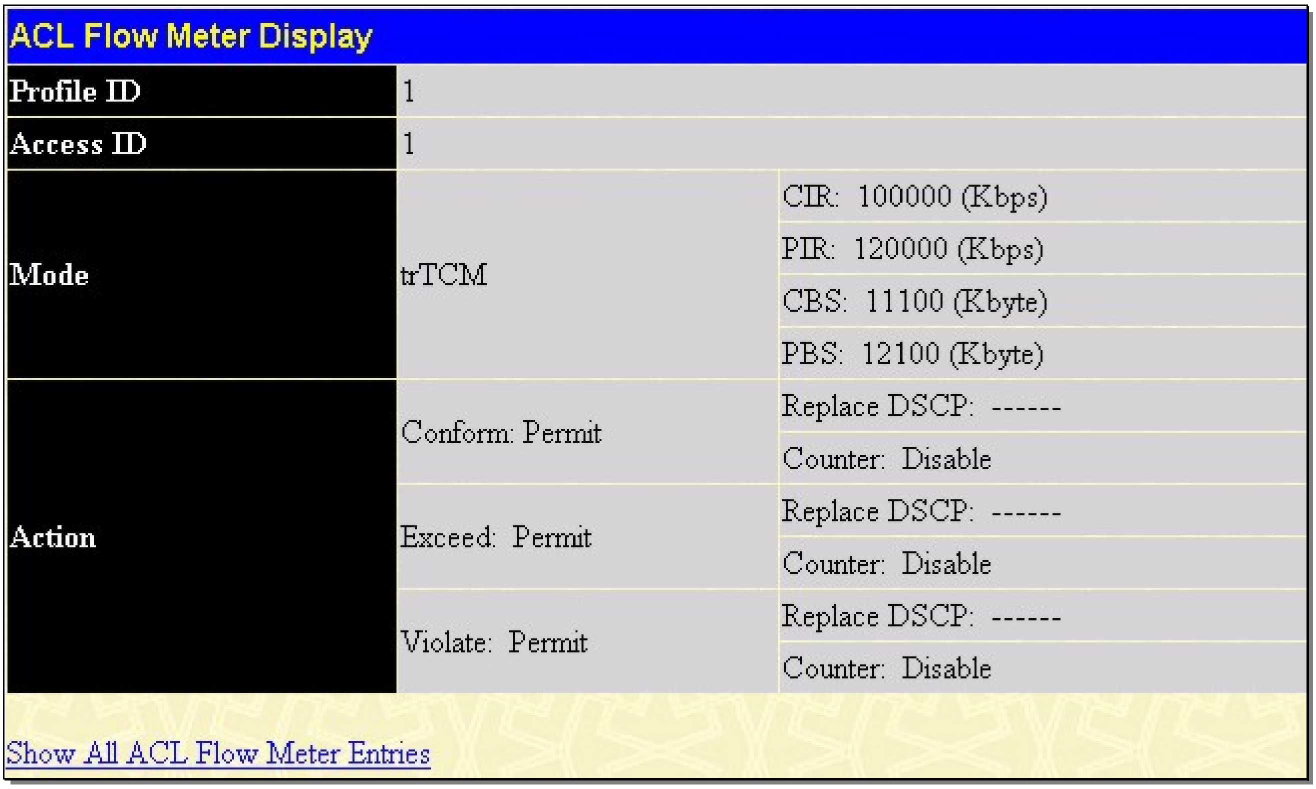
Figure 6- 22. ACL Flow Meter Configuration window

The following fields may be configured:

Parameter	Description
Profile ID (1-14)	Enter the pre-configured Profile ID for which to configure the ACL Flow Metering parameters.
Access ID (1-128)	Enter the pre-configured Access ID for which to configure the ACL Flow Metering parameters.
Mode	In this field the user may choose they type of mode to be employed for the ACL Flow Meter function, and then the limits of the packet flow.
trTCM	Choosing this field will allow users to employ the Two Rate Three Color Mode and set the

	following parameters to determine the color rate of the IP packet flow. CIR – The Committed Information Rate can be set between 0 and 156249. IP flow rates at or below this level will be considered green. IP flow rates that exceed this rate but not the PIR rate are considered yellow. PIR – The Peak information Rate. IP flow rates that exceed this setting will be considered as red. This field must be set at an equal or higher value than the CIR. CBS – The Committed Burst Size. Used to gauge packets that are larger than the normal IP packets. Click the check box to employ the CBS. This field does not have to be set for this feature to function properly but is to be used in conjunction with the CIR setting. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. PBS - The Peak Burst Size. This optional field is to be used in conjunction with the PIR. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.
srTCM	Choosing this field will allow users to employ the Single Rate Three Color Mode and set the following parameters to determine the color rate of the IP packet flow. CIR – The Committed Information Rate can be set between 0 and 156249. The color rates are based on the following two fields which are used in conjunction with the CIR. CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. Packet flows that are lower than this configured value are marked green. Packet flows that exceed this value but are less than the EBS value are marked yellow. EBS – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS. Packet flows that exceed this value are marked as red.
Action	This field is used to determine the course of action when a packet flow has been marked as a color, based on the following fields.
Conform	This field denotes the green packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by ticking the Counter check box.
Exceed	This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. Users may also choose to count yellow packets by ticking the Counter check box.
Violate	This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. Users may also choose to count yellow packets by ticking the Counter check box.

Click **Apply** to save changes made. To view the ACL Flow Meter configurations for a particular Profile and Access ID, click its corresponding View button, as seen in the **ACL Flow Meter Table** window that will display the following read-only window.



ACL Flow Meter Display

Profile ID	1	
Access ID	1	
Mode	trTCM	CIR: 100000 (Kbps)
		PIR: 120000 (Kbps)
		CBS: 11100 (Kbyte)
		PBS: 12100 (Kbyte)
Action	Conform: Permit	Replace DSCP: ------
		Counter: Disable
	Exceed: Permit	Replace DSCP: ------
		Counter: Disable
	Violate: Permit	Replace DSCP: ------
		Counter: Disable

Figure 6- 23. ACL Flow Meter Display window

CPU Interface Filtering

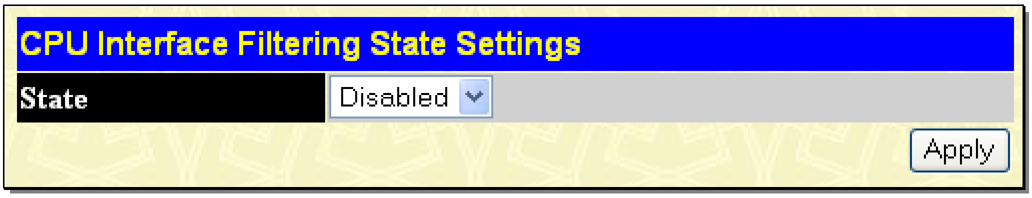
Due to a chipset limitation and the need for extra switch security, the Switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP, Packet Content Mask and IPv6 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 State

In the following window, the user may globally enable or disable the CPU Interface Filtering mechanism by using the pull-down menu to change the running state.

To view this window, click **ACL > CPU Interface Filtering > CPU Interface Filtering State**, as shown below:



CPU Interface Filtering State Settings

State: Disabled

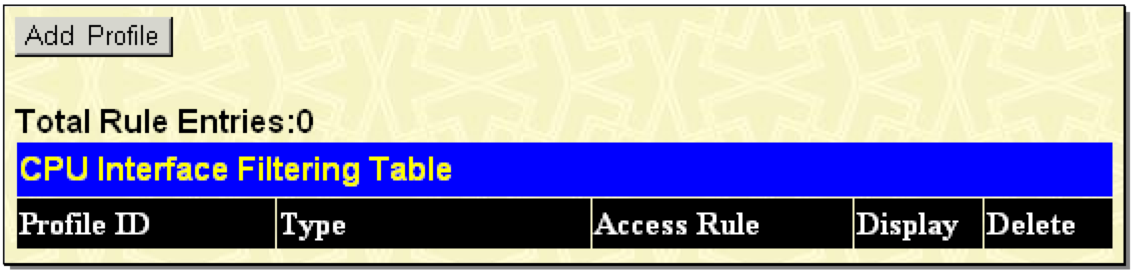
Figure 6- 24. CPU Interface Filtering State Settings window

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

CPU Interface Filtering Table

This window allows the user to create a new profile for the CPU Interface Filtering Table.

To view this windw, click **ACL** > **CPU Interface Filtering** > **CPU Interface Filtering Table**, as shown below:



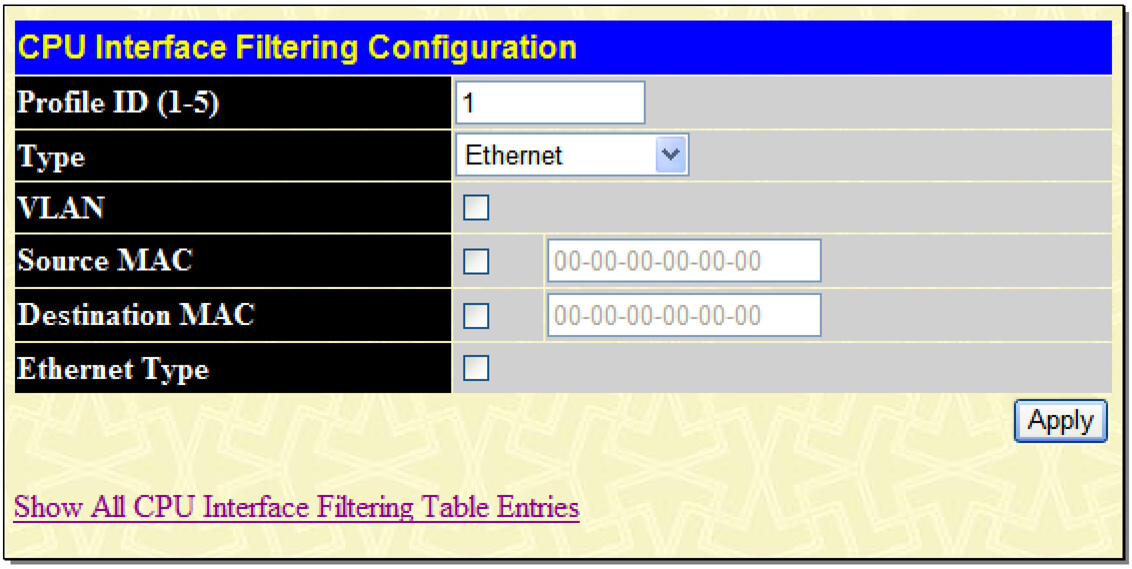
Total Rule Entries:0

CPU Interface Filtering Table

Profile ID	Type	Access Rule	Display	Delete

Figure 6- 25. CPU Interface Filtering Table window

To add an entry to the CPU Interface Filtering Table, click the **Add Profile** button. This will open the **CPU Interface Filtering Profile Configuration** window, as shown below: There are four **CPU Access Profile Configuration** windows; 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. Users can switch between the four **CPU Access Profile Configuration** windows by using the Type drop-down menu. The window shown below is the **CPU Interface Filtering Configuration** window for Ethernet.



CPU Interface Filtering Configuration

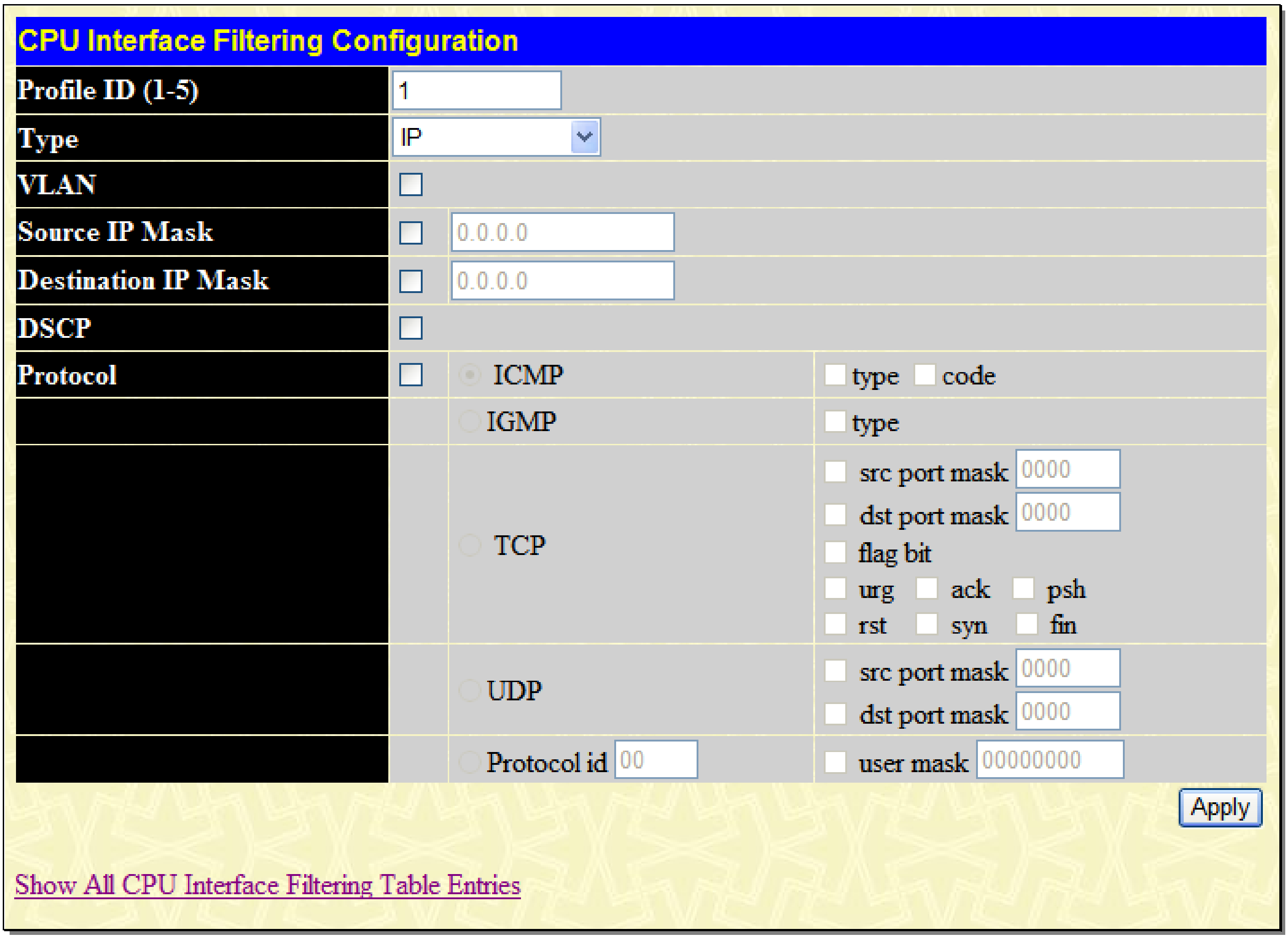
Profile ID (1-5)	1	
Type	Ethernet	
VLAN	□	
Source MAC	□	00-00-00-00-00-00
Destination MAC	□	00-00-00-00-00-00
Ethernet Type	□	

Figure 6- 26. CPU Interface Filtering Configuration window (Ethernet)

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from *1 to 5*.
Type	Select profile based on *Ethernet* (MAC Address), *IP* address or *Packet Content Mask* 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.
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.
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 window shown below is the **CPU Interface Filtering Configuration** for IP window.



CPU Interface Filtering Configuration

Profile ID (1-5): 1

Type: IP

VLAN: □

Source IP Mask: □ 0.0.0.0

Destination IP Mask: □ 0.0.0.0

DSCP: □

Protocol: □

○ ICMP □ type □ code

○ IGMP □ type

○ TCP □ src port mask 0000 □ dst port mask 0000 □ flag bit □ urg □ ack □ psh □ rst □ syn □ fin

○ UDP □ src port mask 0000 □ dst port mask 0000

○ Protocol id 00 □ user mask 00000000

Figure 6- 27. CPU Interface Filtering Configuration window (IP)

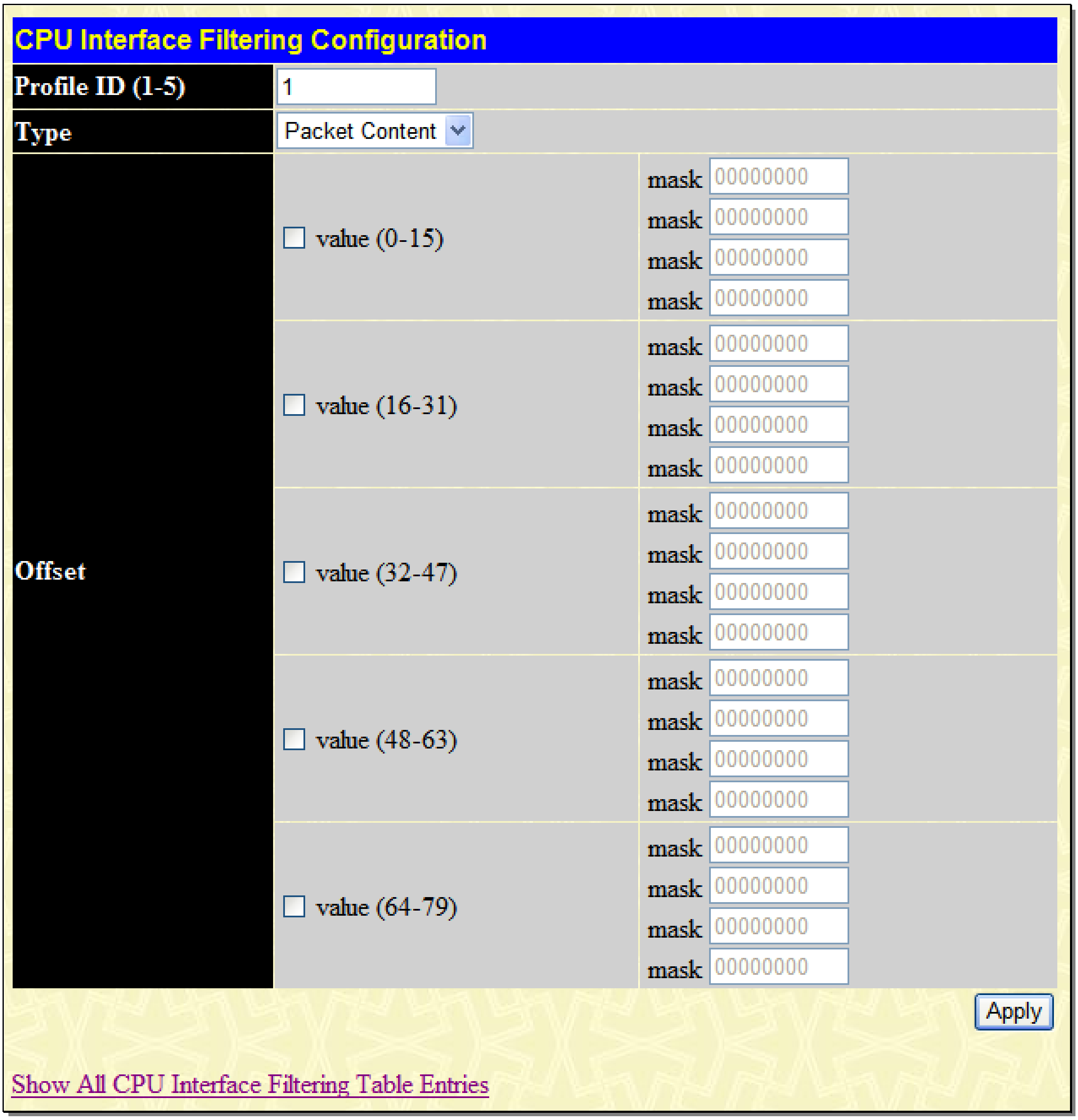
The following parameters can be modified:

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from *1* to *5*.
Type	Select profile based on *Ethernet* (MAC Address), *IP* address or *Packet Content Mask* 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.
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the criterion, 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. Users must then specify what protocol(s) to include according to the following guidelines: Select ICMP to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select Type to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select Type to further specify that the access profile will apply an IGMP type value. Select TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). src port mask - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. dst port mask - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. Select UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. src port mask - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). dst port mask - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Protocol id - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff).

Click **Apply** to set this entry in the Switch's memory.

The window shown below is the **CPU Interface Filtering Configuration** window for the Packet Content Mask.



CPU Interface Filtering Configuration

Profile ID (1-5)	1	
Type	Packet Content	
Offset	□ value (0-15)	mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (16-31)	mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (32-47)	mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (48-63)	mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (64-79)	mask 00000000 mask 00000000 mask 00000000 mask 00000000

Figure 6- 28. CPU Interface Filtering Configuration window (Packet Content)

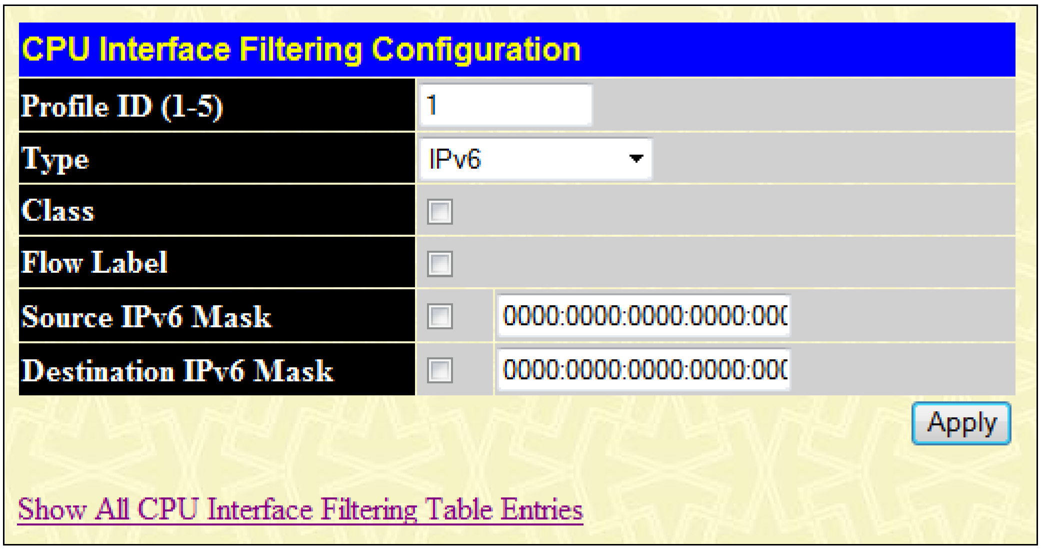
This window will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the Packet Content Mask:

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from *1 to 5*.
Type	Select profile based on *Ethernet* (MAC Address), *IP* address or *Packet Content Mask* 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* t instruct the Switch to examine the IPv6 address in each frame's 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.

The window shown below is the IPv6 configuration window.



CPU Interface Filtering Configuration

Profile ID (1-5)	1	
Type	IPv6	
Class	□	
Flow Label	□	
Source IPv6 Mask	□	0000:0000:0000:0000:00(
Destination IPv6 Mask	□	0000:0000:0000:0000:00(

Figure 6- 29. CPU Interface Filtering Configuration window (IPv6)

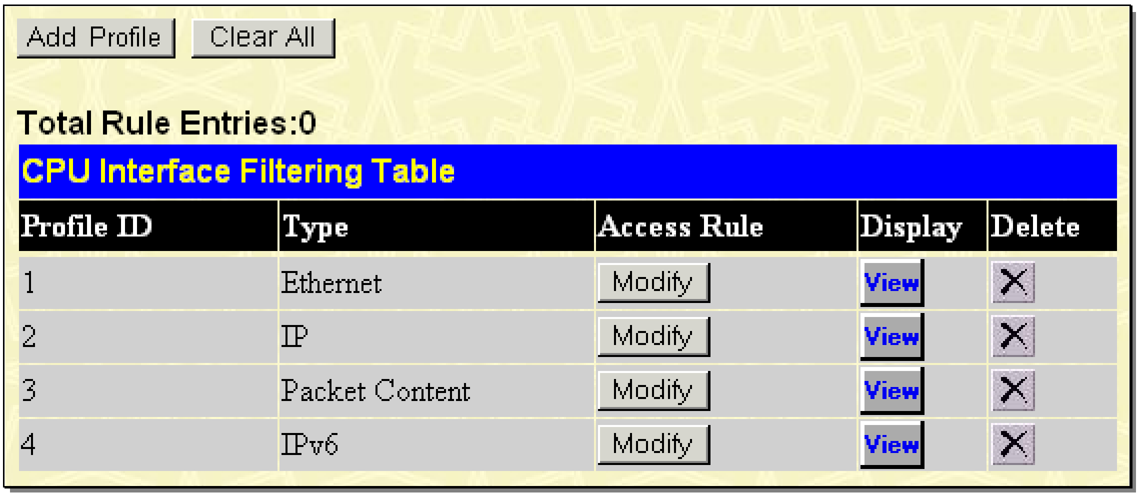
The following fields are used to configure the Packet Content Mask:

Parameter	Description
Profile ID	This is the identifier number for this profile set. Up to five profile ID configurations can be created.
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 part of each packet header.
Class	Tick this check box to 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 of IPv4.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.

Click **Apply** to implement changes made.

To establish the rule for a previously created CPU Access Profile:

To view this window, click **ACL** > **CPU Interface Filtering > CPU Interface Filtering Table**, as shown below:



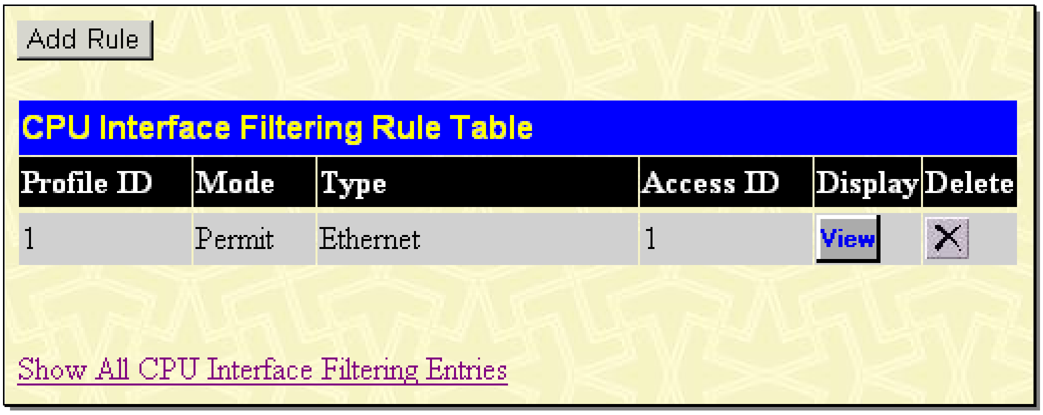
Total Rule Entries:0

CPU Interface Filtering Table

Profile ID	Type	Access Rule	Display	Delete
1	Ethernet	Modify	View	☒
2	IP	Modify	View	☒
3	Packet Content	Modify	View	☒
4	IPv6	Modify	View	☒

Figure 6- 30. CPU Interface Filtering Table window - Add

In this window, the user may add a rule to a previously created CPU access profile by clicking the corresponding **Add Rule** button of the entry to configure Ethernet, IPv4, Packet Content Mask, or IPv6.



CPU Interface Filtering Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Ethernet	1	View	☒

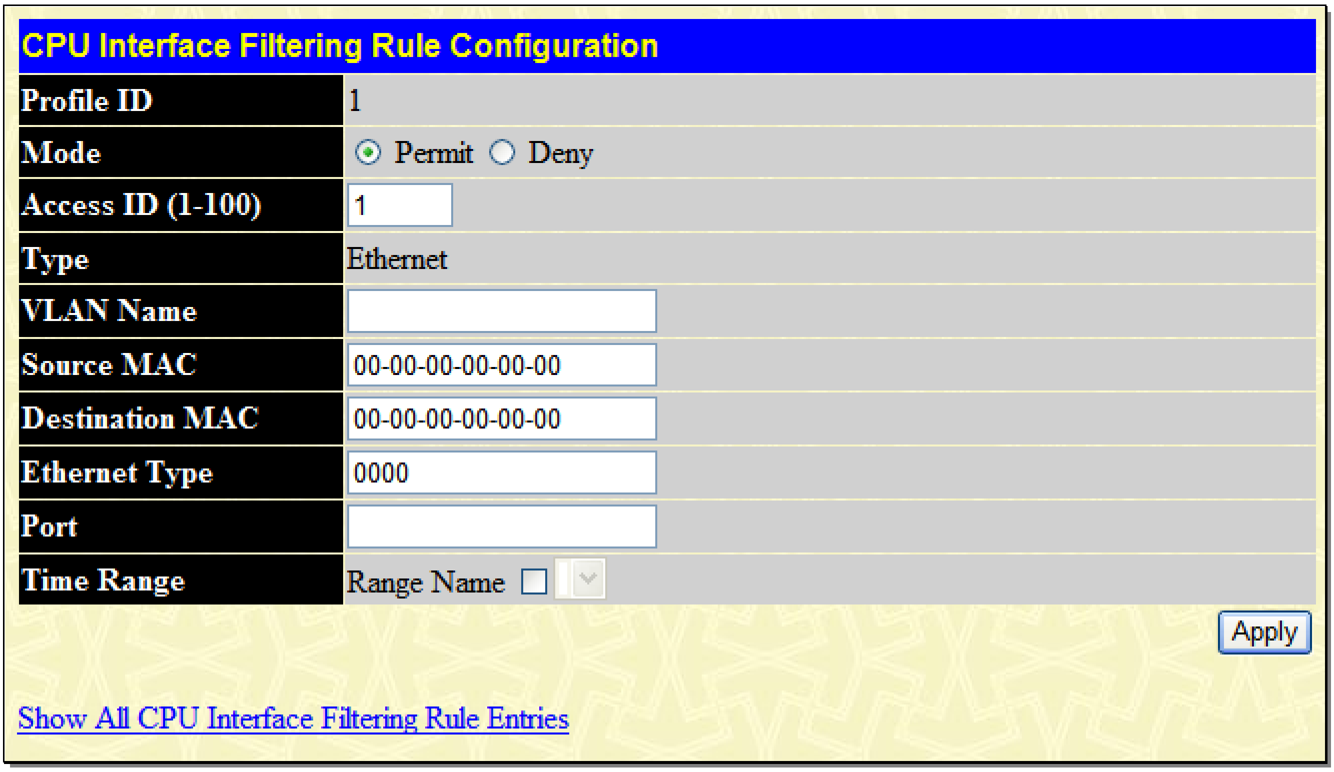
Show All CPU Interface Filtering Entries

Figure 6- 31. CPU Interface Filtering Rule Table window

Click the **Add Rule** button to continue on to the **CPU Interface Filtering Rule Table** window. A new and unique window, for Ethernet, IP, Packet Content and IPv6 will open as shown in the examples below.

To change a rule for a previously created CPU Access Profile Rule:

The **CPU Interface Filtering Rule Configuration** window allows the user to create a rule for a previously created CPU Access Profile.



CPU Interface Filtering Rule Configuration

Profile ID	1
Mode	● Permit ○ Deny
Access ID (1-100)	1
Type	Ethernet
VLAN Name	
Source MAC	00-00-00-00-00-00
Destination MAC	00-00-00-00-00-00
Ethernet Type	0000
Port	
Time Range	Range Name □

Show All CPU Interface Filtering Rule Entries

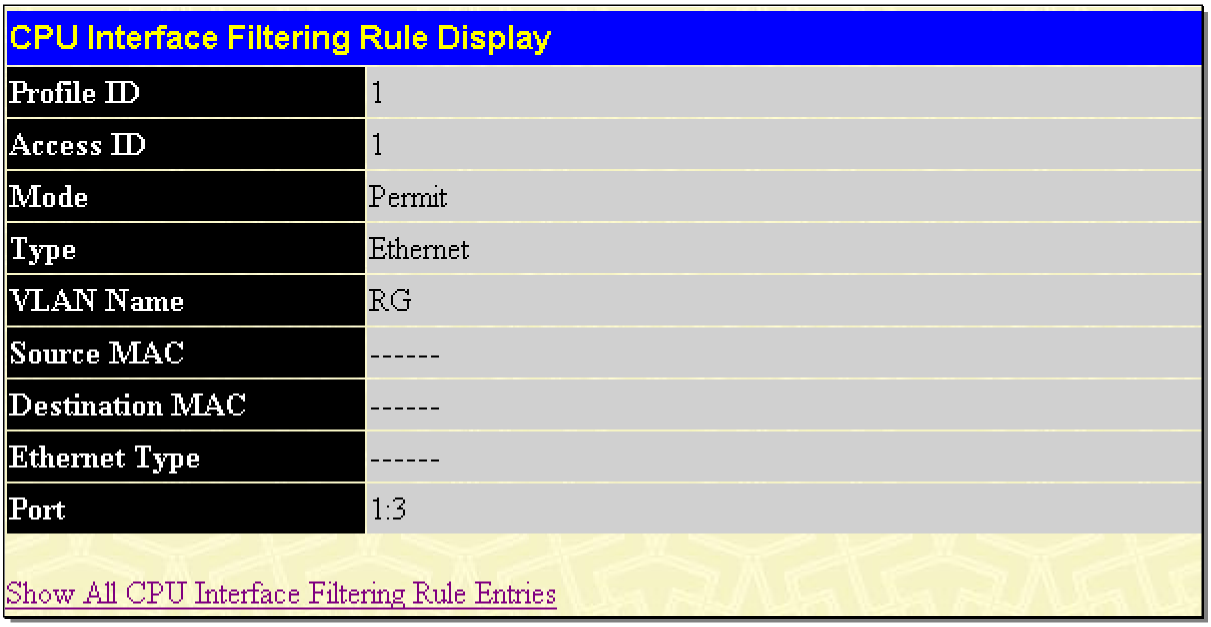
Figure 6- 32. CPU Interface Filtering Rule Configuration window (Ethernet)

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 do not 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 to 100*.
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 part of 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.
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 0-9.
Port	The CPU Access Rule may be configured on a per-port basis by entering the port number of the Switch.

Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this CPU access rule will be implemented on the Switch.

To view the settings of a previously configured rule, click View in the **CPU Interface Filtering Rule Table** to view the following window:



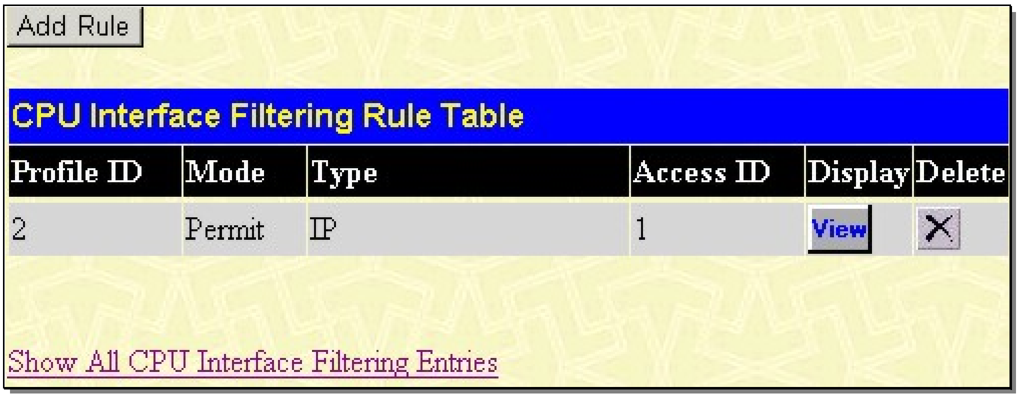
CPU Interface Filtering Rule Display

Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
VLAN Name	RG
Source MAC	------
Destination MAC	------
Ethernet Type	------
Port	1:3

Show All CPU Interface Filtering Rule Entries

Figure 6- 33. CPU Interface Filtering Rule Display window (Ethernet)

The following window is the **CPU Interface Filtering Rule Table** for IP.



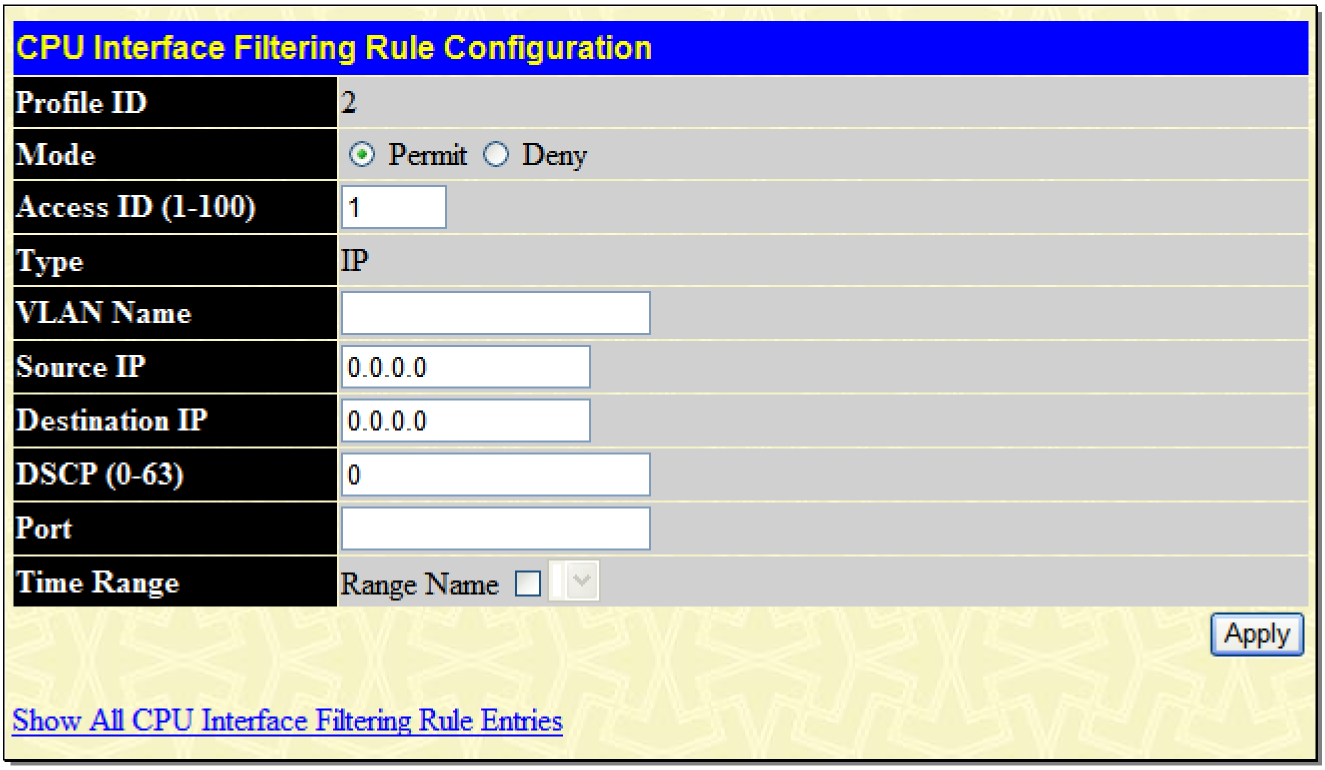
CPU Interface Filtering Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	IP	1	View	☒

Show All CPU Interface Filtering Entries

Figure 6- 34. CPU Interface Filtering Rule Table window (IP)

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. The following window is used for the CPU IP Rule configuration.



CPU Interface Filtering Rule Configuration

Profile ID	2
Mode	● Permit ○ Deny
Access ID (1-100)	1
Type	IP
VLAN Name	
Source IP	0.0.0.0
Destination IP	0.0.0.0
DSCP (0-63)	0
Port	
Time Range	Range Name □

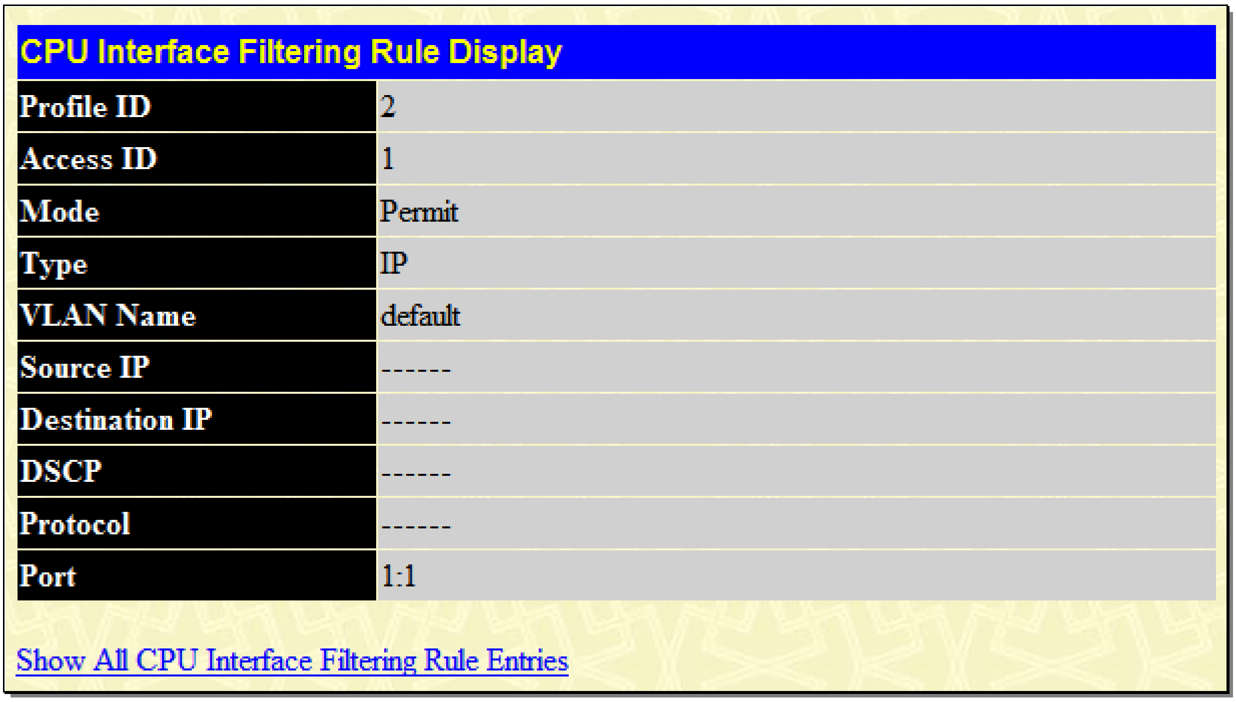
Figure 6- 35. CPU Interface Filtering Rule Configuration window (IP)

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 do not 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* to *100*.
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 part of 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*.
Port	The CPU Access Rule may be configured on a per-port basis by entering the port number of the Switch.
Time Range	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this CPU

	access rule will be implemented on the Switch.

To view the settings of a previously correctly configured rule, click View in the **CPU Interface Filtering Rule Table** to view the following window:



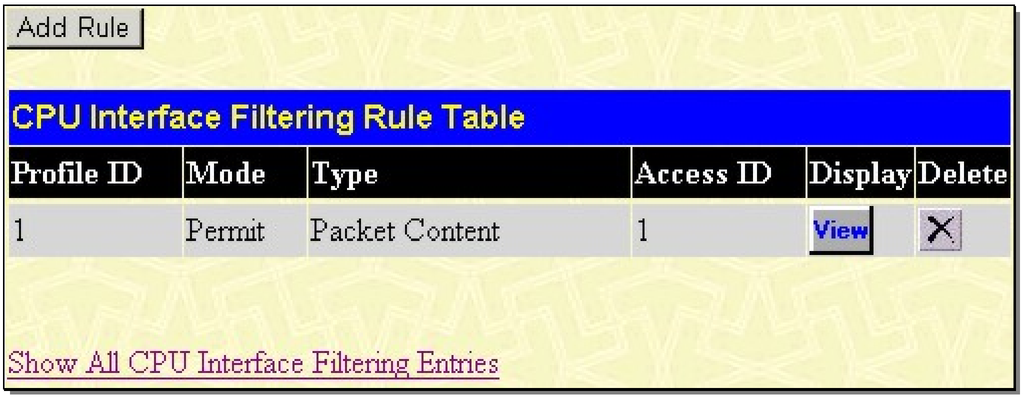
CPU Interface Filtering Rule Display

Profile ID	2
Access ID	1
Mode	Permit
Type	IP
VLAN Name	default
Source IP	------
Destination IP	------
DSCP	------
Protocol	------
Port	1:1

Show All CPU Interface Filtering Rule Entries

Figure 6- 36. CPU Interface Filtering Rule Display window (IP)

The following window is the CPU Interface Filtering Rule Table for Packet Content.



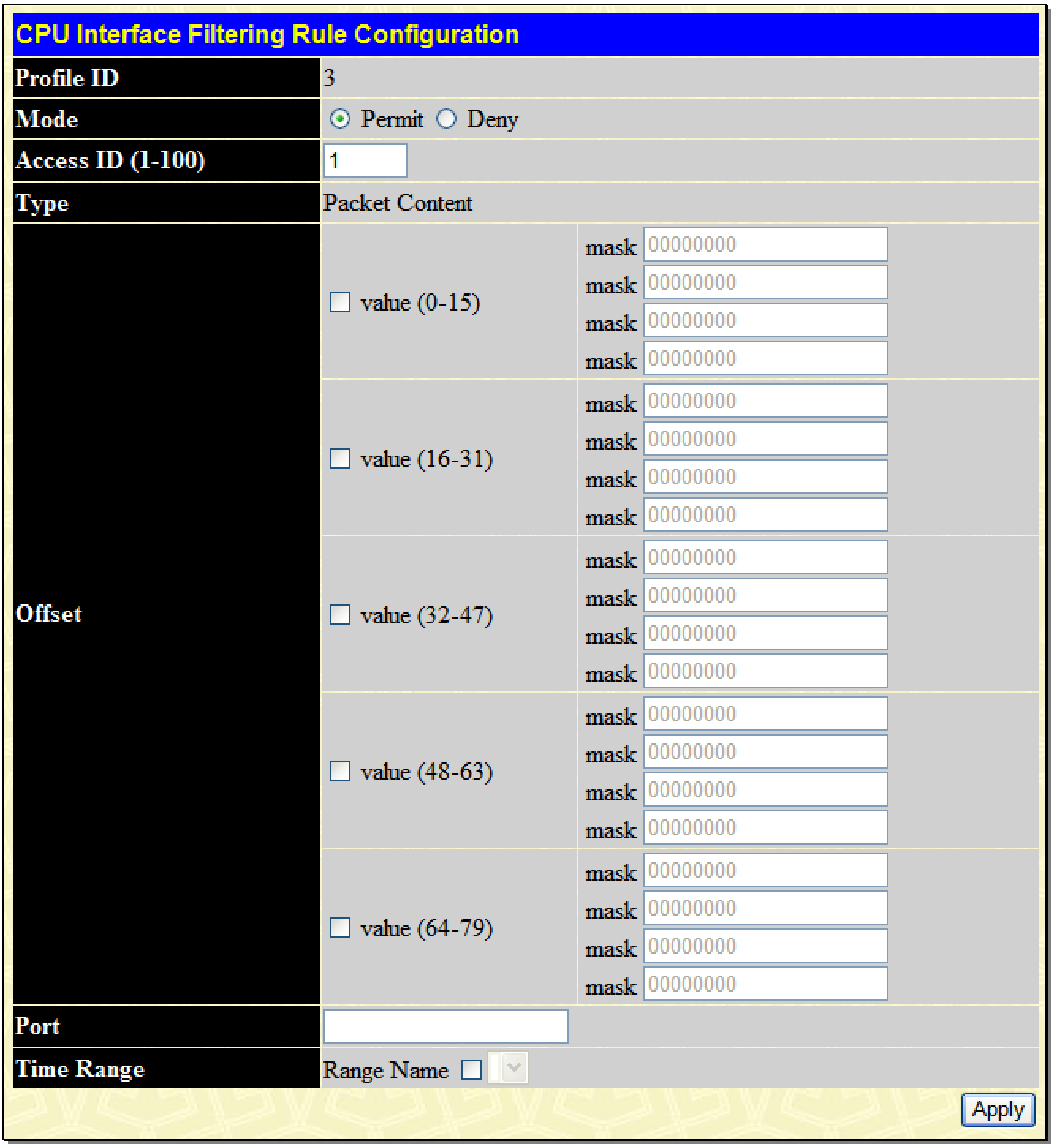
CPU Interface Filtering Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Packet Content	1	View	☒

Show All CPU Interface Filtering Entries

Figure 6- 37. CPU Interface Filtering Rule Table window (Packet Content)

To remove a previously created rule, select it and click the ☒ button. To add a new CPU Access Rule, click the **Add Rule** button:



CPU Interface Filtering Rule Configuration

Profile ID	3
Mode	● Permit ○ Deny
Access ID (1-100)	1
Type	Packet Content
Offset	□ value (0-15) mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (16-31) mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (32-47) mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (48-63) mask 00000000 mask 00000000 mask 00000000 mask 00000000
	□ value (64-79) mask 00000000 mask 00000000 mask 00000000 mask 00000000
Port	
Time Range	Range Name □

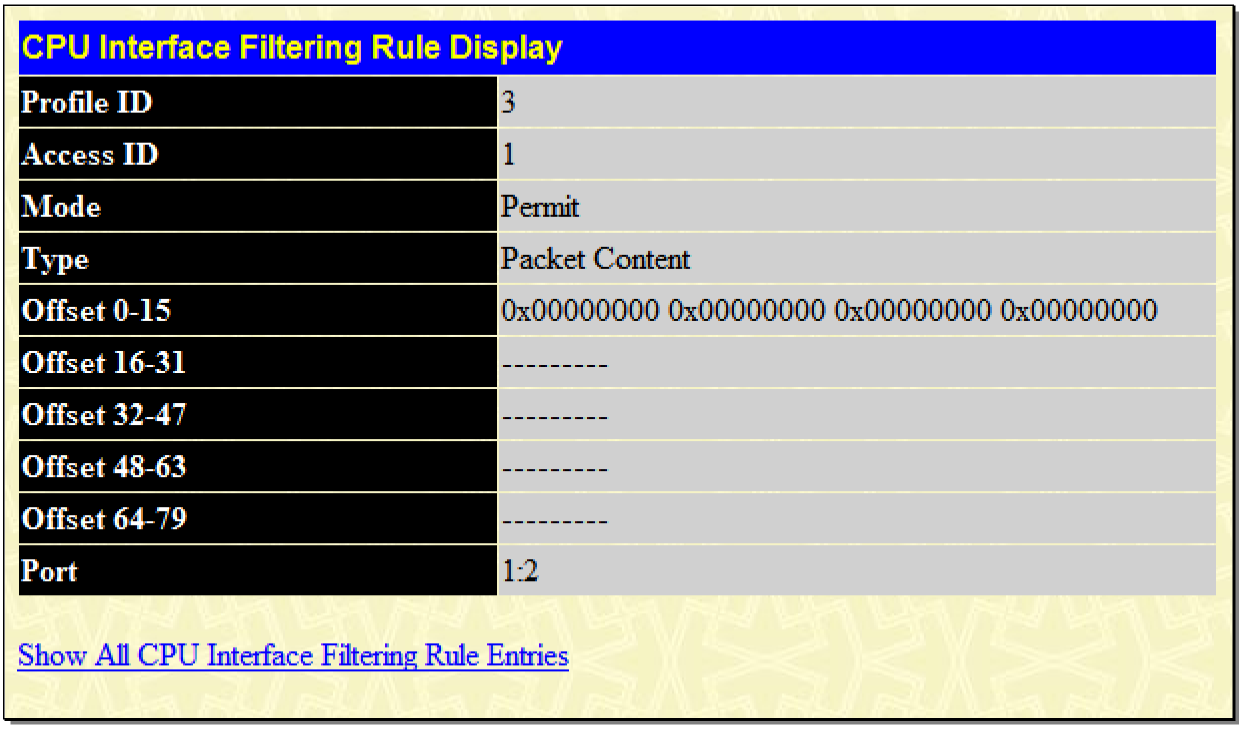
Figure 6- 38. CPU Interface Filtering Rule Configuration window (Packet Content Mask)

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 packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
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 part 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.
Port	The CPU Access Rule may be configured on a per-port basis by entering the port number of the Switch.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this CPU access rule will be implemented on the Switch.

To view the settings of a previously correctly configured rule, click View in the **CPU Interface Filtering Rule Table** to view the following window:

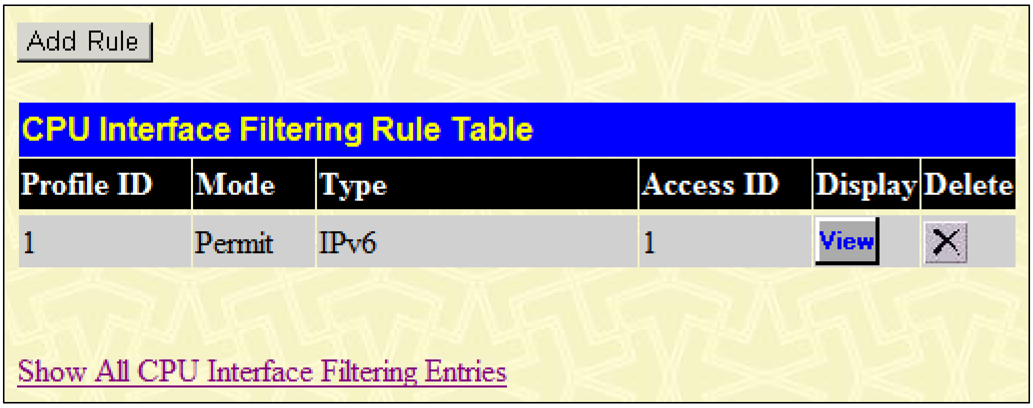


CPU Interface Filtering Rule Display

Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	---------
Offset 32-47	---------
Offset 48-63	---------
Offset 64-79	---------
Port	1:2

Figure 6- 39. CPU Interface Filtering Rule Display window (Packet Content)

The following window is the **CPU Interface Filtering Rule Table** for IPv6.



Add Rule

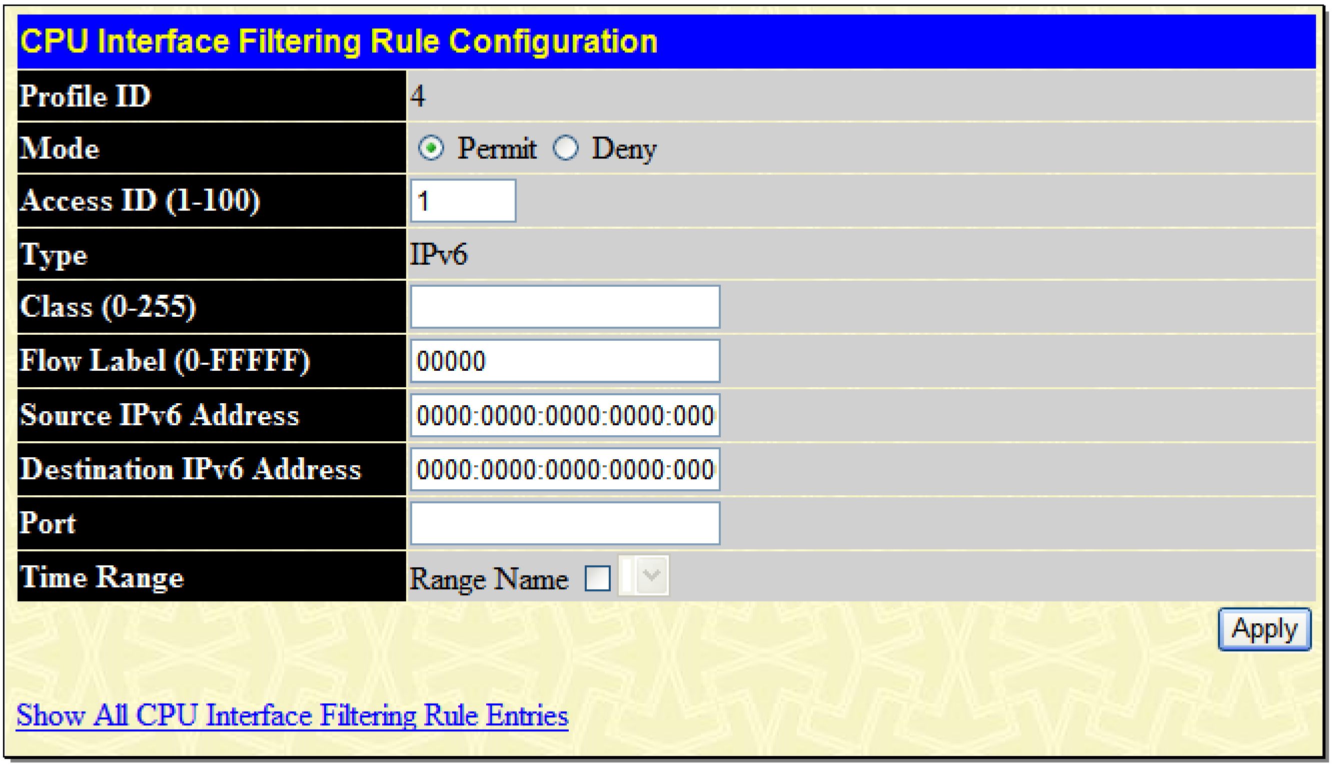
CPU Interface Filtering Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	IPv6	1	View	☒

Show All CPU Interface Filtering Entries

Figure 6- 40. CPU Interface Filtering Rule Table window (IPv6)

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. The following window is used for the CPU IP Rule configuration.



CPU Interface Filtering Rule Configuration

Profile ID	4
Mode	● Permit ○ Deny
Access ID (1-100)	1
Type	IPv6
Class (0-255)	
Flow Label (0-FFFFF)	00000
Source IPv6 Address	0000:0000:0000:0000:000
Destination IPv6 Address	0000:0000:0000:0000:000
Port	
Time Range	Range Name □

Apply

Show All CPU Interface Filtering Rule Entries

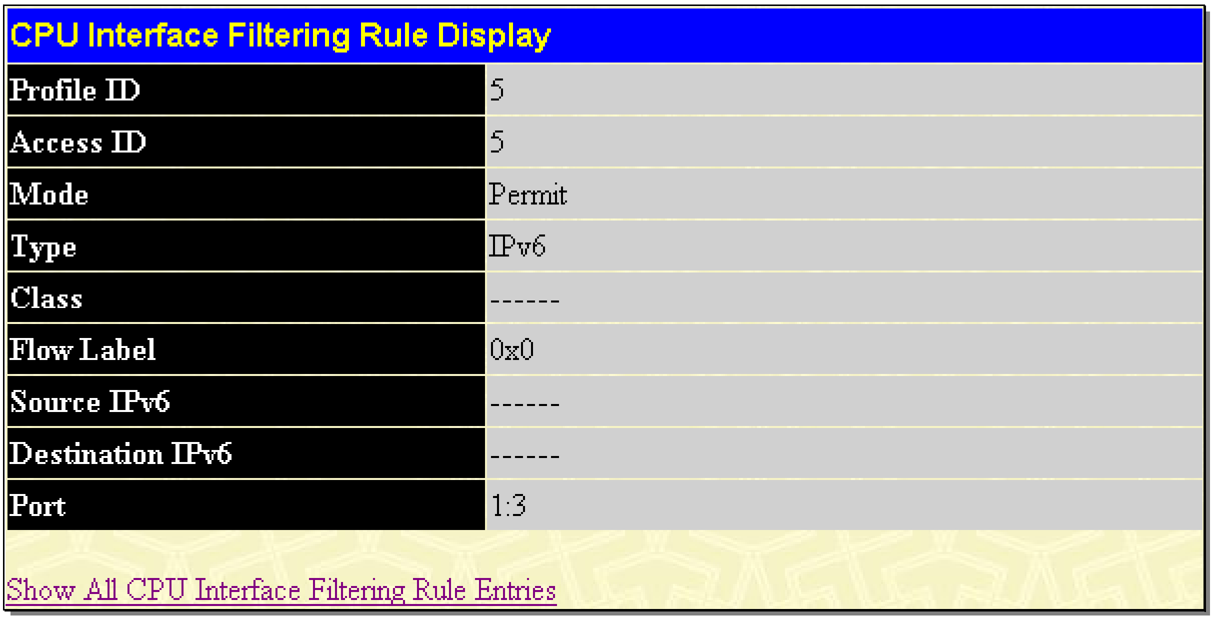
Figure 6- 41. CPU Interface Filtering Rule Configuration window (IPv6)

The following parameters may be viewed or modified:

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 (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content 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 part of each packet header.
Class (0-255)	Entering a value between *0* and *255* 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 of IPv4.
Flow Label (0-FFFFF)	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.
Port	The CPU Access Rule may be configured on a per-port basis by entering the port number of the Switch.
Time Range	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this CPU access rule will be implemented on the Switch.

To view the settings of a previously correctly configured rule, click View in the **CPU Interface Filtering Rule Table** to view the following window:



CPU Interface Filtering Rule Display

Profile ID	5
Access ID	5
Mode	Permit
Type	IPv6
Class	------
Flow Label	0x0
Source IPv6	------
Destination IPv6	------
Port	1:3

Show All CPU Interface Filtering Rule Entries

Figure 6- 42. CPU Interface Filtering Rule Display window (IPv6)

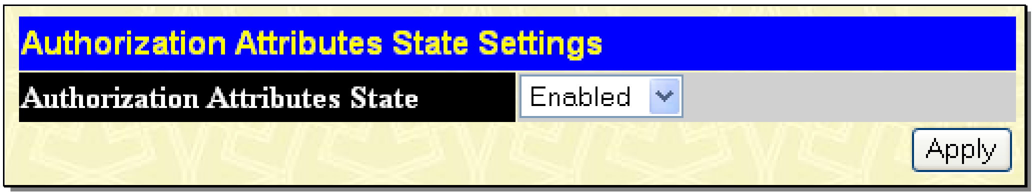
Section 7

Security

Authorization Attributes State Settings

This window allows the user to enable or disable the authorization attributes state.

To view this window, click **Security > Authorization Attributes State Settings**, as shown below:



Authorization Attributes State Settings

Authorization Attributes State: Enabled

Figure 7- 1. Authorization Attributes State Settings window

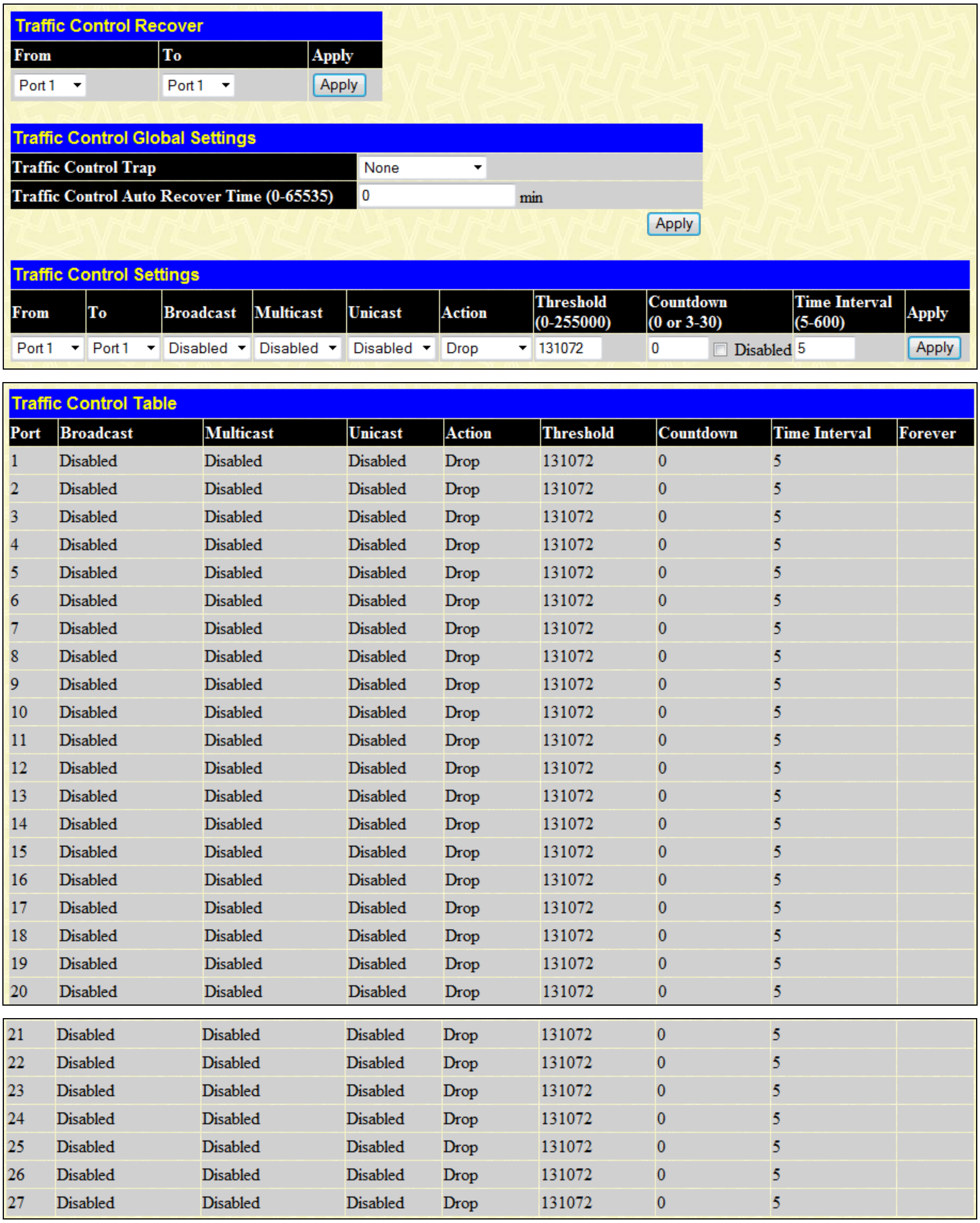
Traffic Control

On a computer network, packets such as multicast packets and broadcast packets continually flood the network as normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the *Drop* option of the Action field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field.

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



Traffic Control Recover

From	To	Apply
Port 1	Port 1	Apply

Traffic Control Global Settings

Traffic Control Trap	None
Traffic Control Auto Recover Time (0-65535)	0 min

Apply

Traffic Control Settings

From	To	Broadcast	Multicast	Unicast	Action	Threshold (0-255000)	Countdown (0 or 3-30)	Time Interval (5-600)	Apply
Port 1	Port 1	Disabled	Disabled	Disabled	Drop	131072	0 □ Disabled	5	Apply

Traffic Control Table

Port	Broadcast	Multicast	Unicast	Action	Threshold	Countdown	Time Interval	Forever
1	Disabled	Disabled	Disabled	Drop	131072	0	5	
2	Disabled	Disabled	Disabled	Drop	131072	0	5	
3	Disabled	Disabled	Disabled	Drop	131072	0	5	
4	Disabled	Disabled	Disabled	Drop	131072	0	5	
5	Disabled	Disabled	Disabled	Drop	131072	0	5	
6	Disabled	Disabled	Disabled	Drop	131072	0	5	
7	Disabled	Disabled	Disabled	Drop	131072	0	5	
8	Disabled	Disabled	Disabled	Drop	131072	0	5	
9	Disabled	Disabled	Disabled	Drop	131072	0	5	
10	Disabled	Disabled	Disabled	Drop	131072	0	5	
11	Disabled	Disabled	Disabled	Drop	131072	0	5	
12	Disabled	Disabled	Disabled	Drop	131072	0	5	
13	Disabled	Disabled	Disabled	Drop	131072	0	5	
14	Disabled	Disabled	Disabled	Drop	131072	0	5	
15	Disabled	Disabled	Disabled	Drop	131072	0	5	
16	Disabled	Disabled	Disabled	Drop	131072	0	5	
17	Disabled	Disabled	Disabled	Drop	131072	0	5	
18	Disabled	Disabled	Disabled	Drop	131072	0	5	
19	Disabled	Disabled	Disabled	Drop	131072	0	5	
20	Disabled	Disabled	Disabled	Drop	131072	0	5	
21	Disabled	Disabled	Disabled	Drop	131072	0	5	
22	Disabled	Disabled	Disabled	Drop	131072	0	5	
23	Disabled	Disabled	Disabled	Drop	131072	0	5	
24	Disabled	Disabled	Disabled	Drop	131072	0	5	
25	Disabled	Disabled	Disabled	Drop	131072	0	5	
26	Disabled	Disabled	Disabled	Drop	131072	0	5	
27	Disabled	Disabled	Disabled	Drop	131072	0	5	

Figure 7- 2. Traffic Control Recover Settings window

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.

The user may set the following parameters:

Parameter	Description
Traffic Control Recover Settings	

Unit	Select the switch to configure.
From/To	Select the ports to be recovered.
Traffic Control Global Settings	
Traffic Control Trap	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: *None* – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. *Storm Occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. *Storm Cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. *Both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. This function cannot be implemented in the Hardware mode. (When Drop is chosen in the Action field.
Traffic Control Auto Recover Time (0-65535)	Enter the time allowed for auto recovery from shutdown for a port. The default value is *0*, which means no auto recovery is possible and the port remains in shutdown forever mode. This requires manual entry of the CLI command “config ports [<portlist> | all] state enable" to return the port to a forwarding state.
Traffic Control Settings	
Unit	Select the unit you wish to configure.
From/To	Select the ports of this Switch to configure for Storm Control.
Broadcast	Enables or disable Broadcast Storm Control.
Multicast	Enables or disables Multicast Storm Control.
Unicast	Enables or disables Unicast Storm control.
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 Storm Control Recover setting at the top of this window. 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.
Threshold (0-255000)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The Threshold can be set from *0* to *255000* with a default setting of *131072*.
Count Down (0 or 3-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. 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*, *3* to *30* minutes. *0* is the default setting for this field and *0* will denote that the port will never shutdown. To disable the count down option, tick the **Disabled** option.
Time Interval (5-600)	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 *600* seconds with the default setting of *5* seconds.

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 until the user recovers these ports.

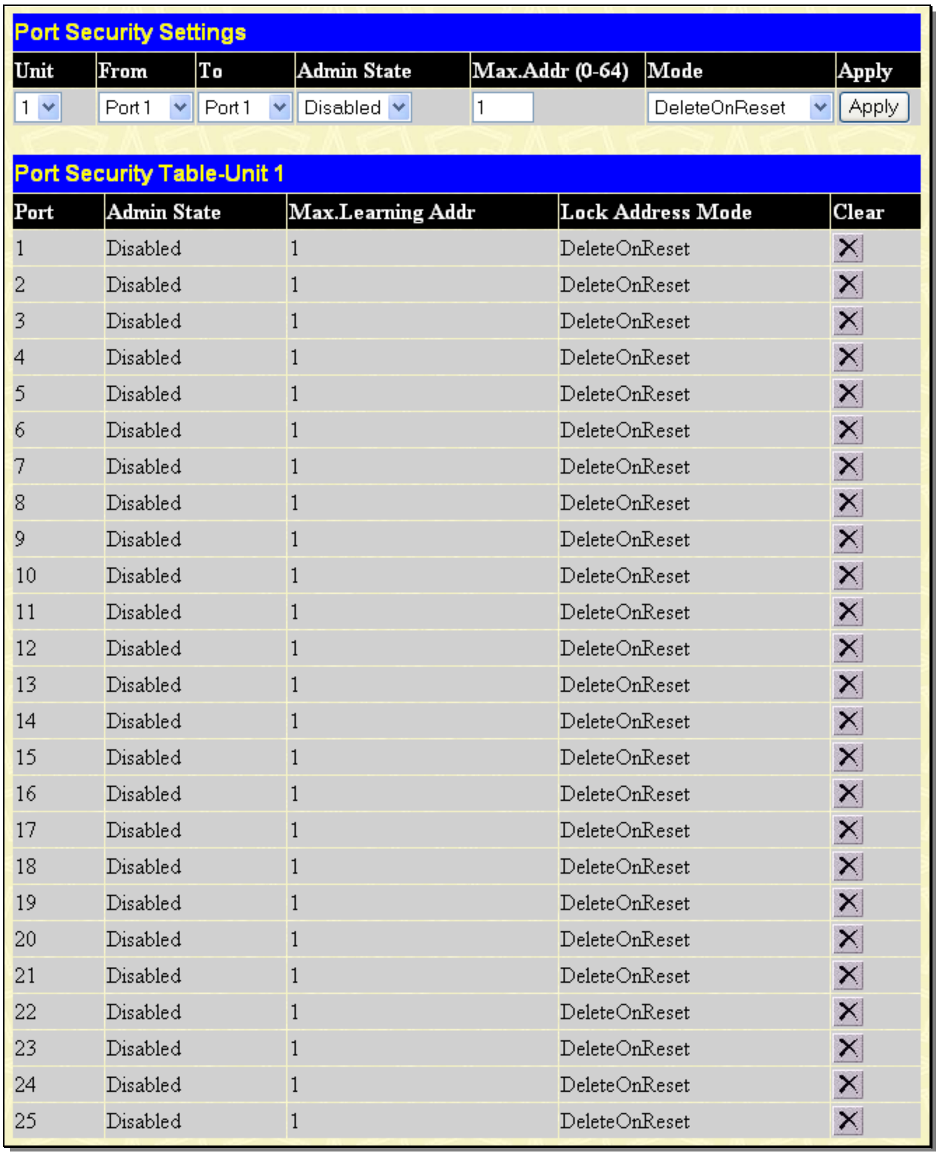
Port Security

Port Security Settings

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

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

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



Port Security Settings

Unit	From	To	Admin State	Max.Addr (0-64)	Mode	Apply
1	Port 1	Port 1	Disabled	1	DeleteOnReset	Apply

Port Security Table-Unit 1

Port	Admin State	Max.Learning Addr	Lock Address Mode	Clear
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	☒

Figure 7- 3. Port Security Settings window

The following parameters can be set:

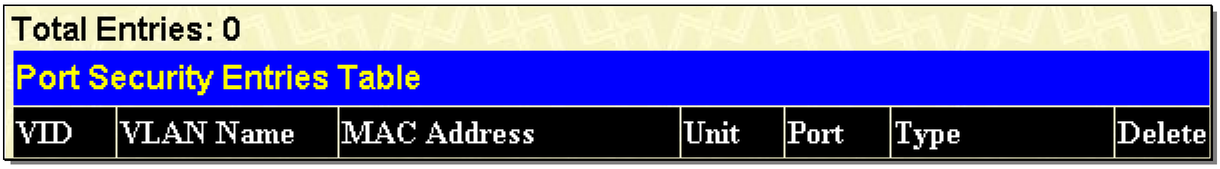
Parameter	Description
Unit	Select the unit to configure.
From/To	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows users to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Addr. (0-64)	The number 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. *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

Port Security Entries

This 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 Security** > **Port Security Entries**, as shown below:



Total Entries: 0

Port Security Entries Table

VID	VLAN Name	MAC Address	Unit	Port	Type	Delete

Figure 7- 4. Port Security Entries Table window

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 on reset. 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. Only entries marked *Secured_Permanent* can 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.
Unit	Enter the unit to configure.
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* and *Del_On_Reset* can be deleted.
Delete	Click the ☒ in this field to delete the corresponding MAC address that was either deleted on reset or permanently learned by the Switch.

IP-MAC-Port Binding

General Overview

The Switch features IP-MAC-Port Binding (IMPB), a D-Link security application used most often on edge switches directly connected to network hosts. IMPB is also an integral part of D-Link's End-to-End Security Solution (E2ES). The primary purpose of IP-MAC-Port Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch. Specifically, IMPB binds together the four-byte IP address and the six-byte Ethernet link layer MAC address to allow the transmission of data between the layers.

The IMPB function is port-based, meaning that a user can enable or disable the function on any individual port. Once IMPB is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the "IMPB white list". If an unauthorized user tries to access an IMPB-enabled port, the system will block access by dropping its packet. The creation of the IMPB white list can be manually configured by CLI or Web.

Common IP Management Security Issues

Currently, certain limitations and issues in IP management structures can lead to serious security problems. Auditing mechanisms, such as syslog, application log, firewall log, etc, are mainly based on client IP information. However, such log information is meaningless if the client IP address can be easily changed. IP conflict, the most common problem in today's networks, is another major security concern. Without IMPB, any user can change an IP address manually and cause conflict with other resources, such as other PCs, core switches, routers or servers. Not only does this duplicate IP create an auditing issue, it also poses potential risk to the entire network.

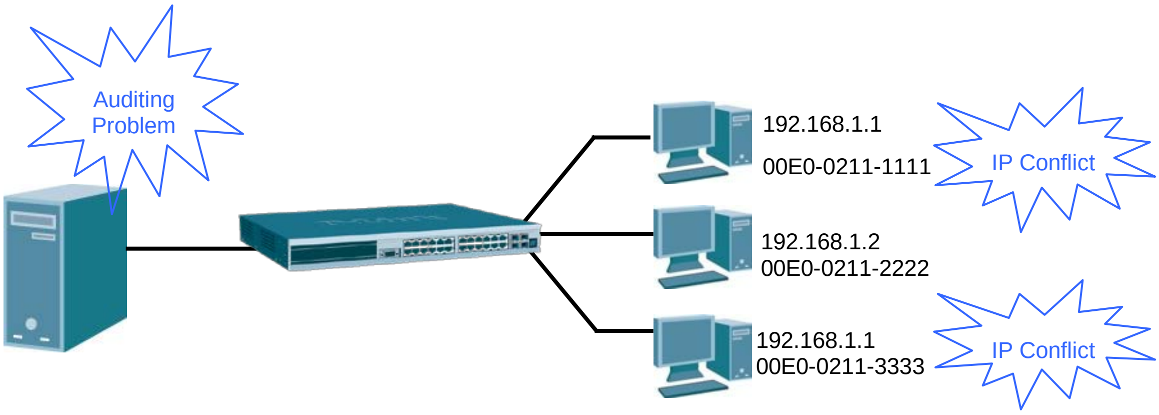


Figure 7- 5. Common IP Management IP Security Issues

ARP spoofing attacks in which malicious users intercept traffic or interrupt connections by manipulating ARP packets are another serious challenge in securing today's network. Further information on how ARP spoofing attacks work can be found in the Appendix, "Mitigating ARP Spoofing Attack via Packet Content ACL," located in the back of this manual.

Solutions to Improve IP Management Security

D-Link has introduced IMPB technology to protect networks from attacks. By using IP-MAC-Port Binding, all packets are dropped by a switch when the combination of MAC address, IP address, and connected port is not in the IMPB white list. IMPB allows the user to choose either ARP or ACL mode. In addition, an IMPB white list can be dynamically created with the DHCP snooping option. DHCP snooping is a global setting and can be enabled on top of ACL or ARP mode. Each option has its advantages and disadvantages.

ARP Mode

In ARP Mode, a switch performs ARP Packet Inspection in which it checks the IP-MAC pairs in ARP packets with the IMPB white list and denies unauthorized ones. An advantage of ARP mode is that it does not consume any ACL rules on the Switch. Nonetheless, since the switch only checks ARP packets, it cannot block unauthorized clients who do not send out ARP packets.

ACL Mode

In ACL Mode, a switch performs IP Packet Inspection in addition to ARP Packet Inspection. Essentially, ACL rules will be used to permit statically configured IMPB entries and deny other IP packets with the incorrect IP-MAC pairs. The distinct advantage of ACL Mode is that it ensures better security by checking both ARP Packets and IP Packets. However, doing so requires the use of ACL rules. ACL Mode can be viewed as an enhanced version of ARP Mode because ARP Mode is enabled by default when ACL Mode is selected.

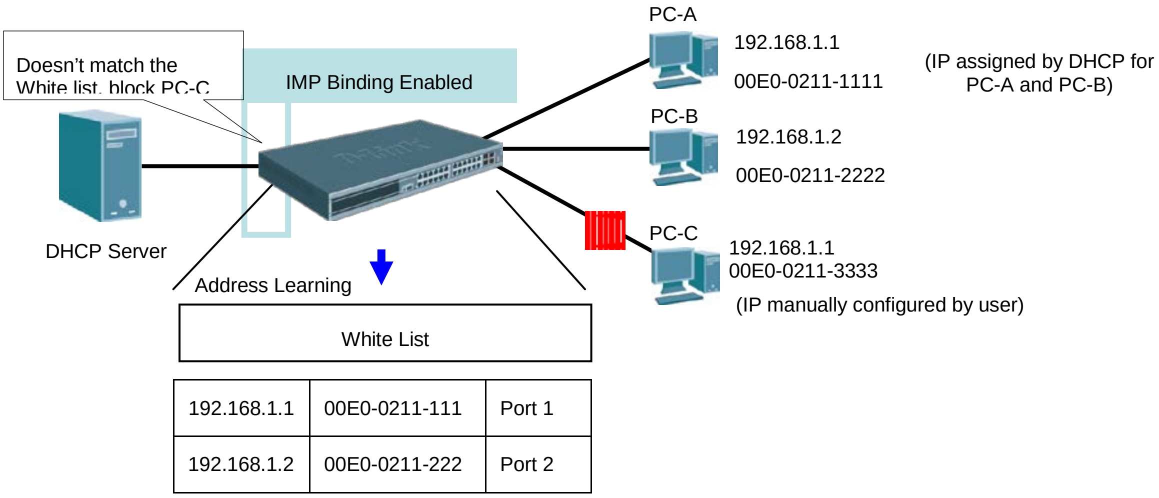
Strict and Loose State

Other than ACL and ARP mode, users can also configure the state on a port for granular control. There are two states: Strict and Loose, and only one state can be selected per port. If a port is set to Strict state, all packets entering the port are denied (dropped) by default. The switch will continuously compare all IP and ARP packets it receives on that port with its IMPB entries. If the IP-MAC pair in the packet matches the IMPB entry, the MAC address will be unblocked and subsequent packets sent from this client will be forwarded. On the other hand, if a port is set to Loose state, all packets entering the port are permitted (forwarded) by default. The switch will continuously compare all ARP packets it receives on that port with its IMPB entries. If the IP-MAC pair in the ARP packet does not match the IMPB white list, the MAC address will be blocked and subsequent packets sent from this client will be dropped.

DHCP Snooping Option

If DHCP snooping is enabled, the switch learns IP-MAC pairs by snooping DHCP packets automatically and then saves them to the IP-MAC-Port Binding white list. This enables a hassle-free configuration because the administrator does not need to manually enter each IMPB entry. A prerequisite for this is that the valid DHCP server's IP-MAC pair must be configured on the switch's IMPB while list first; otherwise the DHCP server packets will be dropped. DHCP snooping is generally considered to be more secure because it enforces all clients to acquire IP through the DHCP server. Additionally, it makes IP information auditable because clients cannot manually configure their own IP address.

An example of DHCP snooping in which PC-A and PC-B get their IP addresses from a DHCP server is depicted below. The switch snoops the DHCP conversation between PC-A, PC-B, and the DHCP server. The IP address, MAC address, and connecting ports of both PC-A and PC-B are learned and stored in the switch's IMPB white list. Therefore, these PCs will be able to connect to the network. Then there is PC-C, whose IP address is manually configured by the user. Since this PC's IP-MAC pair does not match the one on the Switch's IMPB white list, traffic from PC-C will be blocked.



192.168.1.1	00E0-0211-111	Port 1
192.168.1.2	00E0-0211-222	Port 2

Figure 7- 6. DHCP Snooping Example

ARP Inspection

ARP spoofing can attack hosts, switches, and routers connected to a Layer 2 network by "poisoning" their ARP caches. As the figure below shows, Host C can "poison" the ARP caches of Host B by broadcasting forged ARP responses with bindings (IP B, MAC C). As a result, Host C intercepts the traffic sent to Host B. IMPB was developed to prevent this kind of ARP spoofing (including Netcut and Netcut restore attacks).

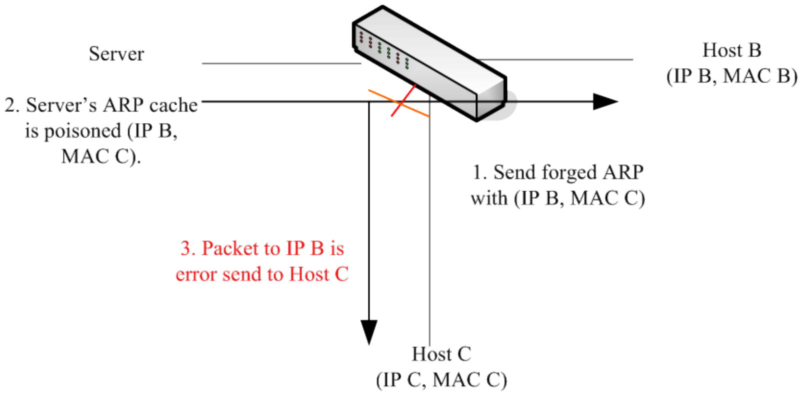

Server
2. Server's ARP cache is poisoned (IP B, MAC C).
Host B (IP B, MAC B)
1. Send forged ARP with (IP B, MAC C)
3. Packet to IP B is error send to Host C
Host C (IP C, MAC C)

Figure 7- 7. ARP Cache Poisoning

When the user configures strict mode and enables IMPB on a port, ARP inspection is enabled. For an ARP inspection active port: All ARP packets should be captured to the CPU (including broadcast ARP and unicast ARP packets) and the CPU will make the decision to either forward or drop.

The switch will validate the ARP packets by retrieving the sender's MAC/ IP address from the ARP packet payload and sender hardware address. If the IP/ MAC address are in the IMPB forwarding list, the ARP packets will be forwarded. Otherwise, the ARP packet will be discarded.

Strict State Behavior Change

As the figure below shows, in a mixed network (both IPv4 and IPv6 used), if illegal IPv4-A packets are detected and there are write-blocked FDB entries, then IPv6-Global also cannot access the network. To avoid this case, do not write-block FDB. Not write-blocking FDB can also avoid netcut attacks and recover attacks.

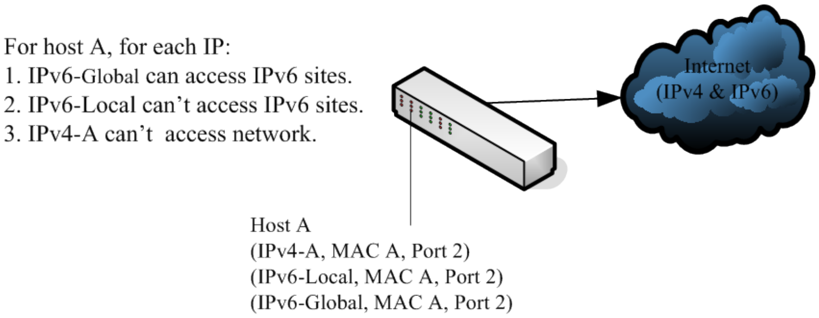

For host A, for each IP:
1. IPv6-Global can access IPv6 sites.
2. IPv6-Local can't access IPv6 sites.
3. IPv4-A can't access network.
Internet (IPv4 & IPv6)
Host A
(IPv4-A, MAC A, Port 2)
(IPv6-Local, MAC A, Port 2)
(IPv6-Global, MAC A, Port 2)

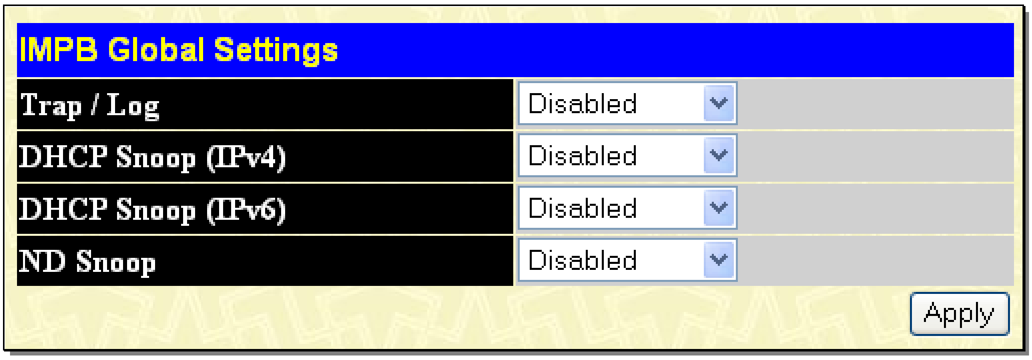
Figure 7- 8. IPv4 and IPv6 Sharing

When enabling Strict state, the Switch will stop writing dropped FDB entries on these ports. If the Switch detects legal packets, the Switch will need to create the FDB forwarding entries. ACL mode always runs under Strict state. When a user enables ACL mode on some ports, these ports will change from Loose state to Strict state and the configuration will also change to Strict state. For compound authentication And mode (IMPB+1X, IMPB+WAC, IMPB+JWAC), the ports always run in Strict state.

IMPB Global Settings

This window is used to enable or disable IP-MAC-port binding global settings.

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



IMPB Global Settings

Trap / Log: Disabled

DHCP Snoop (IPv4): Disabled

DHCP Snoop (IPv6): Disabled

ND Snoop: Disabled

Figure 7- 9. IMPB Global Settings window

The following parameters can be set:

Parameter	Description
Trap / Log	This field will enable and disable the sending of trap log messages for IP-MAC binding. When *Enabled*, the Switch will send a trap log message to the SNMP agent and the Switch log when address binding module detects illegal IP and MAC addresses.
DHCP Snoop (IPv4)	Use the pull-down menu to enable or disable the DHCP snooping state (IPv4) for IP-MAC-port binding.
DHCP Snoop (IPv6)	Use the pull-down menu to enable or disable the DHCP snooping state (IPv6) for IP-MAC-port binding.
ND Snoop	Use the pull-down menu to enable or disable the ND snooping state for IP-MAC-port binding.

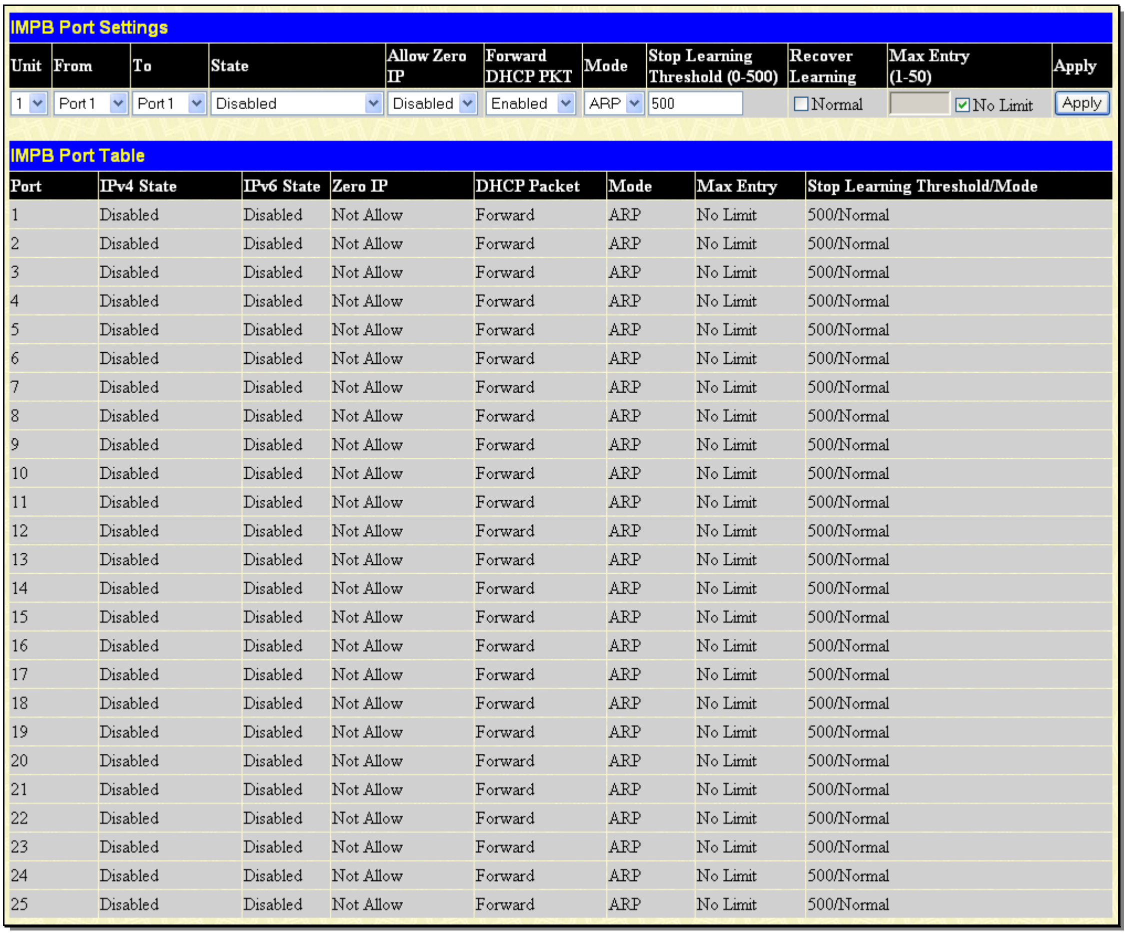
Click **Apply** to implement the settings made.

IMPB Port Settings

This window is used to configure IMP settings on a port basis.

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with Strict or Loose State, enable or disable Allow Zero IP and Forward DHCP Packet fields, and configure the port's Max IMPB entry.

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



IMPB Port Settings

Unit	From	To	State	Allow Zero IP	Forward DHCP PKT	Mode	Stop Learning Threshold (0-500)	Recover Learning	Max Entry (1-50)		Apply
1	Port 1	Port 1	Disabled	Disabled	Enabled	ARP	500	□Normal		☑No Limit	Apply

IMPB Port Table

Port	IPv4 State	IPv6 State	Zero IP	DHCP Packet	Mode	Max Entry	Stop Learning Threshold/Mode
1	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
2	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
3	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
4	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
5	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
6	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
7	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
8	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
9	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
10	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
11	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
12	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
13	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
14	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
15	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
16	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
17	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
18	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
19	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
20	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
21	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
22	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
23	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
24	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
25	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal

Figure 7- 10. IMPB Port Settings window

The following fields can be set or modified:

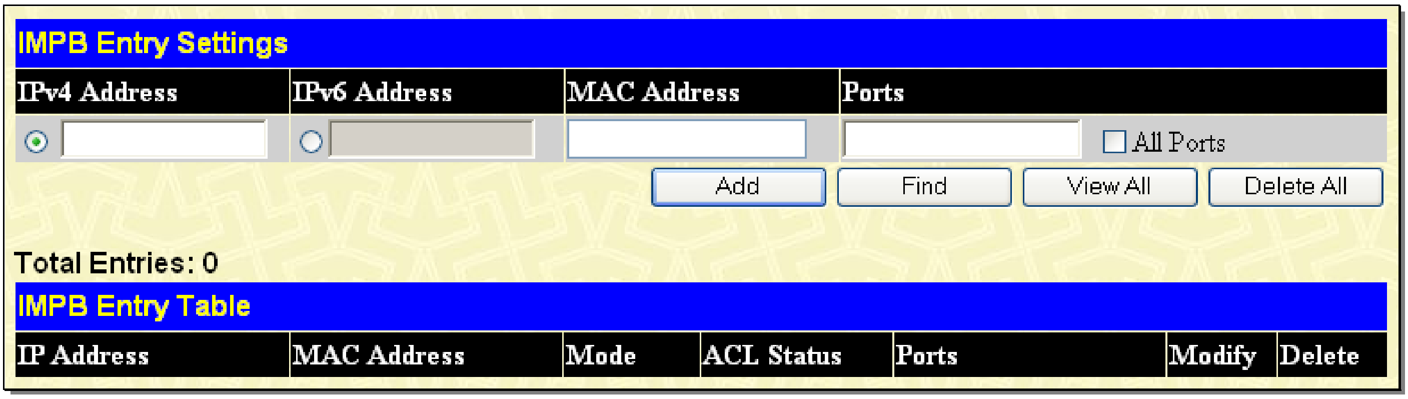
Parameter	**Description**
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From/To	Select a port or range of ports to set for IP-MAC-port binding.
State	Use the pull-down menu to enable or disable these ports for IP-MAC-port binding. The choices are: *Enabled (Strict)* – This state provides a stricter method of control. If the user selects this mode, all packets are blocked by the Switch by default. The Switch will compare all incoming ARP and IP Packets and attempt to match them against the IMPB white list. If the IP-MAC pair matches the white list entry, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the Strict state uses more CPU resources from checking every incoming ARP and IP packet, it enforces better security and is thus the recommended setting. *Enabled (Loose)* – This mode provides a looser way of control. If the user selects loose mode, the Switch will forward all packets by default. However, it will still inspect incoming ARP packets and compare them with the Switch's IMPB white list entries. If the IP-MAC pair of a packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources because the Switch only checks incoming ARP packets. However, it also means that Loose state cannot block users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets. *Enabled (IPv6)* - Enable the IPv6 packet checking. All packets are dropped by default until a legal IP packet is detected. *Enabled (All)* – Enable both IPv6 and IPv4 packet checking. All packets are dropped by default

	until a legal IP packet is detected. *Enabled (Strict+IPv6)* - Enable the IPv6 packet checking in strict mode. All packets are dropped by default until a legal IP packet is detected. *Enabled (Strict+All)* - Enable both IPv6 and IPv4 packet checking in strict mode. All packets are dropped by default until a legal IP packet is detected. *Enabled (Loose+IPv6)* - Enable IPv6 packet checking. All packets are dropped by default until a legal IP packet is detected. *Enabled (Loose+All)* - Enable both IPv6 and IPv4 packet checking. All packets are dropped by default until a legal IP packet is detected. *Disabled* - Disable the IPv4 packet checking. *Disabled (IPv6)* - Disable the IPv6 packet checking. *Disabled (All)* - Disable both IPv4 and IPv6 packet checking.
Allow Zero IP	Use the pull-down menu to enable or disable this feature. Once *Enabled*, the Switch will allow ARP packets with a Source IP of 0.0.0.0 to pass through. This is useful in some scenarios when a client (for example, a wireless Access Point) sends out an ARP request packet before accepting the IP address from a DHCP server. In this case, the ARP request packet sent out from the client will contain a Source IP of 0.0.0.0. The Switch will need to allow such packets to pass, or else the client cannot know if there is another duplicate IP address in the network.
Forward DHCP PKT	By default, the Switch will forward all DHCP packets. However, if the port state is set to Strict, all DHCP packets will be dropped. In that case, select *Enabled* so that the port will forward DHCP packets even under Strict state. Enabling this feature also ensures that DHCP snooping works properly.
Mode	*ARP* – ARP mode is the default mode that applies to IMPB enabled ports. In ARP mode, if the Switch identifies the host is legal, the host's MAC will be programed to *L2 FDB with allowed*; otherwise the host's MAC will be programmed to *L2 FDB with drop*. ARP mode for security access control is based on Layer 2 MAC address. *ACL* – ACL mode provides strict security for IP level traffic. If ACL mode is enabled, the static configured IMPB entries with ACL mode will be applied to hardware ACL table. If the ACL mode is disabled, the ACL entries will be removed from the hardware ACL table.
Stop Learning Threshold (0-500)	Whenever a MAC address is blocked by the Switch, it will be recorded in the Switch's L2 Forwarding Database (FDB) and associated with a particular port. To prevent the Switch FDB from overloading in case of an ARP DoS attack, the administrator can configure the threshold when a port should stop learning illegal MAC addresses. Enter a Stop Learning threshold between *0* and *500*. Entering 500 means the port will enter the Stop Learning state after 500 illegal MAC entries and will not allow additional MAC entries, both legal or illegal, to be learned on this port. In the Stop Learning state, the port will also automatically purge all blocked MAC entries on this port. Traffic from legal MAC entries are still forwarded. Entering *0* means no limit has been set and the port will keep learning illegal MAC addresses.
Recover Learning	Use the Normal check box to recover learning. This feature can only be applied when a port is already in the Stop Learning state. Tick to recover the port back to normal state, under which the port will start learning both illegal and legal MAC addresses again.
Max Entry (1-50)	Enter the maximum number of IP-MAC-port binding dynamic entries. By default, the per port maximum dynamic entry is "No Limit." The maximum dynamic entry threshold is from *1* to *50*. Tick the No Limit check box to allow no limit. This setting is only for DHCP snooping for IPv4. ND snooping and DHCP snooping for IPv6 are not supported.

IMPB Entry Settings

The table on this window, which is also known as the “IMPB white list,” is used to create Static IP-MAC-Port Binding entries on the Switch.

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



IMPB Entry Settings

IPv4 Address	IPv6 Address	MAC Address	Ports
●	○		□ All Ports

Total Entries: 0

IMPB Entry Table

IP Address	MAC Address	Mode	ACL Status	Ports	Modify	Delete

Figure 7- 11. IMPB Entry Settings window

The following fields can be set or modified:

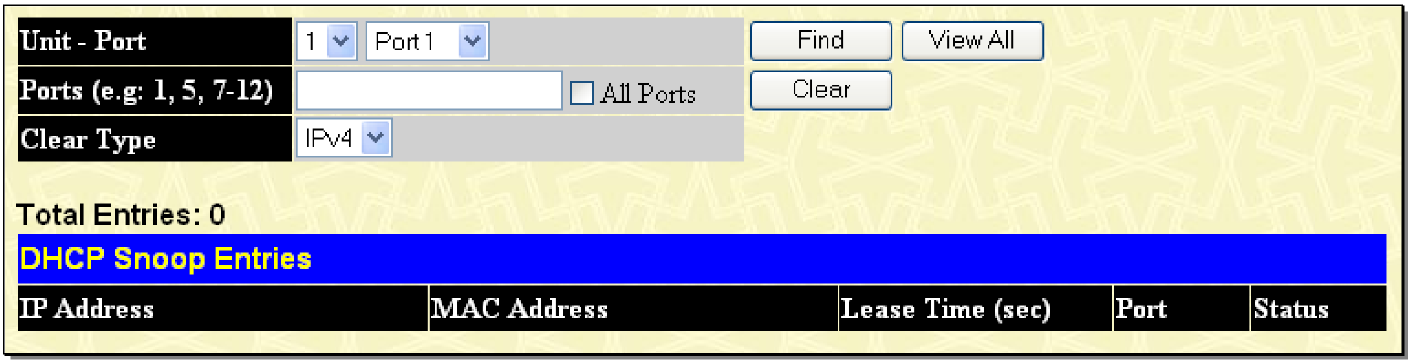
Parameter	Description
IPv4 Address	Enter the IPv4 address to bind to the MAC address set below.
IPv6 Address	Enter the IPv6 address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Ports	Specify the switch ports for which to configure this IP-MAC-port binding entry (IP Address + MAC Address). Tick the All Ports check box to configure this entry for all ports on the Switch.

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

DHCP Snoop Entries

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

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



Unit - Port	1 Port 1
Ports (e.g: 1, 5, 7-12)	□ All Ports
Clear Type	IPv4

Total Entries: 0

DHCP Snoop Entries

IP Address	MAC Address	Lease Time (sec)	Port	Status

Figure 7- 12. DHCP Snoop Entries window

The following fields can be set:

Parameter	Description
Unit - Port	Use the pull-down menu to choose the Switch ID number of the Switch in the switch stack and the port on the Switch.

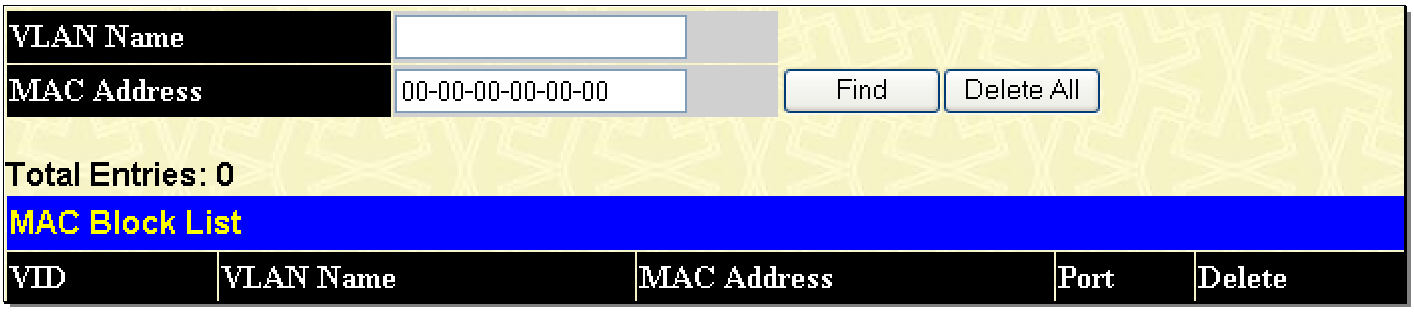
Ports (e.g: 1, 5, 7-12)	Specify the switch ports or tick the All Ports check box to select all ports.
Clear Type	Use the pull-down menu to select the *IPv4*, *IPv6* or *All* type.

To view particular port settings, choose the unit - port number and click **Find**. To view all entries on the window, click **View All**. To delete an entry, enter the port number, choose the Clear Type, and click **Clear**.

MAC Block List

This window is used to view unauthorized devices that have been blocked by IP-MAC-Port binding restrictions.

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



VLAN Name	
MAC Address	00-00-00-00-00-00

Total Entries: 0

MAC Block List

VID	VLAN Name	MAC Address	Port	Delete

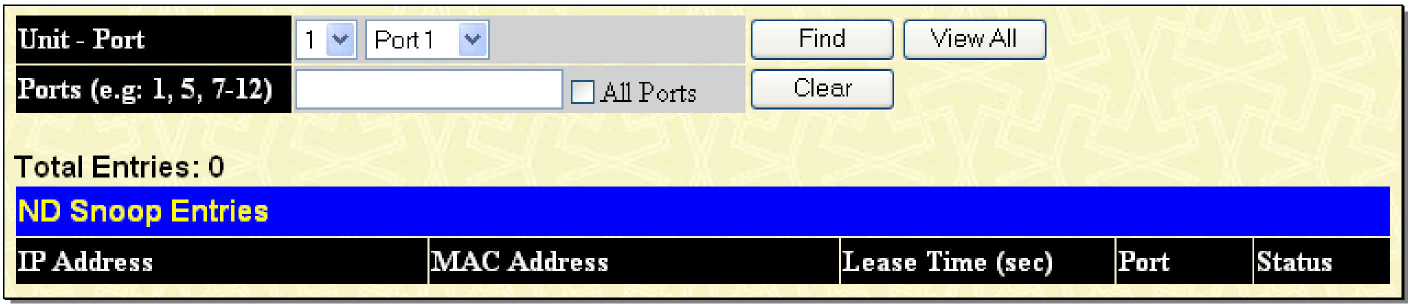
Figure 7- 13. MAC Block List window

To find an unauthorized device MAC address that has been blocked by the IP-MAC port 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 port. To delete all the entries in this window, click **Delete All**.

ND Snoop Entries

This table is used to view ND snooping entries on specific ports.

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



Unit - Port	1 Port 1
Ports (e.g: 1, 5, 7-12)	☐ All Ports

Total Entries: 0

ND Snoop Entries

IP Address	MAC Address	Lease Time (sec)	Port	Status

Figure 7- 14. NP Snoop Entries window

The following fields can be set:

Parameter	Description
Unit - Port	Use the pull-down menu to choose the Switch ID number of the Switch in the switch stack and the port on the Switch.
Ports (e.g: 1, 5, 7-12)	Specify the switch ports or tick the **All Ports** check box to select all ports.

To view particular port settings, choose the unit - port number from the pull-down menu and click **Find**. To view all entries on the window, click **View All**. To delete an entry, enter the port number, and click **Clear**.

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:

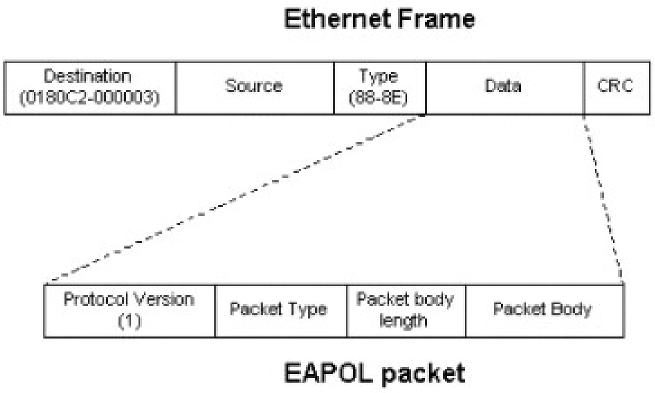


Figure 7- 15. The EAPOL Packet

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

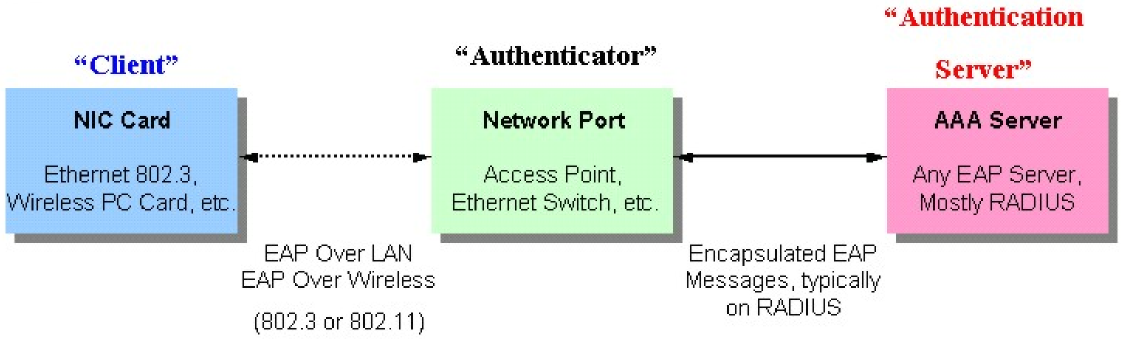

"Client"
NIC Card
Ethernet 802.3, Wireless PC Card, etc.
"Authenticator"
Network Port
Access Point, Ethernet Switch, etc.
"Authentication Server"
AAA Server
Any EAP Server, Mostly RADIUS
EAP Over LAN
EAP Over Wireless
(802.3 or 802.11)
Encapsulated EAP Messages, typically on RADIUS

Figure 7- 16. 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.

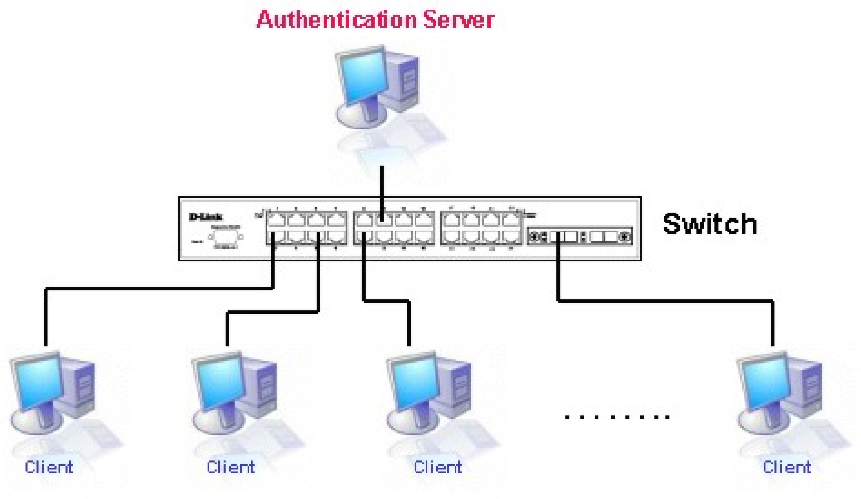


Figure 7- 17. The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing 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. (DGS-3600 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)

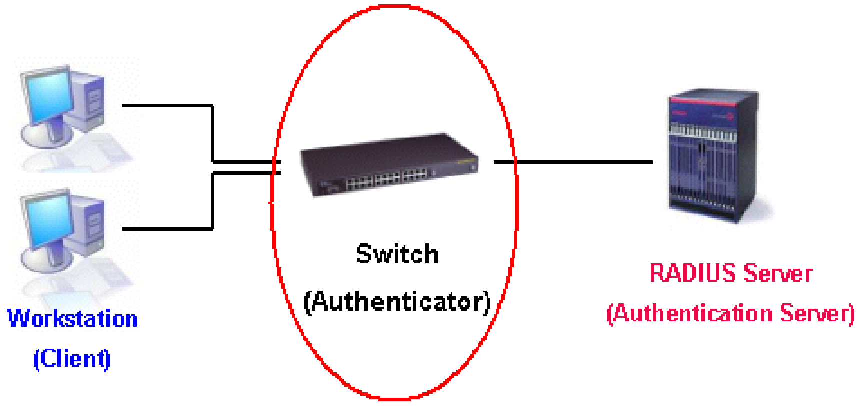


Figure 7- 18. The Authenticator

Client

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

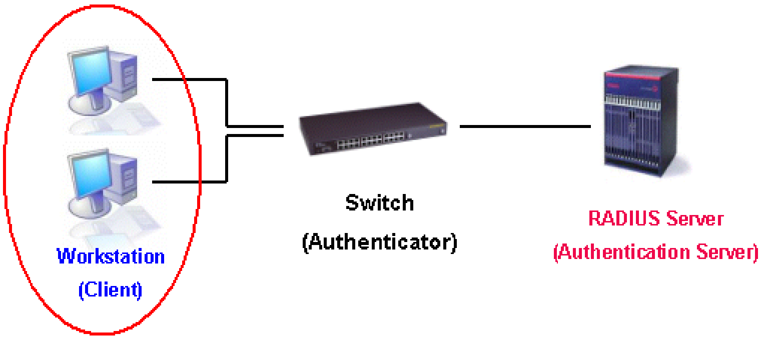


Figure 7- 19. The Client

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 able 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.

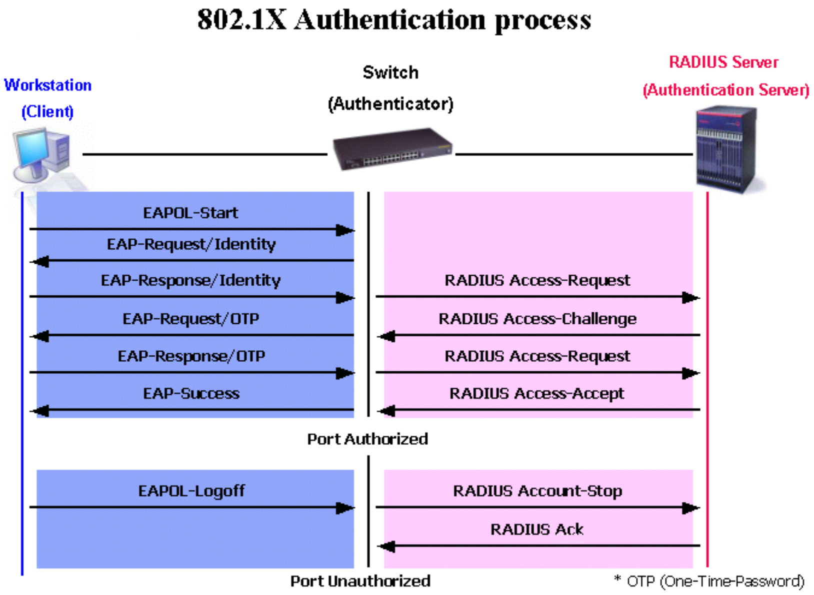


Figure 7- 20. The 802.1X Authentication Process

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

- **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.
- **MAC-Based Access Control** – Using this method, the Switch will automatically learn up to 128 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

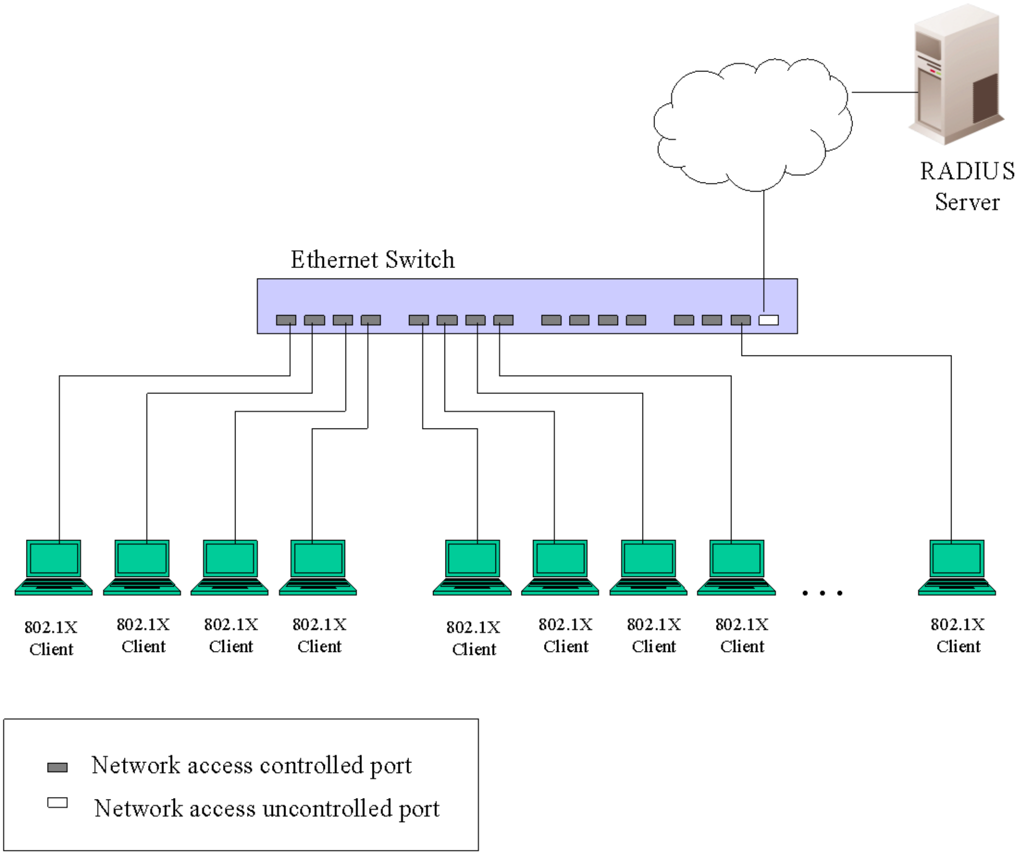


Figure 7- 21. Example of Typical Port-Based Configuration

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

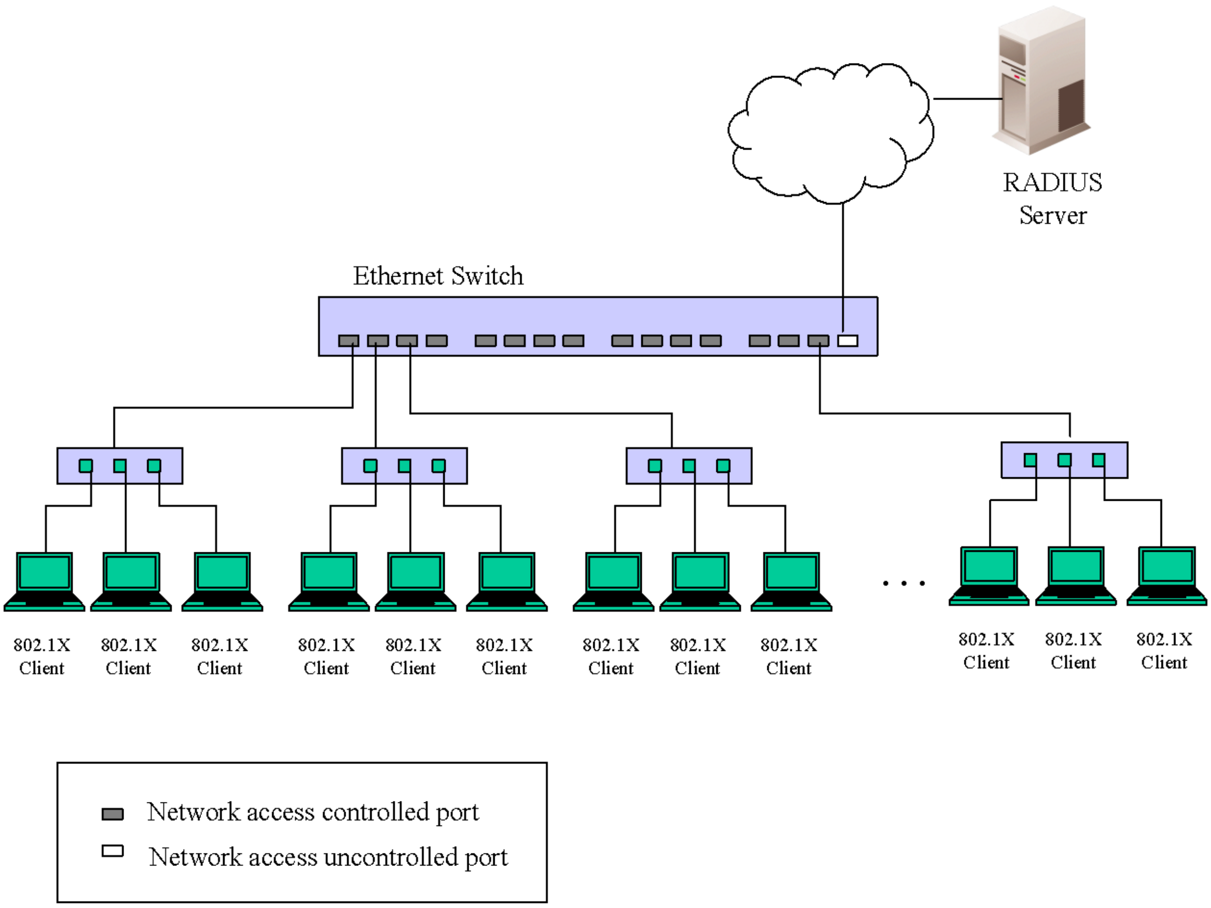


Figure 7- 22. Example of Typical MAC-Based Configuration

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.

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

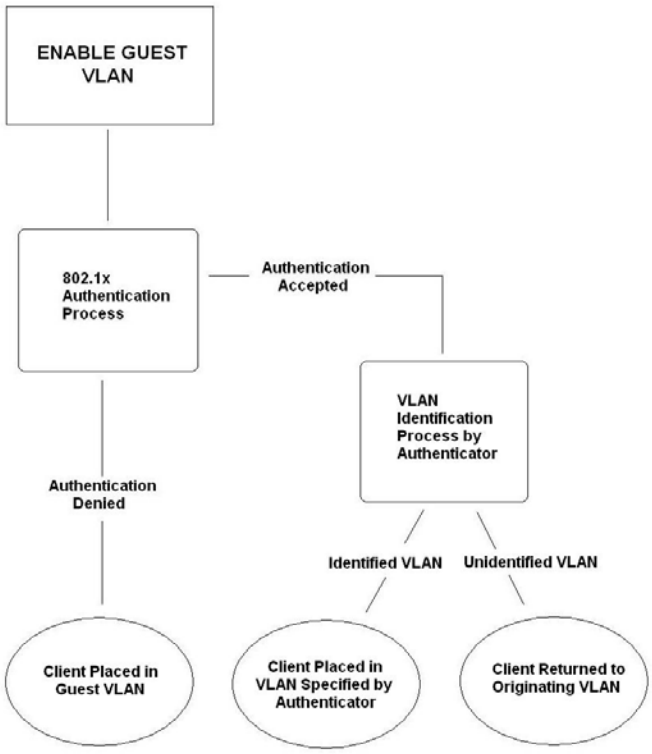

ENABLE GUEST VLAN
802.1x Authentication Process
Authentication Accepted
VLAN Identification Process by Authenticator
Authentication Denied
Identified VLAN
Unidentified VLAN
Client Placed in Guest VLAN
Client Placed in VLAN Specified by Authenticator
Client Returned to Originating VLAN

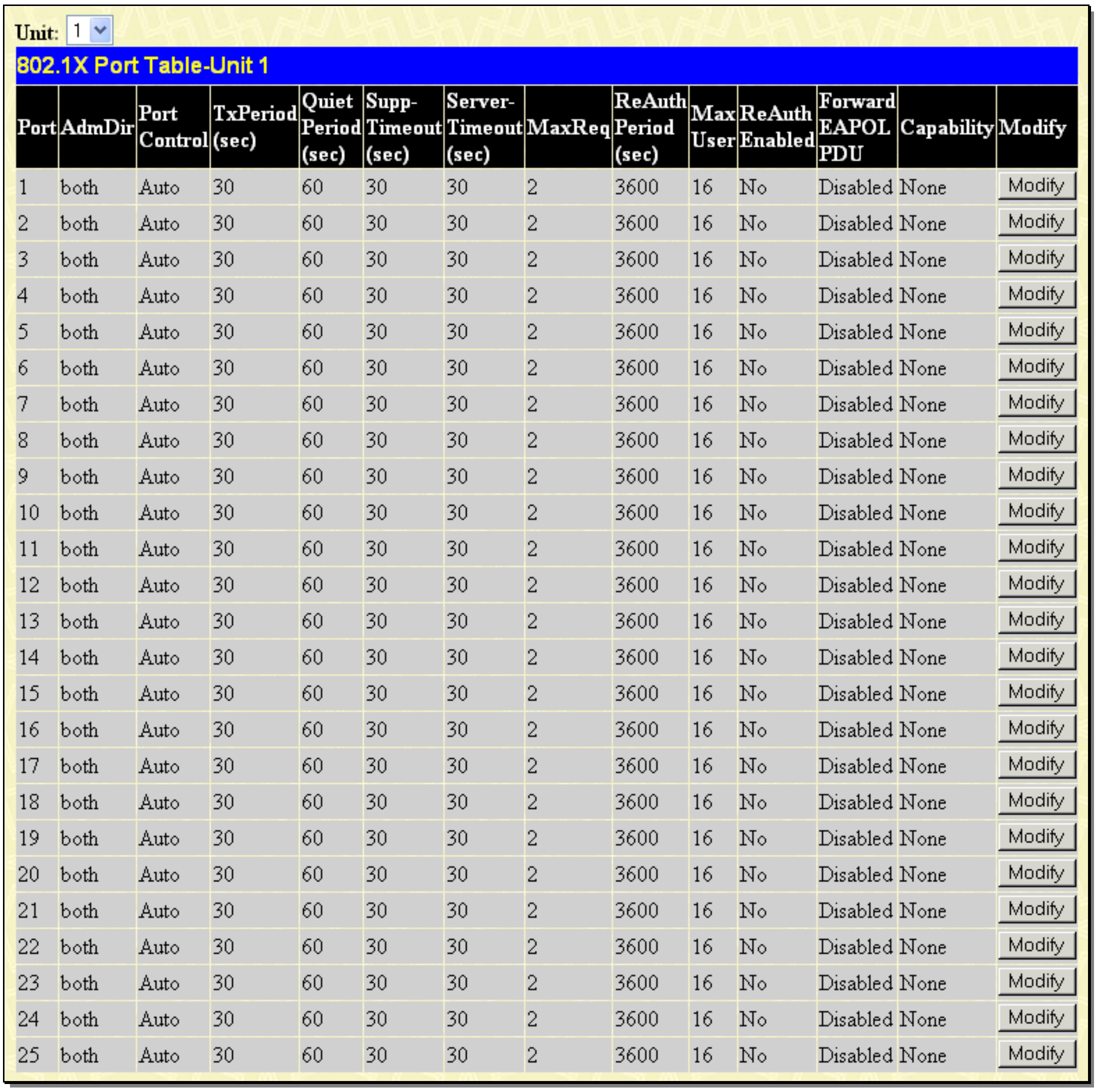
Figure 7- 23. Guest VLAN Authentication Process

Limitations Using the Guest VLAN

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

802.1X Port Settings

To view this window, click **Security** > **802.1X** > **802.1X Port Settings**, as shown below:



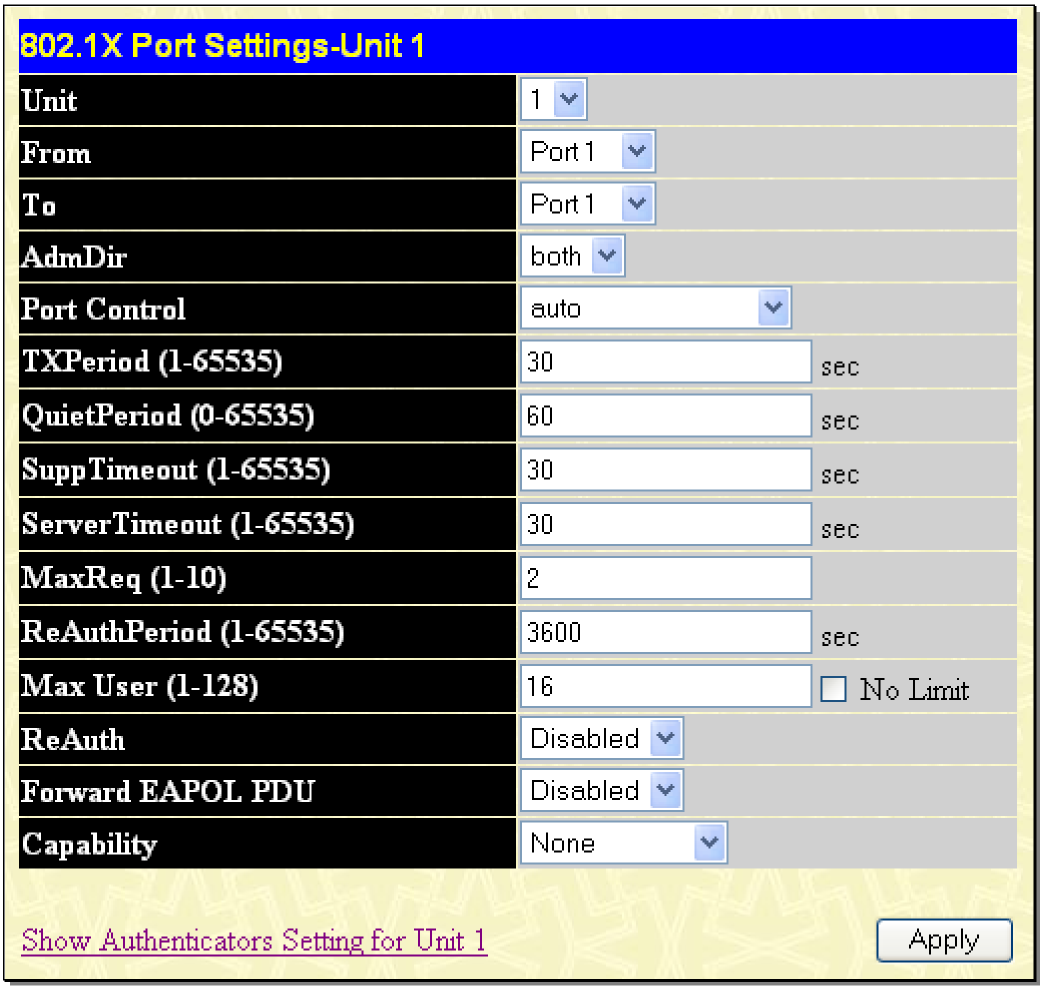
Unit: 1

802.1X Port Table-Unit 1

Port	AdmDir	Port Control	TxPeriod (sec)	Quiet Period (sec)	Supp-Timeout (sec)	Server-Timeout (sec)	MaxReq	ReAuth Period (sec)	Max User	ReAuth Enabled	Forward EAPOL PDU	Capability	Modify
1	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
2	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
3	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
4	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
5	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
6	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
7	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
8	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
9	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
10	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
11	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
12	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
13	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
14	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
15	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
16	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
17	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
18	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
19	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
20	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
21	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
22	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
23	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
24	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
25	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify

Figure 7- 24. 802.1X Port Table window

To configure the settings by port, click on its corresponding **Modify** button, which will display the following table to configure:



802.1X Port Settings-Unit 1

Unit	1
From	Port 1
To	Port 1
AdmDir	both
Port Control	auto
TXPeriod (1-65535)	30 sec
QuietPeriod (0-65535)	60 sec
SuppTimeout (1-65535)	30 sec
ServerTimeout (1-65535)	30 sec
MaxReq (1-10)	2
ReAuthPeriod (1-65535)	3600 sec
Max User (1-128)	16 □ No Limit
ReAuth	Disabled
Forward EAPOL PDU	Disabled
Capability	None

Figure 7- 25. 802.1X Port Settings window (Modify)

This window allows users to set the following features:

Parameter	Description
Unit	Select the unit to configure.
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.
Port Control	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.

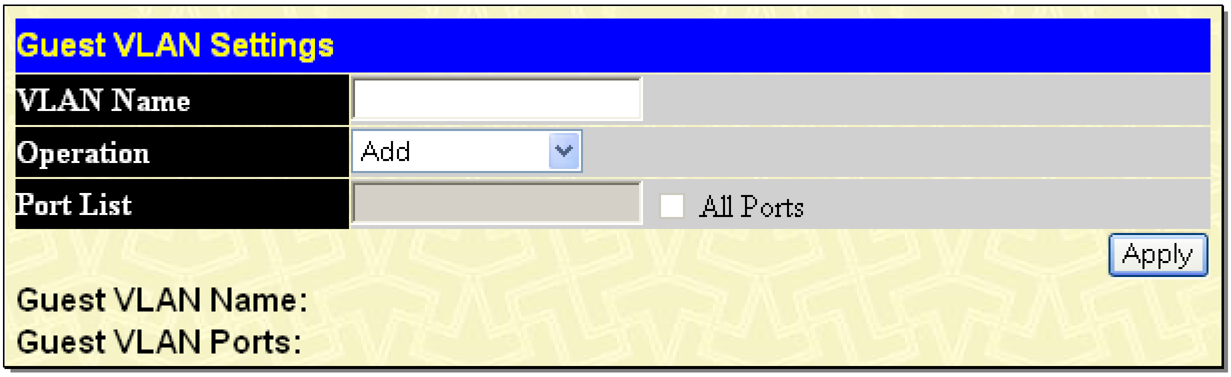
	The default setting is *Auto*.
TXPeriod (1-65535)	This sets the TX Period of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
QuietPeriod (0-65535)	This allows the setting of the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is 2.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.
Max User (1-128)	This allows the setting of the maximum number of users. The default setting is *16* users. Ticking No Limit means support for a maximum of 128 users.
ReAuth	Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.
Forward EAPOL PDU	This enables or disables the Switch retransmit EAPOL PDU Request on a per port basis.
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 configuration changes.

Guest VLAN Settings

To set a Guest 802.1X VLAN, the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

To view this window, click **Security** > **802.1X** > **Guest VLAN Settings**, as shown below:



Guest VLAN Settings

VLAN Name	
Operation	Add
Port List	□ All Ports

Guest VLAN Name:

Guest VLAN Ports:

Figure 7- 26. Guest VLAN Settings 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.

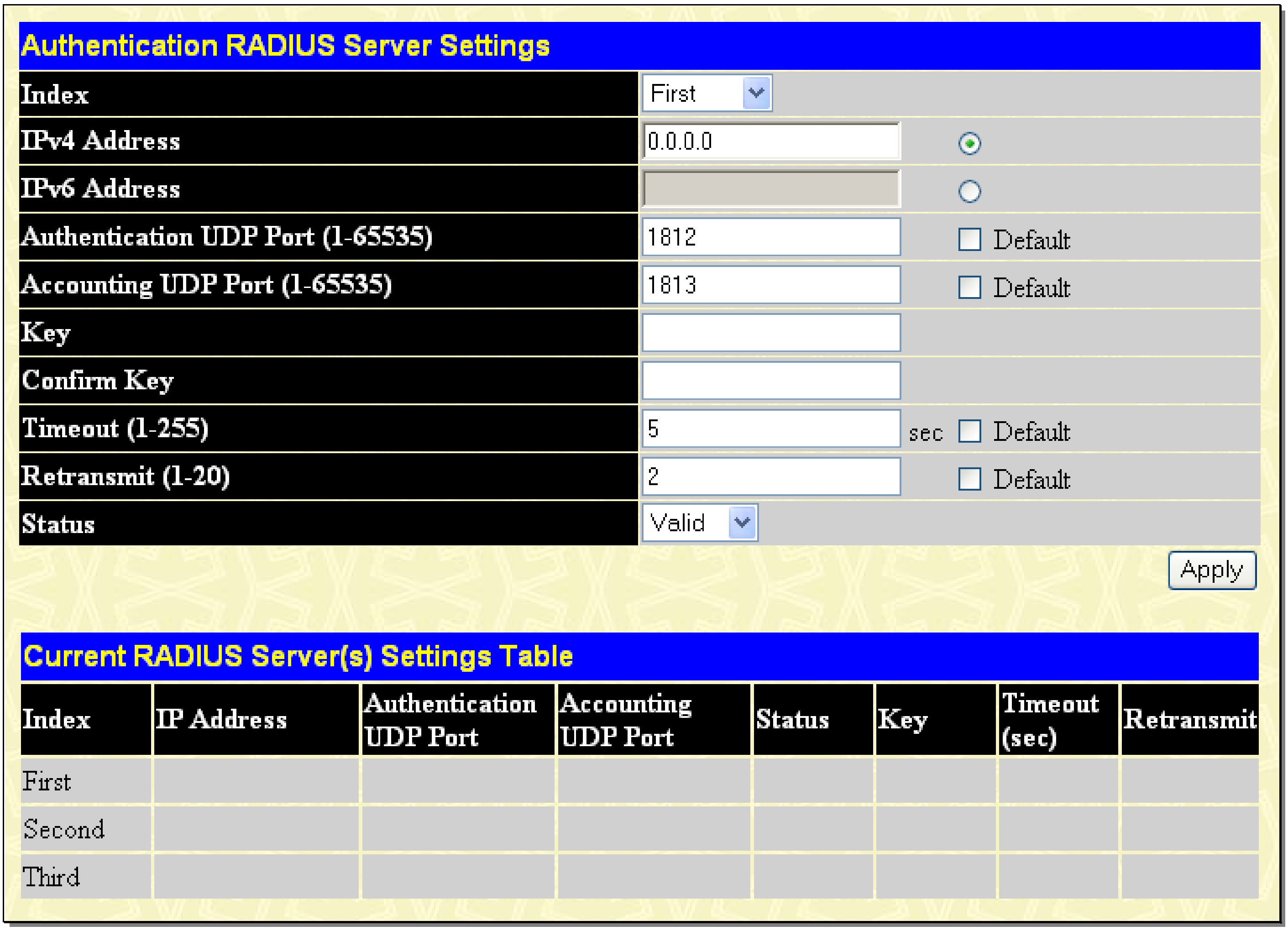
Operation	The user has four choices in configuring the Guest 802.1X VLAN, which are: *Enabled Ports* – Selecting this option will enable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message. *Disabled Ports* - Selecting this option will disable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message. *Add* – Selecting this option will add the VLAN entered in the VLAN Name window above. *Delete* – Selecting this option will delete the VLAN entered in the VLAN Name window above.
Port List	Enter the ports to be operational for the Gust VLAN. Checking the All box will select all ports to be enabled.

Click **Apply** to implement the guest 802.1X VLAN settings entered. Only one VLAN may be assigned as the 802.1X Guest VLAN.

Authentication RADIUS Server Settings

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.

To view this window, click **Security** > **802.1X** > **Authentication RADIUS Server Settings**, as shown below:



Authentication RADIUS Server Settings

Index	First	
IPv4 Address	0.0.0.0	●
IPv6 Address		○
Authentication UDP Port (1-65535)	1812	□ Default
Accounting UDP Port (1-65535)	1813	□ Default
Key		
Confirm Key		
Timeout (1-255)	5	sec □ Default
Retransmit (1-20)	2	□ Default
Status	Valid	

Current RADIUS Server(s) Settings Table

Index	IP Address	Authentication UDP Port	Accounting UDP Port	Status	Key	Timeout (sec)	Retransmit
First							
Second							
Third							

Figure 7- 27. Authentication RADIUS Server Settings window

This window displays the following information:

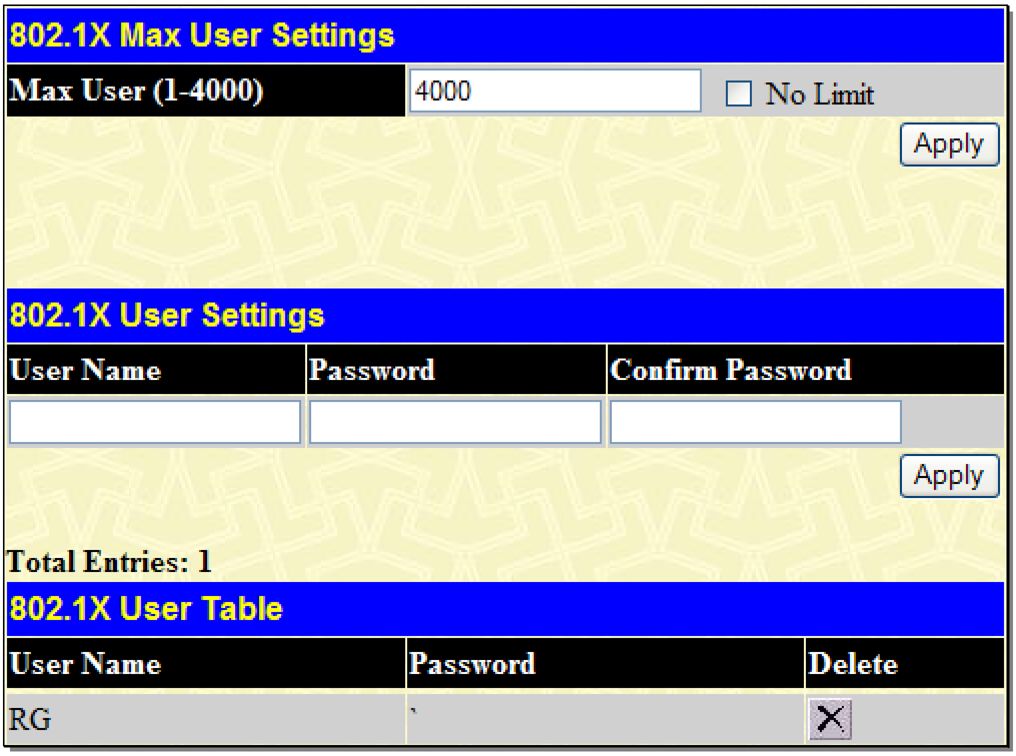
Parameter	Description

Index	Choose the desired RADIUS server to configure: *First, Second* or *Third*.
IPv4 Address	Click the radio button and enter the RADIUS server IPv4 address.
IPv6 Address	Click the radio button and enter the RADIUS server IPv6 address.
Authentication UDP Port (1-65535)	Enter the RADIUS authentic server(s) UDP port. The default port is *1812*. Alternatively, users can tick the Default check box.
Accounting UDP Port (1-65535)	Enter the RADIUS account server(s) UDP port. The default port is *1813*. Alternatively, users can tick the Default check box.
Key	Enter 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.
Timeout (1-255)	Enter a timeout value between *1* and *255* seconds. The default value is *5* seconds. Alternatively, users can tick the Default check box.
Retransmit (1-20)	Enter a retransmit value between *1* and *20*. The default value is *2*. Alternatively, users can tick the Default check box.
Status	This allows users to set the RADIUS Server as *Valid* (Enabled) or *Invalid* (Disabled).

802.1X User Settings

This window allows the user to set different local users on the Switch and set a global limitation on the maximum number of users that can be learned via 802.1X authentication.

To view this window, click **Security** > **802.1X** > **802.1X User Settings**, as shown below:



802.1X Max User Settings

Max User (1-4000): 4000 □ No Limit

802.1X User Settings

User Name	Password	Confirm Password

Total Entries: 1

802.1X User Table

User Name	Password	Delete
RG	`	☒

Figure 7- 28. 802.1X User Settings window

This window allows setting of the following features:

Parameter	Description

Max User (1-4000)	Enter the maximum number of users to be allowed. Tick the No Limit check box to specify that there will be the maximum number of users. By default there is no limit.
User Name	Enter the User Name of the new profile to be created.
Password	Enter a password for the new user.
Confirm Password	Re-enter the password entered in the field above.

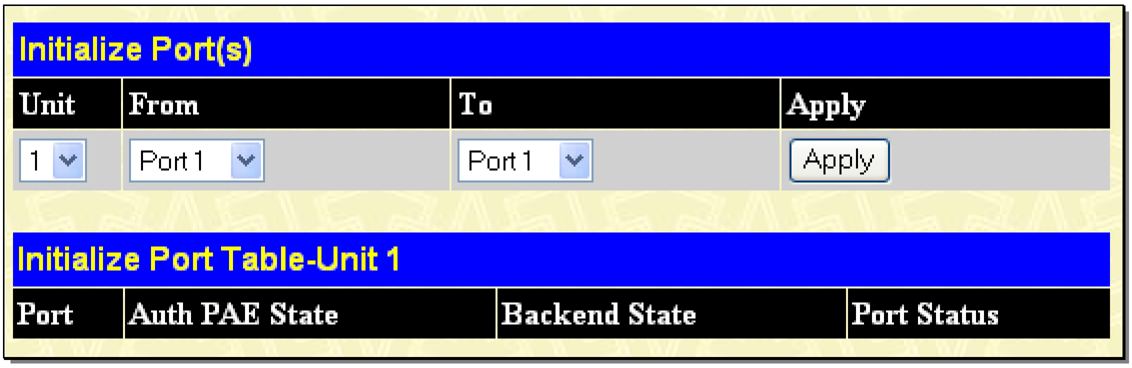
Click **Apply** to implement the changes. The new User will be displayed in the 802.1X User Table. To remove a user, click the corresponding ☒ button.

NOTE: The user must first globally enable 802.1X in the **DGS-3600 Web Management Tool** window before setting up ports.

Initialize Port(s)

Existing 802.1X port and MAC settings are displayed and can be configured using the window below.

To view this window, click **Security > 802.1X > Initialize Port(s)**, as shown below:



Initialize Port(s)

Unit	From	To	Apply
1	Port 1	Port 1	Apply

Initialize Port Table-Unit 1

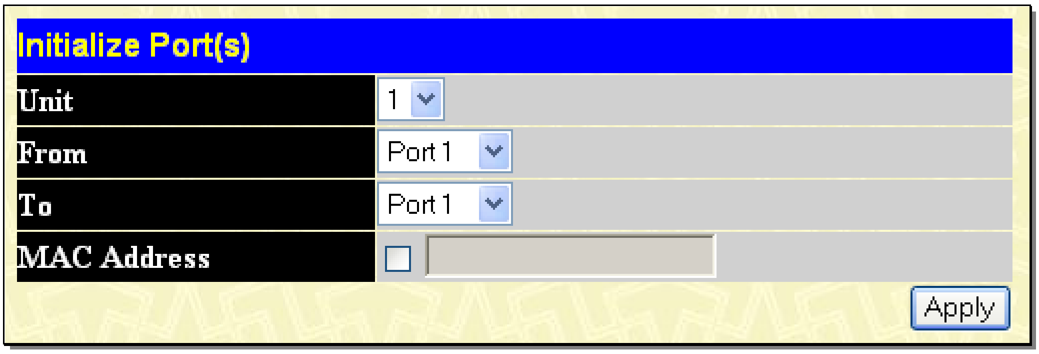
Port	Auth PAE State	Backend State	Port Status

Figure 7- 29. Initialize Port window (Port-based 802.1X)

This window allows initialization of a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s).

To initialize ports for the MAC side of 802.1X, the user must first enable 802.1X by MAC address in the **DGS-3600 Web Management Tool** window.

Click **Security > 802.1X > Initialize Port(s)**, as shown below:



Initialize Port(s)

Unit	1
From	Port 1
To	Port 1
MAC Address	□

Figure 7- 30. Initialize Ports window (MAC-based 802.1X)

To initialize ports, first choose the switch in the switch stack by using the pull-down menu and then choose 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 ticking the corresponding check box. To begin the initialization, click **Apply**.

This window displays the following information:

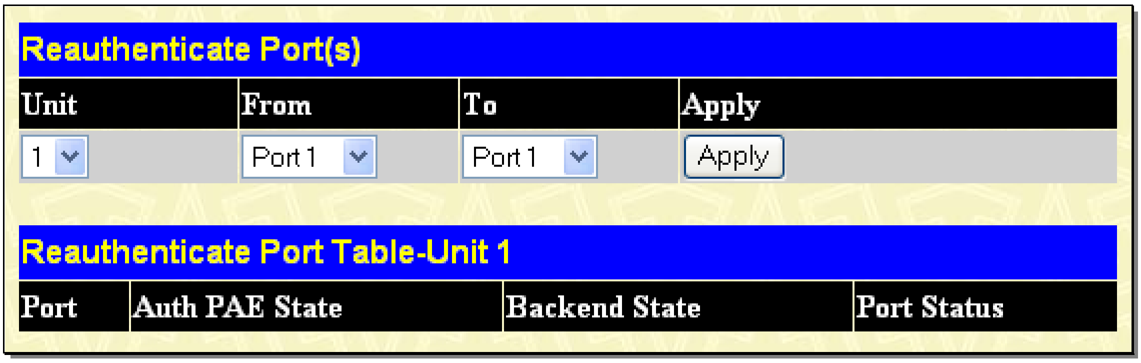
Parameter	Description
Unit	Select the switch to configure.
From/To	Select ports to be initialized.
Port	A read-only field indicating a port on the Switch.
Auth PAE State	The Authenticator PAE State will display one of the following: Initialize, Disconnected, Connecting, Authenticating, Authenticated, 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.*
MAC Address	The MAC address of the Switch connected to the corresponding port, if any.

NOTE: The user must first globally enable 802.1X in the **DGS-3600 Web Management Tool** window before initializing ports. Information in the Initialize Ports Table cannot be viewed before enabling 802.1X.

Reauthenticate Port(s)

This window allows reauthentication 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**.**

To view this window, click **Security > 802.1X > Reauthenticate Port(s)**, as shown below:



Reauthenticate Port(s)

Unit	From	To	Apply
1	Port 1	Port 1	Apply

Reauthenticate Port Table-Unit 1

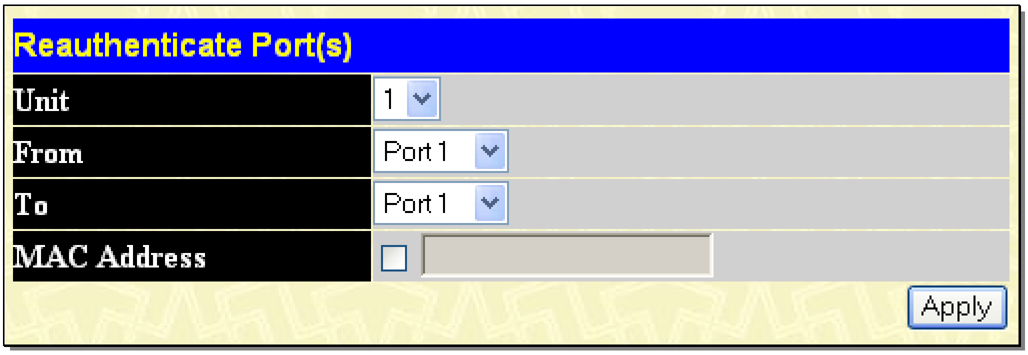
Port	Auth PAE State	Backend State	Port Status

Figure 7- 31. Reauthenticate Port window

NOTE: The user must first globally enable 802.1X in the **DGS-3600 Web Management Tool** window before initializing ports. Information in the Initialize Ports Table cannot be viewed before enabling 802.1X.

To reauthenticate ports for the MAC side of 802.1X, the user must first enable 802.1X by MAC address in the **DGS-3600 Web Management Tool** window.

Click **Security > 802.1X > Reauthenticate Port(s)** as shown below:



Reauthenticate Port(s)

Unit	1
From	Port 1
To	Port 1
MAC Address	□

Figure 7- 32. Reauthenticate Port(s) window (MAC-based 802.1X)

To reauthenticate ports, first choose the switch in the switch stack by using the pull-down menu and then 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 ticking the corresponding check box. To begin the reauthentication, click **Apply**.

This window displays the following information:

Parameter	Description
Unit	Select the switch to configure.
From/To	Select the range of ports to reauthenticated.
Port	The port number of the reauthenticated port.
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.
MAC Address	Displays the physical address of the Switch where the port resides.

Web-based Access Control (WAC)

Web-based Access Control is another port-based access control method implemented similarly to the 802.1X port-based access control method previously stated. This function will allow user authentication through a RADIUS server or through the local authentication set on the Switch when a user is trying to access the network via the Switch, if the port connected to the user is enabled for this feature.

The user attempting to gain Web access will be prompted for a user name and password before being allowed to accept HTTP packets from the Switch. Once authenticated, the user will be placed in a target VLAN (if have) 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.

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 steps all parties of the authentication go through for a successful Web-based Access Control process.

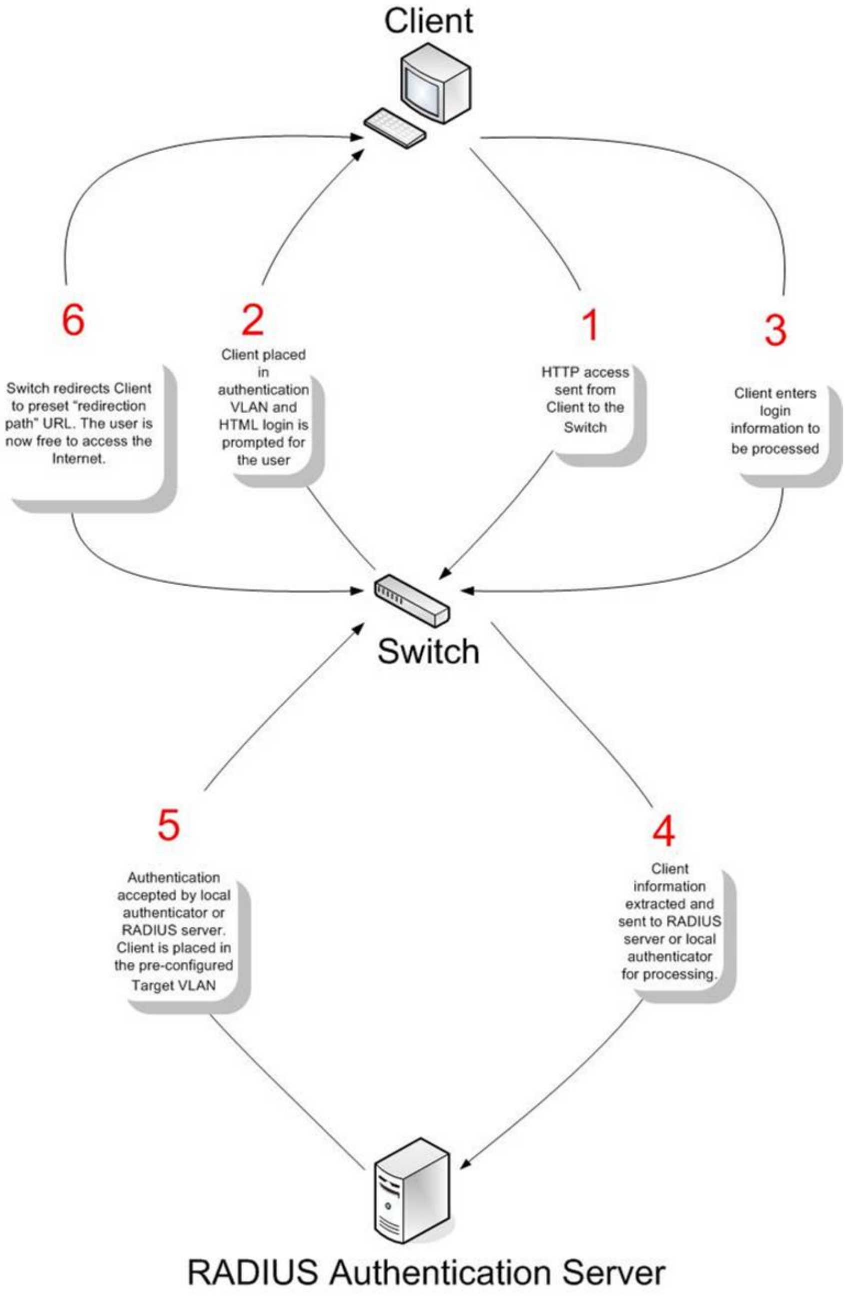

Client
6
Switch redirects Client to preset "redirection path" URL. The user is now free to access the Internet.
2
Client placed in authentication VLAN and HTML login is prompted for the user
1
HTTP access sent from Client to the Switch
3
Client enters login information to be processed
Switch
5
Authentication accepted by local authenticator or RADIUS server. Client is placed in the pre-configured Target VLAN
4
Client information extracted and sent to RADIUS server or local authenticator for processing.
RADIUS Authentication Server

Figure 7- 33. The 6-Step WAC Authentication Process

Conditions and Limitations

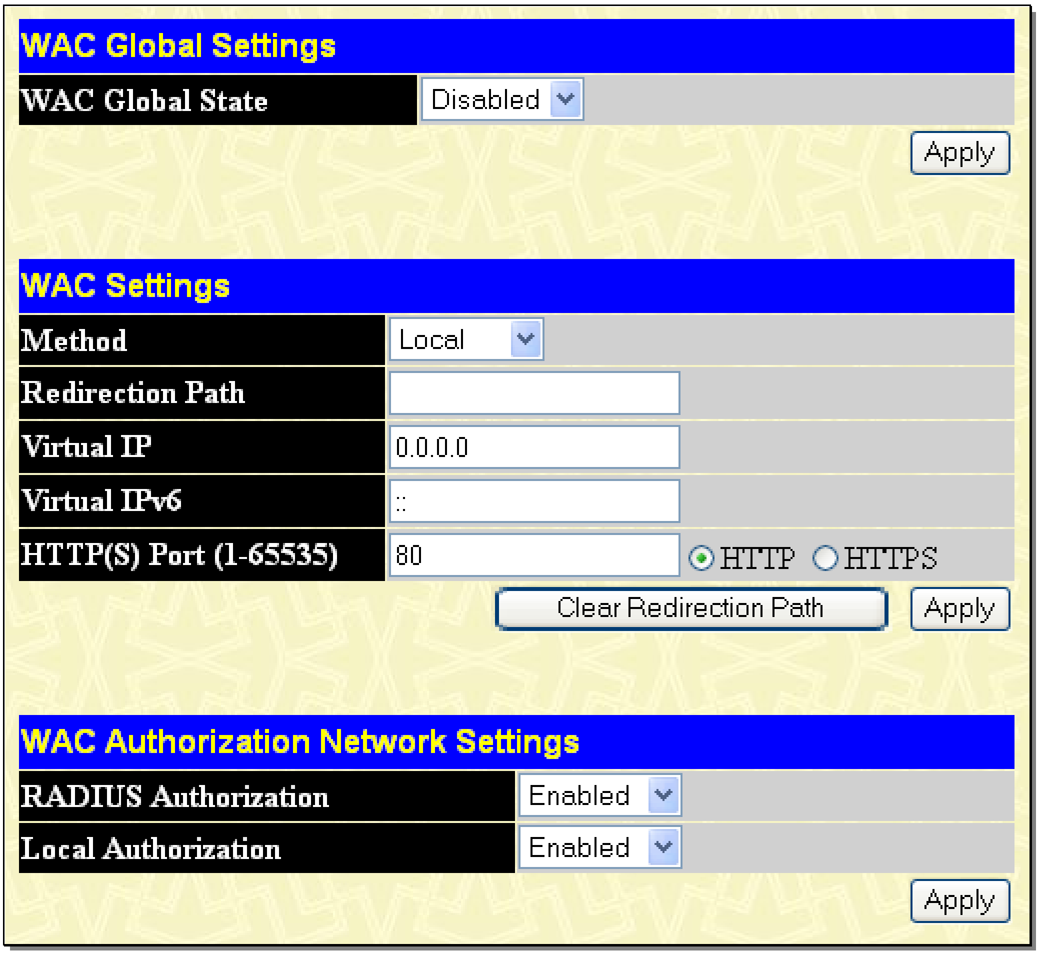
1. The subnet of the authentication VLAN's IP interface must be the same as that of the client. If not configured properly, the authentication will be permanently denied by the authenticator. It cannot be a Guest VLAN.
2. If the client is utilizing DHCP to attain an IP address, the authentication VLAN 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.

WAC Global Settings

This window is used to enable and configure the Web-based Access Control Global State on the Switch.

To view this window, click **Security** > **Web-based Access Control (WAC)** > **WAC Global Settings**, as shown below:



WAC Global Settings

WAC Global State	Disabled

WAC Settings

Method	Local
Redirection Path	
Virtual IP	0.0.0.0
Virtual IPv6	::
HTTP(S) Port (1-65535)	80 ● HTTP ○ HTTPS

WAC Authorization Network Settings

RADIUS Authorization	Enabled
Local Authorization	Enabled

Figure 7- 34. WAC Global Settings window

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

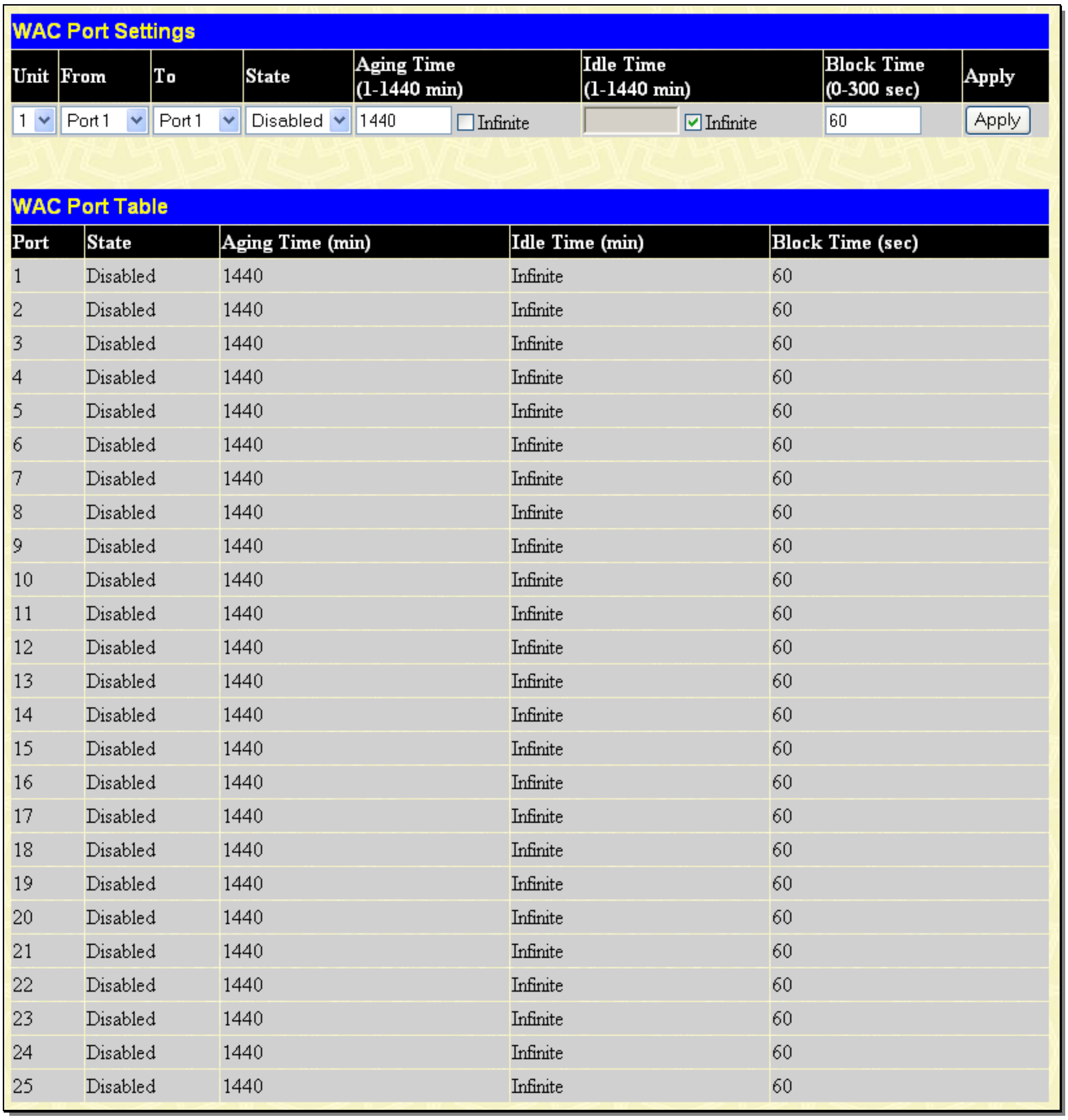
Parameter	Description
WAC Global Settings	
WAC Global State	Toggle the State field to either *Enabled* or *Disabled* for the Web-based Access Control settings of the Switch.
WAC Settings	
Method	Use the pull-down menu to choose the authenticator for Web-based Access Control. The user may choose: *Local* – 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.

Redirection Path	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.
Virtual IP	Enter a virtual IP address so that the TCP packets sent to the virtual IP will get a reply. If the virtual IP is enabled, the TCP packets sent to the virtual IP or physical IPIF's IP address will both get a reply. When the virtual IP is set to *0.0.0.0* the function will be disabled. To ensure that this function works correctly, the virtual IP address must not be configurable, that is, it cannot be an IP address that exists on the subnet.
Virtual IPv6	Enter a virtual IPv6 address so that the TCP packets sent to the virtual IP for IPv6 will get a reply. If the virtual IP for IPv6 is enabled, the TCP packets sent to the virtual IP or physical IPIF's IPv6 address will both get a reply. When the virtual IPv6 is set to "::", the function will be disabled. To ensure that this function works correctly, the virtual IPv6 address must not be configured to be an IPv6 address that exists on the subnet.
HTTP(S) Port (1-65535)	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.
WAC Authorization Network Settings	
RADIUS Authorization	Enable or disable RADIUS authorization.
Local Authorization	Enable or disable local authorization.

Click **Apply** to implement changes made.

WAC Port Settings

To view this window, click **Security > Web-based Access Control (WAC) > WAC Port Settings**, as shown below:



WAC Port Settings

Unit	From	To	State	Aging Time (1-1440 min)	Idle Time (1-1440 min)	Block Time (0-300 sec)	Apply
1	Port 1	Port 1	Disabled	1440 □ Infinite	☑ Infinite	60	Apply

WAC Port Table

Port	State	Aging Time (min)	Idle Time (min)	Block Time (sec)
1	Disabled	1440	Infinite	60
2	Disabled	1440	Infinite	60
3	Disabled	1440	Infinite	60
4	Disabled	1440	Infinite	60
5	Disabled	1440	Infinite	60
6	Disabled	1440	Infinite	60
7	Disabled	1440	Infinite	60
8	Disabled	1440	Infinite	60
9	Disabled	1440	Infinite	60
10	Disabled	1440	Infinite	60
11	Disabled	1440	Infinite	60
12	Disabled	1440	Infinite	60
13	Disabled	1440	Infinite	60
14	Disabled	1440	Infinite	60
15	Disabled	1440	Infinite	60
16	Disabled	1440	Infinite	60
17	Disabled	1440	Infinite	60
18	Disabled	1440	Infinite	60
19	Disabled	1440	Infinite	60
20	Disabled	1440	Infinite	60
21	Disabled	1440	Infinite	60
22	Disabled	1440	Infinite	60
23	Disabled	1440	Infinite	60
24	Disabled	1440	Infinite	60
25	Disabled	1440	Infinite	60

Figure 7- 35. WAC Port Settings window

The following parameters can be configured:

Parameter	Description
Unit	Use the drop-down menu to select the unit to configure.
From/To	Enter the range of ports to configure.
State	Enable or disable the WAC port settings on the specified ports.
Aging Time (1-1440 min)	This parameter specifies the period of time a host will keep in authenticated state after it succeeds to authenticate. Enter a value between *0* and *1440* minutes. The default setting is *1440* minutes. To maintain a constant Port Configuration tick the Infinite box in the WAC configuration window.
Idle Time (1-1440 min)	This parameter specifies the period of time during which there is no traffic for an authenticated host and the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. A value of Infinite indicates the Idle state of the authenticated host on the port will never be checked. The default setting is Infinite.
Block Time (0-300 sec)	This parameter specifies the period of time a host will keep in a blocked state after it fails to authenticate. Enter a value between *0* and *300* seconds. The default setting is *0* seconds.

Click **Apply** to implement the changes.

WAC User Account

This window is used to set up user accounts for the Web-based Access Control.

To view this window, click **Security > Web-based Access Control (WAC) > WAC User Account**, as shown below:

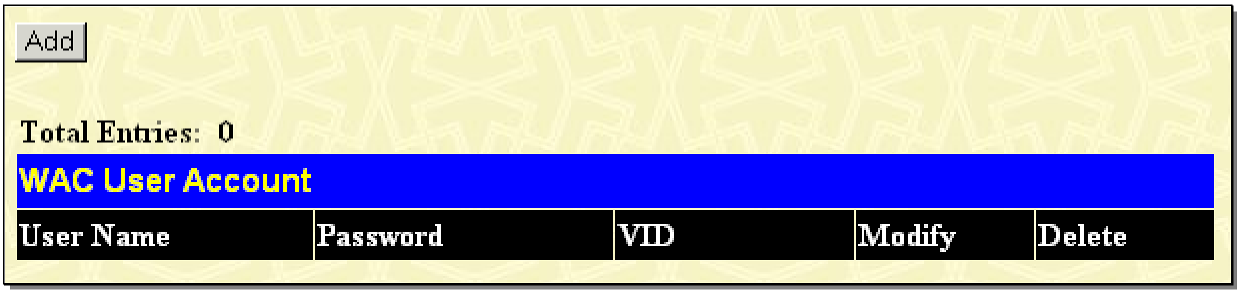


Figure 7- 36. WAC User Account window

Click the **Add** button to display a window to configure the WAC user account, as shown below:

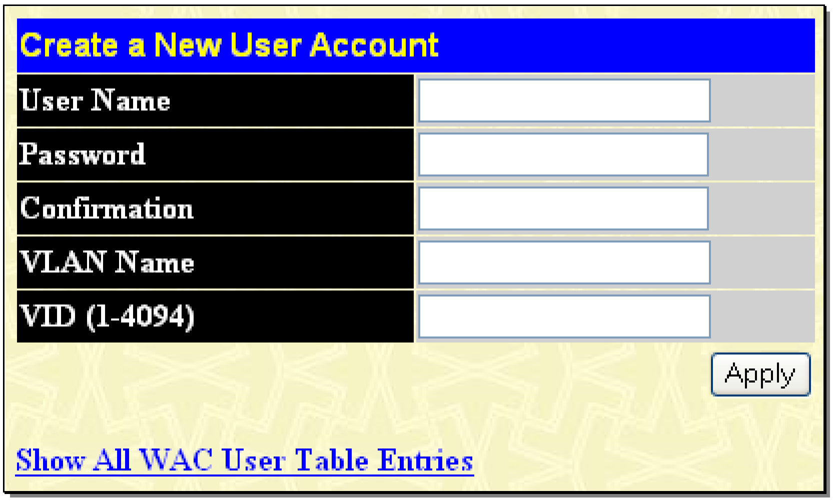
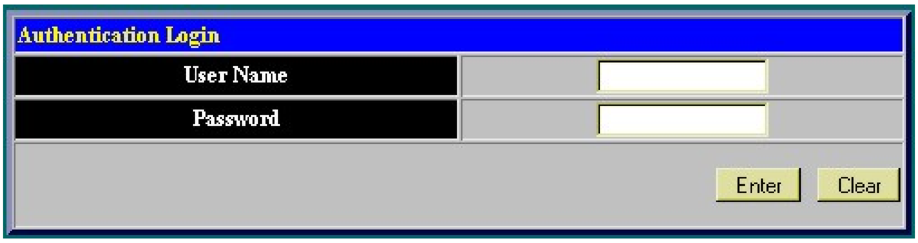


Figure 7- 37. Create a New User Account window

To set the User Account settings for the Web-based Access Control by the Switch, complete the following fields.

Parameter	Description
User Name	Enter the username of up to 15 alphanumeric characters of the guest wishing to access the web through this process. This field is for administrators who have selected *local* as their Web-based authenticator.
Password	Enter the password the administrator has chosen for the selected user. This field is case sensitive and must be a complete alphanumeric string. This field is for administrators who have selected *local* as their Web-based authenticator.
Confirmation	Retype the Password in this field to confirm.
VLAN Name	Enter the VLAN name of a previously configured VLAN to which successfully authenticated Web user will be mapped.
VID (1-4094)	Enter the VLAN ID number of a previously configured VLAN to which successfully authenticated Web user will be mapped.

The following window displays the Authentication Login windows that guest users will be prompted with once attempting Web-based Access Control. Enter the user name and the password configured in the previous window and click **Enter** to access the VLAN previously assigned by the Switch administrator for successful authentication.

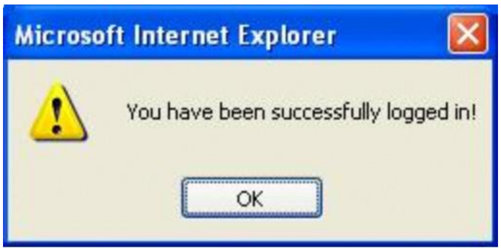


Authentication Login

User Name	
Password	

Figure 7- 38. Web-based Access Control Authentication Login window

After successfully logging in, the user will be prompted with this window, verifying that the user has successfully authenticated the WAC port.



Microsoft Internet Explorer

You have been successfully logged in!

Figure 7- 39. WAC Logout window

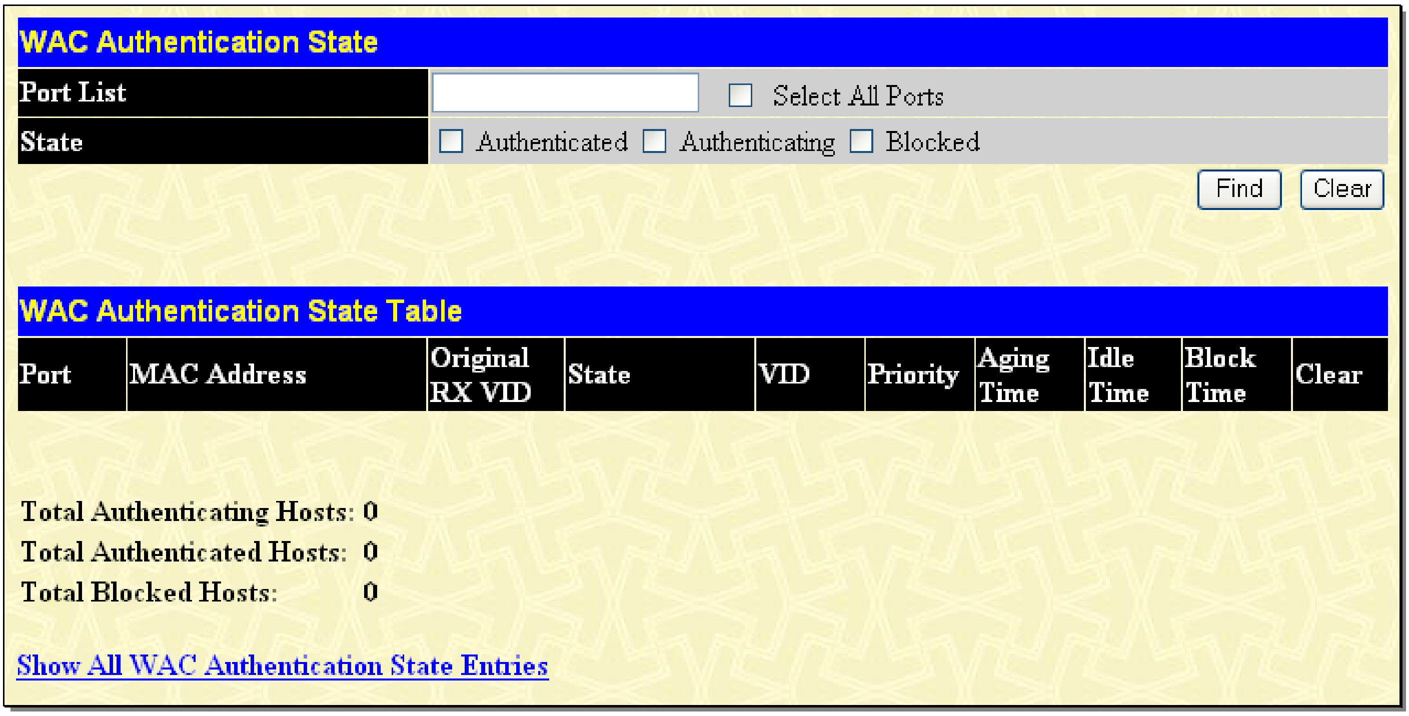
NOTE: The previous logout screen may have some problems when using Netscape 7.0.

If the port where Web-Access Control is preset to be moved to a VLAN without an IPIF interface, the previous logout screen may also not be presented when logging in.

WAC Authentication State

This window is used to enable and configure Web-based Access Control Host Table Settings on the Switch.

To view this window, click **Security** > **Web-based Access Control (WAC)** > **WAC Authentication State**, as shown below:



WAC Authentication State

Port List	☐ Select All Ports
State	☐ Authenticated ☐ Authenticating ☐ Blocked

WAC Authentication State Table

Port	MAC Address	Original RX VID	State	VID	Priority	Aging Time	Idle Time	Block Time	Clear

Total Authenticating Hosts: 0

Total Authenticated Hosts: 0

Total Blocked Hosts: 0

Figure 7- 40. WAC Authentication State window

The following parameters can be configured:

Parameter	Description

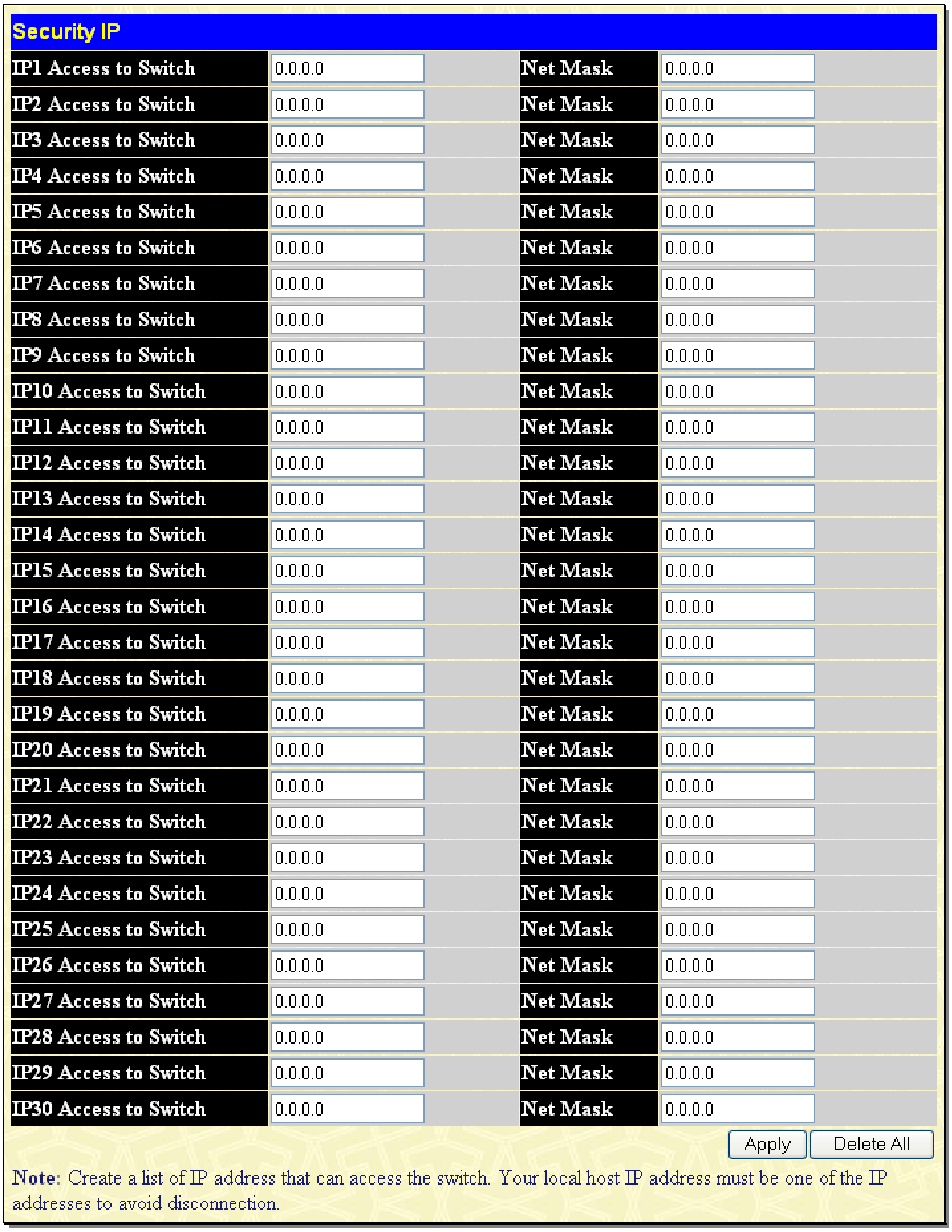
Port List	Enter the ports you wish to *Find* or *Clear*. Tick the *All Ports* check box to select all ports.
State	Select the state of the ports. Choose between *Authenticated*, *Authenticating* or *Blocked*.

Click **Find** to display the Host table entries or click **Clear** to remove an entry.

Trust Host

The Switch allows users to enter trusted host secure IP addresses and netmasks used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

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



Security IP

IP1 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP2 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP3 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP4 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP5 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP6 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP7 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP8 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP9 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP10 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP11 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP12 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP13 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP14 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP15 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP16 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP17 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP18 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP19 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP20 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP21 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP22 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP23 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP24 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP25 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP26 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP27 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP28 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP29 Access to Switch	0.0.0.0	Net Mask	0.0.0.0
IP30 Access to Switch	0.0.0.0	Net Mask	0.0.0.0

Note: Create a list of IP address that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

Figure 7- 41. Security IP window

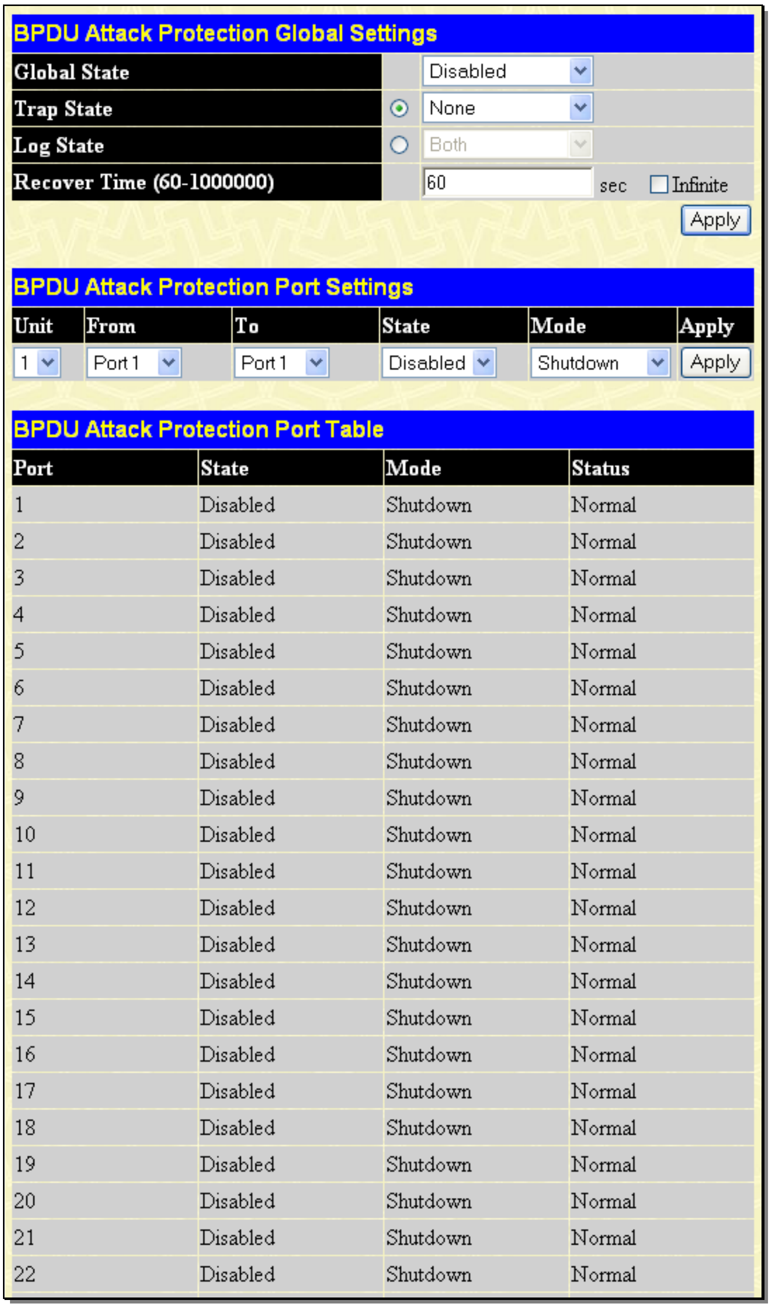
Use the Security IP Management to permit remote stations to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management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

BPDU Attack Protection Settings

This window is used to configure the BPDU protection function for the ports on the Switch. In generally, there are two states in BPDU protection function. One is the normal state, and another is the under attack state. The under attack state has three modes: drop, block, and shutdown. A BPDU protection-enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on SPT-disabled port. BPDU protection has high priority than FBPDU setting configured by configure STP command in determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has high priority than BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

To view this window, click **Security > BPDU Attack Protection Settings**, as shown below:



BPDU Attack Protection Global Settings

Global State		Disabled
Trap State	●	None
Log State	○	Both
Recover Time (60-1000000)		60 sec ☐ Infinite

BPDU Attack Protection Port Settings

Unit	From	To	State	Mode	Apply
1	Port 1	Port 1	Disabled	Shutdown	Apply

BPDU Attack Protection Port Table

Port	State	Mode	Status
1	Disabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal
10	Disabled	Shutdown	Normal
11	Disabled	Shutdown	Normal
12	Disabled	Shutdown	Normal
13	Disabled	Shutdown	Normal
14	Disabled	Shutdown	Normal
15	Disabled	Shutdown	Normal
16	Disabled	Shutdown	Normal
17	Disabled	Shutdown	Normal
18	Disabled	Shutdown	Normal
19	Disabled	Shutdown	Normal
20	Disabled	Shutdown	Normal
21	Disabled	Shutdown	Normal
22	Disabled	Shutdown	Normal

Figure 7- 42. BPDU Attack Protection Global Settings window

The following parameters can be configured:

Parameter	Description
Global State	Enable or disable the BPDU attack protection global state.
Trap State	Enable or disable the BPDU attack trap state.
Log State	Enable or disable the BPDU attack log state.
Recover Time (60-1000000)	Enter the BPDU protection Auto-Recovery recovery timer. The default value is *60*. If Infinite is ticked, the port will not be auto recovered.
Unit	Select the unit to be configured.
From/To	Select the port or range of ports to be configured.
State	Enable or disable BPDU attack protection for the specified individual ports.
Mode	Select the BPDU attack protection mode: *Drop*, *Block*, or *Shutdown*. *Drop* - Drop all received BPDU packets when the port enters under_attack state. *Block* - Drop all packets (include BPDU and normal packets) when the port enters the under attack state. *Shutdown* - Shut down the port when the port enters the under attack state.

Click **Apply** to implement changes made.

ARP Spoofing Prevention Settings

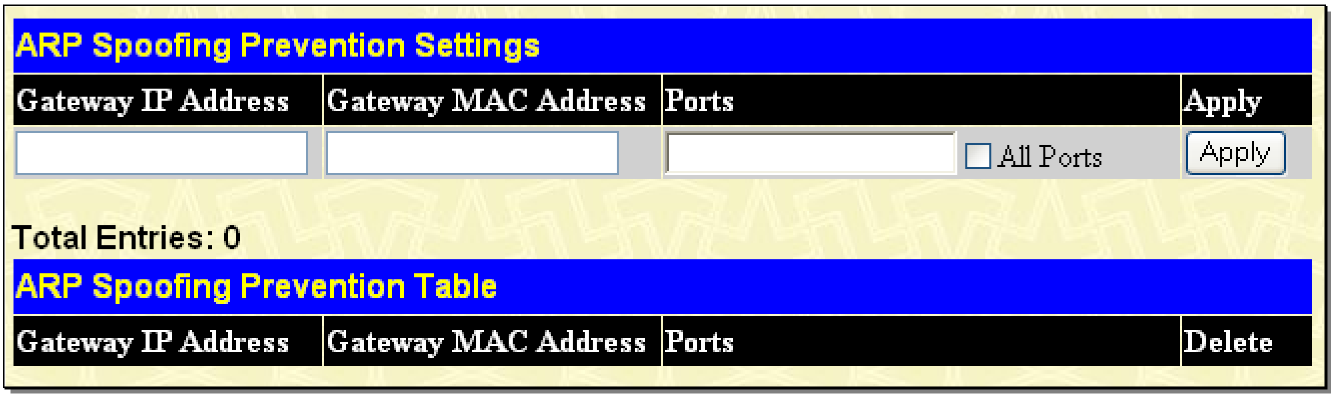
ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send fake or spoofed ARP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

To prevent an ARP spoofing attack, Packet Content ACL is used to block the invalid ARP packets which contain a faked gateway’s MAC and IP binding. Packet Content ACL can inspect any specified content in the first 48 bytes of a packet. 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 HEX format.

The configuration logic is as follows:

- The traffic can only pass through the Switch if the ARP entry matches a source MAC address in the Ethernet frame, the sender MAC address, or the sender IP address in the ARP protocol.
- The Switch will deny all other ARP packets which claim they are from the gateway’s IP.

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



ARP Spoofing Prevention Settings

Gateway IP Address	Gateway MAC Address	Ports	Apply
		□ All Ports	Apply

Total Entries: 0

ARP Spoofing Prevention Table

Gateway IP Address	Gateway MAC Address	Ports	Delete

Figure 7- 43. ARP Spoofing Prevention Settings window

The following parameters can be configured:

Parameter	Description
Gateway IP Address	Enter the gateway IP address.
Gateway MAC Address	Enter the gateway MAC address.
Ports	Enter the port or range of ports to be configured. Alternatively, tick the All Ports check box to configure all of the ports.

Click **Apply** to implement changes made.

Access Authentication Control

The TACACS/XTACACS/TACACS+/RADIUS commands allow users to secure access to the Switch using the TACACS/XTACACS/TACACS+/RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS/XTACACS/TACACS+/RADIUS authentication is enabled on the Switch, it will contact a TACACS/XTACACS/TACACS+/RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- Extended TACACS (XTACACS) - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- TACACS+ (Terminal Access Controller Access Control System plus) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS/XTACACS/TACACS+/RADIUS security function to work properly, a TACACS/XTACACS/TACACS+/RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS/XTACACS/TACACS+/RADIUS server to verify, and the server will respond with one of three messages:

- The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- The server will not accept the username and password and the user is denied access to the Switch.
- The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS/XTACACS/TACACS+/RADIUS/local/none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

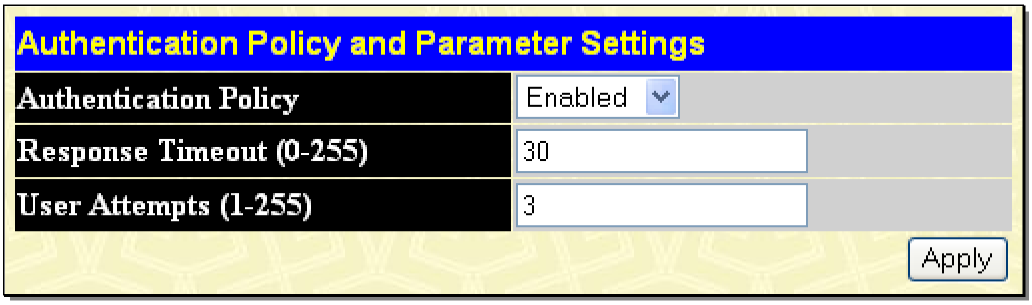
Please note that users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.

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 view this window, click **Security > Access Authentication Control > Authentication Policy and Parameter Settings**, as shown below:



Authentication Policy and Parameter Settings

Authentication Policy	Enabled
Response Timeout (0-255)	30
User Attempts (1-255)	3

Figure 7- 44. Authentication Policy and Parameter Settings window

The following parameters can be set:

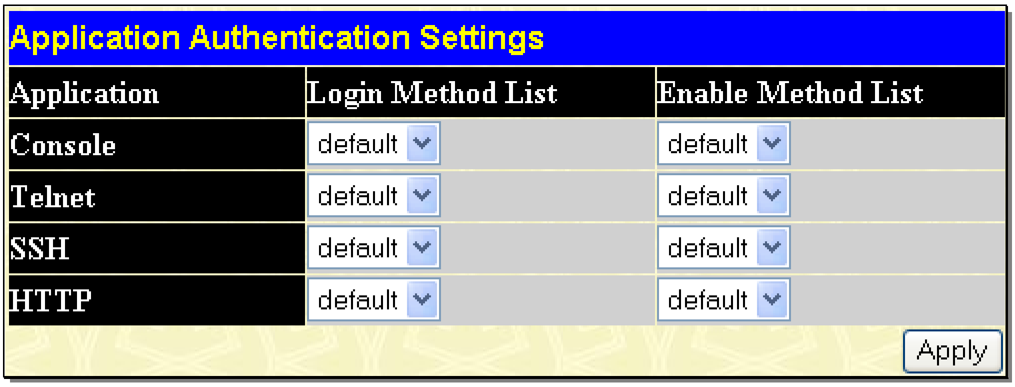
Parameters	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds.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

Click **Apply** to implement changes made.

Application Authentication Settings

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

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



Application Authentication Settings

Application	Login Method List	Enable Method List
Console	default	default
Telnet	default	default
SSH	default	default
HTTP	default	default

Figure 7- 45. Application Authentication Settings window

The following parameters can be set:

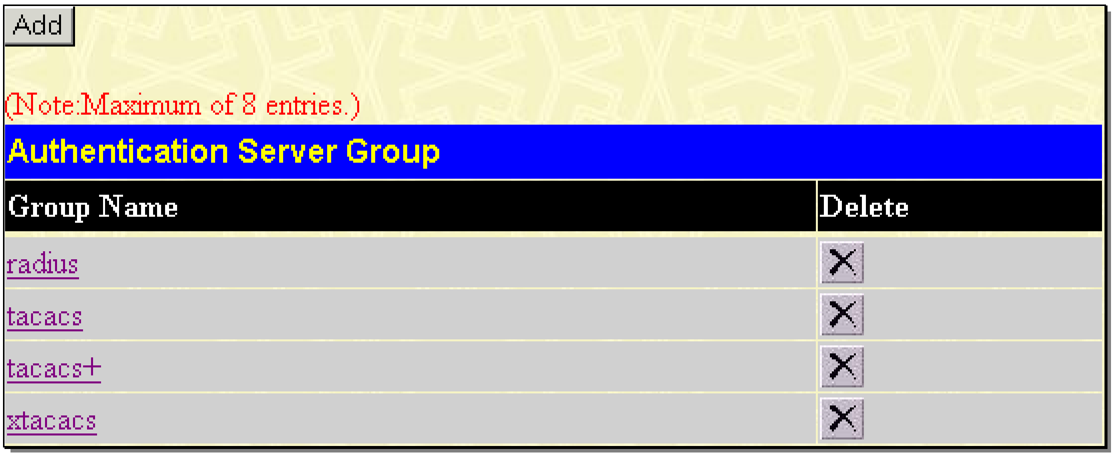
Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH and the WEB (HTTP) application.
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 four 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 this window, click **Security** > **Access Authentication Control** > **Authentication Server Group**, as shown below:



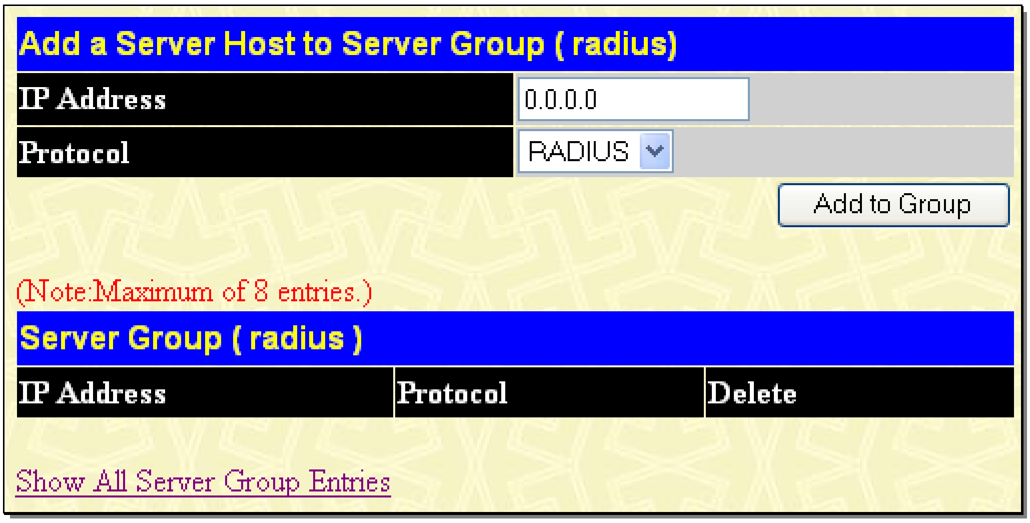
(Note:Maximum of 8 entries.)

Authentication Server Group

Group Name	Delete
radius	☒
tacacs	☒
tacacs+	☒
xtacacs	☒

Figure 7- 46. Authentication Server Group window

This window 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.



Add a Server Host to Server Group (radius)

IP Address	0.0.0.0
Protocol	RADIUS

(Note:Maximum of 8 entries.)

Server Group (radius)

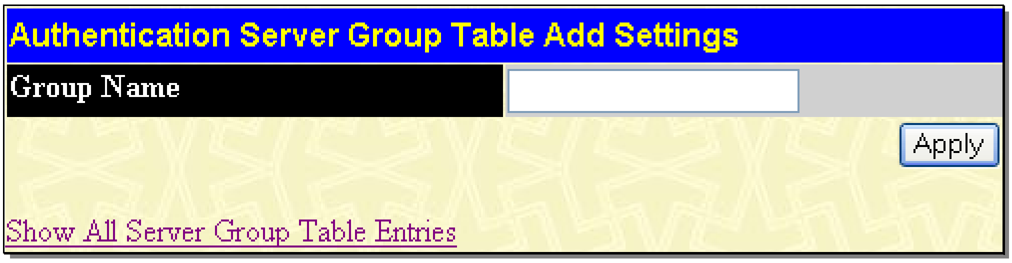
IP Address	Protocol	Delete

Show All Server Group Entries

Figure 7- 47. Add a Server Host to Server Group (radius) 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.

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.



Authentication Server Group Table Add Settings

Group Name	

Show All Server Group Table Entries

Figure 7- 48. Authentication Server Group Table Add Settings window

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.

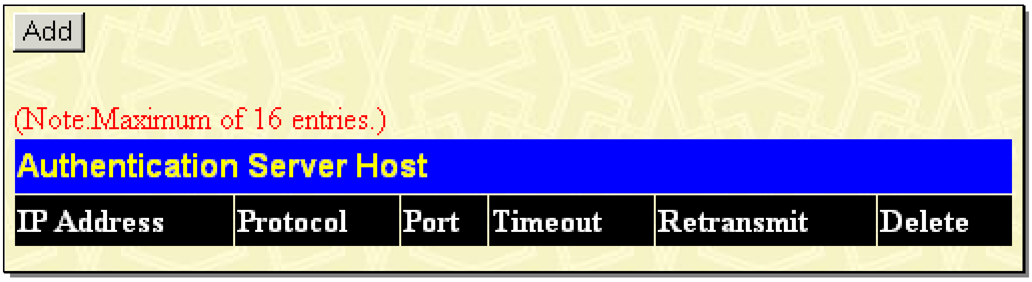
NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

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 this window, click **Security** > **Access Authentication Control** > **Authentication Server Host**, as shown below:



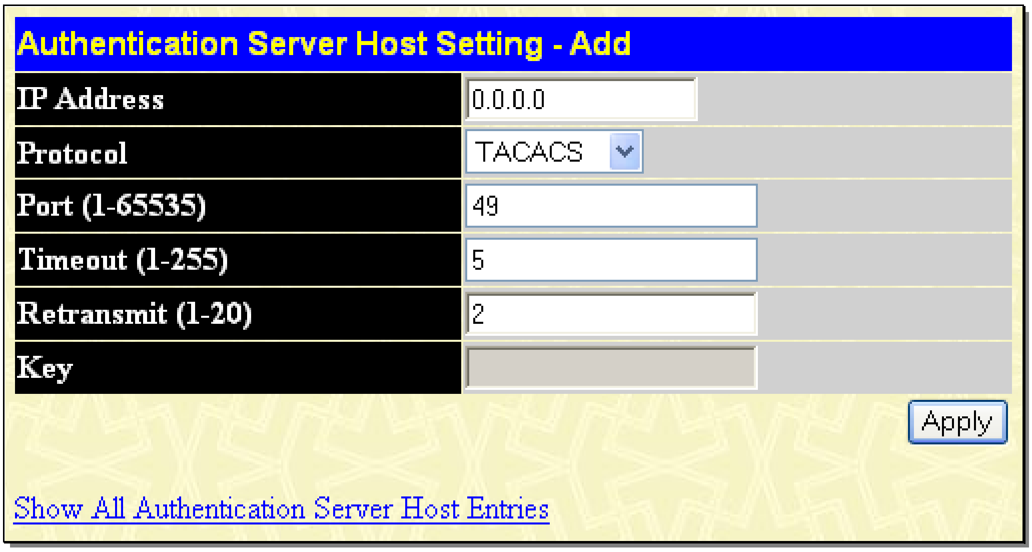
(Note:Maximum of 16 entries.)

Authentication Server Host

IP Address	Protocol	Port	Timeout	Retransmit	Delete

Figure 7- 49. Authentication Server Host window

To add an Authentication Server Host, click the **Add** button, revealing the following window:



Authentication Server Host Setting - Add

IP Address	0.0.0.0
Protocol	TACACS
Port (1-65535)	49
Timeout (1-255)	5
Retransmit (1-20)	2
Key	

Show All Authentication Server Host Entries

Figure 7- 50. Authentication Server Host Setting – Add window

To edit an Authentication Server Host, click the IP address hyperlink.

Configure the following parameters to add or edit an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host 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 (1-20)	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.

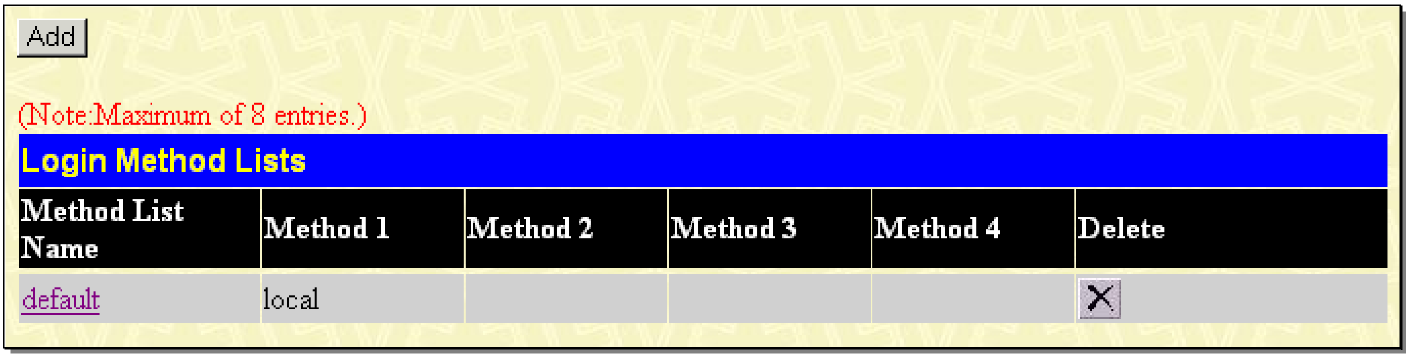
NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other

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.

Successful login using any of these techniques will give the user a "User" privilege only. To upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator. (See the Enable Admin part of this section for more detailed information concerning the Enable Admin command.)

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



(Note:Maximum of 8 entries.)

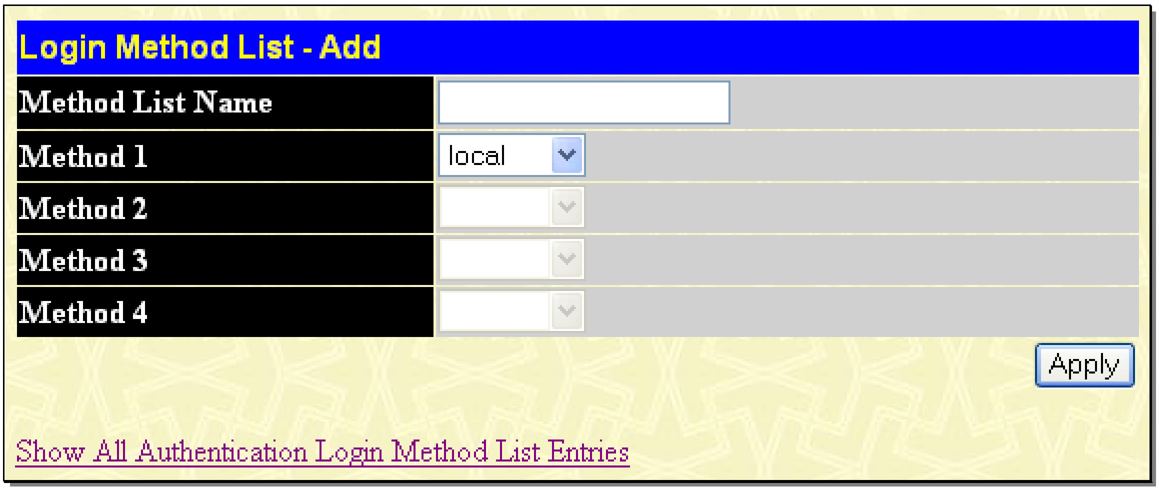
Login Method Lists

Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local				☒

Figure 7- 51. Login Method Lists window

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the ☒ 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:



Login Method List - Add

Method List Name	
Method 1	local
Method 2	
Method 3	
Method 4	

Show All Authentication Login Method List Entries

Figure 7- 52. 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 an authentication to access the Switch.

Enable Method Lists

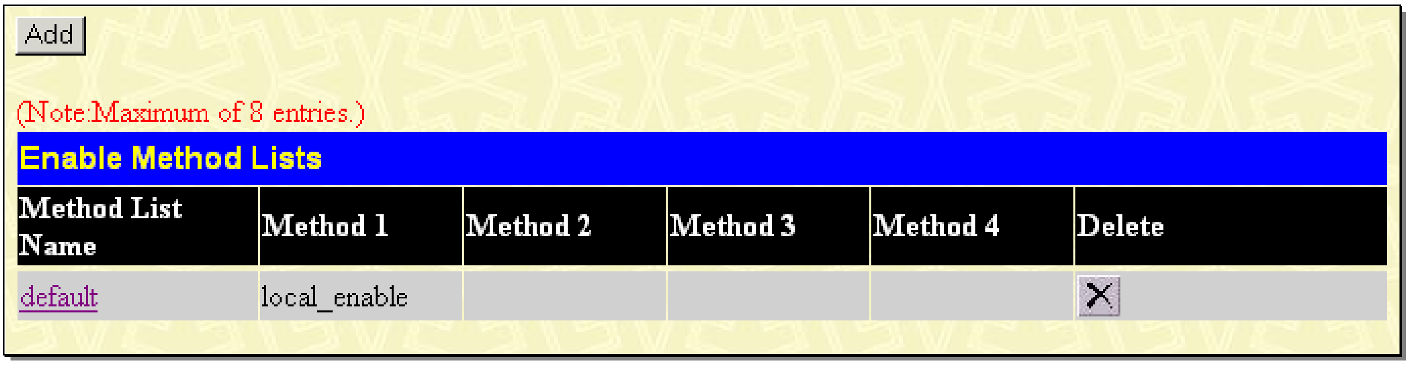
This window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain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

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

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

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

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



(Note:Maximum of 8 entries.)

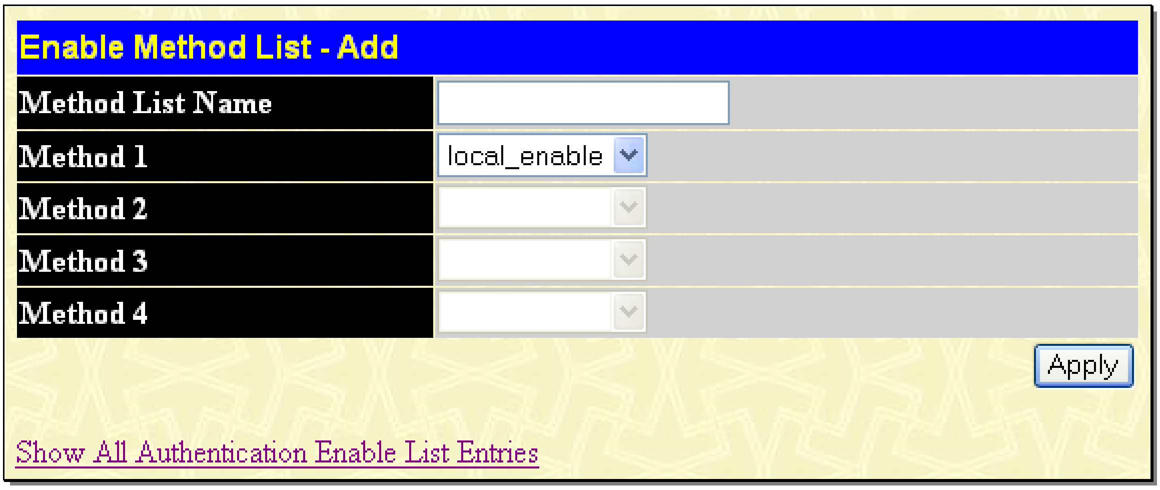
Enable Method Lists

Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local_enable				☒

Figure 7- 53. Enable Method Lists 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:



Enable Method List - Add

Method List Name	
Method 1	local_enable
Method 2	
Method 3	
Method 4	

Figure 7- 54. Enable Method List - Add window

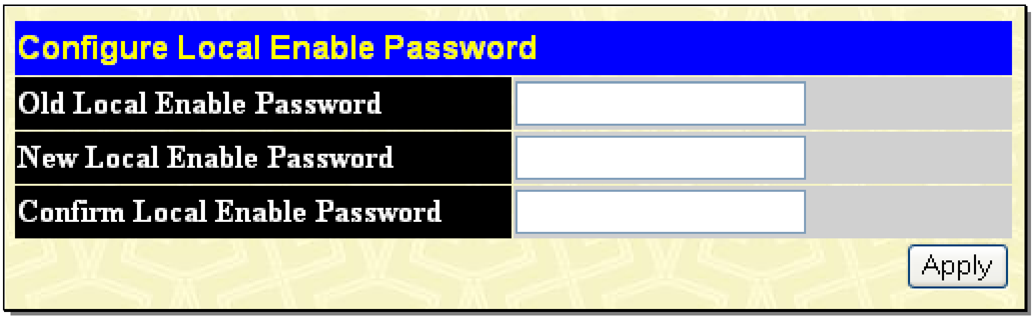
To define an Enable Login Method List, set the following parameters and click **Apply**:

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 an 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 this window, click **Security** > **Access Authentication Control** > **Configure Local Enable Password**, as shown below:


Configure Local Enable Password

Old Local Enable Password	
New Local Enable Password	
Confirm Local Enable Password	

Figure 7- 55. Configure Local Enable Password window

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

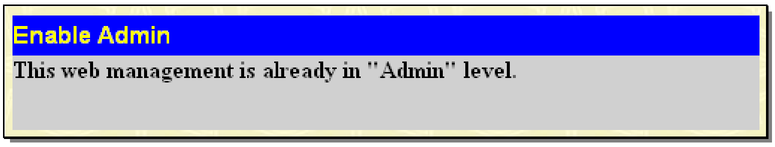
Parameter	Description
Old Local Enable Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level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

Enable Admin

The **Enable Admin** window is for users who have logged on to the Switch on the normal user level, and wish to be promoted to the administrator level. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

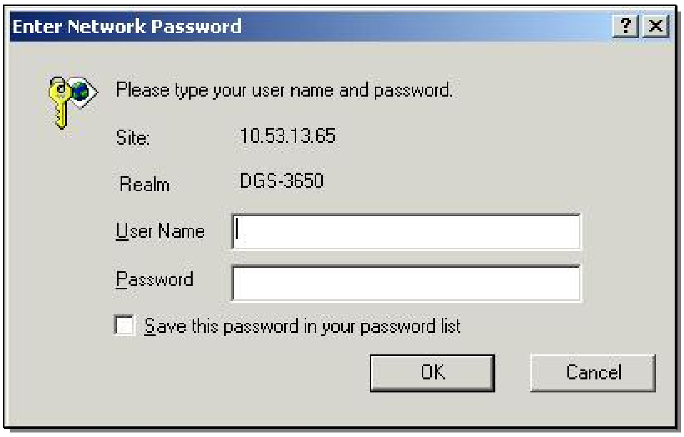
When this window appears, click the **Enable Admin** button revealing a dialog box for the user to enter authentication (password, username). A successful entry will promote the user to Administrator level privileges on the Switch.

To view this window, click **Security** > **Access Authentication Control** > **Enable Admin**, as shown.


Enable Admin

This web management is already in "Admin" level.

Figure 7- 56. Enable Admin window


Enter Network Password

Please type your user name and password.

Site: 10.53.13.65

Realm DGS-3650

User Name

Password

□ Save this password in your password list

Figure 7- 57. Enter Network Password dialog box

RADIUS Accounting Settings

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

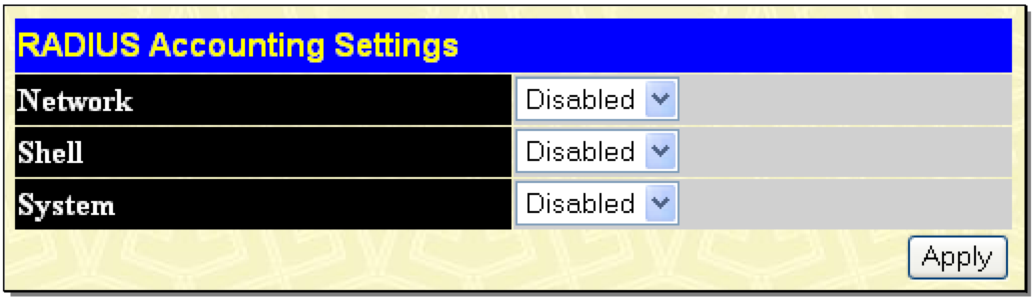
- Account Status Type
- Account Terminate Cause
- Account Authentic
- Account Delay Time
- Account Session Time
- Username
- Service Type
- NAS IP Address
- NAS Identifier
- Calling Station ID

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

- **Network** – When enabled, the Switch will send informational packets to a remote RADIUS server when 802.1X users connect to the physical ports on the switch to access the network. Network accounting only works when 802.1X is enabled
- **Shell** – When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet, or SSH.
- **System** – When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot.

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

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



RADIUS Accounting Settings

Network	Disabled
Shell	Disabled
System	Disabled

Figure 7- 58. RADIUS Accounting Settings window

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.

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 Global Settings window, as seen below. The user may enter up to 1024 MAC addresses locally on the Switch but only 1024 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, 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:

Once this feature is enabled for a port, the Switch will clear the FDB of that port.

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.

A port accepts a maximum of 1024 authenticated MAC addresses in local mode and 4000 MAC addresses in radius mode 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.

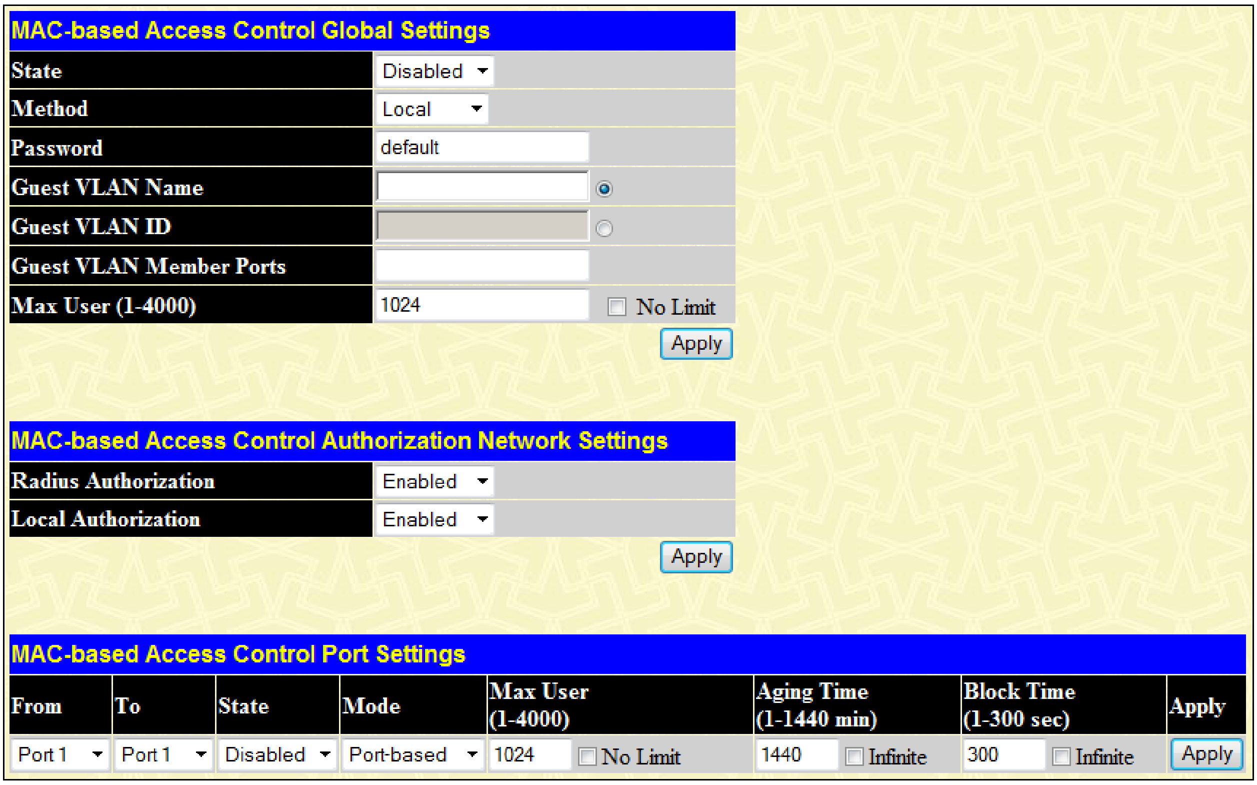
Ports that have been enabled for Link Aggregation, stacking, 802.1X authentication, 802.1X Guest VLAN, Port Security, GVRP or Web-based authentication cannot be enabled for the MAC-based Authentication.

MAC-based Access Control Guest VLAN cannot be a member of a Web-based authentication VLAN.

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 enable these Settings, click **Security > MAC-based Access Control > MAC-based Access Control Global Settings**, as shown below:



MAC-based Access Control Global Settings

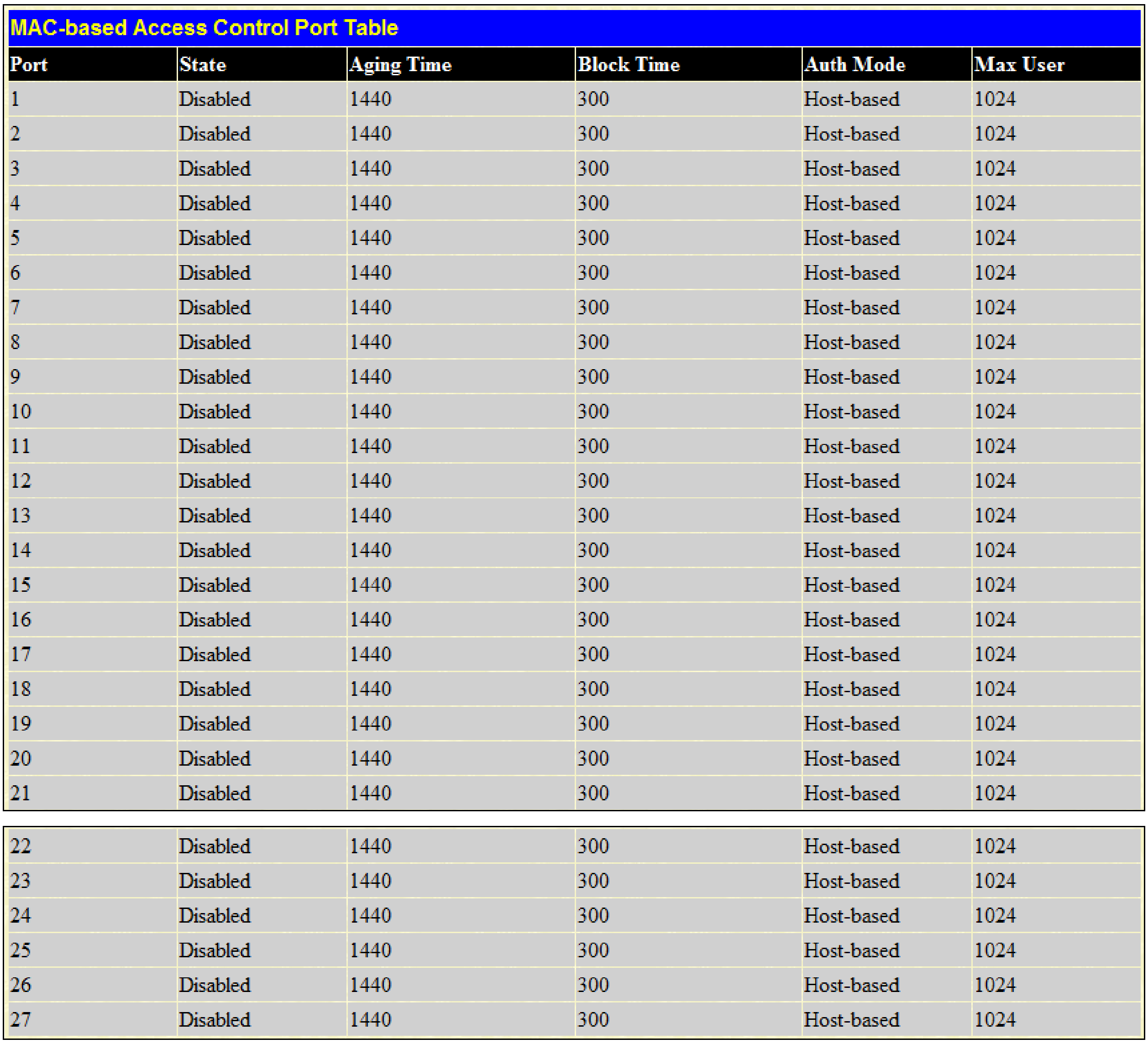
State	Disabled
Method	Local
Password	default
Guest VLAN Name	●
Guest VLAN ID	○
Guest VLAN Member Ports	
Max User (1-4000)	1024 □ No Limit

MAC-based Access Control Authorization Network Settings

Radius Authorization	Enabled
Local Authorization	Enabled

MAC-based Access Control Port Settings

From	To	State	Mode	Max User (1-4000)	Aging Time (1-1440 min)	Block Time (1-300 sec)	Apply
Port 1	Port 1	Disabled	Port-based	1024 □ No Limit	1440 □ Infinite	300 □ Infinite	Apply



MAC-based Access Control Port Table

Port	State	Aging Time	Block Time	Auth Mode	Max User
1	Disabled	1440	300	Host-based	1024
2	Disabled	1440	300	Host-based	1024
3	Disabled	1440	300	Host-based	1024
4	Disabled	1440	300	Host-based	1024
5	Disabled	1440	300	Host-based	1024
6	Disabled	1440	300	Host-based	1024
7	Disabled	1440	300	Host-based	1024
8	Disabled	1440	300	Host-based	1024
9	Disabled	1440	300	Host-based	1024
10	Disabled	1440	300	Host-based	1024
11	Disabled	1440	300	Host-based	1024
12	Disabled	1440	300	Host-based	1024
13	Disabled	1440	300	Host-based	1024
14	Disabled	1440	300	Host-based	1024
15	Disabled	1440	300	Host-based	1024
16	Disabled	1440	300	Host-based	1024
17	Disabled	1440	300	Host-based	1024
18	Disabled	1440	300	Host-based	1024
19	Disabled	1440	300	Host-based	1024
20	Disabled	1440	300	Host-based	1024
21	Disabled	1440	300	Host-based	1024
22	Disabled	1440	300	Host-based	1024
23	Disabled	1440	300	Host-based	1024
24	Disabled	1440	300	Host-based	1024
25	Disabled	1440	300	Host-based	1024
26	Disabled	1440	300	Host-based	1024
27	Disabled	1440	300	Host-based	1024

Figure 7- 59. MAC-based Access Control Global Settings window

The following parameters may be viewed or set:

Parameter	Description
MAC-based Access Control Global Settings	
State	Use the pull-down menu to globally enable or disable the MAC-based Access Control function on the Switch.
Method	Use the pull-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based Access Control. This MAC address list can be configured in the MAC-based Access Control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
Guest VLAN Name	Select the method of identification, Guest VLAN name, before entering the name of the Guest VLAN being used for this function.
Guest VLAN ID	Select the method of identification, Guest VLAN ID, before entering the ID of the Guest VLAN being used for this function.
Guest VLAN Member Ports	Enter the list of ports that you wish to configure for the Guest VLAN.
Max User (1-4000)	Enter the number of maximum users from *1* to *4000*. The default value is *1024*.
MAC-based Access Control Authorization Network Settings	
RADIUS Authorization	Enable or disable RADIUS authorization.
Local Authorization	Enable or disable local authorization.
MAC-based Access Control Port Settings	
Unit	Enter the unit to configure.
From/To	Enter the Port range.
State	Use the pull-down menu to enable or disable the MAC-based Access Control function on individual ports.
Mode	*Port-based*: In this mode, if one of the attached hosts is successfully authorized, all hosts on the same port will be granted access to the network. If the port authorization fails, this port will continue authenticating. *Host-based*: In this mode, every user can individually authenticate and access the network.
Max User (1-4000)	Enter the number of maximum users from *1* to *4000*. Alternatively, tick the No Limit check box.
Aging Time (1-1440 min)	A time period (configurable per port) between 1-1440 minutes, during which an authenticated host will stay in an authenticated state. When the aging time has expired, the host will be moved back to an unauthenticated state. Alternatively, tick the Infinite check box.When aging time is set to infinite, it will disable the aging time.

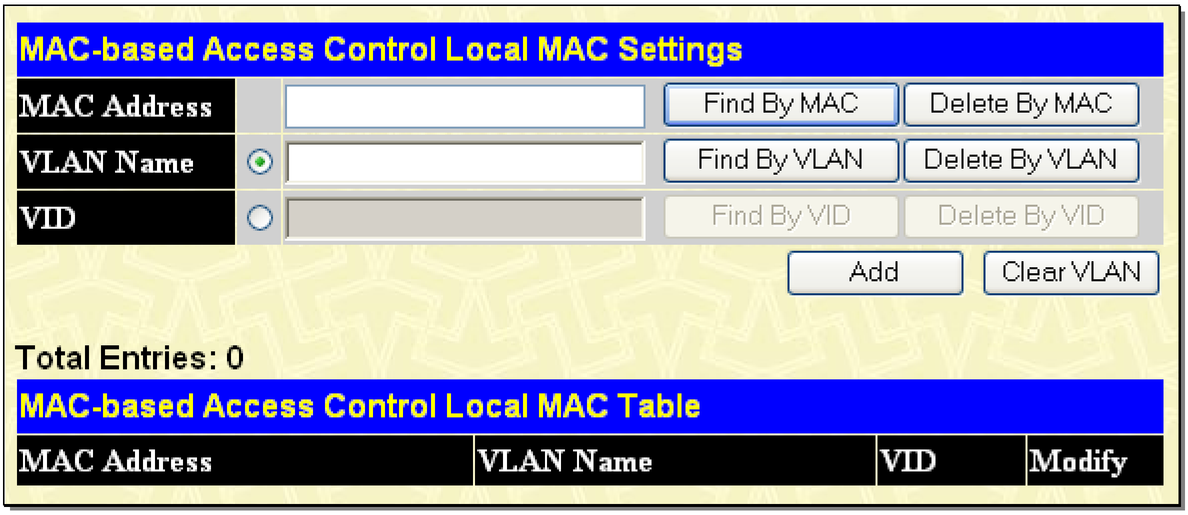
Block Time (1-300 sec)	If a host fails to pass the authentication it will be blocked for a period of time referred to as hold time (per port configurable). During this time, this host can't proceed to the authenticating process (unless the user clears the database manually). As a result, this hold mechanism can prevent the switch from frequent authentication which consumes too much computing power. Alternatively, tick the Infinite check box.

Click **Apply** to implement settings.

MAC-based Access Control Local MAC Settings

The following window is used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 1024 MAC addresses to be authenticated using the local method configured here.

To enable these settings, click **Security** > **MAC-based Access Control** > **MAC-based Access Control Local MAC Settings**, as shown below:



Total Entries: 0

MAC-based Access Control Local MAC Table

MAC Address	VLAN Name	VID	Modify

Figure 7- 60. MAC-based Access Control Local MAC Settings window

To set the following parameters:

Parameter	Description
MAC Address	To search for a previously configured MAC address, enter the address and click **Find By MAC**. If you want to add the entry to the MAC-based Access Control Local MAC Table, click the **Add** button. To delete an entry click the **Delete By MAC** button.
VLAN Name/VID	To search for a previously configured VLAN Name/VLAN ID, enter the information and click **Find By VLAN**. If you want to add the entry to the MAC-based Access Control Local MAC Table, click the **Add** button. To delete an entry click the **Delete By VLAN** button.

To edit an entry click the corresponding **Modify** button.

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 will drop all ARP and 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 initially stop all ingress 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 stop accepting all 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.

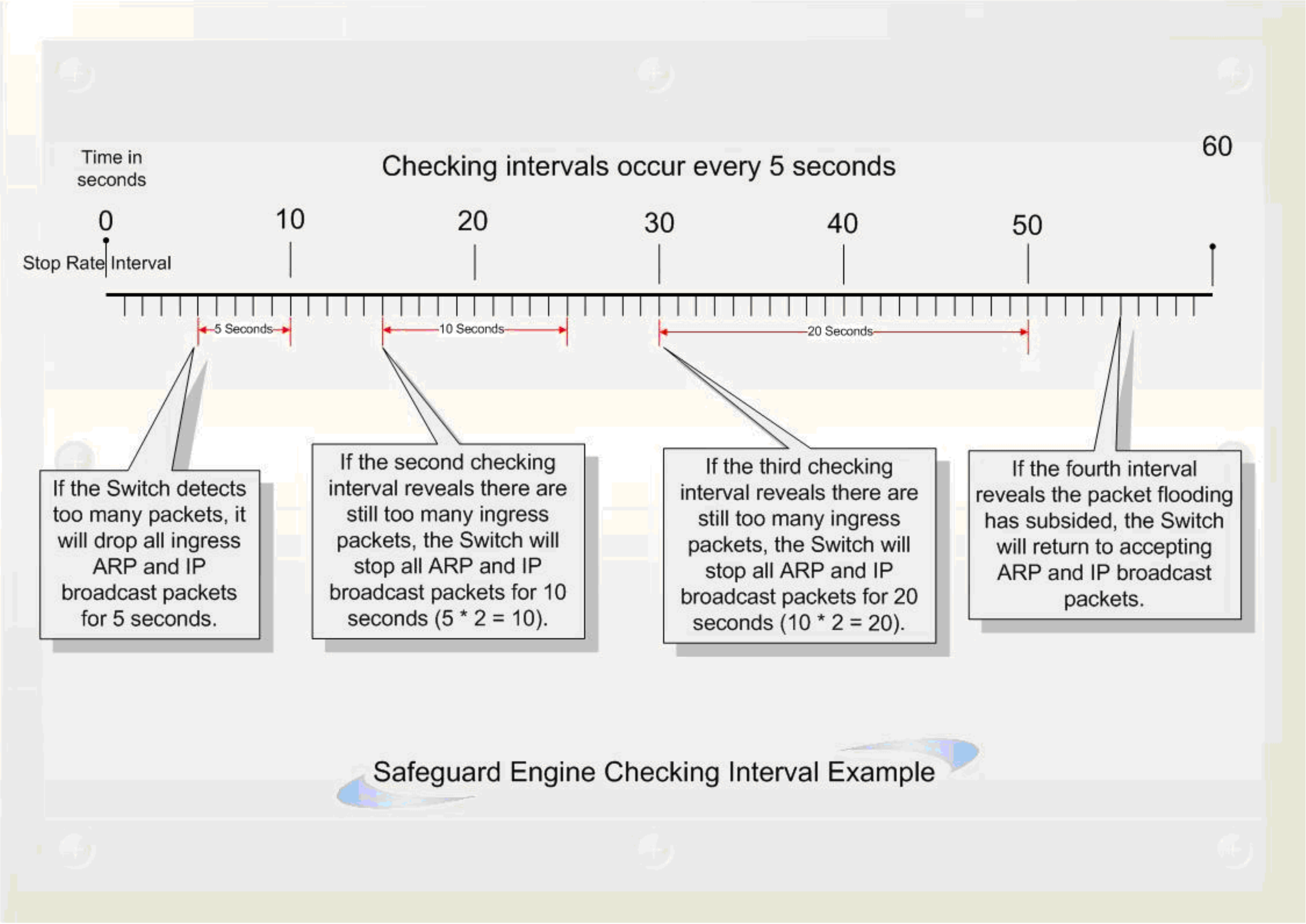

Time in seconds
Checking intervals occur every 5 seconds
0
10
20
30
40
50
60
Stop Rate Interval
5 Seconds
10 Seconds
20 Seconds
If the Switch detects too many packets, it will drop all ingress ARP and IP broadcast packets for 5 seconds.
If the second checking interval reveals there are still too many ingress packets, the Switch will stop all ARP and IP broadcast packets for 10 seconds (5 * 2 = 10).
If the third checking interval reveals there are still too many ingress packets, the Switch will stop all ARP and IP broadcast packets for 20 seconds (10 * 2 = 20).
If the fourth interval reveals the packet flooding has subsided, the Switch will return to accepting ARP and IP broadcast packets.
Safeguard Engine Checking Interval Example

Figure 7- 61. Safeguard Engine example

For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will discard 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 dropping ARP and IP broadcast packets will return to 5 seconds and the process will resume.

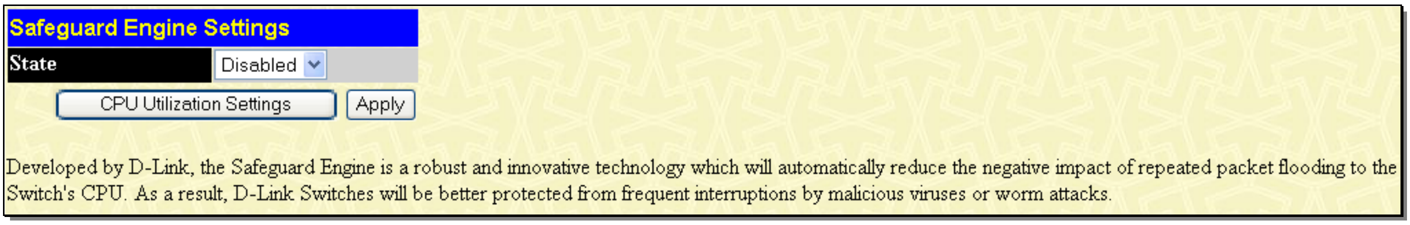
Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.

NOTICE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

To window is used to enable Safeguard Engine or configure advanced Safeguard Engine settings for the Switch.

To configure the Safeguard Engine settings, click **Security** > **Safeguard Engine** > **Safeguard Engine Settings**, as shown below:,



Safeguard Engine Settings

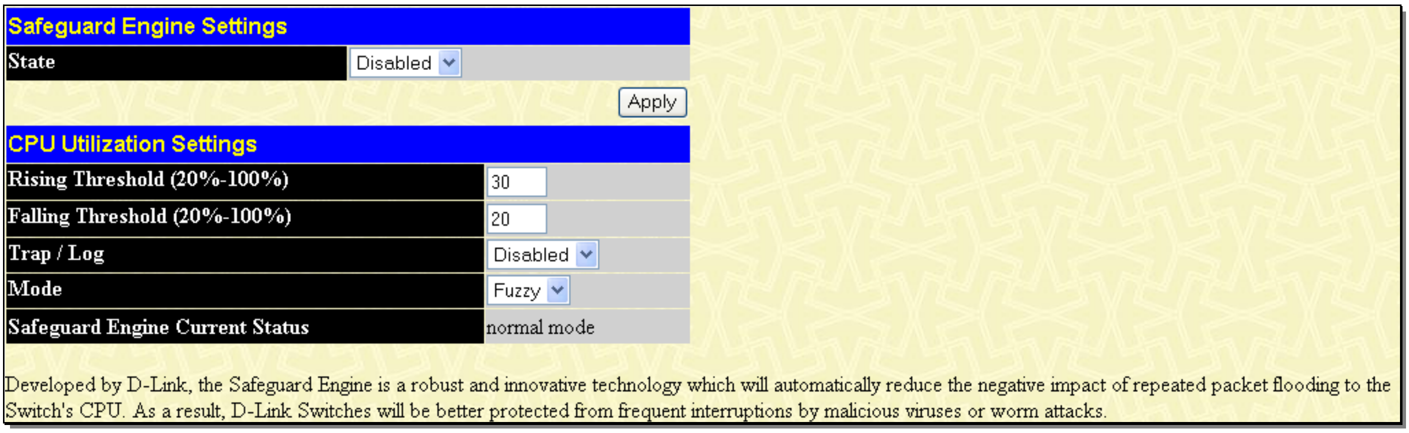
State	Disabled

Developed by D-Link, the Safeguard Engine is a robust and innovative technology which will automatically reduce the negative impact of repeated packet flooding to the Switch's CPU. As a result, D-Link Switches will be better protected from frequent interruptions by malicious viruses or worm attacks.

Figure 7- 62. Safeguard Engine Settings window

To enable the Safeguard Engine option, select *Enabled* with the drop-down State menu and click the **Apply** button.

To configure the advanced settings for Safeguard Engine, click the **CPU Utilization Settings** button to view the following window.



Safeguard Engine Settings

State	Disabled

CPU Utilization Settings

Rising Threshold (20%-100%)	30
Falling Threshold (20%-100%)	20
Trap / Log	Disabled
Mode	Fuzzy
Safeguard Engine Current Status	normal mode

Developed by D-Link, the Safeguard Engine is a robust and innovative technology which will automatically reduce the negative impact of repeated packet flooding to the Switch's CPU. As a result, D-Link Switches will be better protected from frequent interruptions by malicious viruses or worm attacks.

Figure 7- 63. Safeguard Engine Settings window

To configure the following parameters:

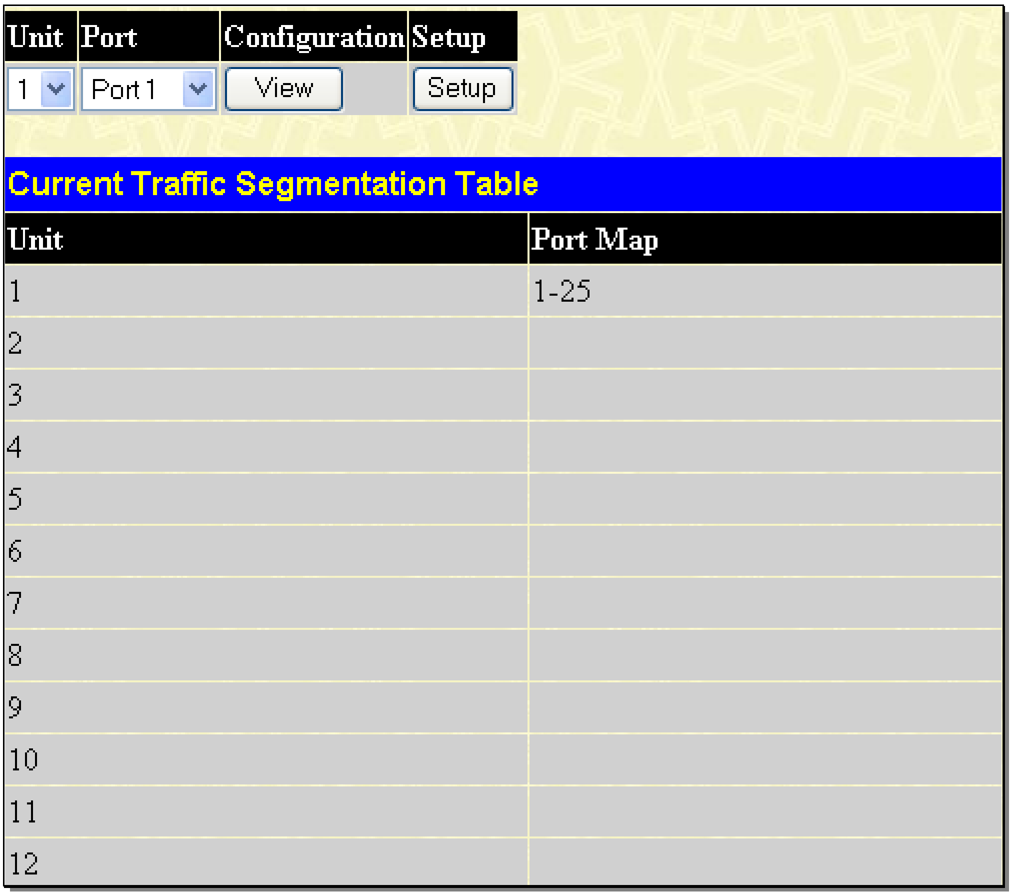
Parameter	Description
State	Use the pull-down menu to globally enable or disable Safeguard Engine settings for the Switch.
Rising Threshold (20%-100%)	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Safeguard Engine state, based on the parameters provided in this window.
Falling Threshold (20%-100%)	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.
Trap/Log	Use the pull-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select: *Fuzzy* – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. *Strict* – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided.

	The default setting is *Fuzzy* mode.

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.

To view the **Traffic Segmentation** window, click **Security** > **Traffic Segmentation**, as shown below:



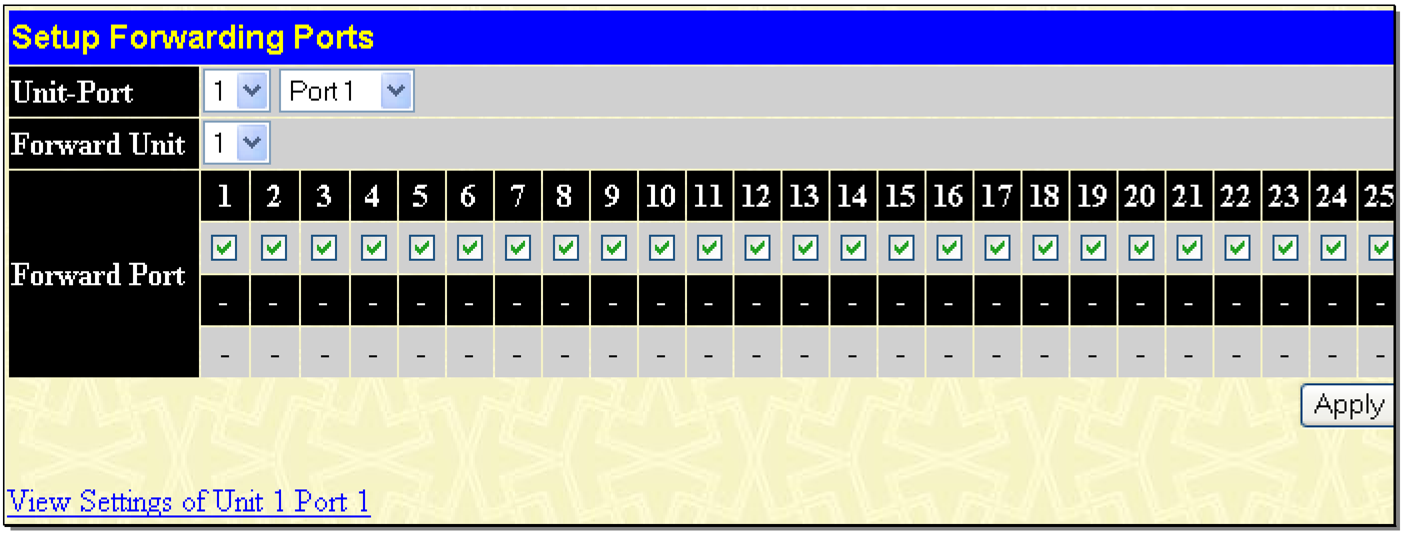
Unit	Port	Configuration	Setup
1	Port 1	View	Setup

Current Traffic Segmentation Table

Unit	Port Map
1	1-25
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Figure 7- 64. Current Traffic Segmentation Table window

This window allows you to view which port on a given switch will be allowed to forward packets to other ports on that switch. Select the unit you wish to configure and a port number from the drop down menu and click **View** 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.



Setup Forwarding Ports

Unit-Port	1	Port 1
Forward Unit	1	

Forward Port	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
	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Apply

View Settings of Unit 1 Port 1

Figure 7- 65. Setup Forwarding Ports window

The user may set the following parameters:

Parameter	Description
Unit/Port	Use the drop-down menu to select the desired unit and port to transmit packets.
Forward Port	Tick the check boxes to select which of the ports on the Switch will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

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

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 ciphersuite 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:
    a. **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.
    b. **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 that 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

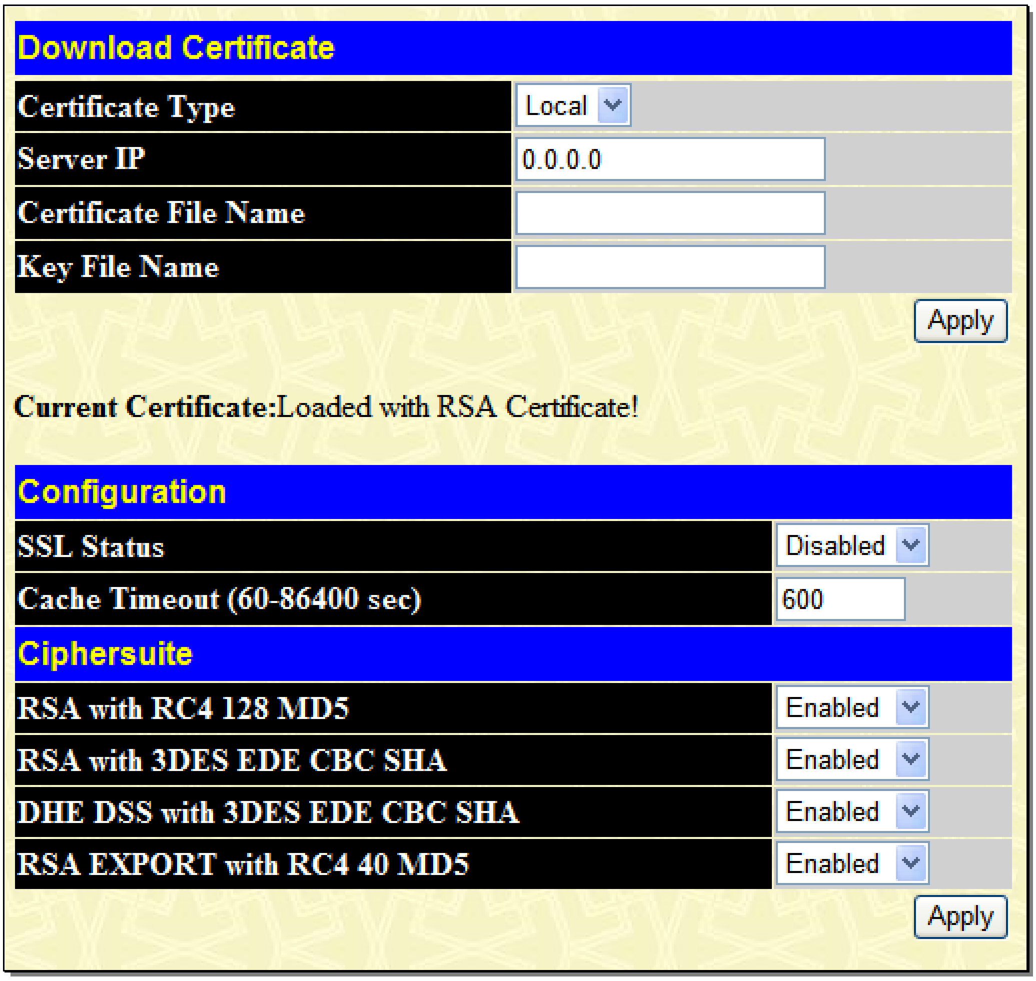
This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the 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**, as shown below:



Download Certificate

Certificate Type	Local
Server IP	0.0.0.0
Certificate File Name	
Key File Name	

Current Certificate:Loaded with RSA Certificate!

Configuration

SSL Status	Disabled
Cache Timeout (60-86400 sec)	600

Ciphersuite

RSA with RC4 128 MD5	Enabled
RSA with 3DES EDE CBC SHA	Enabled
DHE DSS with 3DES EDE CBC SHA	Enabled
RSA EXPORT with RC4 40 MD5	Enabled

Figure 7- 66. Download Certificate window

To download certificates, set the following parameters and click **Apply**.

Parameter	Description
Certificate Type	Enter the type of certificate to be downloaded. 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 sec)	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.
DHE DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is *Enabled* by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is *Enabled* by default.

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 ***DGS-3600 Series CLI Reference Guide***, 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:

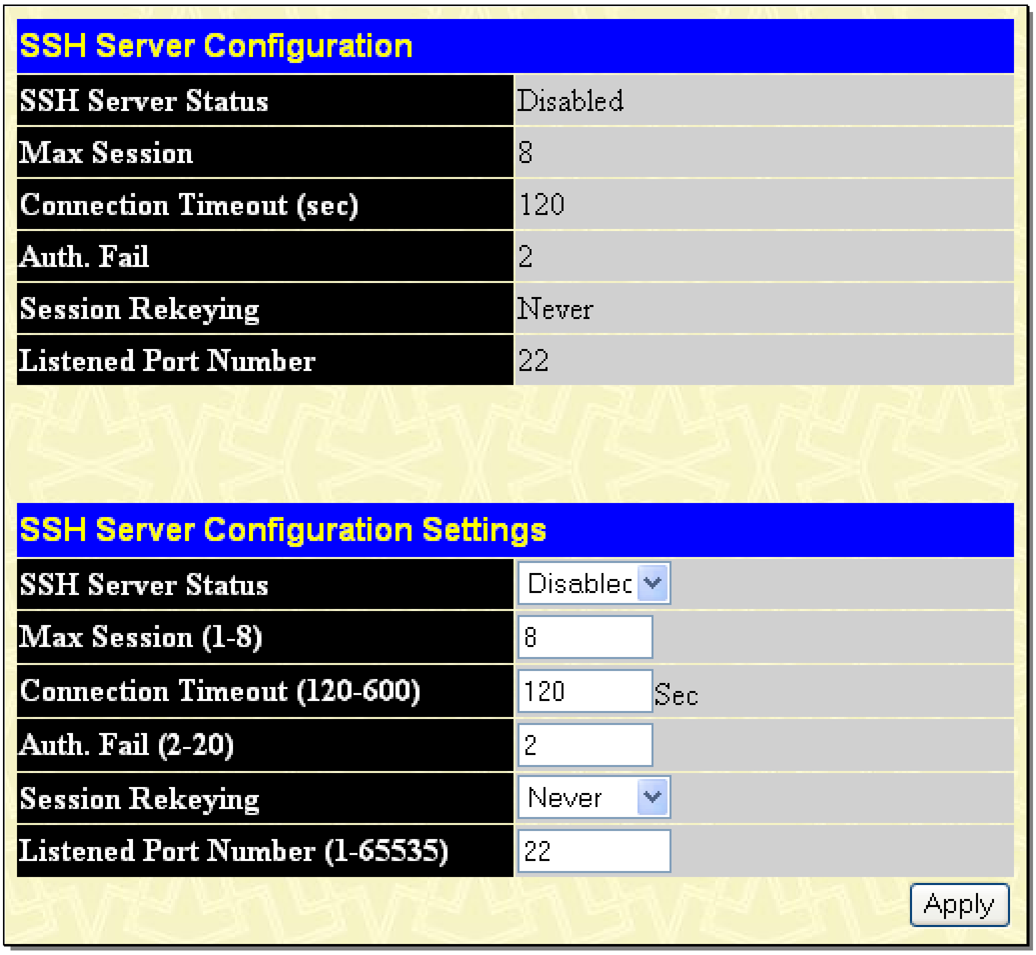
1. Create a user account with admin-level access using the User Accounts window in the Security Management folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication 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.

To view this window, click **Security > SSH > SSH Server Configuration**, as shown below



SSH Server Configuration	
SSH Server Status	Disabled
Max Session	8
Connection Timeout (sec)	120
Auth. Fail	2
Session Rekeying	Never
Listened Port Number	22

SSH Server Configuration Settings	
SSH Server Status	Disablec
Max Session (1-8)	8
Connection Timeout (120-600)	120 Sec
Auth. Fail (2-20)	2
Session Rekeying	Never
Listened Port Number (1-65535)	22

Figure 7- 67. SSH Server Configuration window

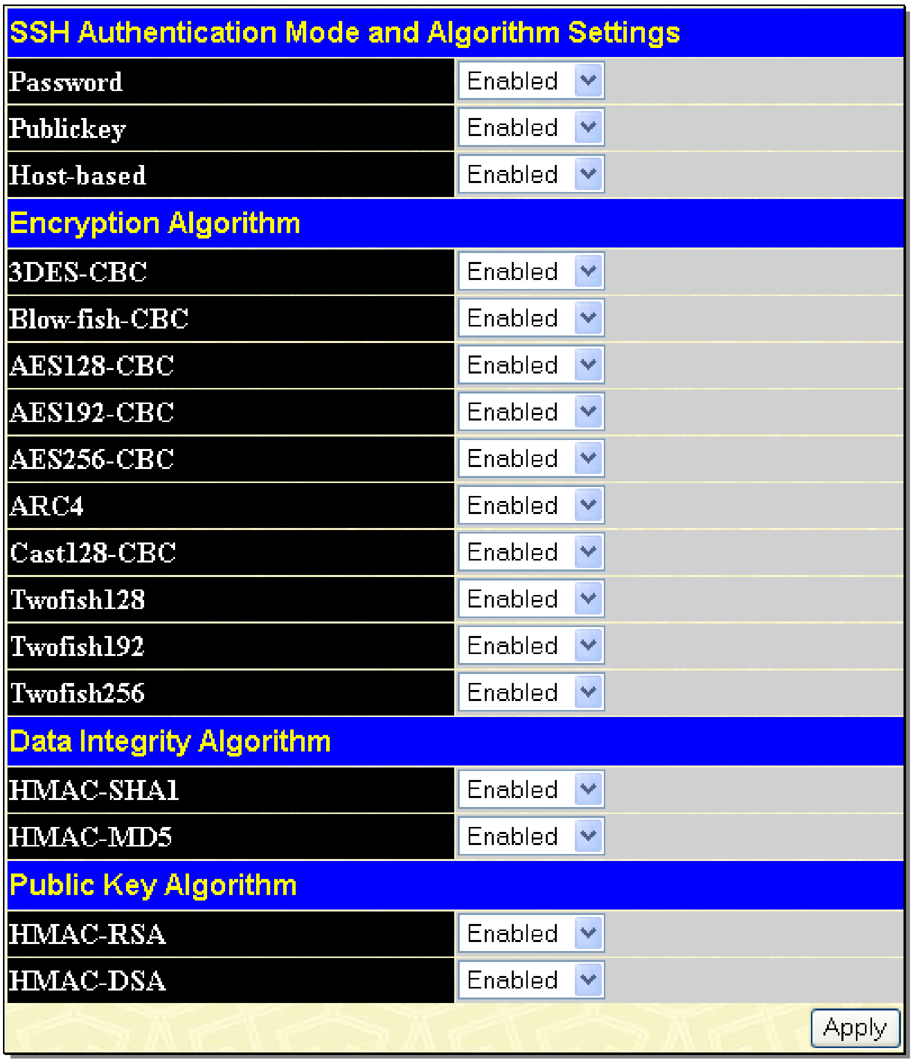
To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

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*.
Connection Timeout (120-600)	Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *120* seconds.
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*.
Listened Port Number (1-65535)	This displays the virtual port number to be used with this feature. The common port number for SSH is 22.

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 view this window, click **Security > SSH > SSH Authentication Mode and Algorithm Settings**, as shown.



SSH Authentication Mode and Algorithm Settings

Password	Enabled
Publickey	Enabled
Host-based	Enabled
Encryption Algorithm	
3DES-CBC	Enabled
Blow-fish-CBC	Enabled
AES128-CBC	Enabled
AES192-CBC	Enabled
AES256-CBC	Enabled
ARC4	Enabled
Cast128-CBC	Enabled
Twofish128	Enabled
Twofish192	Enabled
Twofish256	Enabled
Data Integrity Algorithm	
HMAC-SHA1	Enabled
HMAC-MD5	Enabled
Public Key Algorithm	
HMAC-RSA	Enabled
HMAC-DSA	Enabled

Figure 7- 68. SSH Authenticate Mode and Algorithm Settings 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*.

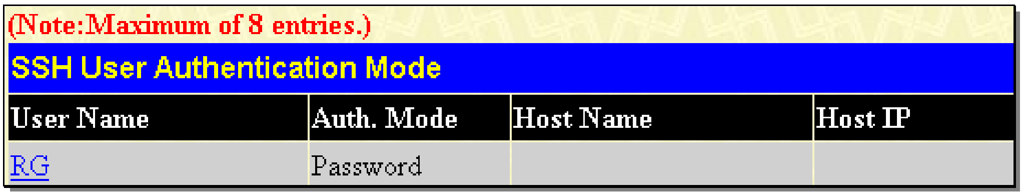
AES192-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
AES256-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. 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 Mode

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

To view this window, click **Security > SSH > SSH User Authentication Mode**, as shown.



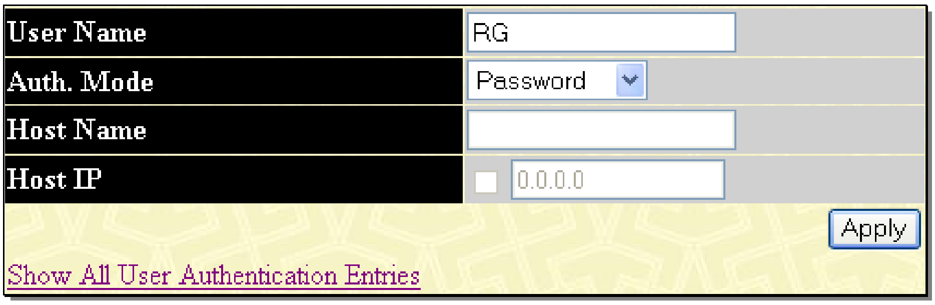
(Note:Maximum of 8 entries.)

SSH User Authentication Mode

User Name	Auth. Mode	Host Name	Host IP
RG	Password		

Figure 7- 69. SSH User Authenticate Mode window

In the example window to the right, the User Account "admin" has been previously set using the User Accounts window in the **Administration** 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.



User Name	RG
Auth. Mode	Password
Host Name	
Host IP	□ 0.0.0.0

Figure 7- 70. SSH User 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 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* – Displays an alphanumeric string of no more than 31 characters to identify the remote SSH user. *Host IP* – Displays the corresponding IP address of the SSH user. *Password* – This parameter should be chosen 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 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.

Compound Authentication

Modern networks employ many authentication methods. The Compound Authentication methods supported by this Switch include 802.1X, MAC-based Access Control (MAC), Web-based Access Control (WAC), Japan Web-based Access Control (JWAC), and IP-MAC-Port Binding (IMPB). The Compound Authentication feature allows clients running different authentication methods to connect to the network using the same switch port.

The Compound Authentication feature can be implemented using one of the following modes:

Any (MAC, 802.1X or WAC) Mode

In the diagram on the right, the Switch port has been configured to allow clients to authenticate using 802.1X, MAC, or WAC. When a client tries to connect to the network, the Switch will try to authenticate the client using one of these methods and if the client passes, it will be granted access to the network.

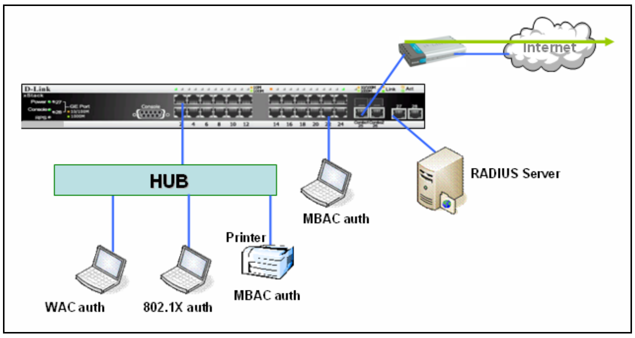


Figure 7- 71. Any Mode example

802.1X & IMPB Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table before trying one of the supported authentication methods. The IMPB Table is used to create a “white list” that checks if the IP streams being sent by authorized hosts have been granted or not. In the above diagram the Switch port has been configured to allow clients to authenticate using 802.1X. If the client is in the IMPB table and tries to connect to the network using this authentication method and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

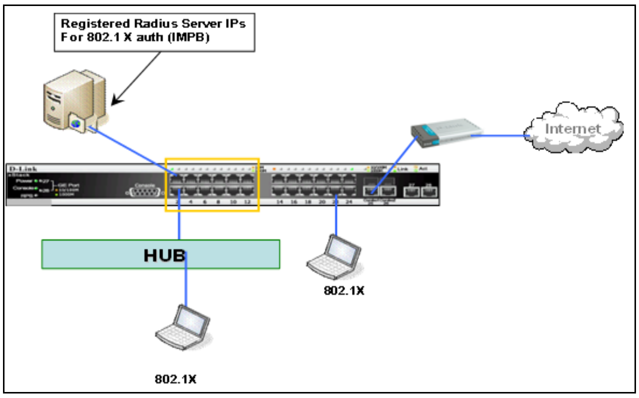


Figure 7- 72. 802.1X & IMPB Mode example

IMPB & WAC/JWAC Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table before trying one of the supported authentication methods. The IMPB Table is used to create a ‘white-list’ that checks if the IP streams being sent by authorized hosts have been granted or not. In the above diagram, the Switch port has been configured to allow clients to authenticate using either WAC or JWAC. If the client is in the IMPB table and tries to connect to the network using either of these supported authentication methods and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

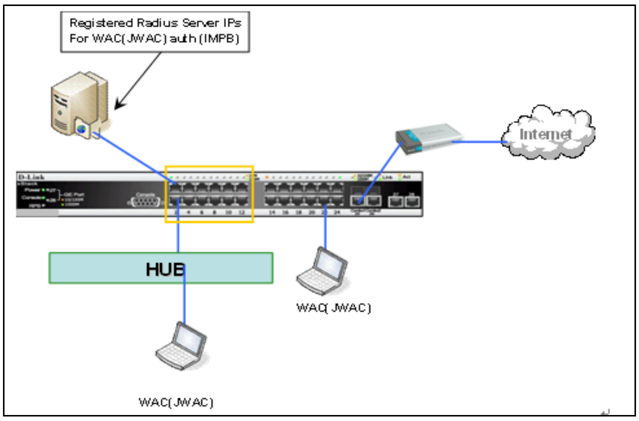
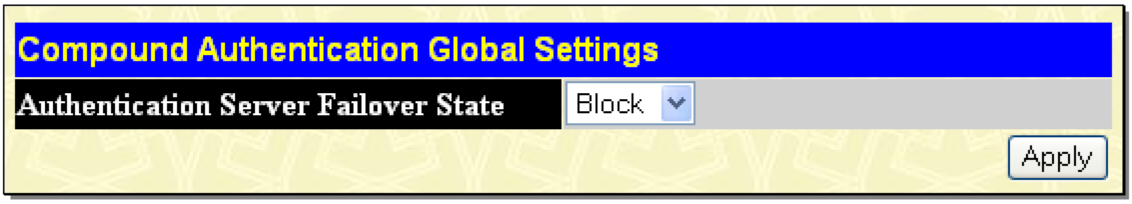


Figure 7- 73. IMPB & WAC/JWAC Mode example

Compound Authentication Global Settings

To view this window, click **Security** > **Compound Authentication** > **Compound Authentication Global Settings**, as shown below:



Compound Authentication Global Settings

Authentication Server Failover State: Block

Figure 7- 74. Compound Authentication Global Settings window

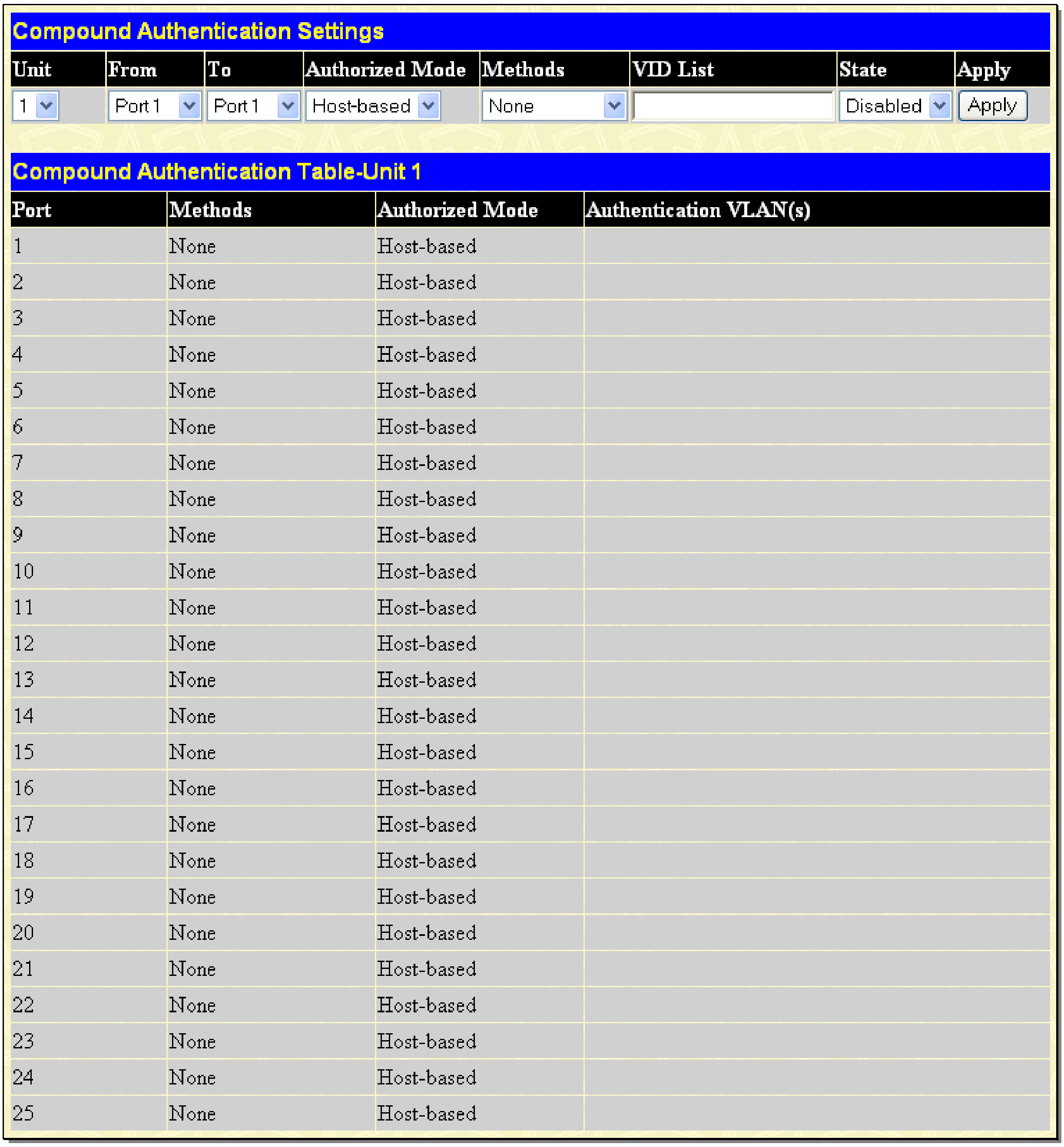
The following parameters may be set:

Parameter	Description
Block	If *Block* is selected, the client is always regarded as an un-authenticated.
Local	If *Local* is selected, the Switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated. Otherwise, the client is regarded as an authenticated.
Permit	If *Permit* is selected, the client is always regarded as an authenticated. If the guest VLAN enabled, the client will stay at the guest VLAN, otherwise, it will stay at the original VLAN.

Compound Authentication Settings

This window is used to configure the authorization mode and authentication method of individual ports.

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



Compound Authentication Settings

Unit	From	To	Authorized Mode	Methods	VID List	State	Apply
1	Port 1	Port 1	Host-based	None		Disabled	Apply

Compound Authentication Table-Unit 1

Port	Methods	Authorized Mode	Authentication VLAN(s)
1	None	Host-based	
2	None	Host-based	
3	None	Host-based	
4	None	Host-based	
5	None	Host-based	
6	None	Host-based	
7	None	Host-based	
8	None	Host-based	
9	None	Host-based	
10	None	Host-based	
11	None	Host-based	
12	None	Host-based	
13	None	Host-based	
14	None	Host-based	
15	None	Host-based	
16	None	Host-based	
17	None	Host-based	
18	None	Host-based	
19	None	Host-based	
20	None	Host-based	
21	None	Host-based	
22	None	Host-based	
23	None	Host-based	
24	None	Host-based	
25	None	Host-based	

Figure 7- 75. Compound Authentication Settings window

The following parameters may be set:

Parameter	Description
Unit	Choose the Unit ID of the switch in the switch stack to configure.
From/To	Select a port or range of ports to be configured.
Authorized Mode	Use the drop-down menu to select either *Port-based* or *Host-based* authorized mode. *Port-based* – If one of the attached hosts passes the authentication process, all hosts on the same port will be granted access to the network. If the user fails the authorization, this port will keep trying until the next authentication. *Host-based* – Each user can be authenticated individually.
Methods	*None* – Specifies that multiple authentication is not enabled. *Any* – Specifies that a client will gain access if it passes any of the authentication methods (802.1X, MAC, or JWAC). *802.1X+IMPB* – Specifies that 802.1X+IMPB can be enabled on a port at the same time. 802.1X will be verified first, and then IMPB will be verified. Both authentication methods need

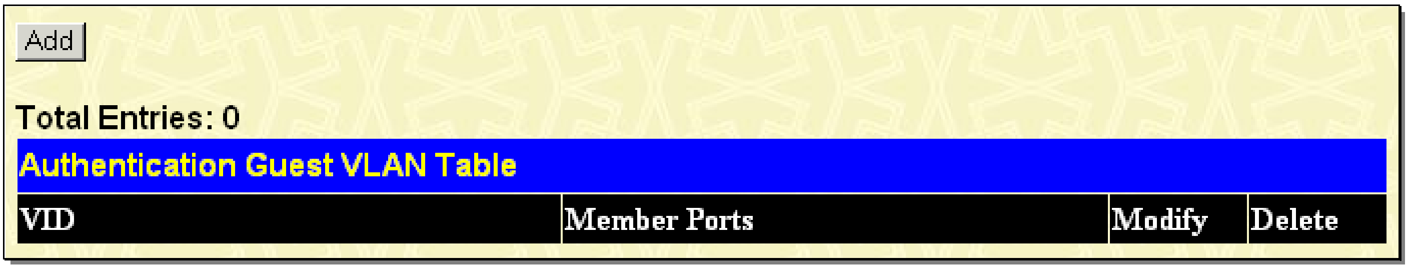
	to be passed. If either authentication method fails, the client will be denied access. *IMPB+JWAC* – Specifies that JWAC and IMPB can be enabled on a port at the same time. JWAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. If either authentication method fails, the client will be denied access.
VID List	Enter a list of VLAN IDs.
State	Use the pull-down menu to enable or disable this function.

Click **Apply** to implement changes made.

Authentication Guest VLAN Settings

This window is used to display and configure the Authentication Guest VLAN settings on the Switch.

To view this window, click **Security > Compound Authentication > Compound Authentication Guest VLAN Settings**, as shown below:



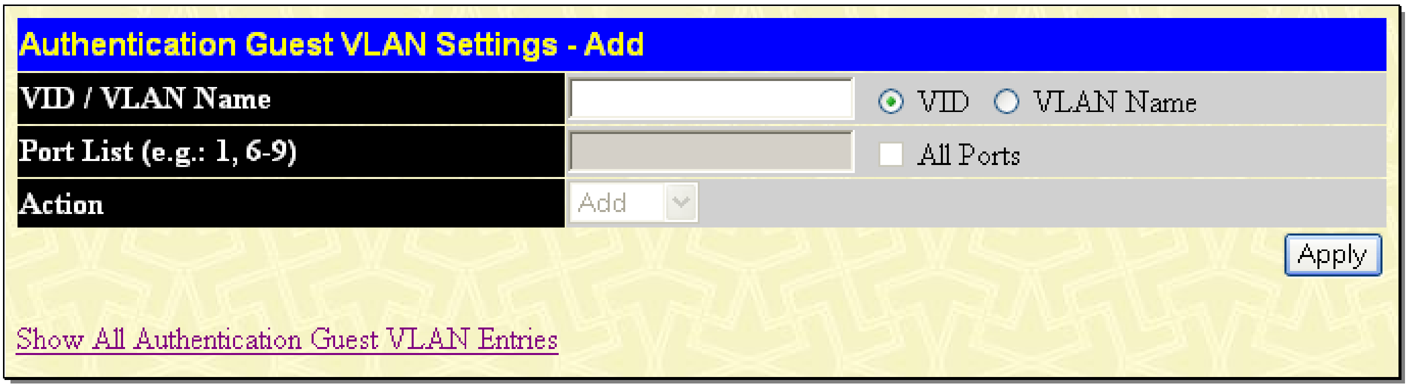
Total Entries: 0

Authentication Guest VLAN Table

VID	Member Ports	Modify	Delete

Figure 7- 76. Authentication Guest VLAN Table window

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


Authentication Guest VLAN Settings - Add

VID / VLAN Name		● VID ○ VLAN Name
Port List (e.g.: 1, 6-9)		□ All Ports
Action	Add	

Figure 7- 77. Authentication Guest VLAN Settings - Add window

The following parameters may be set:

Parameter	Description
VID / VLAN Name	Select either *VID* or *VLAN Name* and enter the appropriate information about a previously configured VLAN.
Port List (e.g.:1,6-9)	Enter the port or list of ports you wish to configure. Check the *Select All Ports* check box to select all ports.
Action	Select the action you wish to apply to the Guest VLAN. Select *Add* to add a port to the Guest VLAN portlist or *Delete* to remove ports from the Guest VLAN portlist.

Click **Apply** to implement changes made.

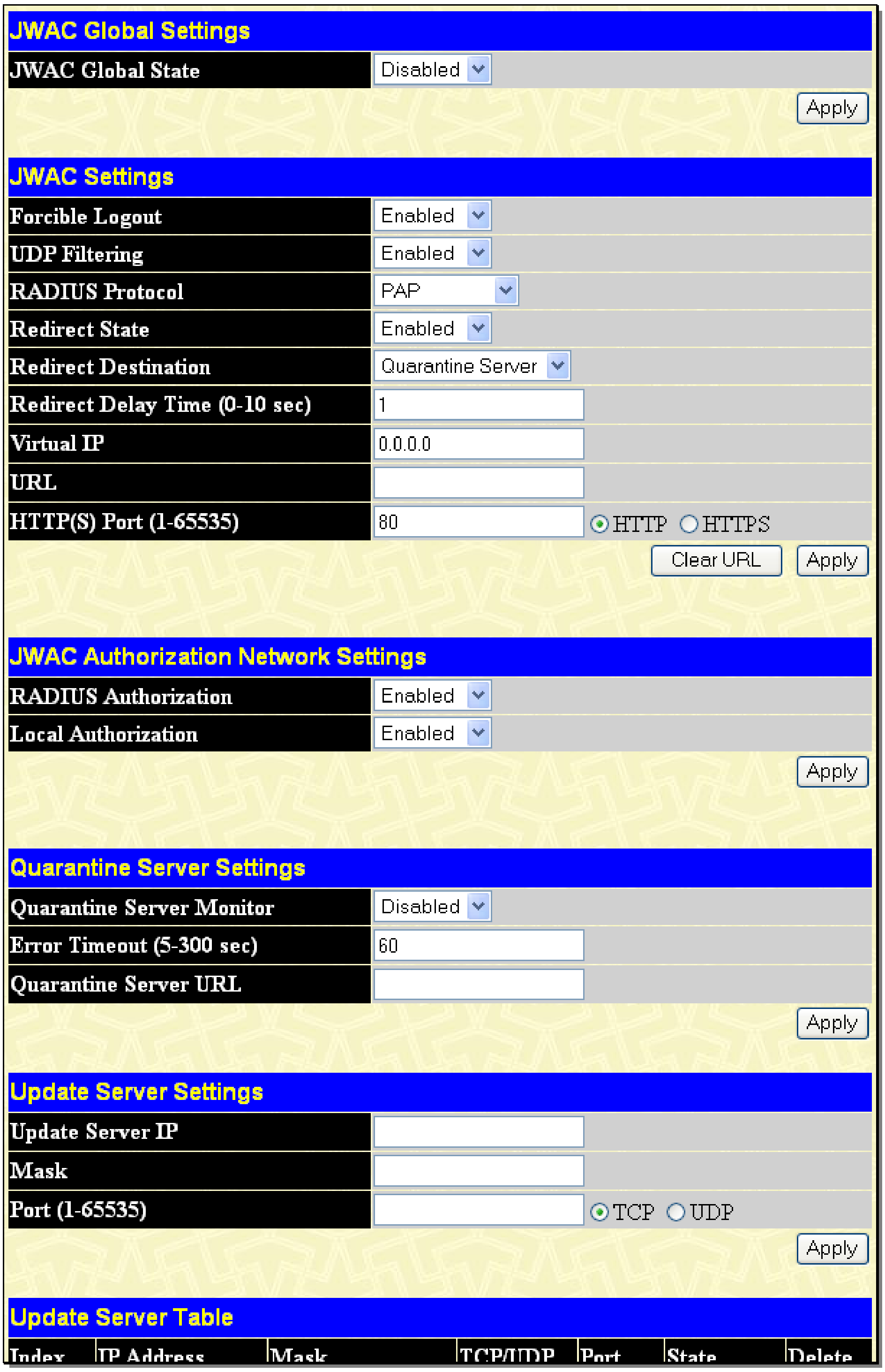
Japanese Web-based Access Control (JWAC)

The JWAC folder contains six windows: JWAC Global Configuration, JWAC Port Settings, JWAC User Account, JWAC Host Information, JWAC Customize Page Language Settings and JWAC Customize Page.

JWAC Global Settings

Use this window to enable and configure Japanese Web-based Access Control on the Switch. Please note that JWAC and Web Authentication are mutually exclusive functions. That is, they cannot be enabled at the same time. To use the JWAC feature, computer users need to pass through the authentication process. For this, the authentication is similar to Web Authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Global Settings**, as shown below:



JWAC Global Settings

JWAC Global State	Disabled

JWAC Settings

Forcible Logout	Enabled
UDP Filtering	Enabled
RADIUS Protocol	PAP
Redirect State	Enabled
Redirect Destination	Quarantine Server
Redirect Delay Time (0-10 sec)	1
Virtual IP	0.0.0.0
URL	
HTTP(S) Port (1-65535)	80 ● HTTP ○ HTTPS

JWAC Authorization Network Settings

RADIUS Authorization	Enabled
Local Authorization	Enabled

Quarantine Server Settings

Quarantine Server Monitor	Disabled
Error Timeout (5-300 sec)	60
Quarantine Server URL	

Update Server Settings

Update Server IP	
Mask	
Port (1-65535)	● TCP ○ UDP

Update Server Table

Index	IP Address	Mask	TCP/UDP	Port	State	Delete

Figure 7- 78. JWAC Global Settings window

To set JWAC for the Switch, complete the following fields:

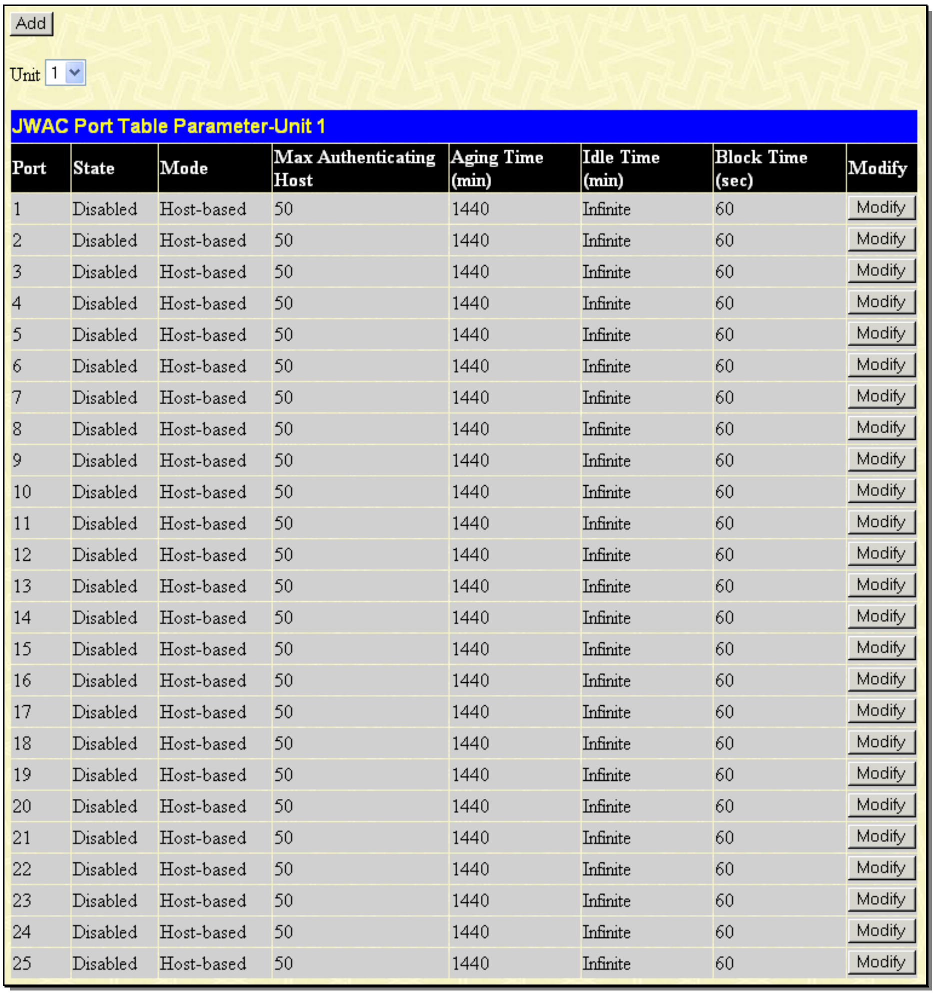
Parameter	Description
JWAC Global Settings	
JWAC Global State	Use this drop-down menu to either enable or disable JWAC on the Switch.
JWAC Settings	
Forcible Logout	This parameter enables or disables JWAC Forcible Logout. When Forcible Logout is *Enabled*, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will move back to the unauthenticated state.
UDP Filtering	This parameter enables or disables JWAC UDP Filtering. When UDP Filtering is *Enabled*, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped
RADIUS Protocol	This parameter specifies the RADIUS protocol used by JWAC to complete a RADIUS authentication. The options include *Local*, *EAP MD5*, *PAP*, *CHAP*, *MS CHAP*, and *MS CHAPv2*.
Redirect State	This parameter enables or disables JWAC Redirect. When the redirect quarantine server is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When the redirect JWAC login page is enabled, the unauthenticated host will be redirected to the JWAC login page in the Switch to finish authentication. When redirect is disabled, only access to the quarantine server and the JWAC login page from the unauthenticated host are allowed, all other web access will be denied. NOTE: When enabling redirect to the quarantine server, a quarantine server must be configured first.
Redirect Destination	This parameter specifies the destination before an unauthenticated host is redirected to either the *Quarantine Server* or the *JWAC Login Page*.
Redirect Delay Time (0-10 sec)	This parameter specifies the Delay Time before an unauthenticated host is redirected to the Quarantine Server or JWAC Login Page. Enter a value between *0* and *10* seconds. A value of *0* indicates no delay in the redirect.
Virtual IP	This parameter specifies the JWAC Virtual IP address that is used to accept authentication requests from an unauthenticated host. Only requests sent to this IP will get a correct response. NOTE: This IP does not respond to ARP requests or ICMP packets.
URL	This parameter is used to set the URL of the virtual IP. Clients can use this FQDN URL to access the JWAC login page instead of the real virtual IP.
HTTP(S) Port (1-65535)	This parameter specifies the TCP port number that the JWAC Switch listens to and uses to finish the authentication process.
JWAC Authorization Network Settings	
RADIUS Authorization	If *Enabled*, the authorized data assigned by the RADUIS server will be accepted when the global authorization attributes are enabled. The default state is *Enabled*.
Local Authorization	If *Enabled*, the authorized data assigned by the Local database will be accepted if the global authorization attributes are enabled. The default state is *Enabled*.
Quarantine Server Settings	
Quarantine Server Monitor	This parameter enables or disables the JWAC Quarantine Server Monitor. When *Enabled*, the JWAC Switch will monitor the Quarantine Server to ensure the server is okay. If the Switch detects no Quarantine Server, it will redirect all unauthenticated HTTP access attempts to the JWAC Login Page forcibly if the Redirect is enabled and the Redirect Destination is configured to be a Quarantine Server.

Error Timeout (5-300 sec)	This parameter is used to set the Quarantine Server Error Timeout. When the Quarantine Server Monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from the Quarantine Server during the configured Error Timeout, the Switch then regards it as not working properly. Enter a value between *5* and *300* seconds.
Quarantine Server URL	This parameter specifies the JWAC Quarantine Server URL. If the Redirect is enabled and the Redirect Destination is the Quarantine Server, when an unauthenticated host sends the HTTP request packets to a random Web server, the Switch will handle this HTTP packet and send back a message to the host to allow it access to the Quarantine Server with the configured URL. When a computer is connected to the specified URL, the quarantine server will request the computer user to input the user name and password to complete the authentication process.
Update Server Settings	
Update Server IP	This parameter specifies the Update Server IP address.
Mask	This parameter specifies the Server IP net mask.
Port (1-65535)	The accessible TCP/UDP port number for the specified update server network.

Click **Apply** to implement changes made.

JWAC Port Settings

To view JWAC port settings for the Switch, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Port Settings**, as shown below:

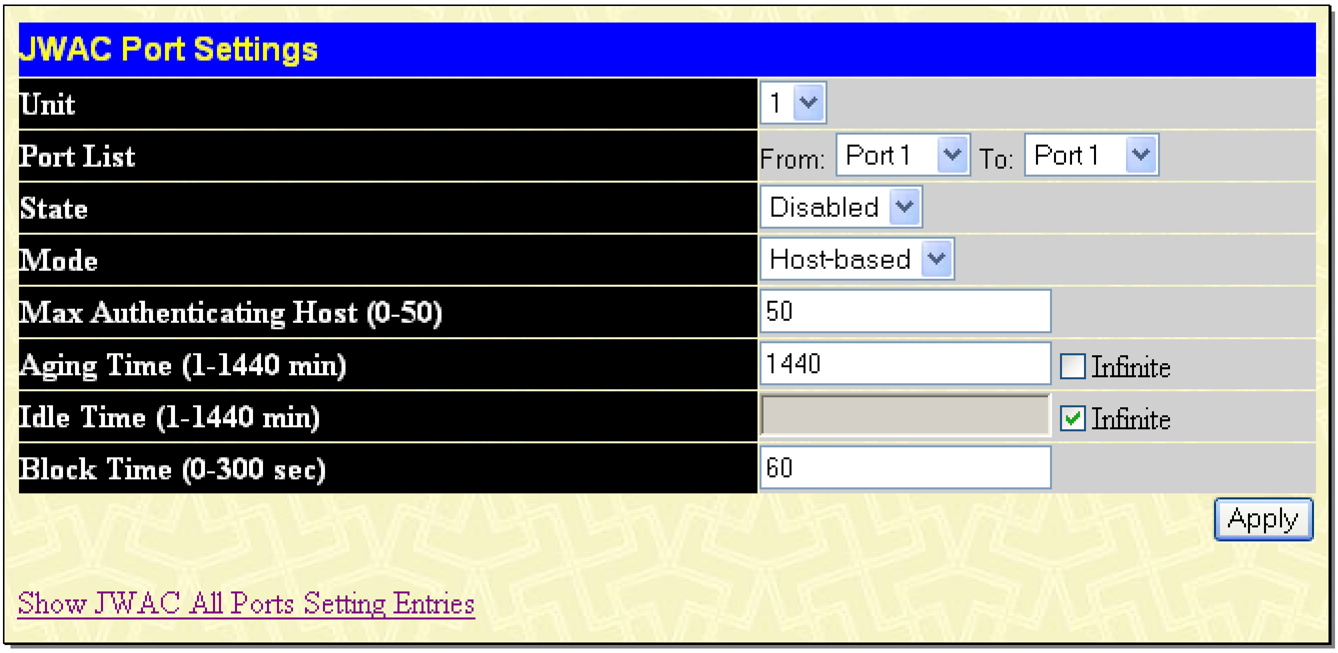


JWAC Port Table Parameter-Unit 1

Port	State	Mode	Max Authenticating Host	Aging Time (min)	Idle Time (min)	Block Time (sec)	Modify
1	Disabled	Host-based	50	1440	Infinite	60	Modify
2	Disabled	Host-based	50	1440	Infinite	60	Modify
3	Disabled	Host-based	50	1440	Infinite	60	Modify
4	Disabled	Host-based	50	1440	Infinite	60	Modify
5	Disabled	Host-based	50	1440	Infinite	60	Modify
6	Disabled	Host-based	50	1440	Infinite	60	Modify
7	Disabled	Host-based	50	1440	Infinite	60	Modify
8	Disabled	Host-based	50	1440	Infinite	60	Modify
9	Disabled	Host-based	50	1440	Infinite	60	Modify
10	Disabled	Host-based	50	1440	Infinite	60	Modify
11	Disabled	Host-based	50	1440	Infinite	60	Modify
12	Disabled	Host-based	50	1440	Infinite	60	Modify
13	Disabled	Host-based	50	1440	Infinite	60	Modify
14	Disabled	Host-based	50	1440	Infinite	60	Modify
15	Disabled	Host-based	50	1440	Infinite	60	Modify
16	Disabled	Host-based	50	1440	Infinite	60	Modify
17	Disabled	Host-based	50	1440	Infinite	60	Modify
18	Disabled	Host-based	50	1440	Infinite	60	Modify
19	Disabled	Host-based	50	1440	Infinite	60	Modify
20	Disabled	Host-based	50	1440	Infinite	60	Modify
21	Disabled	Host-based	50	1440	Infinite	60	Modify
22	Disabled	Host-based	50	1440	Infinite	60	Modify
23	Disabled	Host-based	50	1440	Infinite	60	Modify
24	Disabled	Host-based	50	1440	Infinite	60	Modify
25	Disabled	Host-based	50	1440	Infinite	60	Modify

Figure 7- 79. JWAC Port Table Parameter window

To configure individual JWAC port settings, click the **Add** button, the following window will be displayed.

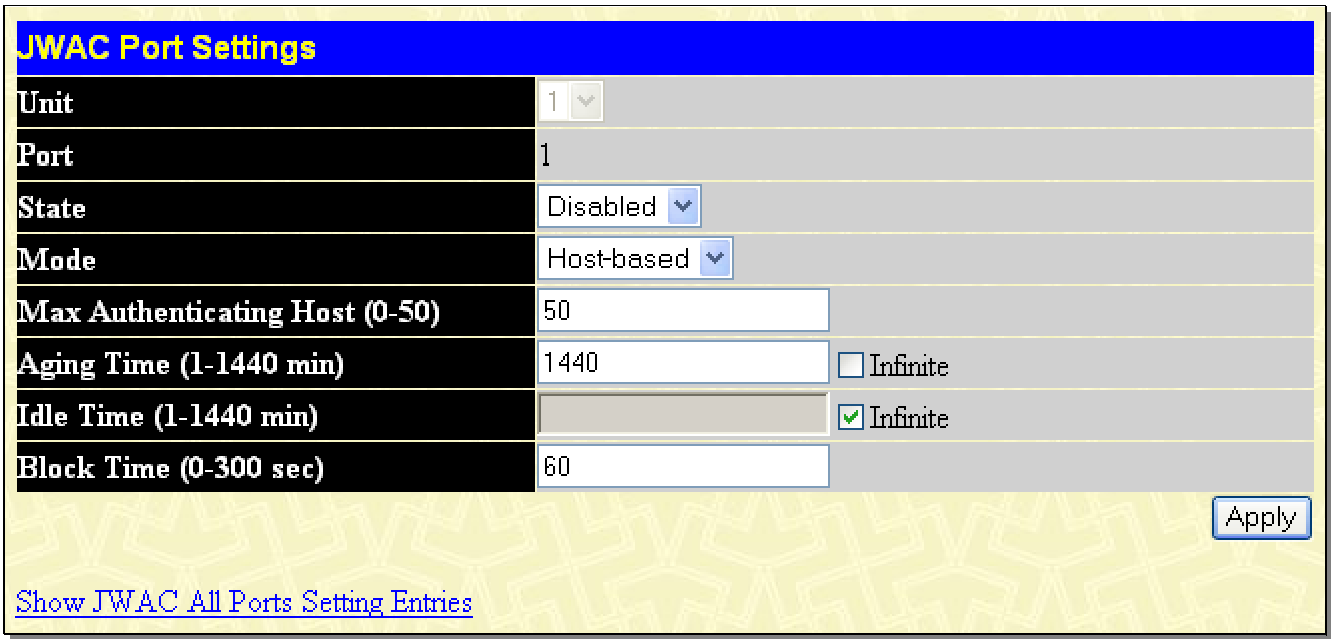


JWAC Port Settings

Unit	1
Port List	From: Port 1 To: Port 1
State	Disabled
Mode	Host-based
Max Authenticating Host (0-50)	50
Aging Time (1-1440 min)	1440 □ Infinite
Idle Time (1-1440 min)	☑ Infinite
Block Time (0-300 sec)	60

Figure 7- 80. JWAC Port Settings window (Add)

To configure the settings by port, click on the corresponding **Modify** button, which will display the following window:



JWAC Port Settings

Unit	1
Port	1
State	Disabled
Mode	Host-based
Max Authenticating Host (0-50)	50
Aging Time (1-1440 min)	1440 □ Infinite
Idle Time (1-1440 min)	☑ Infinite
Block Time (0-300 sec)	60

Figure 7- 81. JWAC Port Settings window (Modify)

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

Parameter	Description
Unit	Choose the Unit ID of the switch in the switch stack to configure.
Port List	Lists the range of Ports that will be configured in this window.
State	This parameter specifies the state of the configured ports.
Mode	Use the drop-down menu to select the mode, choose either *Port Based* or *Host Based*.
Max Authenticating	This parameter specifies the maximum number of host process authentication attempts

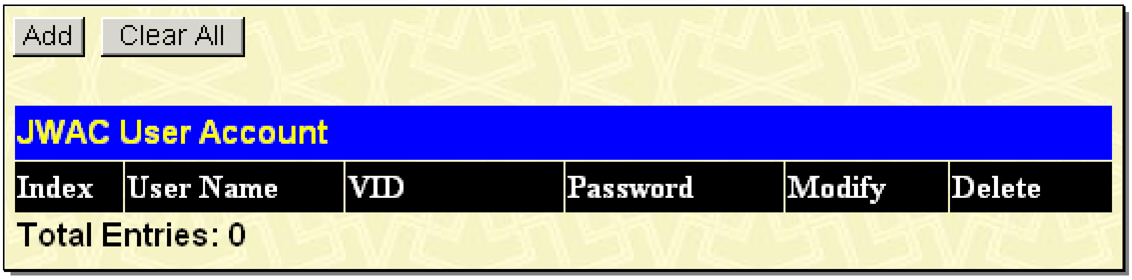
Host (0-50)	allowed on each port at the same time.
Aging Time **(1-1440 min)**	This parameter specifies the period of time a host will keep in authenticated state after it successes to authenticate. Enter a value between *1* and *1440* minutes. The default setting is *1440* minutes. To maintain a constant Port Configuration, tick the Infinite check box.
Idle Time **(1-1440 min)**	This parameter specifies the period of time during which there is no traffic for an authenticated host and the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. A value of Infinite indicates the Idle state of the authenticated host on the port will never be checked. The default setting is Infinite.
Block Time **(0-300 sec)**	This parameter specifies the period of time a host will keep in a blocked state after it fails to authenticate. Enter a value between *0* and *300* seconds. The default setting is *60* seconds.

Click **Apply** to implement changes made.

JWAC User Account

This window is used to configure JWAC user accounts on the Switch.

To view this window, click **Security** > **Japanese Web-based Access Control (JWAC)** > **JWAC User Account**, as shown below:



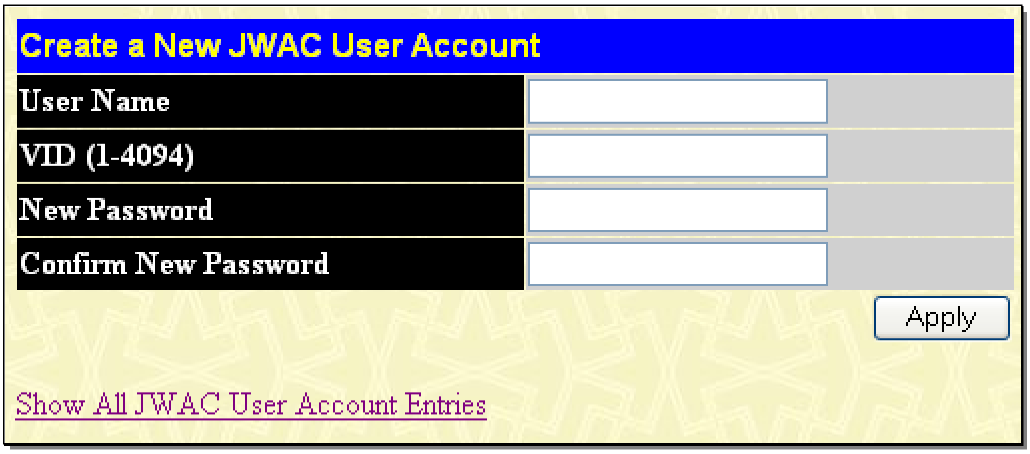
JWAC User Account

Index	User Name	VID	Password	Modify	Delete

Total Entries: 0

Figure 7- 82. JWAC User Account window

To configure JWAC user settings, click the **Add** button, which will open the following window:



Create a New JWAC User Account

User Name	
VID (1-4094)	
New Password	
Confirm New Password	

Figure 7- 83. Create a New JWAC User Account window

The following fields can be configured:

Parameter	Description
User Name	Enter a username of up to 15 alphanumeric characters.
VID(1-4094)	Enter the VLAN ID of the Account you wish to create.

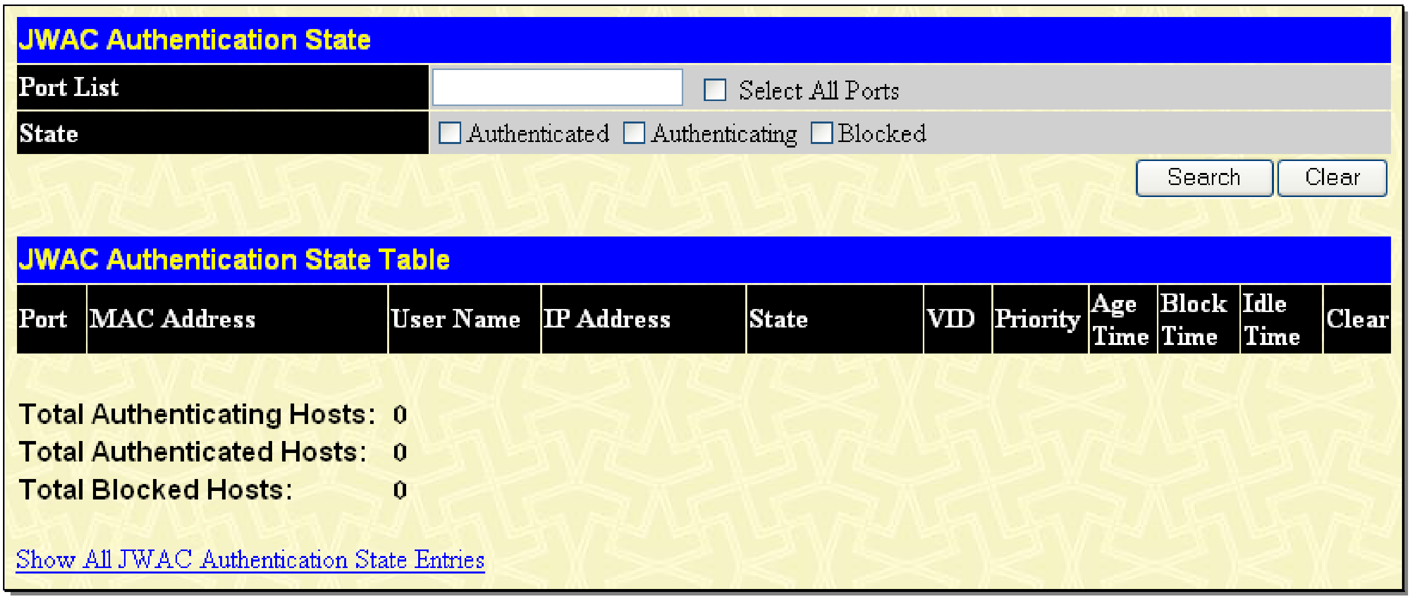
New Password	Enter the password of the user. This field is case-sensitive and must be a complete alphanumeric string.
Confirm New Password	Retype the password entered in the previous field.

Click **Apply** to implement changes made.

JWAC Authentication State

The JWAC Host information Table allows the user to show or delete the hosts, which are handling or have been handled by the Switch.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Authentication State**, as shown below:



JWAC Authentication State

Port List	☐ Select All Ports
State	☐ Authenticated ☐ Authenticating ☐ Blocked

JWAC Authentication State Table

Port	MAC Address	User Name	IP Address	State	VID	Priority	Age Time	Block Time	Idle Time	Clear

Total Authenticating Hosts: 0
Total Authenticated Hosts: 0
Total Blocked Hosts: 0

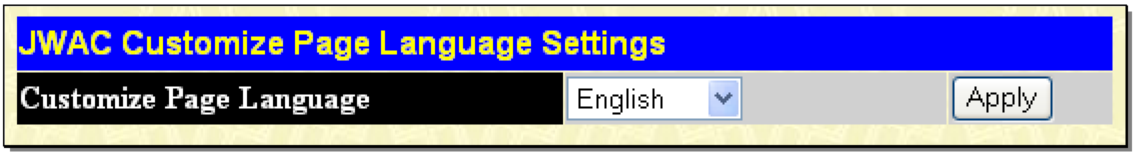
Figure 7- 84. JWAC Authentication State window

To search for hosts, enter the Port List information and click the **Search** button. To clear an entry, enter the Port List information and click the **Clear** button.

JWAC Customize Page Language Settings

This window is used to customize your JWAC language settings on the Switch. Use the drop-down menu to select either English or Japanese and click **Apply**.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language Settings**, as shown below:



JWAC Customize Page Language Settings

Customize Page Language: English

Figure 7- 85. JWAC Customize Page Language Settings window

JWAC Customize Page

This window is used to customize the JWAC feature.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page**, as shown below:

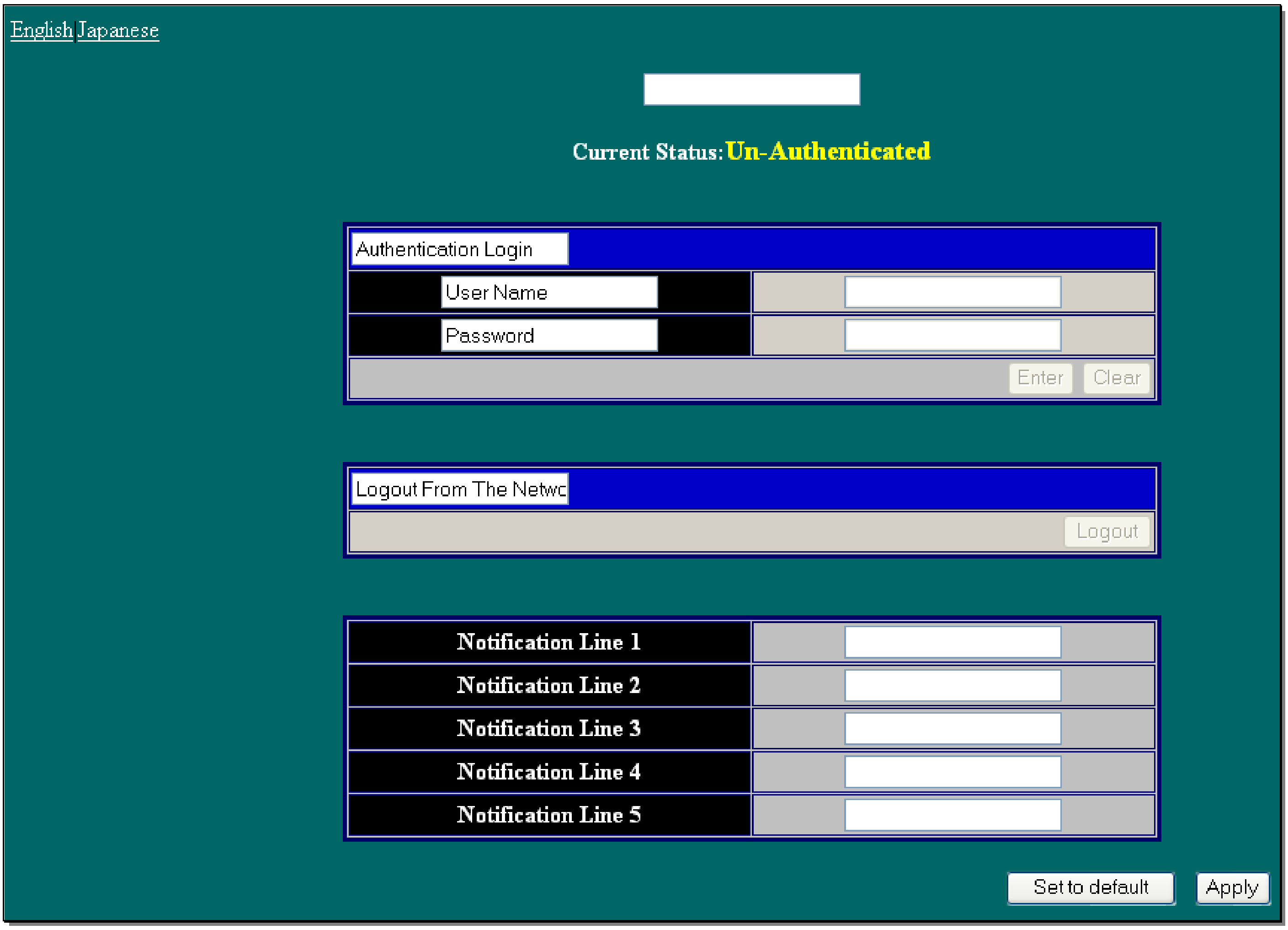


Figure 7- 86. JWAC Customize Page window

This window allows the administrator to customize fields in the JWAC Customize Page. Enter the new information and click **Apply**.

Section 8

Monitoring

Device Status

Stacking Information

Stacking Device

Module Information

DRAM & Flash Utilization

CPU Utilization

Port Utilization

Packets

Errors

Packet Size

Browse Router Port

Browse MLD Router Port

VLAN Status

VLAN Status Port

Port Access Control

MAC Address Table

IGMP Snooping Group

MLD Snooping Group

Trace Route

IGMP Snooping Forwarding

MLD Snooping Forwarding

IP Forwarding Table

Routing Table

Browse IP Multicast Forwarding Table

Browse IP Multicast Interface Table

Browse IGMP Group Table

DVMRP Monitor

PIM Monitor

OSPF Monitor

Switch Logs

Browse ARP Table

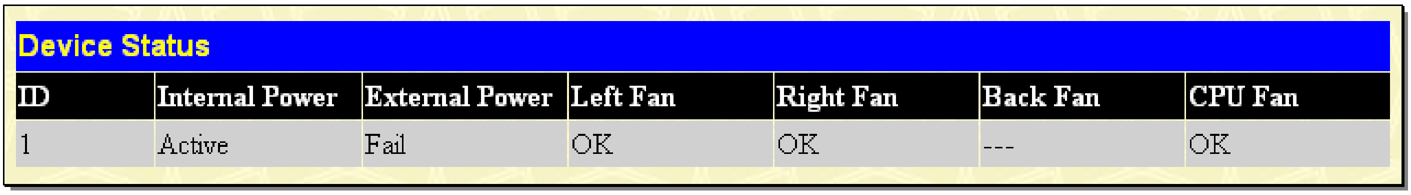
Session Table

MAC Based Access Control Authentication Status

Device Status

This window displays status information for Internal Power, External Power, Side Fan, and Back Fan.

To view the **Device Status** window, click **Monitoring** > **Device Status**, as shown below:



Device Status

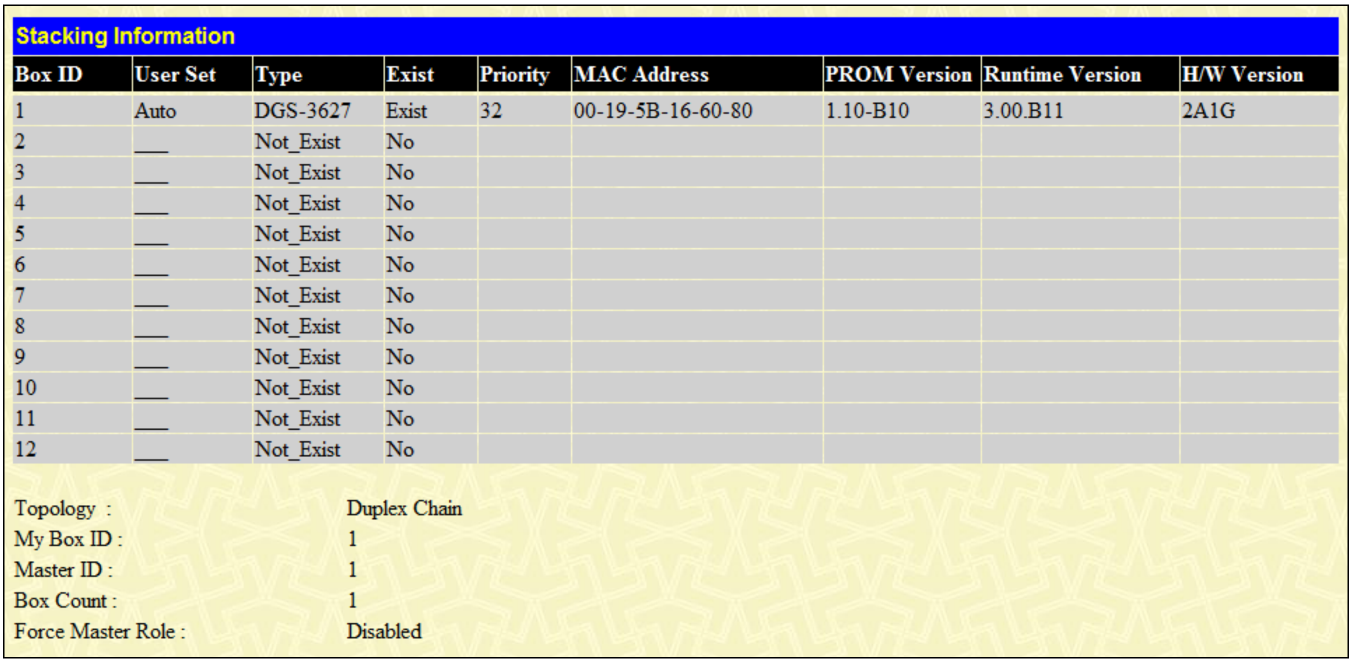
ID	Internal Power	External Power	Left Fan	Right Fan	Back Fan	CPU Fan
1	Active	Fail	OK	OK	---	OK

Figure 8- 1. Device Status window

Stacking Information

This window displays all the Switches that are currently in the stack as well as configuration information about each Switch.

To view the **Stacking Information** window, click **Monitoring** > **Stacking Information**, as shown below:



Stacking Information

Box ID	User Set	Type	Exist	Priority	MAC Address	PROM Version	Runtime Version	H/W Version
1	Auto	DGS-3627	Exist	32	00-19-5B-16-60-80	1.10-B10	3.00.B11	2A1G
2	___	Not_Exist	No					
3	___	Not_Exist	No					
4	___	Not_Exist	No					
5	___	Not_Exist	No					
6	___	Not_Exist	No					
7	___	Not_Exist	No					
8	___	Not_Exist	No					
9	___	Not_Exist	No					
10	___	Not_Exist	No					
11	___	Not_Exist	No					
12	___	Not_Exist	No					

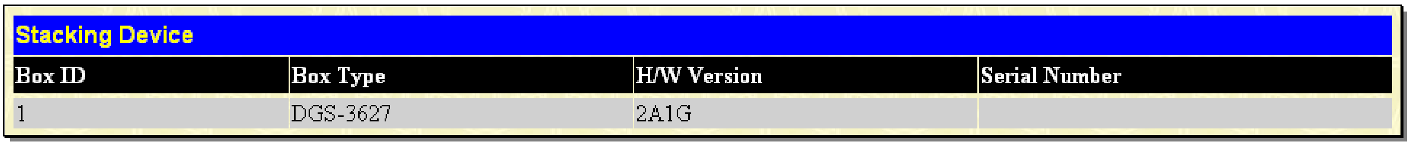
Topology :	Duplex Chain
My Box ID :	1
Master ID :	1
Box Count :	1
Force Master Role :	Disabled

Figure 8- 2. Stacking Information window

Stacking Device

This window displays all the Switches that are currently in the stack as well as configuration information about each Switch.

To view the **Stacking Information** window, click **Monitoring** > **Stacking Device**, as shown below:



Stacking Device

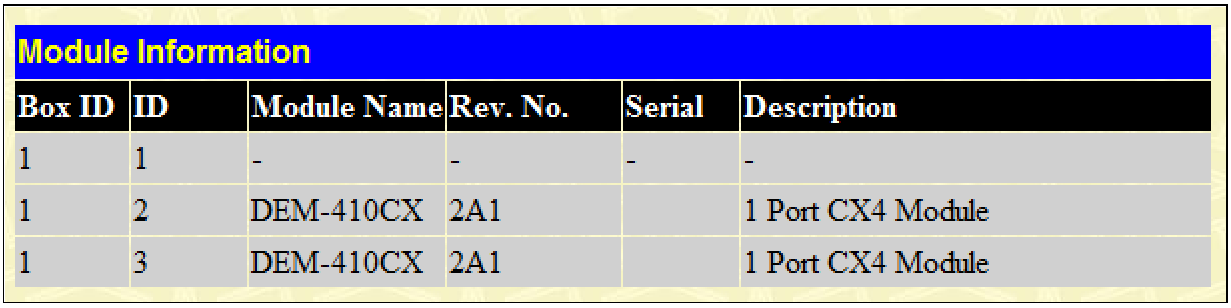
Box ID	Box Type	H/W Version	Serial Number
1	DGS-3627	2A1G	

Figure 8- 3. Stacking Device window

Module Information

This window displays module information of the Switch, including the module name, Revision Number, Serial Number and description.

To view the **Module Information** window, click **Monitoring** > **Module Information**, as shown below:



Module Information

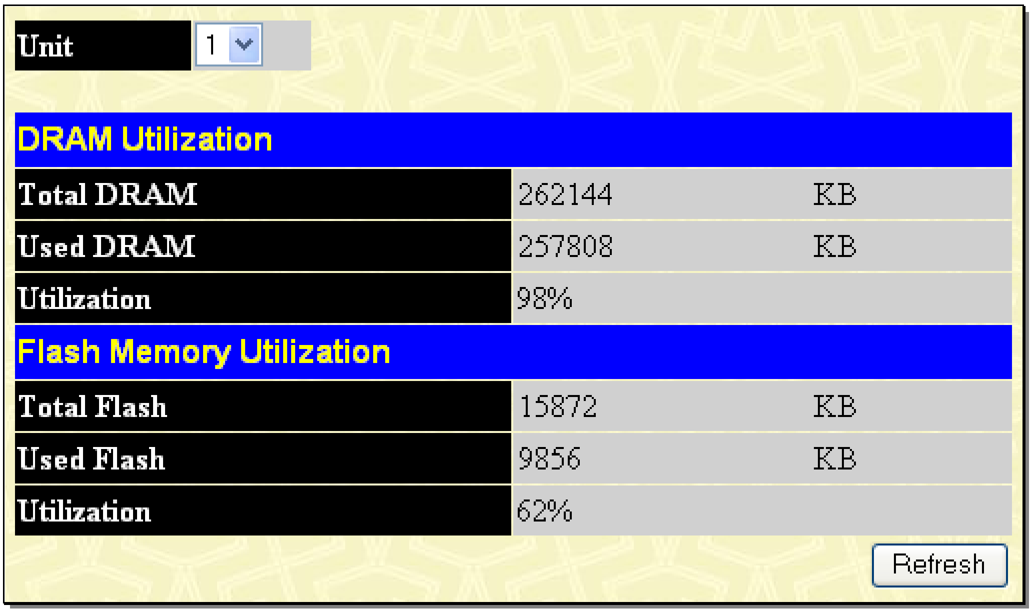
Box ID	ID	Module Name	Rev. No.	Serial	Description
1	1	-	-	-	-
1	2	DEM-410CX	2A1		1 Port CX4 Module
1	3	DEM-410CX	2A1		1 Port CX4 Module

Figure 8- 4. Module Information window

DRAM & Flash Utilization

This window is used to display DRAM and Flash utilization information.

To view this window, click **Monitoring** > **DRAM & Flash Utilization**, as shown below:



Unit: 1

DRAM Utilization

Total DRAM	262144	KB
Used DRAM	257808	KB
Utilization	98%	

Flash Memory Utilization

Total Flash	15872	KB
Used Flash	9856	KB
Utilization	62%	

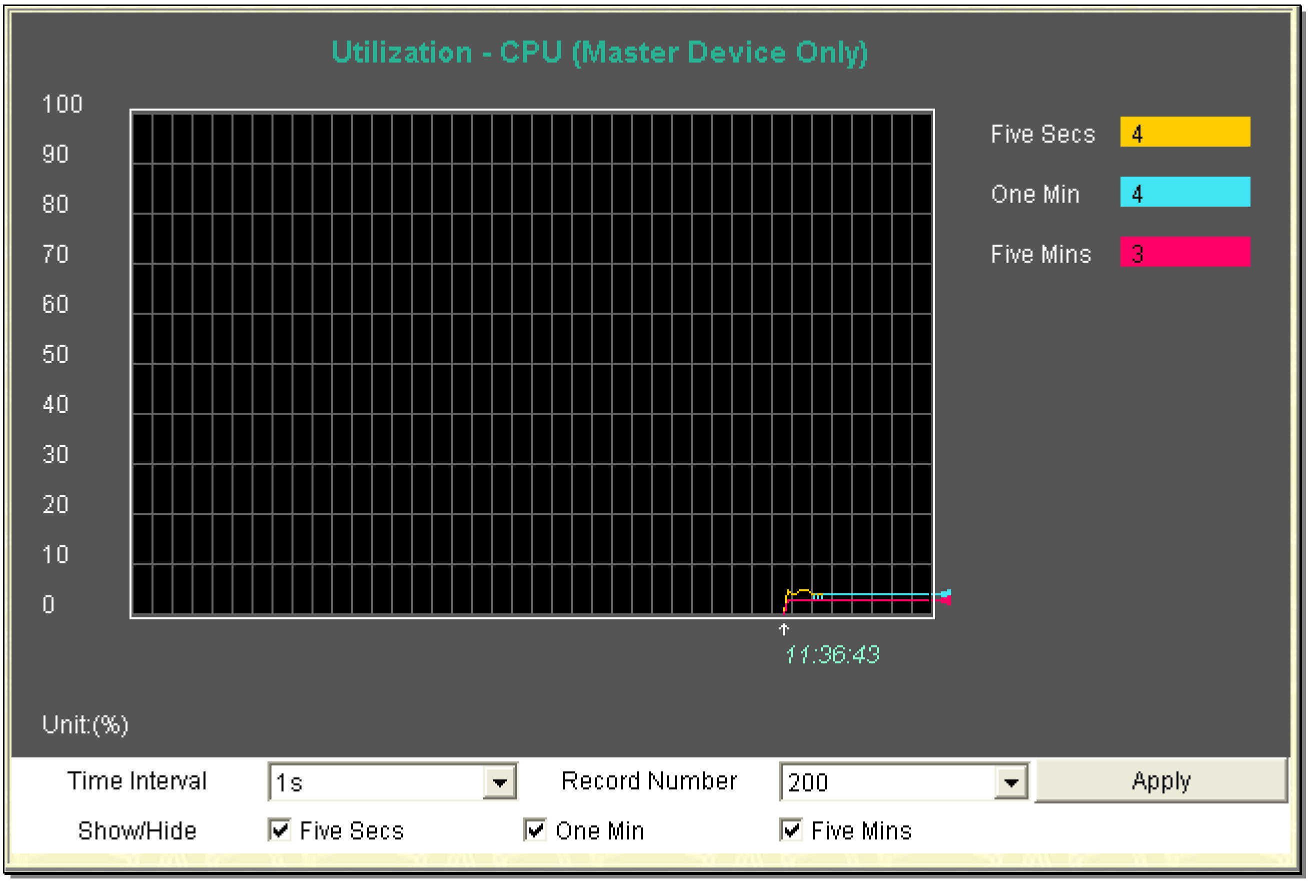
Figure 8- 5. DRAM Utilization window

Please note the Switch reserves memory space during boot-up.

CPU Utilization

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

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



Five Secs 4
One Min 4
Five Mins 3

Time Interval 1s
Record Number 200
Show/Hide ☑ Five Secs ☑ One Min ☑ Five Mins

Figure 8- 6. CPU Utilization window

Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics

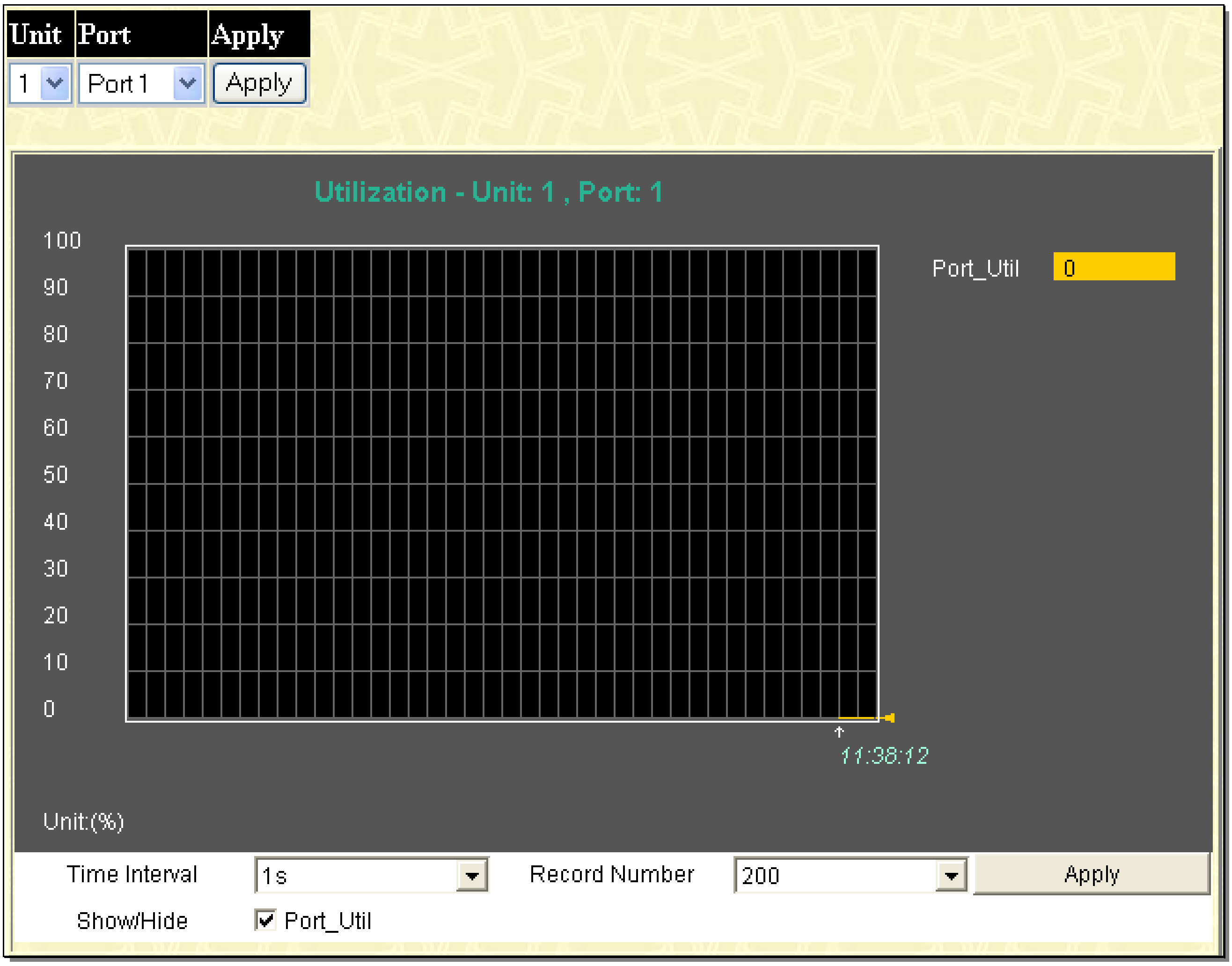
The information is described as follows:

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 *200*.
Show/Hide	These check boxes allow the user to choose the CPU utilization over increments of *Five Secs*, *One Min* and *Five Mins*. Each time increment will be displayed in the window as a specifically colored line. Five seconds will be displayed as yellow, one minute as blue and five minutes as pink.

Port Utilization

This window displays the percentage of the total available bandwidth being used on the port.

To view the port utilization, click **Monitoring** > **Port Utilization**, as shown below:



Unit: 1 Port: Port 1 Apply

Utilization - Unit: 1 , Port: 1

Port_Util 0

Time Interval 1s Record Number 200 Apply

Show/Hide ☑ Port_Util

Figure 8- 7. Port Utilization window

Select a Port number from its 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*.
Show/Hide	Check whether to display Port Utilization.

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 the **Received (RX)** window, click **Monitoring** > **Packets** > **Received (RX)**, as shown below:

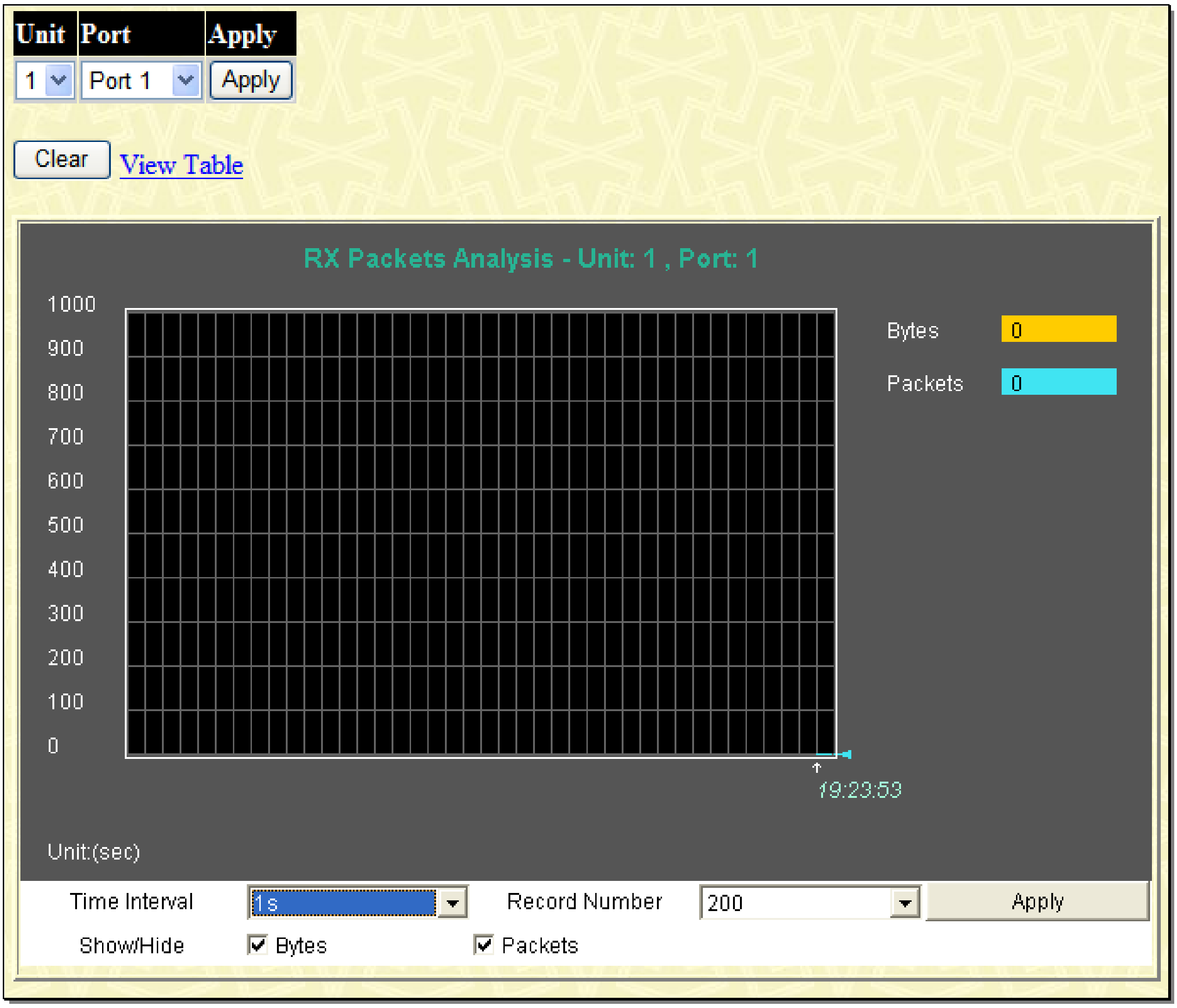
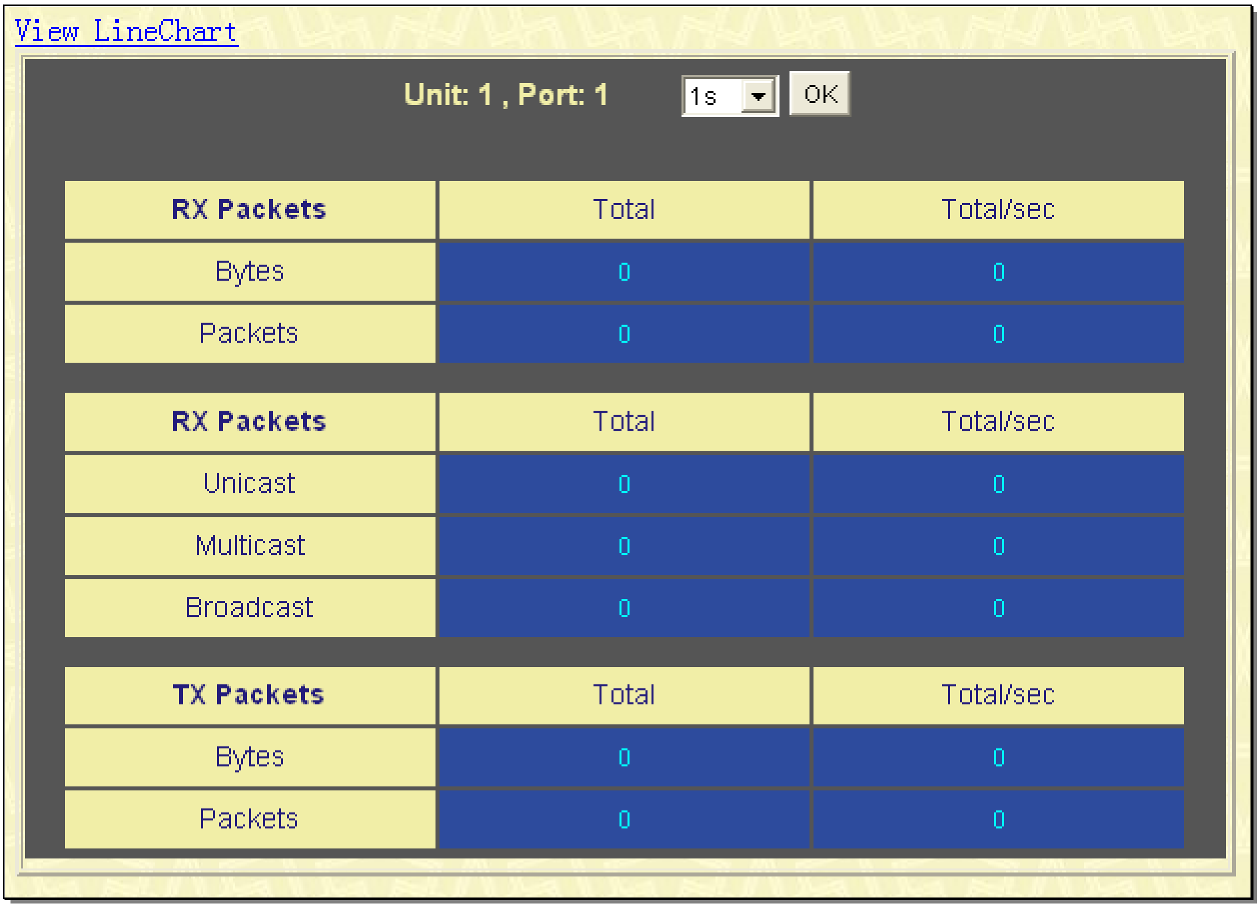


Figure 8- 8. RX Packets Analysis window (line graph for Bytes and Packets)

Select a Port number from its pull-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:



View LineChart

Unit: 1 , Port: 1 1s OK

RX Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

RX Packets	Total	Total/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

TX Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

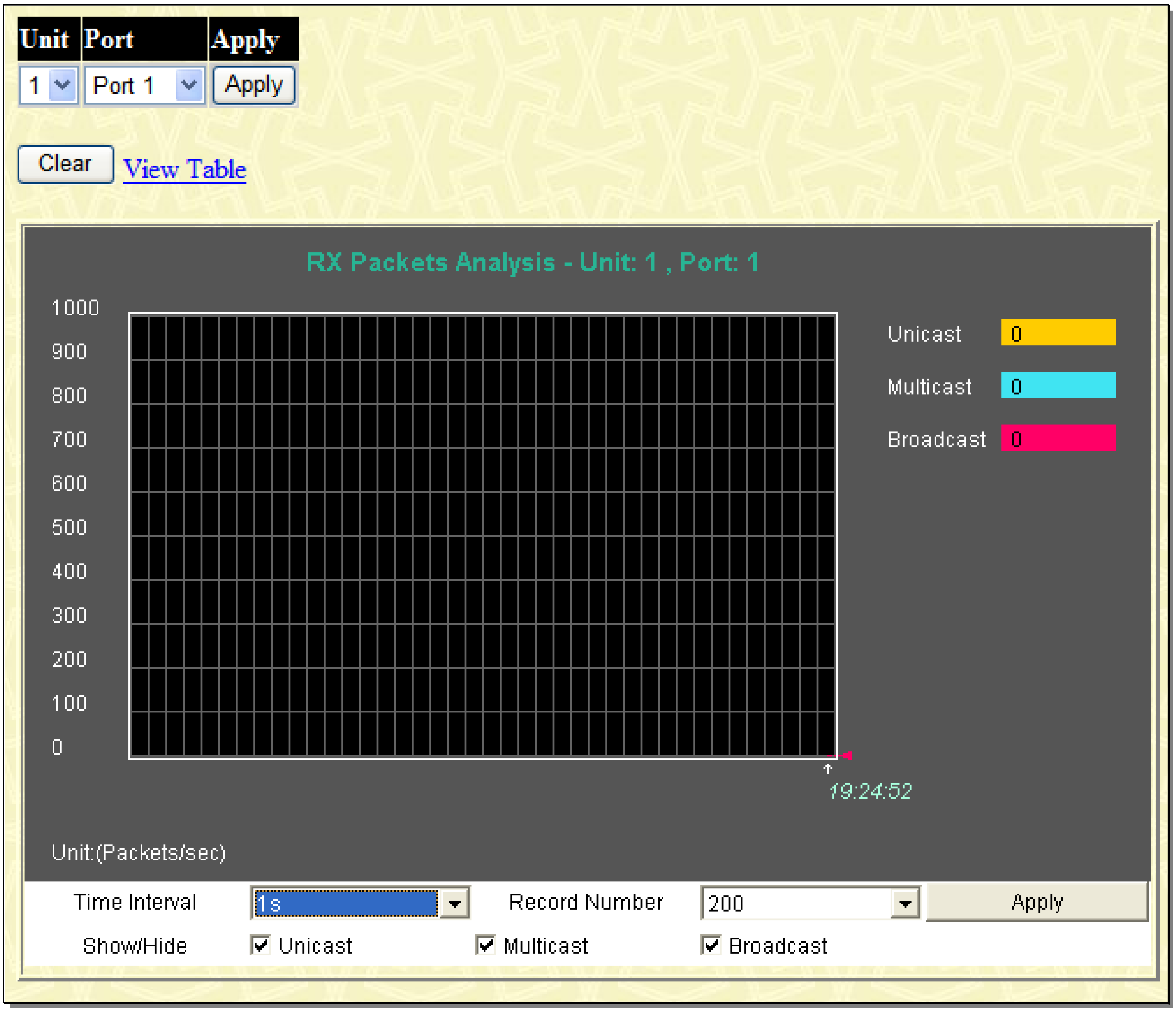
Figure 8- 9. RX Packets Analysis window (table for Bytes and Packets)

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 *200*.
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 the **UMB_cast (RX)** window, click **Monitoring** > **Packets** > **UMB_cast (RX)**, as shown below:



Unit	Port	Apply
1	Port 1	Apply

Clear View Table

RX Packets Analysis - Unit: 1 , Port: 1

Unicast 0

Multicast 0

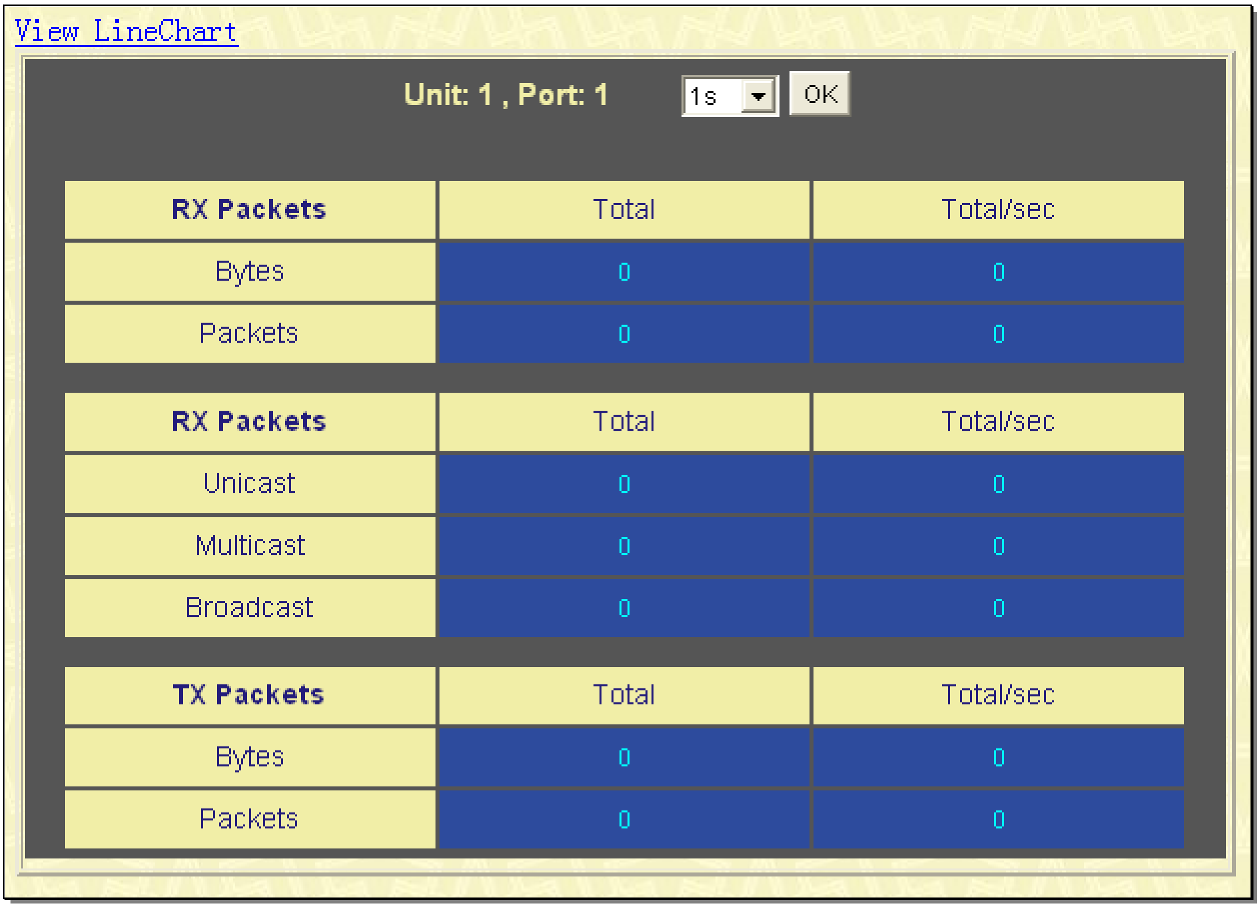
Broadcast 0

Time Interval 1s Record Number 200 Apply

Show/Hide ☑ Unicast ☑ Multicast ☑ Broadcast

Figure 8- 10. 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:



Unit: 1 , Port: 1

RX Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

RX Packets	Total	Total/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

TX Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

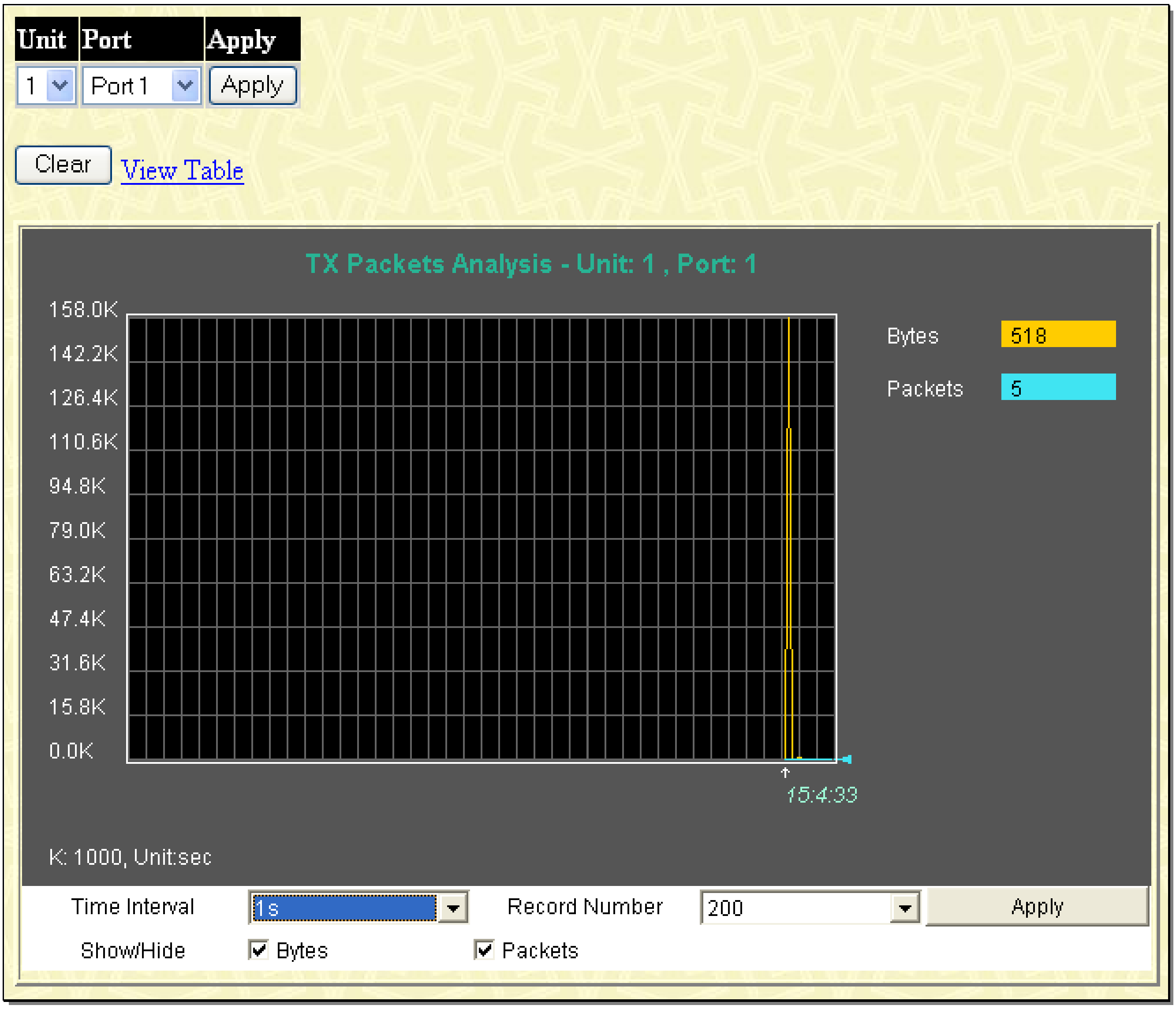
Figure 8- 11. RX Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

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 *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View LineChart	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)**, as shown below:



Unit	Port	Apply
1	Port 1	Apply

Clear View Table

TX Packets Analysis - Unit: 1 , Port: 1

Bytes	518
Packets	5

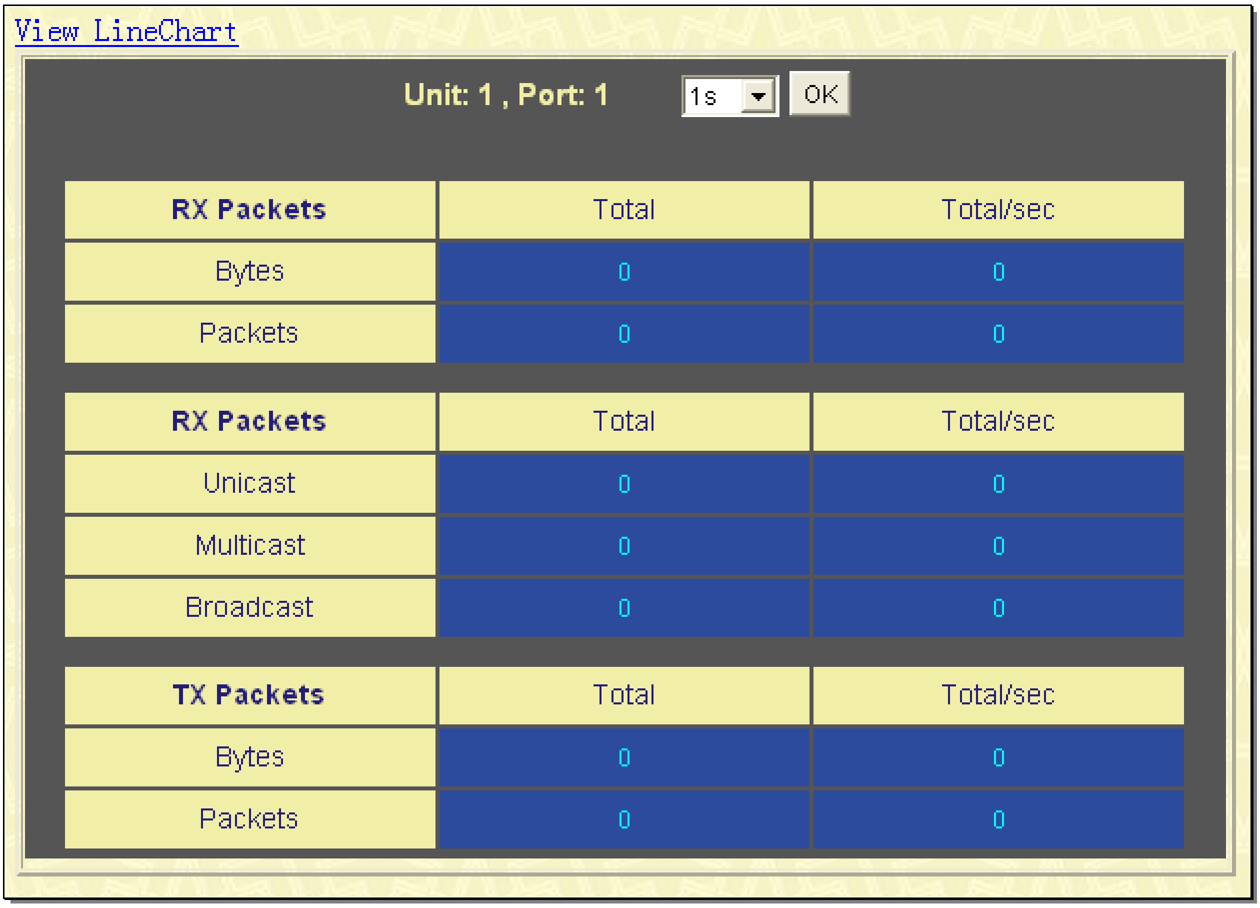
K: 1000, Unit:sec

Time Interval: 1 s
Record Number: 200
Apply

Show/Hide ☑ Bytes ☑ Packets

Figure 8- 12. 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:



View LineChart

Unit: 1 , Port: 1 1s OK

RX Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

RX Packets	Total	Total/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

TX Packets	Total	Total/sec
Bytes	0	0
Packets	0	0

Figure 8- 13. TX Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

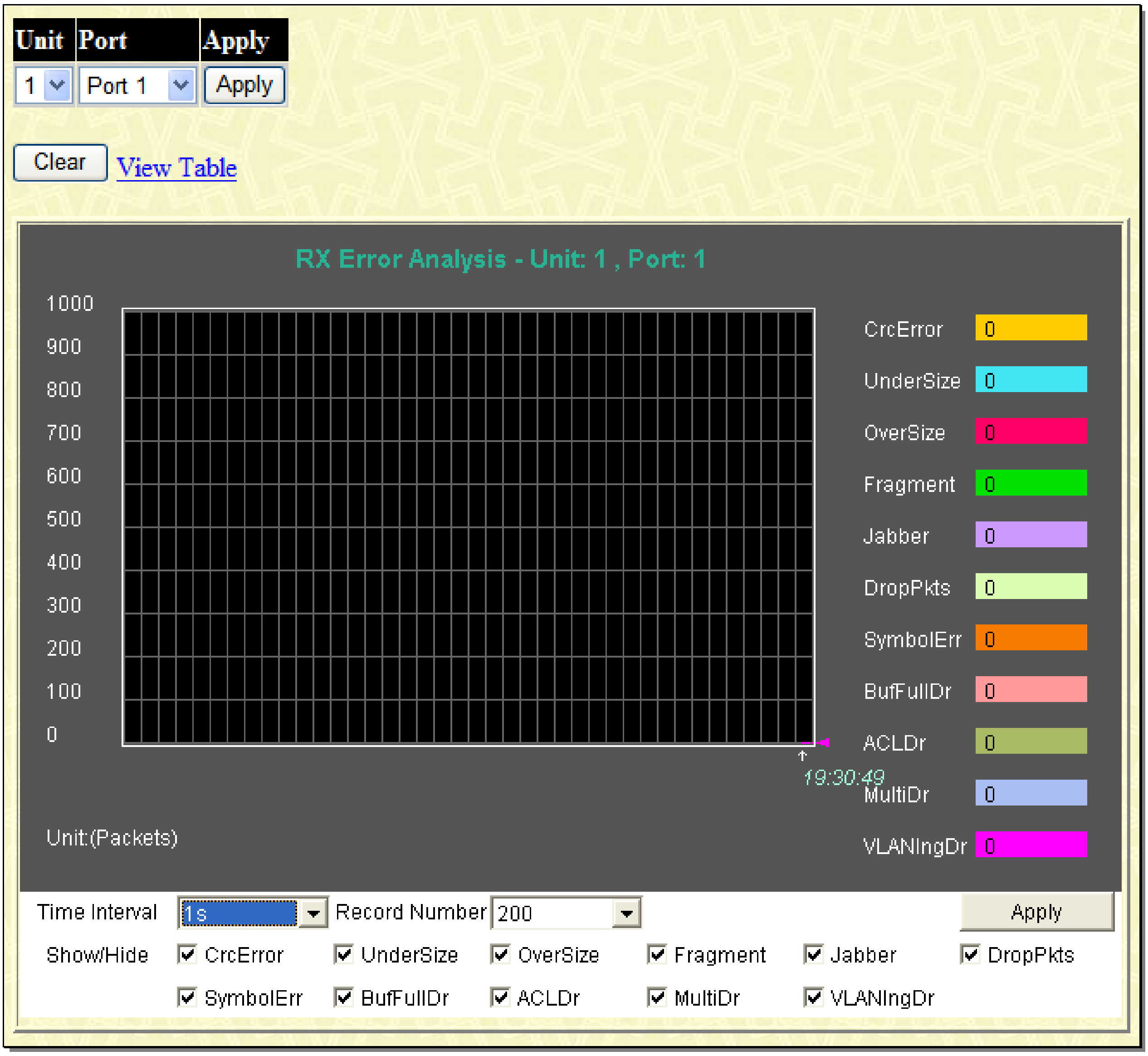
Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on 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 LineChart	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)**, as shown below:



Unit: 1
Port: Port 1

RX Error Analysis - Unit: 1 , Port: 1

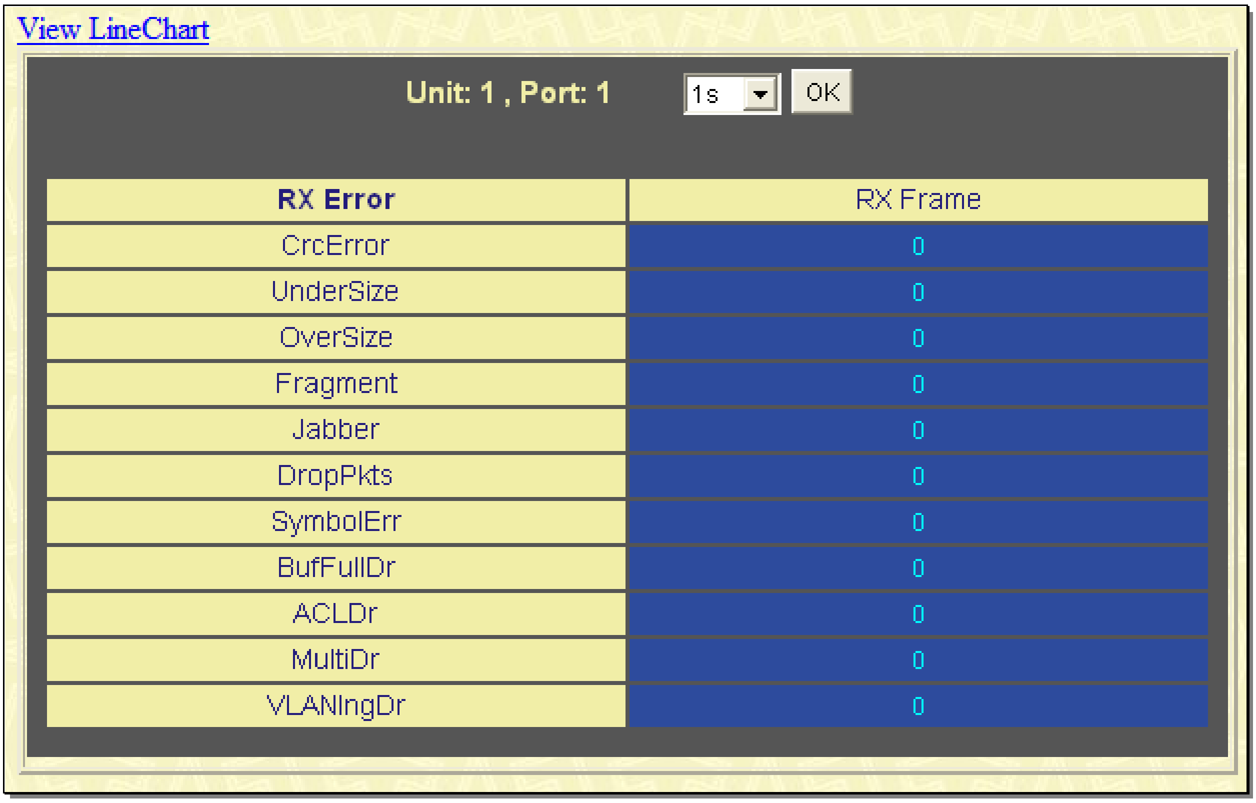
CrcError 0
UnderSize 0
OverSize 0
Fragment 0
Jabber 0
DropPkts 0
SymbolErr 0
BufFullDr 0
ACLDr 0
MultiDr 0
VLANIngDr 0

Time Interval: 1s
Record Number: 200

Show/Hide ☑ CrcError ☑ UnderSize ☑ OverSize ☑ Fragment ☑ Jabber ☑ DropPkts
☑ SymbolErr ☑ BufFullDr ☑ ACLDr ☑ MultiDr ☑ VLANIngDr

Figure 8- 14. RX Error Analysis window (line graph)

To view the Received Error Packets Table, click the link View Table, which will show the following table:



RX Error	RX Frame
CrcError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
DropPkts	0
SymbolErr	0
BufFullDr	0
ACLDr	0
MultiDr	0
VLANIngDr	0

Figure 8- 15. 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 *200*.
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 the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536 octets, or if a VLAN frame of 1540 octets was received.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts the error packets that were received that exceeded 1518 bytes, or for VLAN frames, 1522 bytes, and less than the MAX_PKT_LEN. The MAX_PKT_LEN is equal to 1536 bytes, and 1540 bytes for a VLAN frame.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Symbol	Counts the number of packets received that have errors received in the symbol on the physical labor.
BuFullDr	Incremented for each packet that is discarded while the input buffer is full.
ACLDr	Incremented for each packet that is denied by ACLs.
MultiDr	Incremented for each multicast packet that is discared.

VLANIngDr	Incremented for each packet that is discarded by VLAN ingress checking.
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 LineChart	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)**, as shown below:

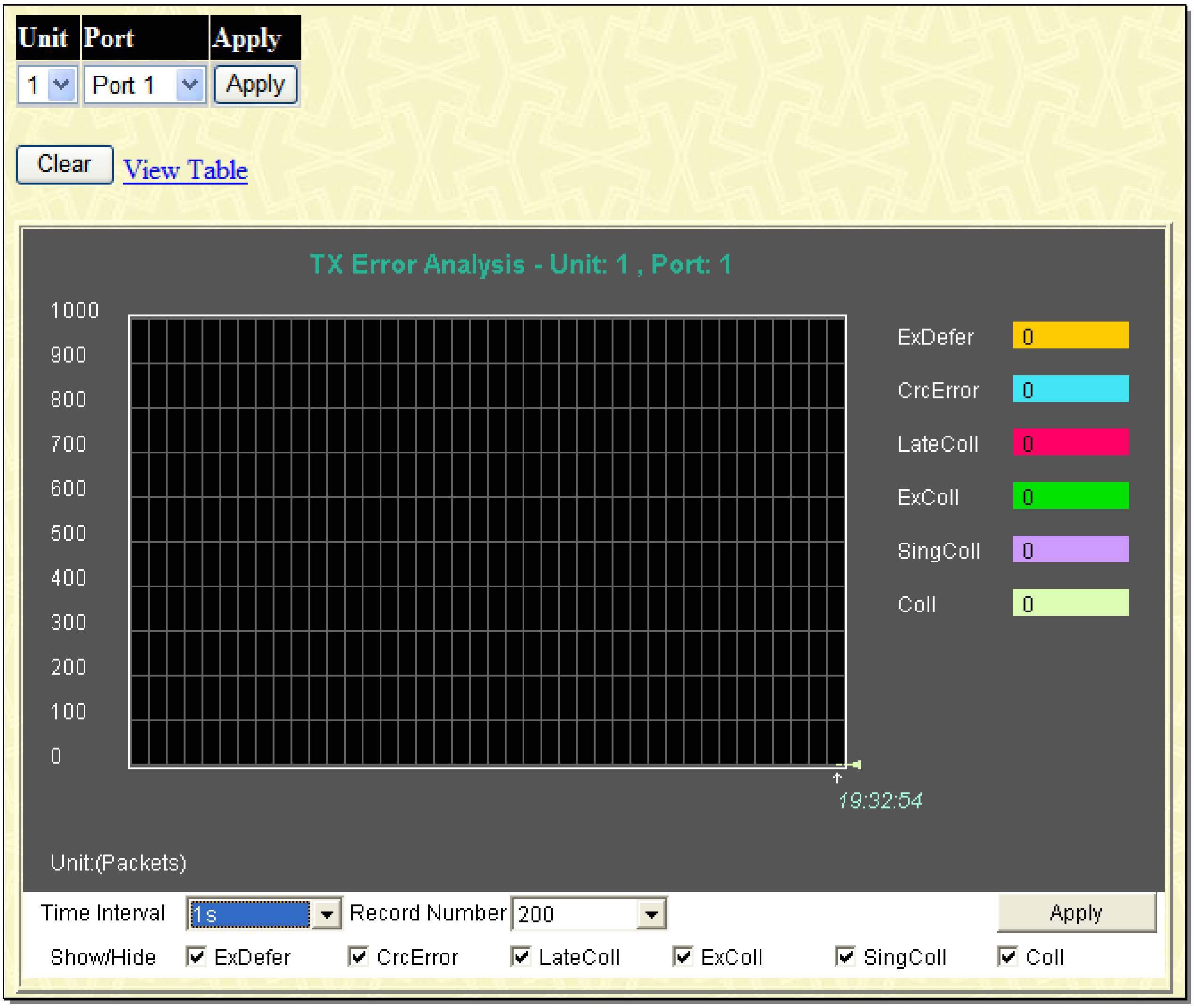
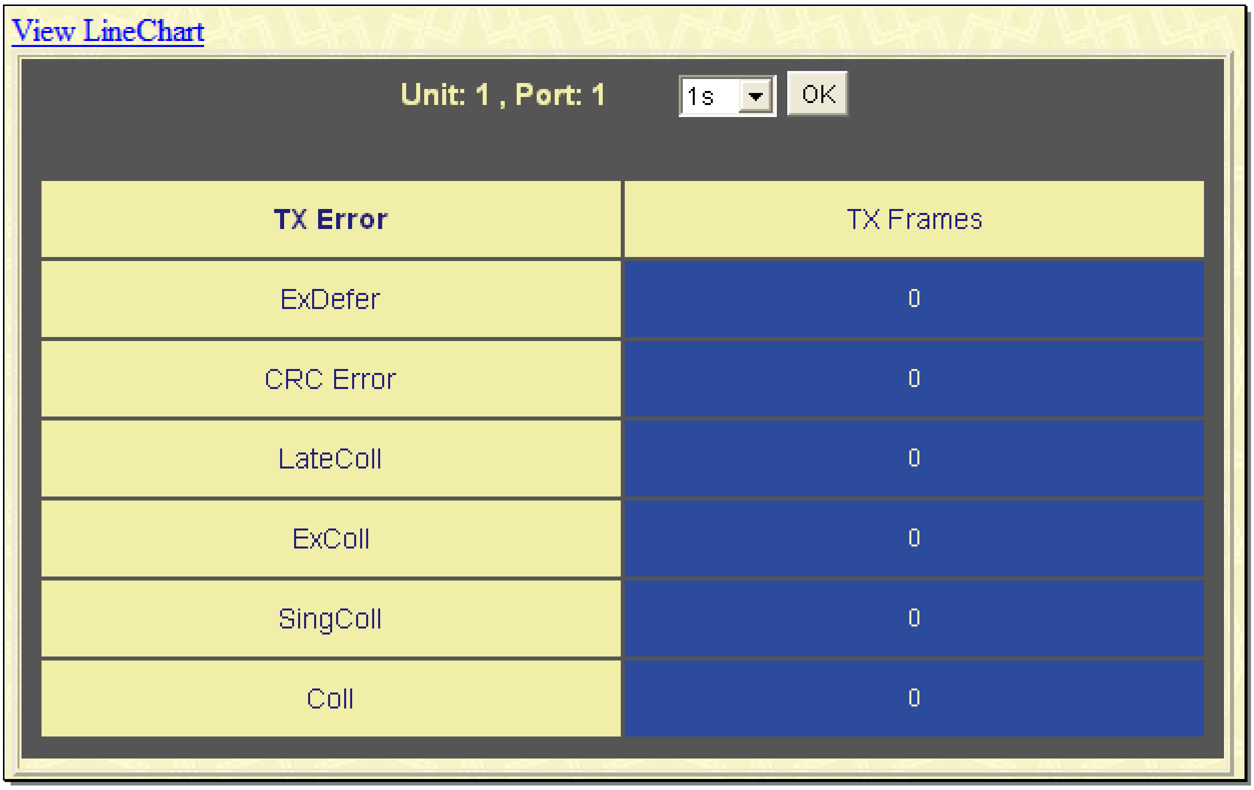


Figure 8- 16. TX Error Analysis window (line graph)

To view the Transmitted Error Packets Table, click the link View Table, which will show the following table:



View LineChart

Unit: 1 , Port: 1 1s OK

TX Error	TX Frames
ExDefer	0
CRC Error	0
LateColl	0
ExColl	0
SingColl	0
Coll	0

Figure 8- 17. TX Error Analysis window (table)

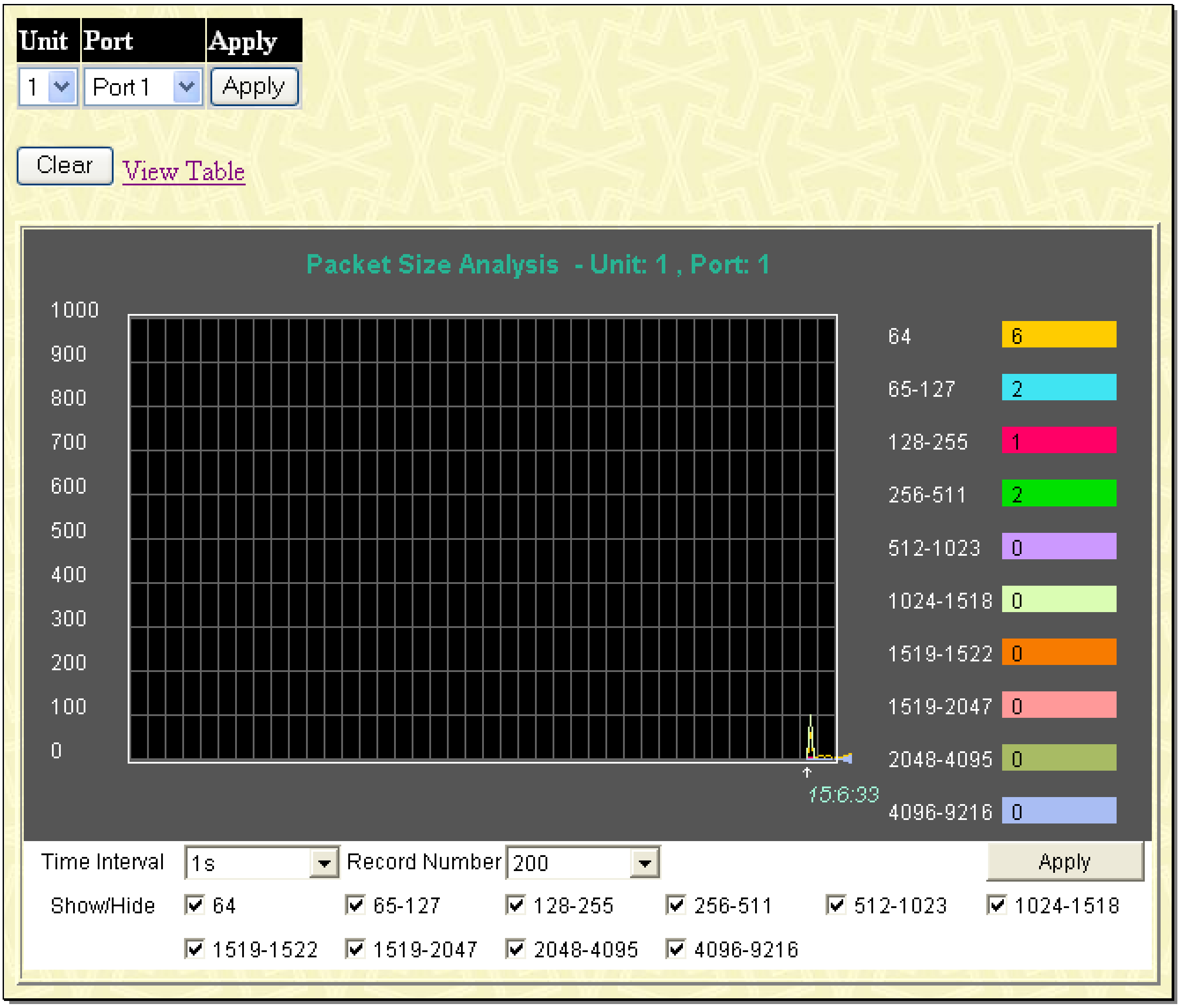
The following fields may be set or viewed:

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 *200*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
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 LineChart	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.

To view this table, click **Monitoring** > **Packet Size**, the following window will be displayed.



Unit	Port	Apply
1	Port 1	Apply

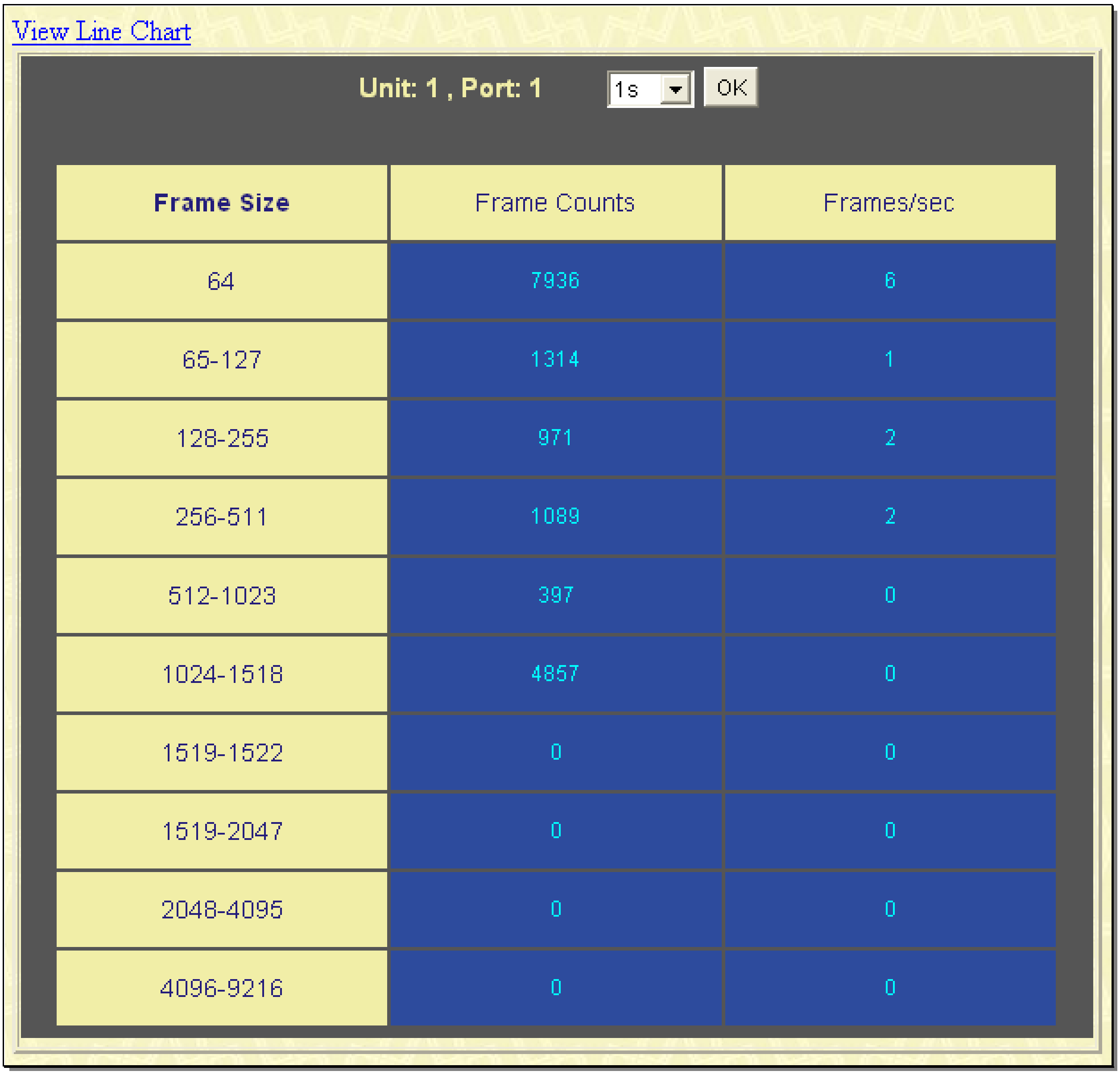
Clear View Table

Time Interval: 1s Record Number: 200 Apply

Show/Hide: ☑ 64 ☑ 65-127 ☑ 128-255 ☑ 256-511 ☑ 512-1023 ☑ 1024-1518 ☑ 1519-1522 ☑ 1519-2047 ☑ 2048-4095 ☑ 4096-9216

Figure 8- 18. RX Size Analysis window (line graph)

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



Unit: 1 , Port: 1

Frame Size	Frame Counts	Frames/sec
64	7936	6
65-127	1314	1
128-255	971	2
256-511	1089	2
512-1023	397	0
1024-1518	4857	0
1519-1522	0	0
1519-2047	0	0
2048-4095	0	0
4096-9216	0	0

Figure 8- 19. TX/RX Packet Size Analysis window (table)

The following fields can be set or viewed:

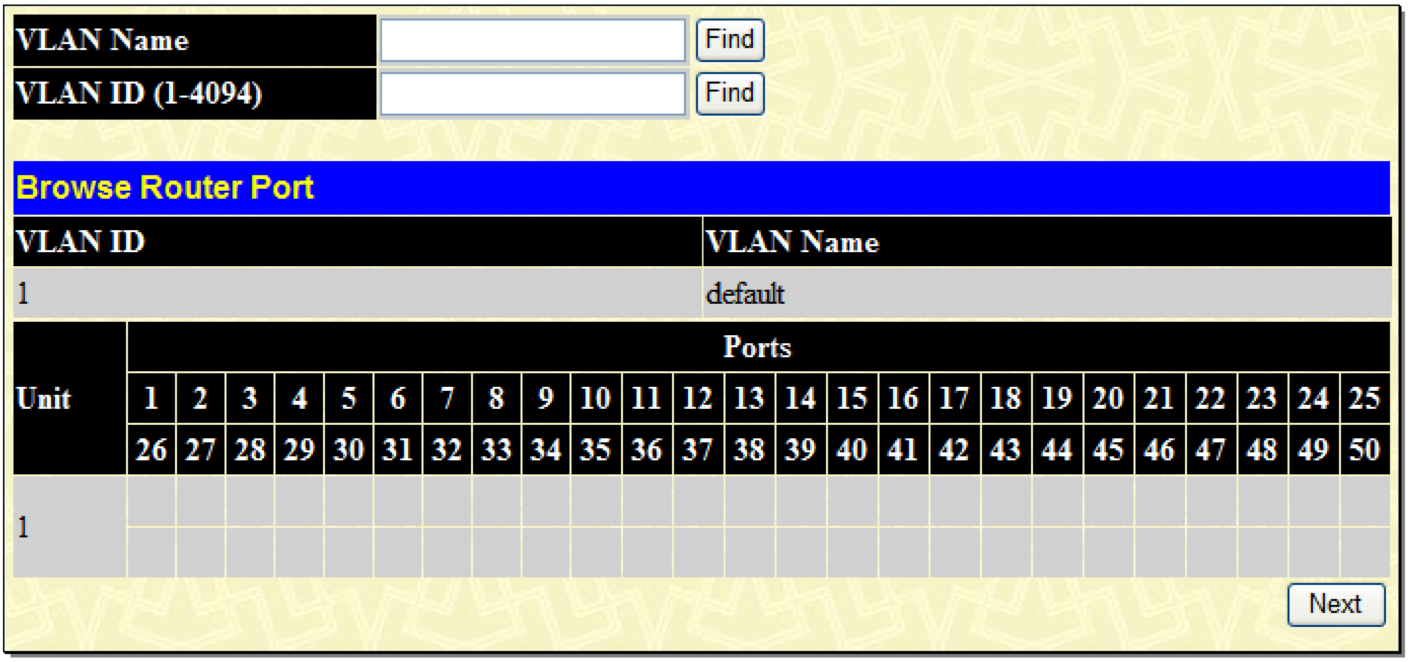
Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023

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

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



VLAN Name	
VLAN ID (1-4094)	

Browse Router Port

VLAN ID	VLAN Name
1	default

Unit	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	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1																									

Figure 8- 20. Browse Router Port window

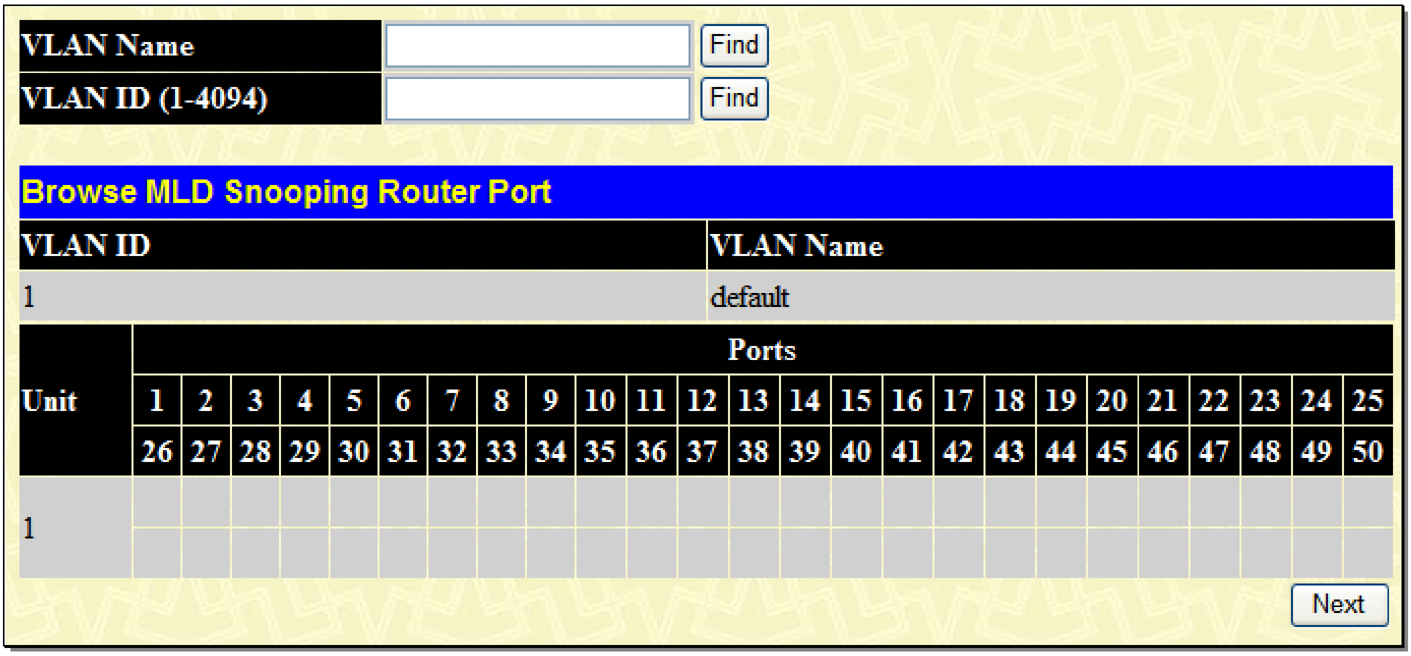
The following fields may be set or viewed:

Parameter	Description
VLAN Name	Enter the VLAN name and then click the **Find** button.
VLAN ID (1-4094)	Enter the VLAN ID and then click the **Find** button.

Browse MLD Router Port

This displays which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the Switch is designated by **D** and a Forbidden port is designated by **F**.

To view this window, click **Monitoring** > **Browse MLD Snooping Router Port**, as shown below:



VLAN Name	
VLAN ID (1-4094)	

Browse MLD Snooping Router Port

VLAN ID	VLAN Name
1	default

Unit	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	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1																									

Figure 8- 21. Browse MLD Snooping Router Port window

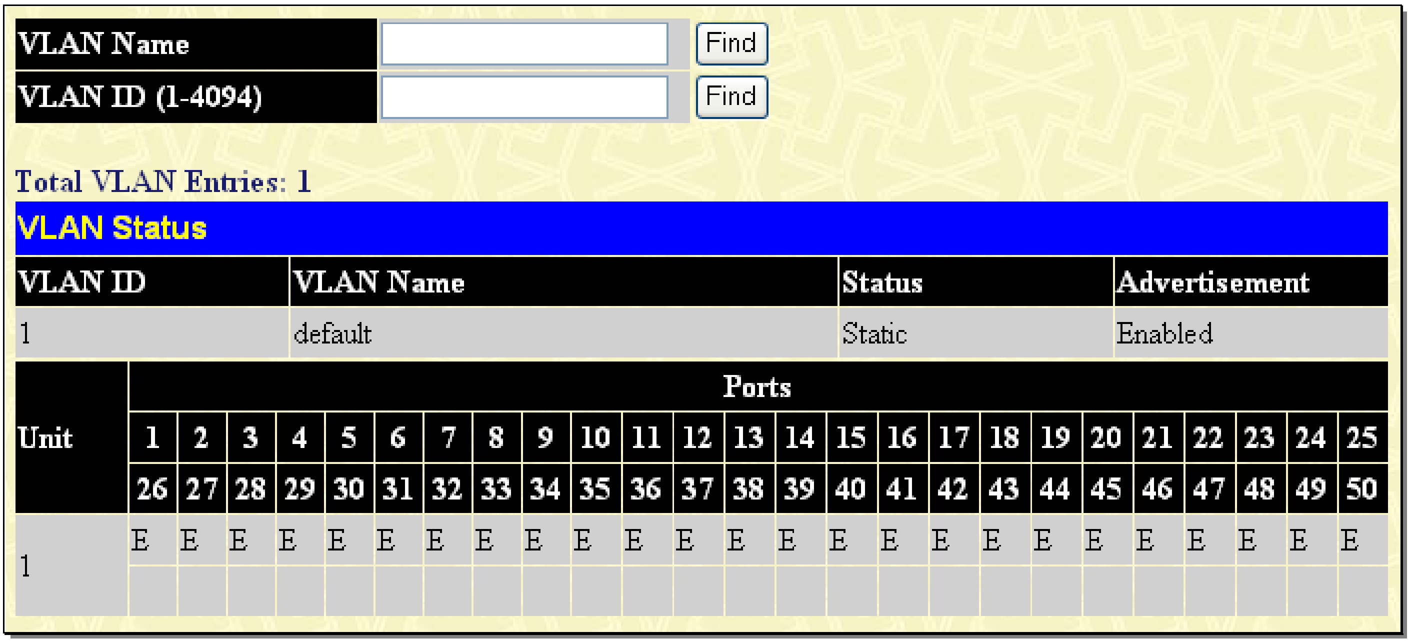
The following fields may be set or viewed:

Parameter	Description
VLAN Name	Enter the VLAN name and then click the **Find** button.
VLAN ID (1-4094)	Enter the VLAN ID and then click the **Find** button.

VLAN Status

This allows the VLAN status for each of the Switch's ports to be viewed by VLAN. This window displays the ports on the Switch that are currently Egress (E) or Tag (T) ports. To view the next VLAN in the list, click the **Next** button.

To view this window, click **Monitoring** > **VLAN Status**, as shown below:



VLAN Name		Find
VLAN ID (1-4094)		Find

Total VLAN Entries: 1

VLAN Status

VLAN ID	VLAN Name	Status	Advertisement
1	default	Static	Enabled

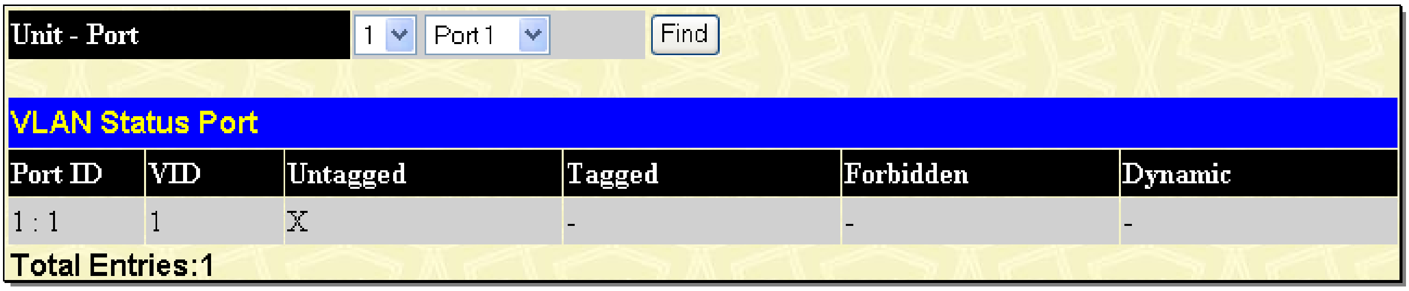
Unit	Ports																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E

Figure 8- 22. VLAN Status window

VLAN Status Port

This read-only window displays the current VLAN status for the port selected using the drop-down menu.

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



Unit - Port	1	Port 1	Find

VLAN Status Port

Port ID	VID	Untagged	Tagged	Forbidden	Dynamic
1 : 1	1	X	-	-	-

Total Entries:1

Figure 8- 23. VLAN Status Port window

Port Access Control

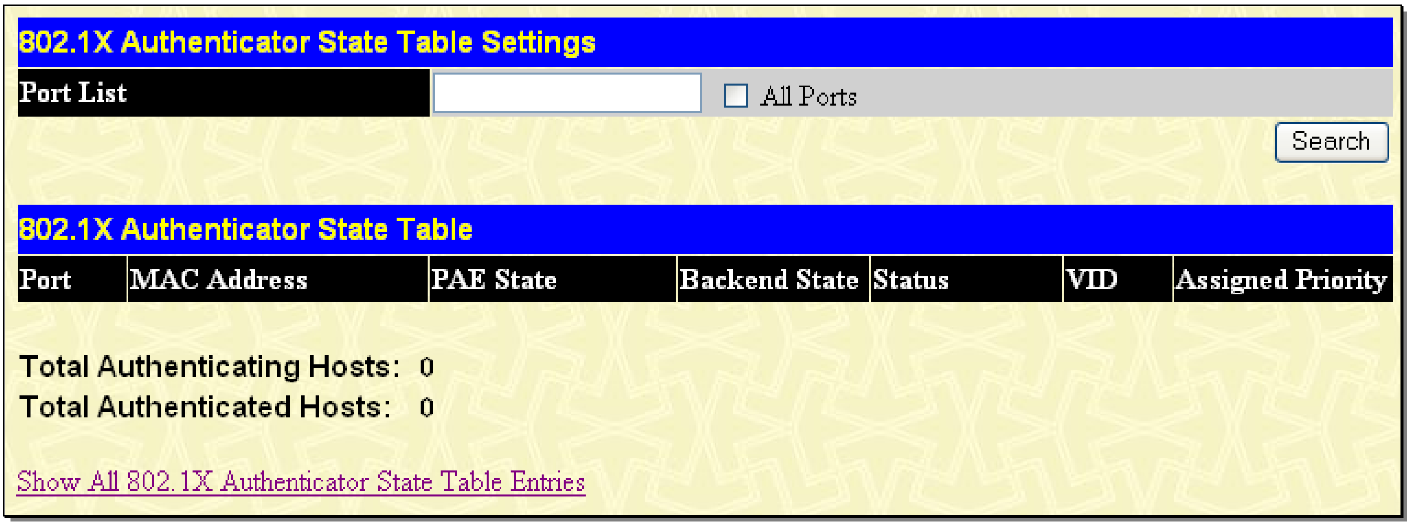
The following windows are used to monitor 802.1X statistics of the Switch, on a per port basis. To view the **Port Access Control** windows, click **monitoring** > **Port Access Control**. There are six windows to monitor.

NOTE: The Authenticator State cannot be viewed on the Switch unless 802.1X is enabled by port or by MAC address. To enable 802.1X, go to the DGS-3600 Web Management Tool window.

Authenticator State

The following section describes the 802.1X Status on the Switch. This window displays the Authenticator State for individual ports on a selected device.

To view the Authenticator State click **Monitoring** > **Port Access Control** > **Authenticator State**, as shown below:



802.1X Authenticator State Table Settings

Port List □ All Ports

Search

802.1X Authenticator State Table

Port	MAC Address	PAE State	Backend State	Status	VID	Assigned Priority

Total Authenticating Hosts: 0

Total Authenticated Hosts: 0

Show All 802.1X Authenticator State Table Entries

Figure 8- 24. 802.1X Authenticator State Table Settings window

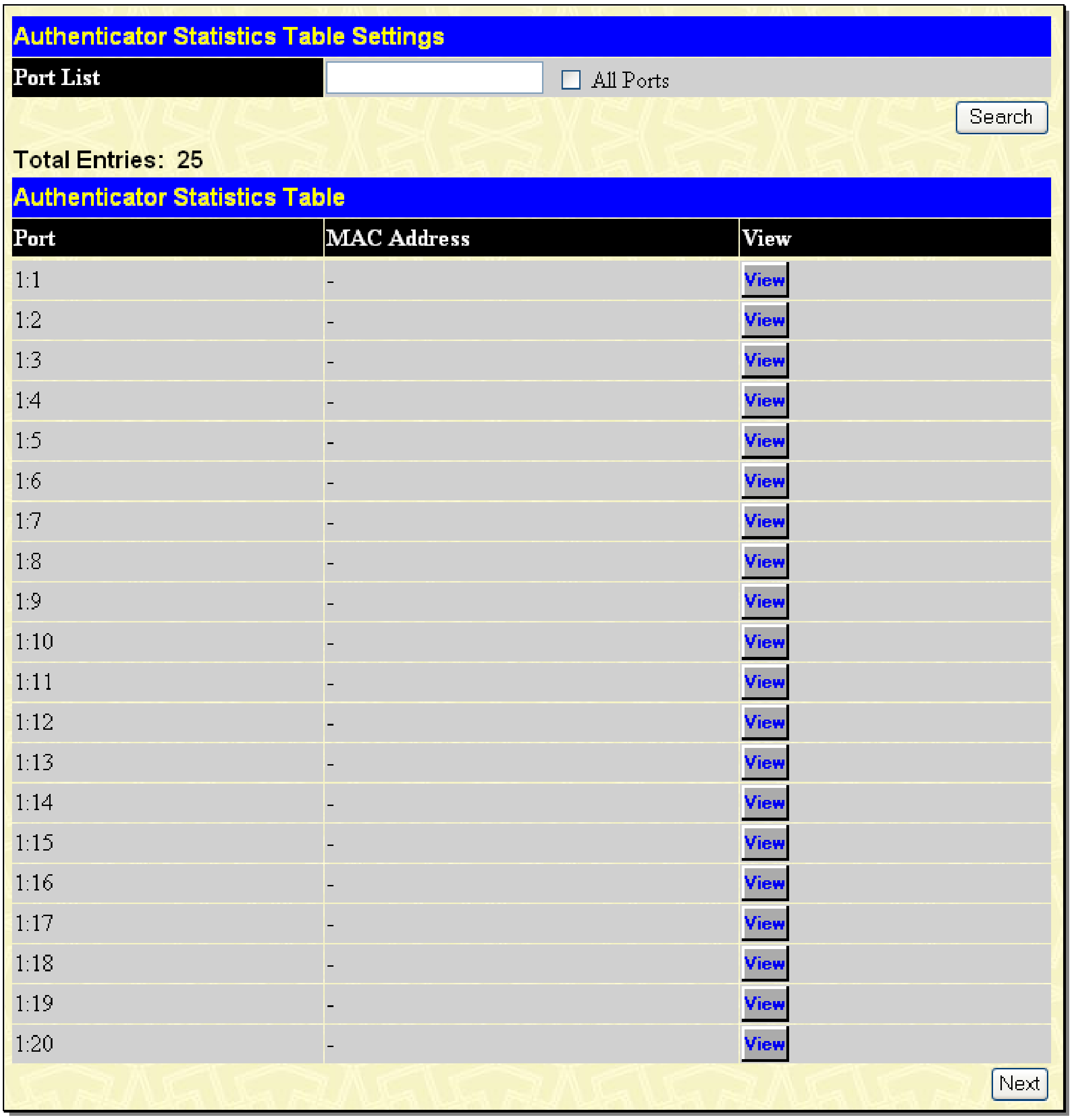
The information on this window is described as follows:

Parameter	Description
Port List	Enter the port or ports for monitoring information to be displayed, or tick the All Ports check box.
Auth PAE State	The Authenticator PAE State value can be: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Backend State	The Backend Authentication State can be Request, Response, Success, Fail, Timeout, Idle, Initialize, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be Authorized, Unauthorized, or N/A.

Authenticator Statistics

This table contains the statistics objects for the Authenticator PAE associated with a port. Enter a port or range of ports, or tick the All Ports check box.

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



Authenticator Statistics Table Settings

Port List		□ All Ports

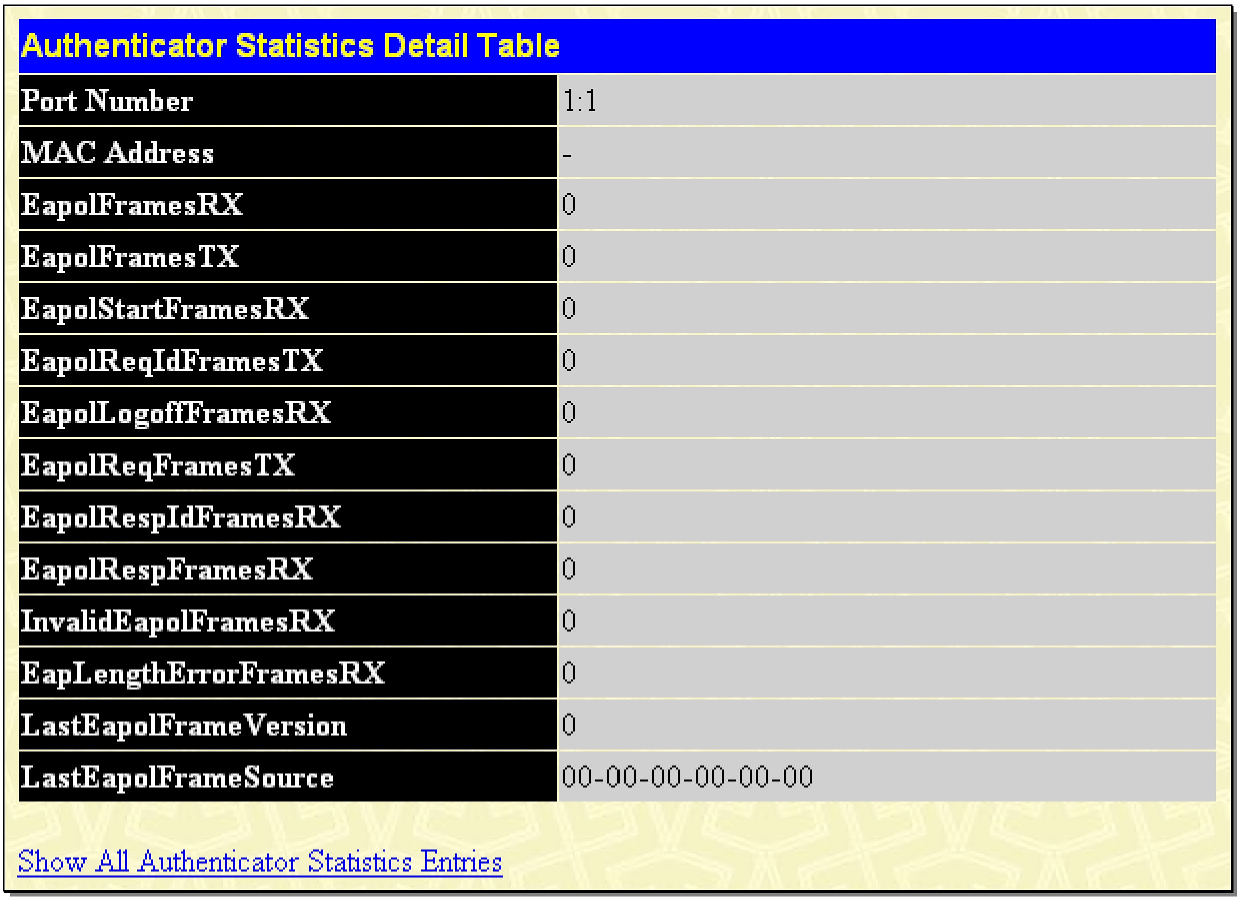
Total Entries: 25

Authenticator Statistics Table

Port	MAC Address	View
1:1	-	View
1:2	-	View
1:3	-	View
1:4	-	View
1:5	-	View
1:6	-	View
1:7	-	View
1:8	-	View
1:9	-	View
1:10	-	View
1:11	-	View
1:12	-	View
1:13	-	View
1:14	-	View
1:15	-	View
1:16	-	View
1:17	-	View
1:18	-	View
1:19	-	View
1:20	-	View

Figure 8- 25. Authenticator Statistics Table Settings window

Click **View** to access the **Authenticator Statistics Detail Table** window, as show below.



Authenticator Statistics Detail Table	
Port Number	1:1
MAC Address	-
EapolFramesRX	0
EapolFramesTX	0
EapolStartFramesRX	0
EapolReqIdFramesTX	0
EapolLogoffFramesRX	0
EapolReqFramesTX	0
EapolRespIdFramesRX	0
EapolRespFramesRX	0
InvalidEapolFramesRX	0
EapLengthErrorFramesRX	0
LastEapolFrameVersion	0
LastEapolFrameSource	00-00-00-00-00-00

Figure 8- 26. Authenticator Statistics Detail Table window

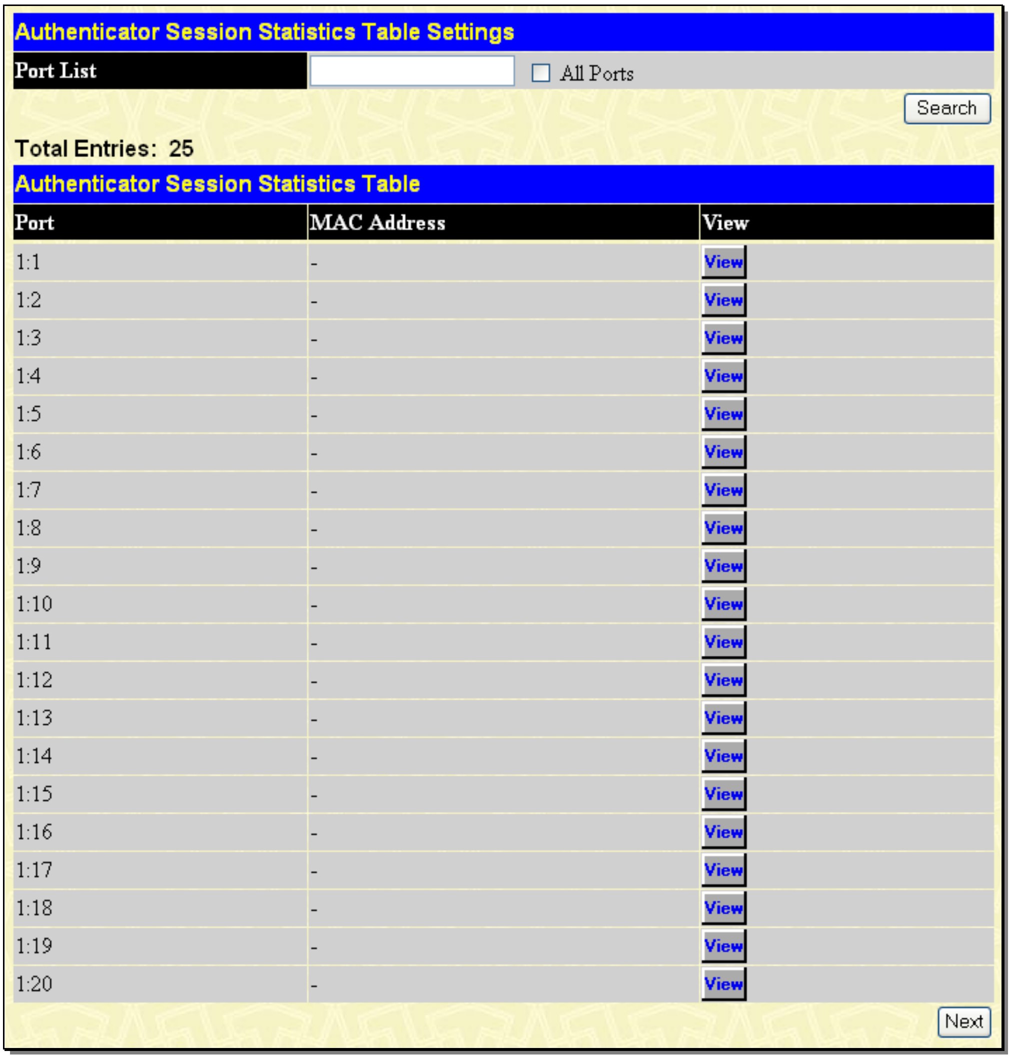
The following fields can be viewed:

Parameter	Description
Port/Port Number	The identification number assigned to the Port by the System in which the Port resides.
MAC Address	
EapolFramesRX	The number of valid EAPOL frames that have been received by this Authenticator.
EapolFramesTX	The number of EAPOL frames that have been transmitted by this Authenticator.
EapolStartFramesRX	The number of EAPOL Start frames that have been received by this Authenticator.
EapolReqIdFramesTX	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolLogoffFramesRX	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolReqFramesTX	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
EapolRespIdFramesRX	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRX	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
InvalidEapolFramesRX	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRX	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Authenticator Session Statistics

This table contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. Enter a port or range of ports, or tick the All Ports check box.

To view the **Authenticator Session Statistics**, click **Monitoring > Port Access Control > Authenticator Session Statistics**, as shown below:



Authenticator Session Statistics Table Settings

Port List	□ All Ports

Search

Total Entries: 25

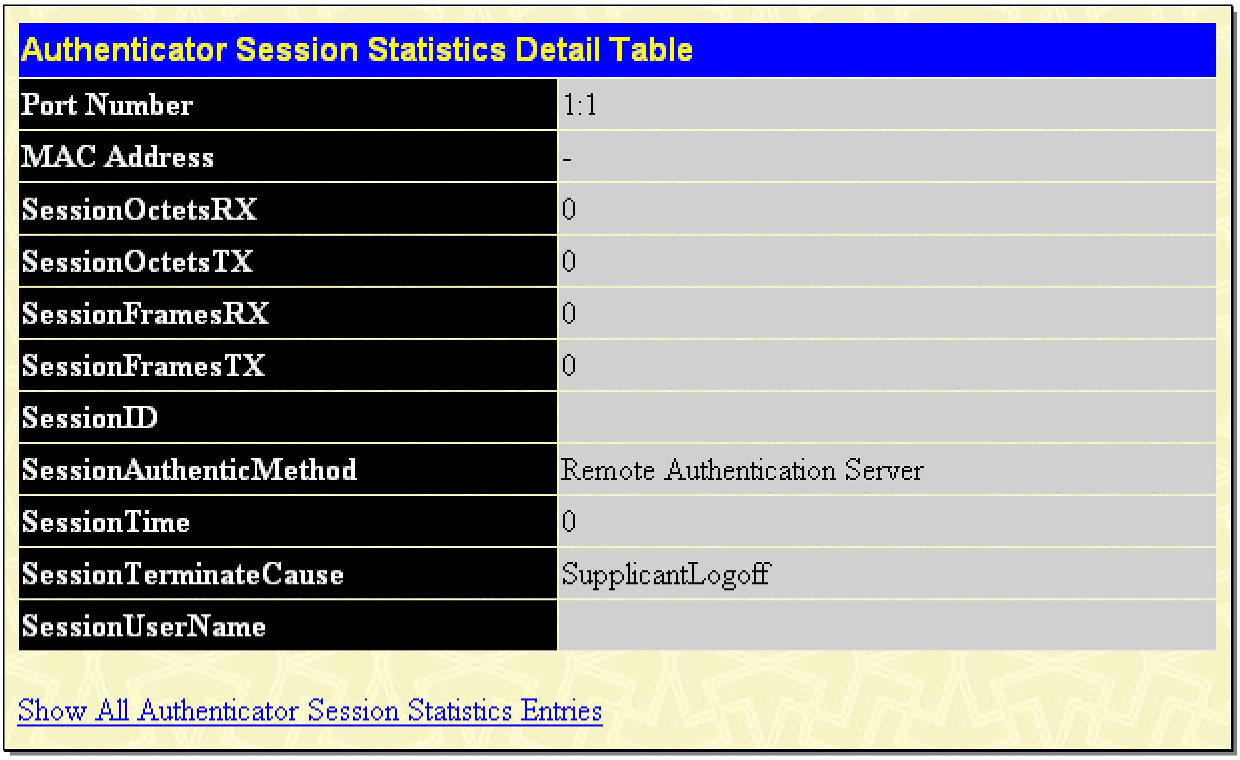
Authenticator Session Statistics Table

Port	MAC Address	View
1:1	-	View
1:2	-	View
1:3	-	View
1:4	-	View
1:5	-	View
1:6	-	View
1:7	-	View
1:8	-	View
1:9	-	View
1:10	-	View
1:11	-	View
1:12	-	View
1:13	-	View
1:14	-	View
1:15	-	View
1:16	-	View
1:17	-	View
1:18	-	View
1:19	-	View
1:20	-	View

Next

Figure 8- 27. Authenticator Session Statistics Table Settings window

Click **View** to access the **Authenticator Statistics Detail Table** window, as show below.



Authenticator Session Statistics Detail Table	
Port Number	1:1
MAC Address	-
SessionOctetsRX	0
SessionOctetsTX	0
SessionFramesRX	0
SessionFramesTX	0
SessionID	
SessionAuthenticMethod	Remote Authentication Server
SessionTime	0
SessionTerminateCause	SupplicantLogoff
SessionUserName	

Show All Authenticator Session Statistics Entries

Figure 8- 28. Authenticator Session Statistics Detail Table window

The following fields can be viewed:

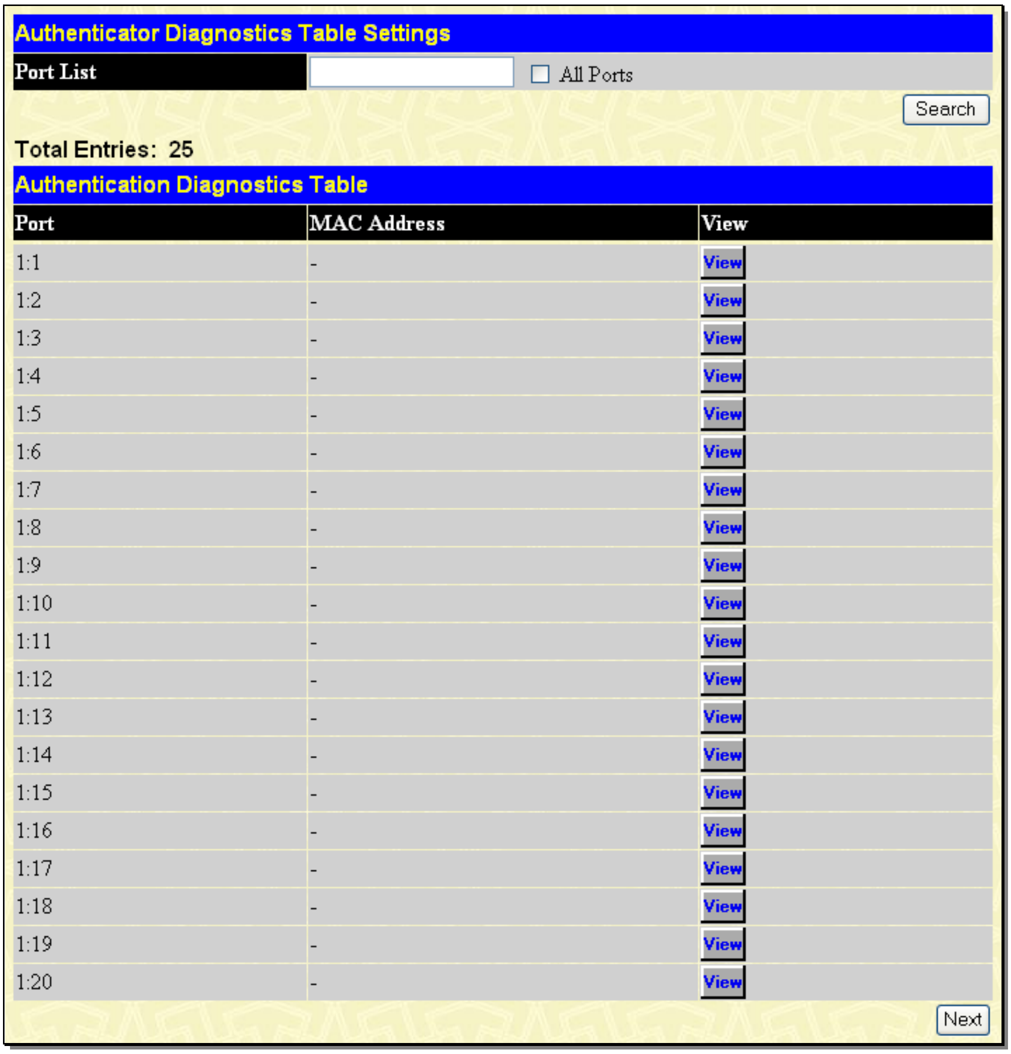
Parameter	Description
Port/Port Number	The identification number assigned to the Port by the System in which the Port resides.
MAC Address	The MAC address of the Switch where the port resides.
SessionOctetsRX	The number of octets received in user data frames on this port during the session.
SessionOctetsTX	The number of octets transmitted in user data frames on this port during the session.
SessionFramesRX	The number of user data frames received on this port during the session.
SessionFramesTX	The number of user data frames transmitted on this port during the session.
SessionID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
SessionAuthentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server – The Authentication Server is external to the Authenticator's System. (2) Local Authentic Server – The Authentication Server is located within the Authenticator's System.
SessionTime	The duration of the session in seconds.
SessionTerminate Cause	The reason for the session termination. There are eight possible reasons for termination. 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization

	7) Port Administratively Disabled 8) Not Terminated Yet
SessionUserName	The User-Name representing the identity of the Supplicant PAE.

Authenticator Diagnostics

This table contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function. Enter a port or range of ports, or tick the All Ports check box.

To view the **Authenticator Diagnostics**, click **Monitoring** > **Port Access Control** > **Authenticator Diagnostics**, as shown below:



Authenticator Diagnostics Table Settings

Port List: ______ □ All Ports

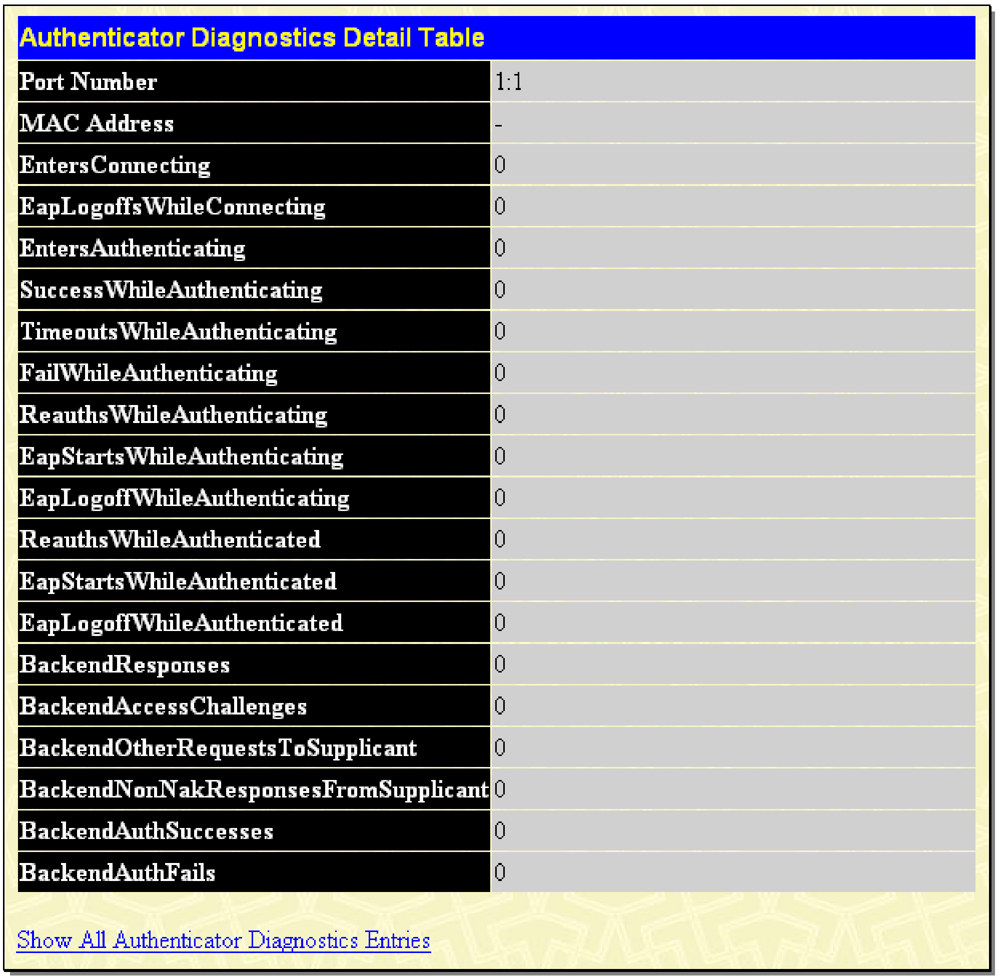
Total Entries: 25

Authentication Diagnostics Table

Port	MAC Address	View
1:1	-	View
1:2	-	View
1:3	-	View
1:4	-	View
1:5	-	View
1:6	-	View
1:7	-	View
1:8	-	View
1:9	-	View
1:10	-	View
1:11	-	View
1:12	-	View
1:13	-	View
1:14	-	View
1:15	-	View
1:16	-	View
1:17	-	View
1:18	-	View
1:19	-	View
1:20	-	View

Figure 8- 29. Authenticator Diagnostics window

Click **View** to access the **Authenticator Statistics Detail Table** window, as show below.



Authenticator Diagnostics Detail Table	
Port Number	1:1
MAC Address	-
EntersConnecting	0
EapLogoffsWhileConnecting	0
EntersAuthenticating	0
SuccessWhileAuthenticating	0
TimeoutsWhileAuthenticating	0
FailWhileAuthenticating	0
ReauthsWhileAuthenticating	0
EapStartsWhileAuthenticating	0
EapLogoffWhileAuthenticating	0
ReauthsWhileAuthenticated	0
EapStartsWhileAuthenticated	0
EapLogoffWhileAuthenticated	0
BackendResponses	0
BackendAccessChallenges	0
BackendOtherRequestsToSupplicant	0
BackendNonNakResponsesFromSupplicant	0
BackendAuthSuccesses	0
BackendAuthFails	0

Figure 8- 30. Authenticator Diagnostics Detail Table window

The following fields can be viewed:

Parameter	Description
Port/Port Number	The identification number assigned to the Port by the System in which the Port resides.
MAC Address	The MAC address of the Switch where the port resides.
EntersConnecting	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
SuccessWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
TimeoutsWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).

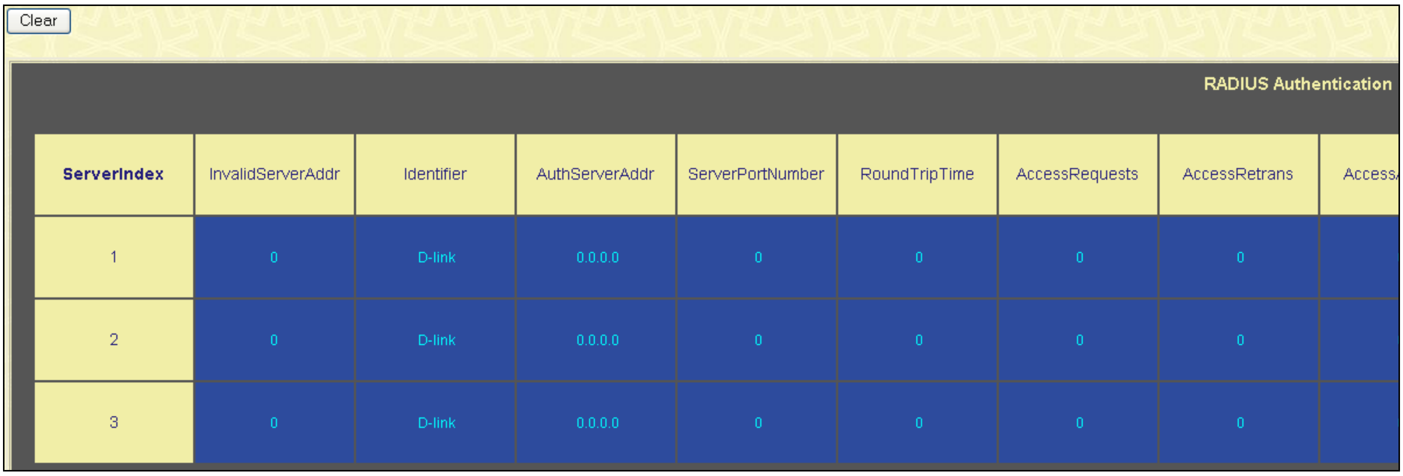
FailWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).
ReauthsWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
EapStartsWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
EapLogoffWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
ReauthsWhileAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
EapStartsWhileAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
EapLogoffWhileAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
BackendResponses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
BackendAccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
BackendOtherRequestToSupplicant	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
BackendAuthSuccesses	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
BackendAuthFails	Counts the number of times that the state machine receives a

	Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

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**, as shown below:



ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	AccessRetrans	Access
1	0	D-link	0.0.0.0	0	0	0	0	
2	0	D-link	0.0.0.0	0	0	0	0	
3	0	D-link	0.0.0.0	0	0	0	0	

Figure 8- 31. 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:

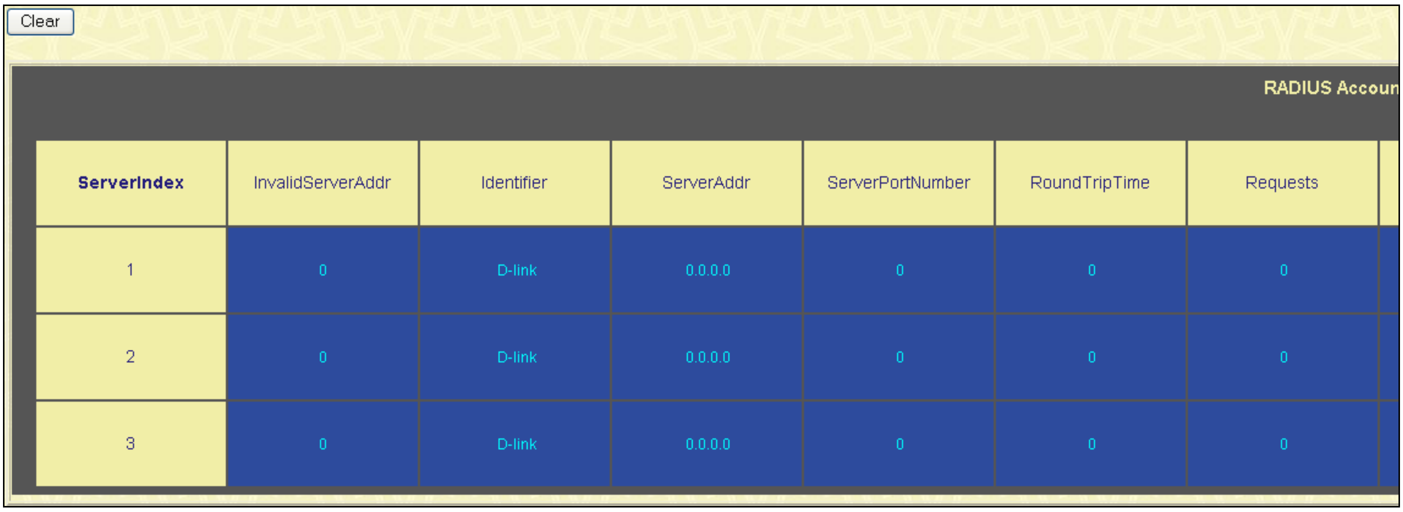
Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client. (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 Account Client

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 Account Client** window, click **Monitoring** > **Port Access Control** > **RADIUS Account Client**, as shown below:



ServerIndex	InvalidServerAddr	Identifier	ServerAddr	ServerPortNumber	RoundTripTime	Requests
1	0	D-link	0.0.0.0	0	0	0
2	0	D-link	0.0.0.0	0	0	0
3	0	D-link	0.0.0.0	0	0	0

Figure 8- 32. RADIUS Account Client window

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

The following fields can be viewed:

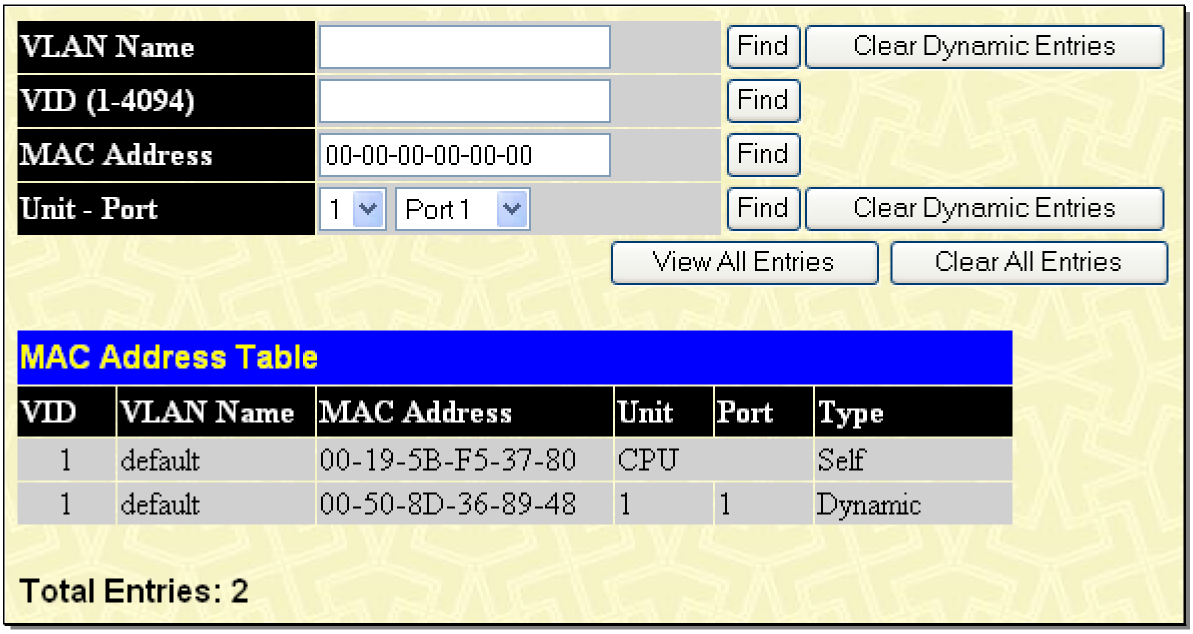
Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.

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 that 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.

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**, as shown below:



VLAN Name	
VID (1-4094)	
MAC Address	00-00-00-00-00-00
Unit - Port	1 Port 1

MAC Address Table

VID	VLAN Name	MAC Address	Unit	Port	Type
1	default	00-19-5B-F5-37-80	CPU		Self
1	default	00-50-8D-36-89-48	1	1	Dynamic

Total Entries: 2

Figure 8- 33. MAC Address Table window

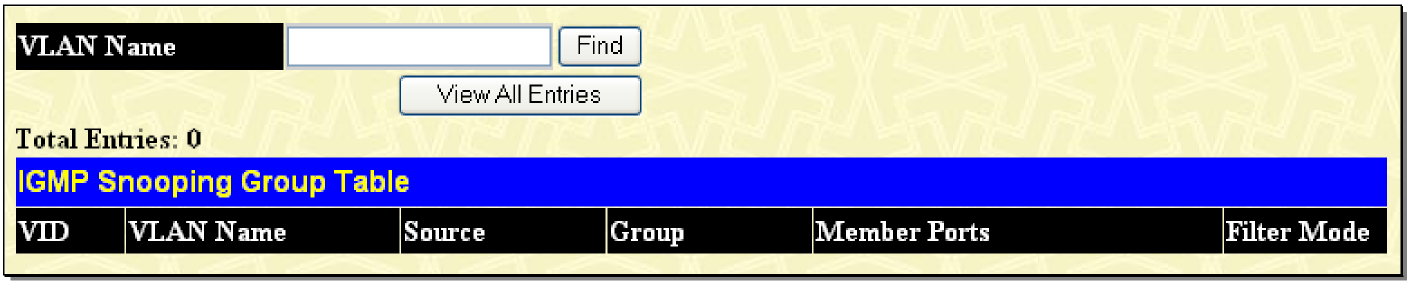
The following fields can be viewed or set:

Parameter	Description
VLAN Name	Enter a VLAN Name for which to browse the forwarding table.
VID (1-4094)	Enter a VLAN ID between 1 and 4094 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.
Unit – Port	The Unit and 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.

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.

To view this window, click **Monitoring** > **IGMP Snooping Group**, as shown below:



VLAN Name		Find
		View All Entries

Total Entries: 0

IGMP Snooping Group Table

VID	VLAN Name	Source	Group	Member Ports	Filter Mode

Figure 8- 34. IGMP Snooping Group Table window

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

NOTE: The Switch supports up to 4K IGMP Snooping groups.

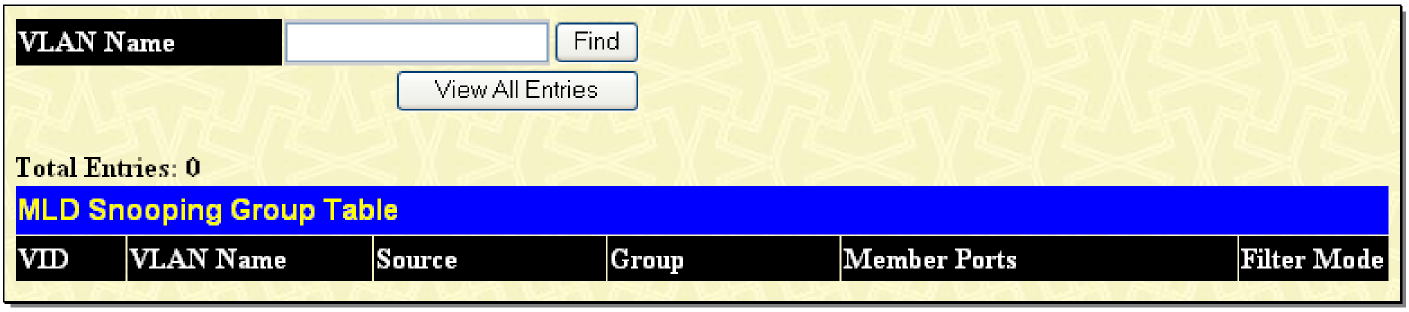
The following field can be viewed:

Parameter	Description
VID	The VLAN ID of the VLAN.
VLAN Name	The VLAN name which the member port belongs to.
Source	Displays the status of the source filtering, which is the ability for a system to report the interest in receiving packets from specific source addresses or sent to a particular multicast address.
Group	Specifies the multicast address of the multicast group.
Member Ports	The ports that are members of the multicast group.
Filter Mode	The Filter Mode will display *Include* or *Exclude* depending on whether or not the multicast-address has been configured to include or exclude the filter.

MLD Snooping Group

The following window allows the user to view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4. The user may browse this table by VLAN Name present in the switch by entering that VLAN Name in the empty field shown below, and clicking the **Find** button.

To view this window, click **Monitoring** > **MLD Snooping Group**, as shown below:



VLAN Name

Total Entries: 0

MLD Snooping Group Table

VID	VLAN Name	Source	Group	Member Ports	Filter Mode

Figure 8- 35. MLD Snooping Group Table window

The following field can be viewed:

Parameter	Description
VID	The VLAN ID of theVLAN.
VLAN Name	The VLAN to which the member port belongs.
Source	Displays the status of the source filtering, which is the ability for a system to report the interest in receiving packets from specific source addresses or sent to a particular multicast address.
Group	The IP address of the MLD multicast group.
Member Ports	The ports that are members of the multicast group.
Filter Mode	The filter mode will display *Include* or *Exclude* depending on whether or not the multicast-address had been configured to include or exclude the filter.

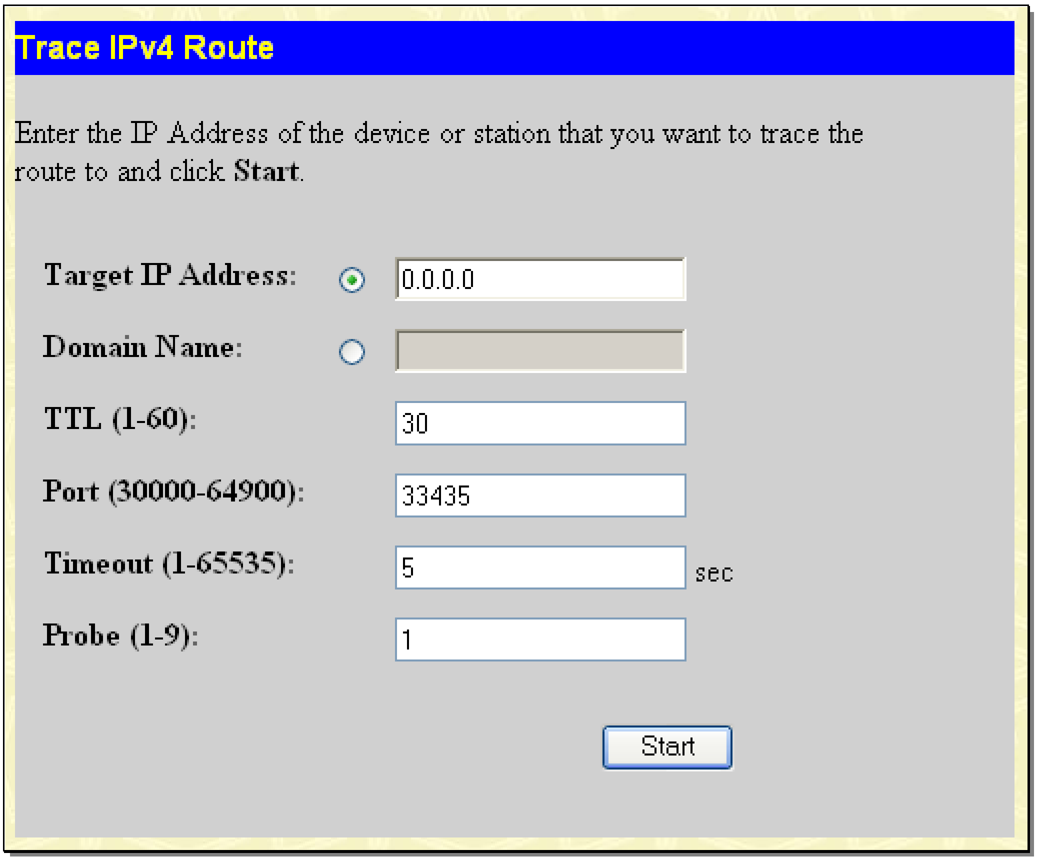
NOTE: To configure MLD snooping for the Switch, go to the **L2 Features** folder and select **MLD Snooping**. Configuration and other information concerning MLD snooping may be found in Section 6 of this manual under MLD Snooping.

Trace Route

The following window will aid the user in back tracing the route taken by a packet before arriving at the Switch. When initiated, the Trace Route program will display the IP addresses of the previous hops a packet takes from the Target IP Address entered in the window, until it reaches the Switch.

Trace Route IPv4 Route

To view this window, click **Monitoring** > **Trace Route** > **Trace IPv4 Route**, as shown below:



Trace IPv4 Route

Enter the IP Address of the device or station that you want to trace the route to and click **Start**.

Target IP Address: ● 0.0.0.0

Domain Name: ○

TTL (1-60): 30

Port (30000-64900): 33435

Timeout (1-65535): 5 sec

Probe (1-9): 1

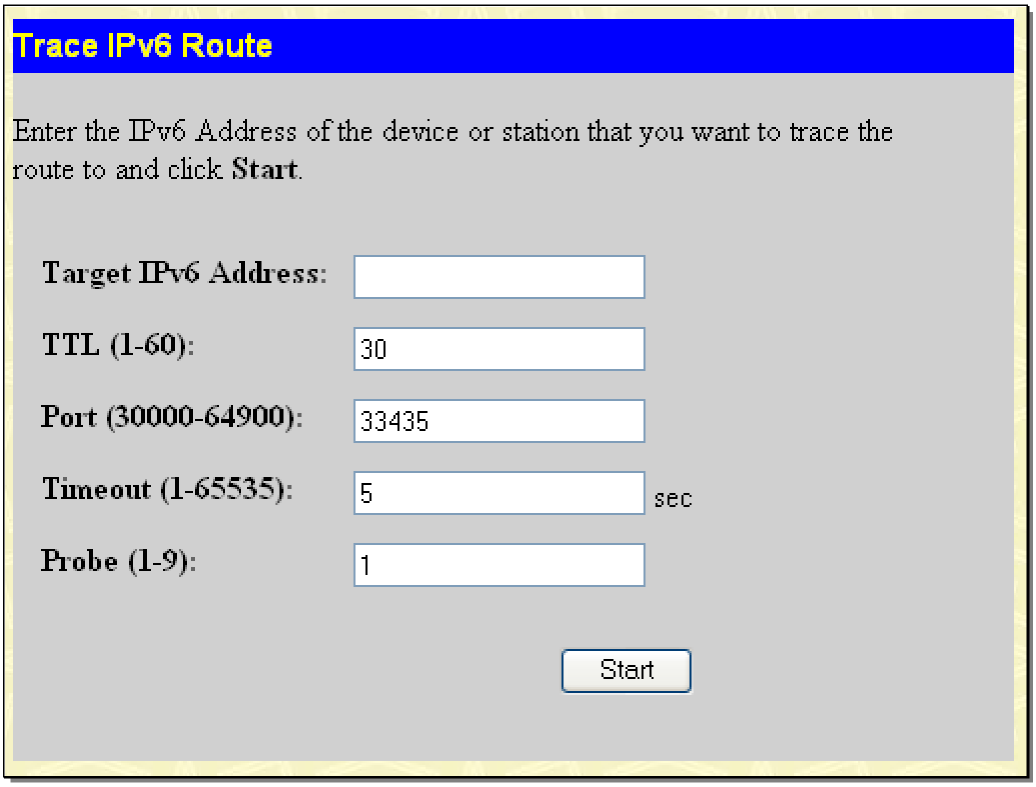
Figure 8- 36. Trace IPv4 Route window

To trace the route of a packet, set the following parameters located in this window, and click **Start**.

Parameter	**Description**
Target IP Address	Enter the IP address of the computer to be traced.
Domain Name	Enter the domain name of the host.
TTL (1-60)	The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.
Port (30000-64900)	The virtual port number. The port number must be above 1024.The value range is from *30000* to *64900*.
Timeout (1-65535)	Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between *1* and *65535* seconds.
Probe (1-9)	The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is *1*.

Trace Route IPv6 Route

To view this window, click **Monitoring** > **Trace Route** > **Trace IPv6 Route**, as shown below:



Trace IPv6 Route

Enter the IPv6 Address of the device or station that you want to trace the route to and click **Start**.

Target IPv6 Address:

TTL (1-60): 30

Port (30000-64900): 33435

Timeout (1-65535): 5 sec

Probe (1-9): 1

Figure 8- 37. Trace IPv6 Route window

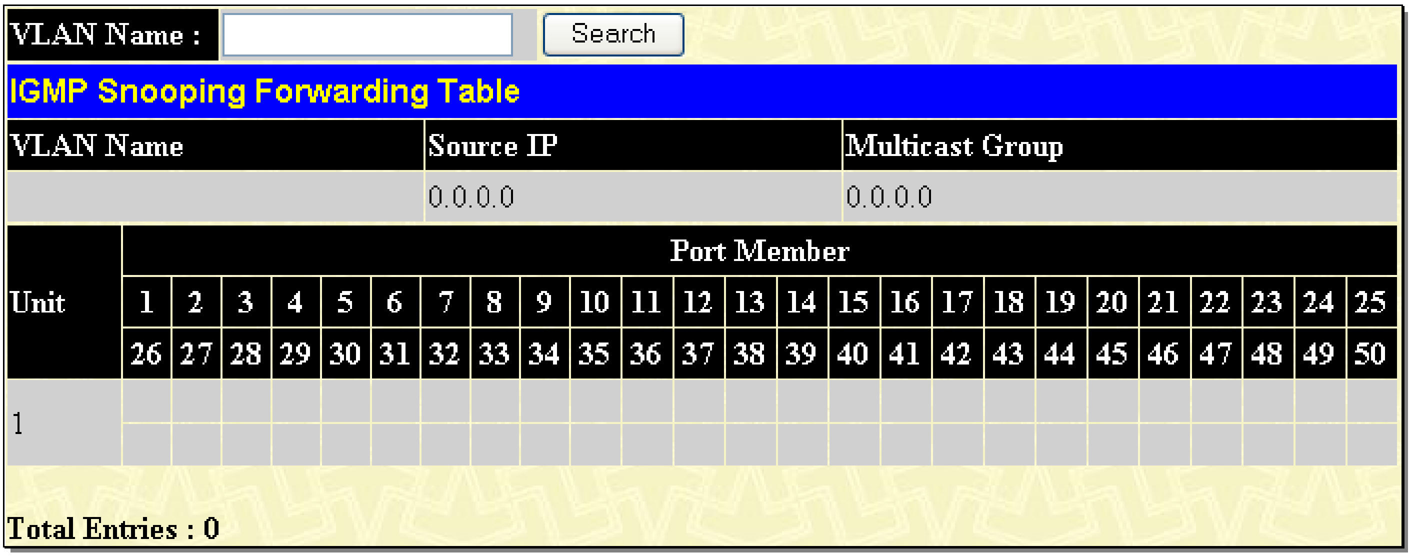
To trace the route of a packet, set the following parameters located in this window, and click **Start**.

Parameter	Description
Target IPv6 Address	Enter the IP address of the computer to be traced.
TTL (1-60)	The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.
Port (30000-64900)	The virtual port number. The port number must be above 1024.The value range is from *30000* to *64900*.
Timeout (1-65535)	Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between *1* and *65535* seconds.
Probe (1-9)	The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is *1*.

IGMP Snooping Forwarding

The IGMP Snooping Forwarding table displays the current multicast traffic that the device has received and which ports it should forward.

To view this window, click **Monitoring** > **IGMP Snooping Forwarding**, as shown below:



IGMP Snooping Forwarding Table

VLAN Name	Source IP	Multicast Group
	0.0.0.0	0.0.0.0

Unit	Port Member																								
	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	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1																									

Total Entries : 0

Figure 8- 38. IGMP Snooping Forwarding Table window

The user may search the IGMP Snooping Forwarding Table by VLAN Name by entering a VLAN name and then clicking **Search**.

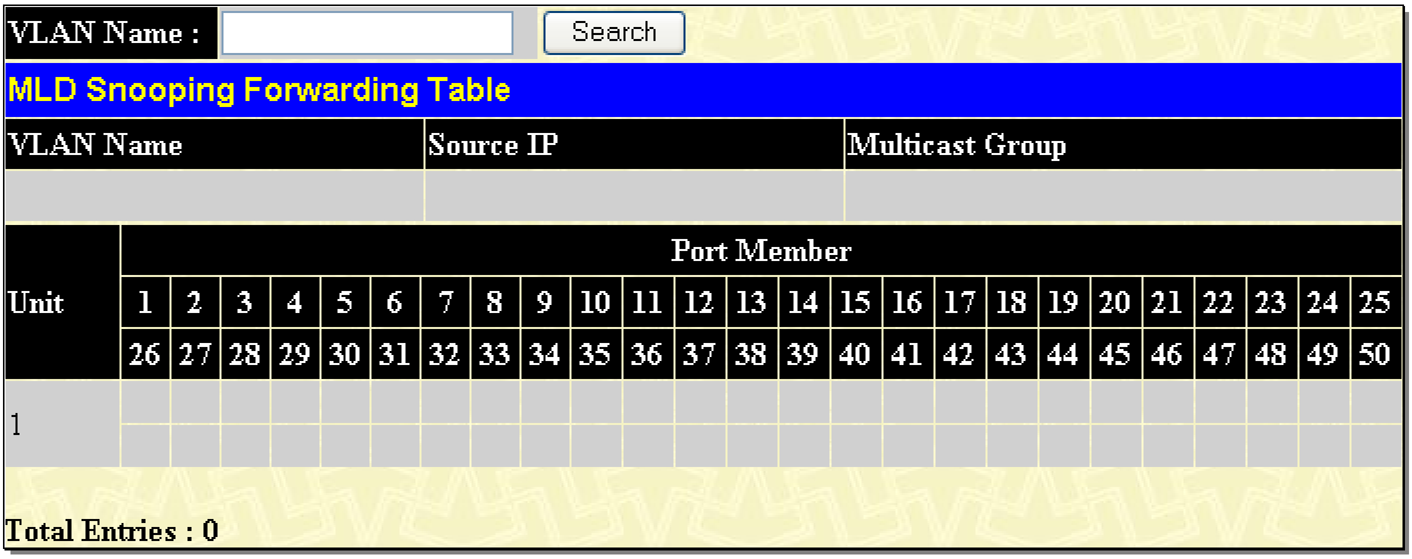
The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name where multicast packets are being received.
Source IP	The Source IP address that is sending multicast packets.
Multicast Group	The Multicast IP address located in the multicast packet.
Port Member	These are the ports where the IP multicast packets are being forwarded.

MLD Snooping Forwarding

The MLD Snooping Forwarding table displays the current multicast traffic entries that the device has received and which ports it should be forwarded to.

To view this window, click **Monitoring** > **MLD Snooping Forwarding**, as shown below:



MLD Snooping Forwarding Table

VLAN Name	Source IP	Multicast Group

Unit	Port Member																								
	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	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1																									

Total Entries : 0

Figure 8- 39. MLD Snooping Forwarding Table window

The user may search the MLD Snooping Forwarding Table by VLAN Name by entering a VLAN name and then clicking **Search**.

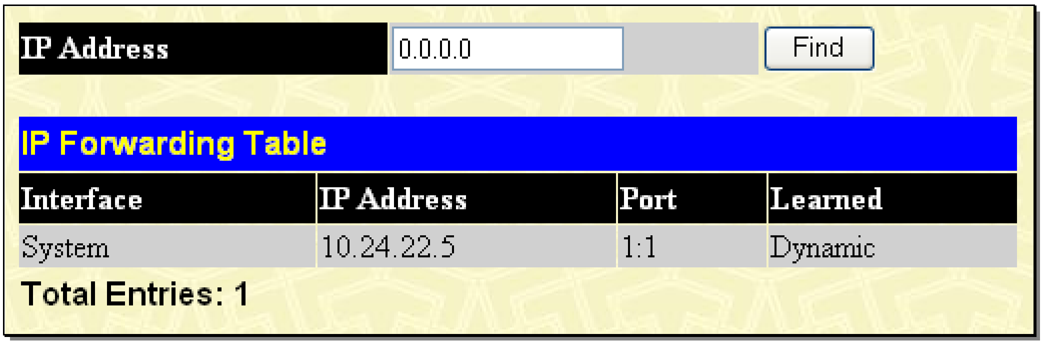
The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name where multicast packets are being received.
Source IP	The Source IP address that is sending multicast packets.
Multicast Group	The Multicast IP address located in the multicast packet.
Port Member	These are the ports where the IP multicast packets are being forwarded.

IP Forwarding Table

The **IP Forwarding Table** window is read-only 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 window and click **Find** to begin your search.

The view this window, click **Monitoring** > **IP Forwarding Table**, as shown below:



IP Address: 0.0.0.0

IP Forwarding Table

Interface	IP Address	Port	Learned
System	10.24.22.5	1:1	Dynamic

Total Entries: 1

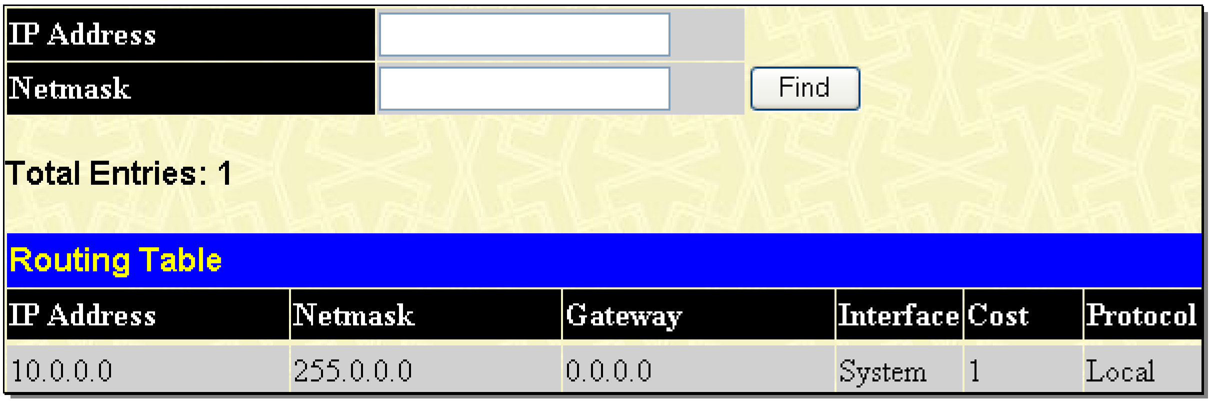
Figure 8- 40. IP Forwarding Table window

Routing Table

Browse Routing Table

This window shows the current IP routing table of the Switch. To find a specific IP route, enter an IP address along with a proper subnet mask in the two fields offered and click **Find**.

To view this window, click **Monitoring** > **Routing Table** > **Browse Routing Table**, as shown below:



IP Address	
Netmask	

Total Entries: 1

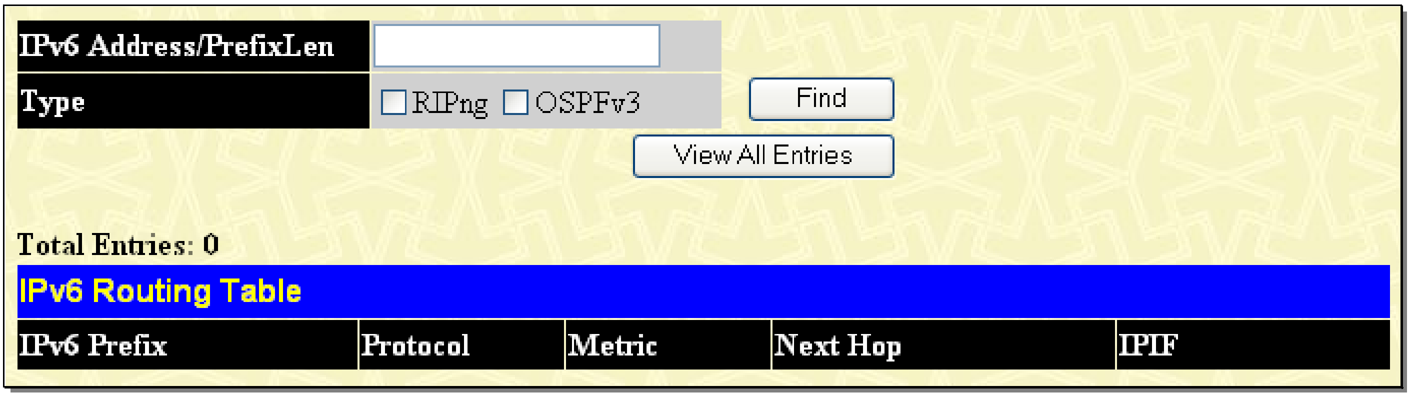
Routing Table

IP Address	Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local

Figure 8- 41. Routing Table window

Browse IPv6 Routing Table

To view this window, click **Monitoring** > **Routing Table** > **Browse IPv6 Routing Table**, as shown below:



IPv6 Address/PrefixLen	
Type	□ RIPng □ OSPFv3

Total Entries: 0

IPv6 Routing Table

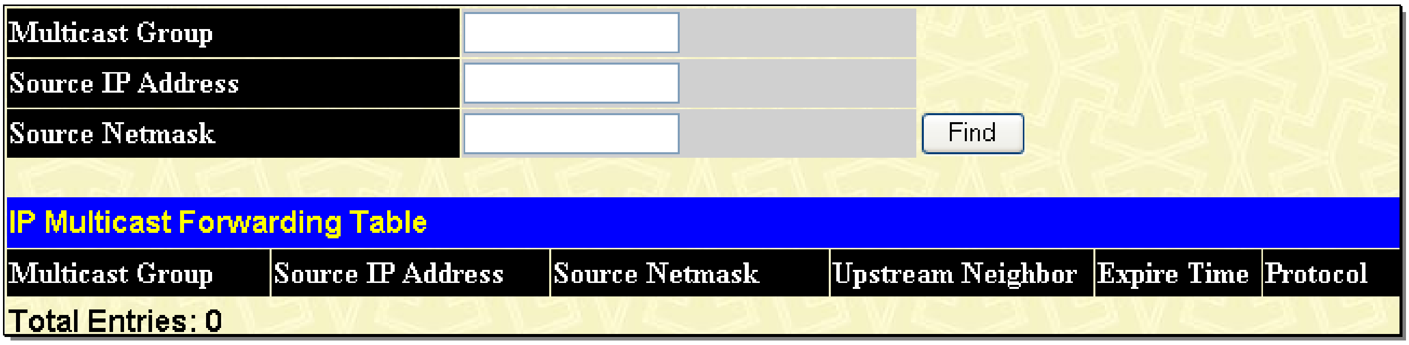
IPv6 Prefix	Protocol	Metric	Next Hop	IPIF

Figure 8- 42. IPv6 Routing 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, a Source IP address or Source Netmask and click **Find**.

To view this window, click **Monitoring** > **Browse IP Multicast Forwarding Table**, as shown below:



Multicast Group	
Source IP Address	
Source Netmask	

IP Multicast Forwarding Table

Multicast Group	Source IP Address	Source Netmask	Upstream Neighbor	Expire Time	Protocol

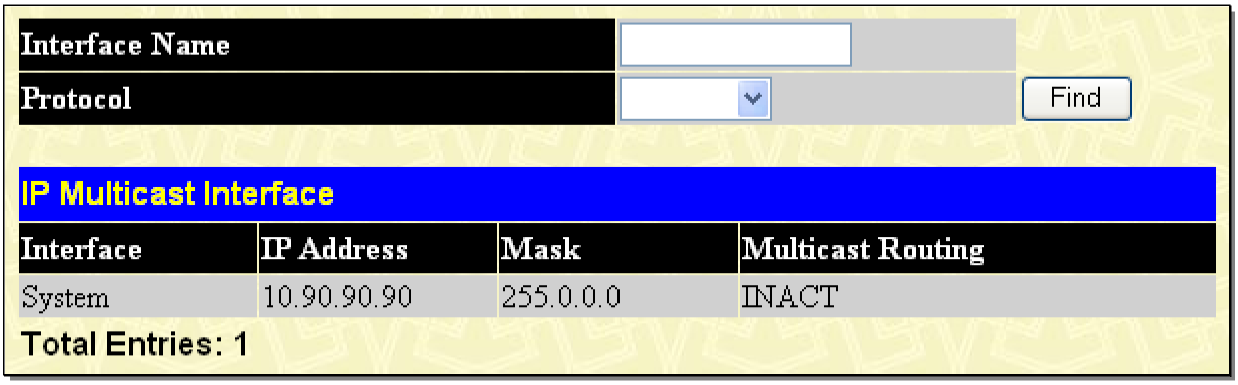
Total Entries: 0

Figure 8- 43. IP Multicast Forwarding Table window

Browse IP Multicast Interface Table

This window will show current IP multicasting interfaces located on the Switch. To search a specific entry, enter a multicast interface name into the Interface Name field or choose a Protocol from the pull down list and click **Find**.

To view this window, click **Monitoring** > **Browse IP Multicast Interface Table**, as shown below:



Interface Name	
Protocol	

IP Multicast Interface

Interface	IP Address	Mask	Multicast Routing
System	10.90.90.90	255.0.0.0	INACT

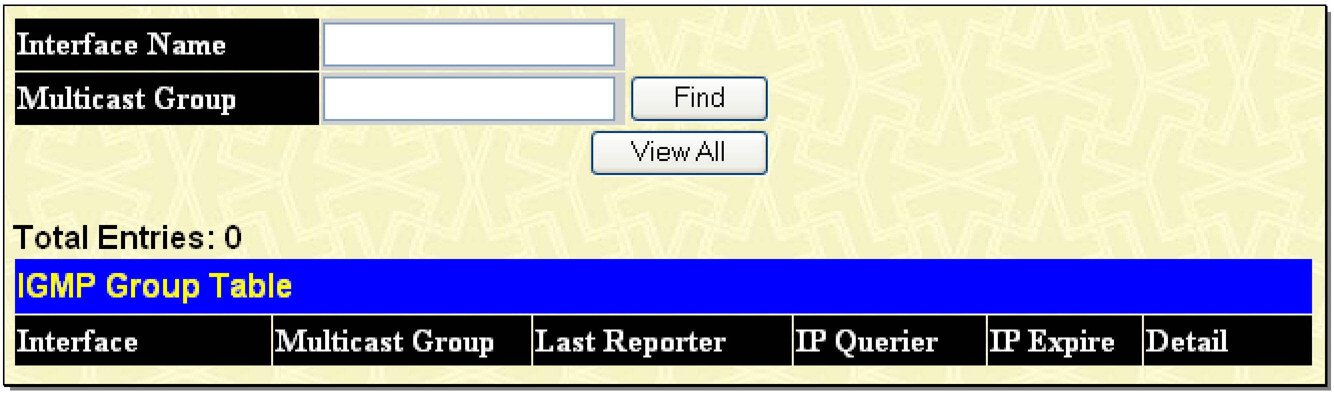
Total Entries: 1

Figure 8- 44. IP Multicast Interface window

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**, as shown below:



Interface Name	
Multicast Group	

Total Entries: 0

IGMP Group Table

Interface	Multicast Group	Last Reporter	IP Querier	IP Expire	Detail

Figure 8- 45. IGMP Group Table window

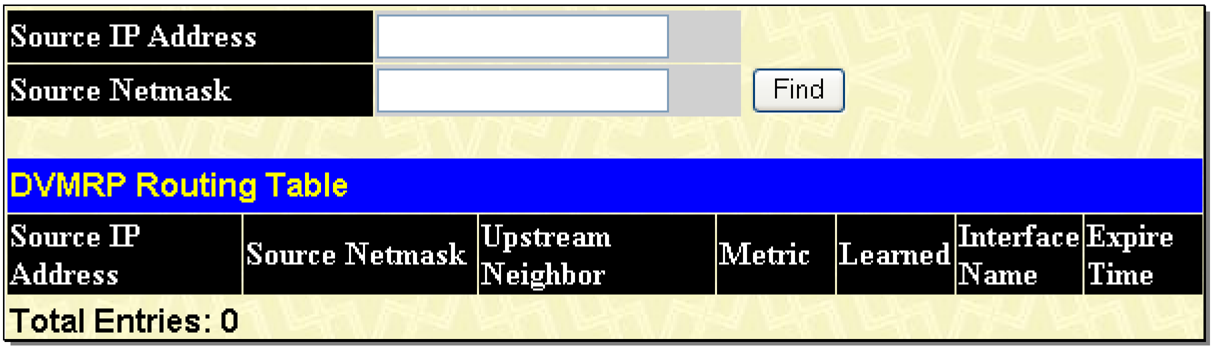
DVMRP Monitor

This folder allows the DVMRP (Distance-Vector Multicast Routing Protocol) to be monitored for each IP interface defined on the Switch. The DVMRP monitor section offers three windows for monitoring: **Browse DVMRP Routing Table**, **Browse DVMRP Neighbor Table**, and **Browse DVMRP Routing Next Hop Table**.

Browse DVMRP Routing Table

Multicast routing information is gathered and stored by DVMRP in the DVMRP Routing Table, this window, 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 window, and click **Find**.

To view this window, click **Monitoring** > **DVMRP Monitor > Browse DVMRP Routing Table**



Source IP Address	
Source Netmask	

DVMRP Routing Table

Source IP Address	Source Netmask	Upstream Neighbor	Metric	Learned	Interface Name	Expire Time

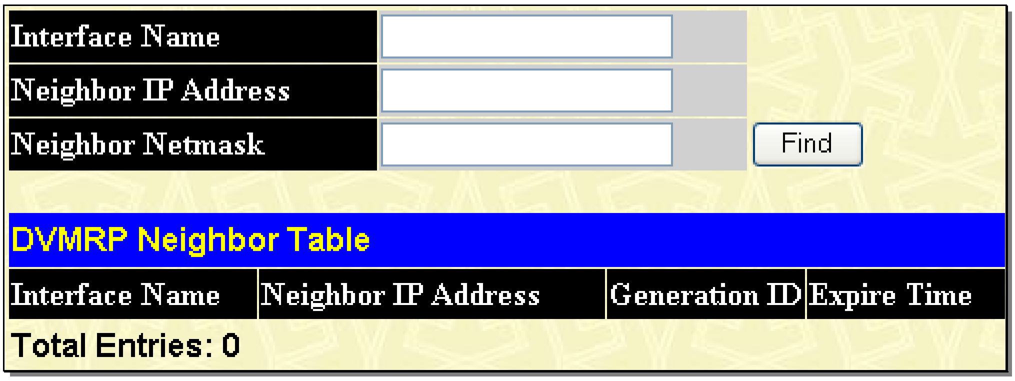
Total Entries: 0

Figure 8- 46. DVMRP Routing Table window

Browse DVMRP Neighbor Table

This table contains information about DVMRP neighbors of the Switch. To search this table, enter an Interface Name, Neighbor Address or Source Netmask 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 window, click **Monitoring** > **DVMRP Monitor > Browse DVMRP Neighbor Table**, as shown below:



Interface Name	
Neighbor IP Address	
Neighbor Netmask	

DVMRP Neighbor Table

Interface Name	Neighbor IP Address	Generation ID	Expire Time

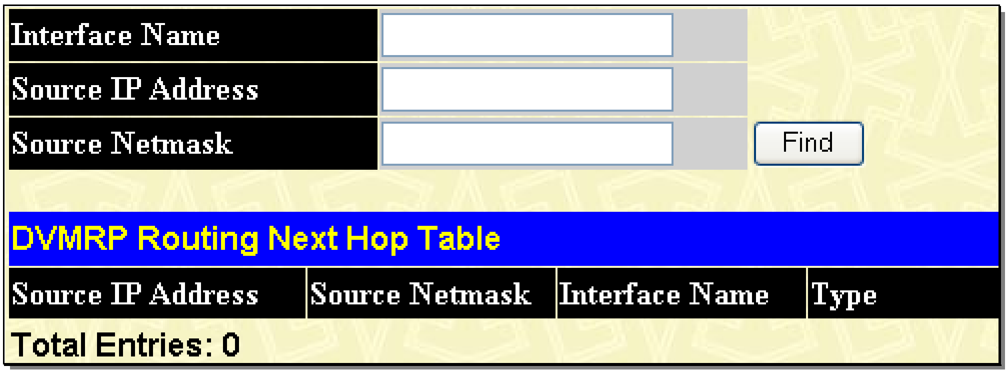
Total Entries: 0

Figure 8- 47. DVMRP Neighbor Table window

Browse DVMRP Routing Next Hop Table

This table contains information regarding the next-hop for forwarding multicast packets on outgoing interfaces. Each entry in the **DVMRP Routing Next Hop Table** window refers to the next-hop of a specific source to a specific multicast group address. To search this table, enter an Interface Name, Source IP Address or Source Netmask 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 Monitoring > Browse DVMRP Routing Next Hop Table**, as shown below:



Interface Name	
Source IP Address	
Source Netmask	

DVMRP Routing Next Hop Table

Source IP Address	Source Netmask	Interface Name	Type

Total Entries: 0

Figure 8- 48. DVMRP Routing Next Hop Table window

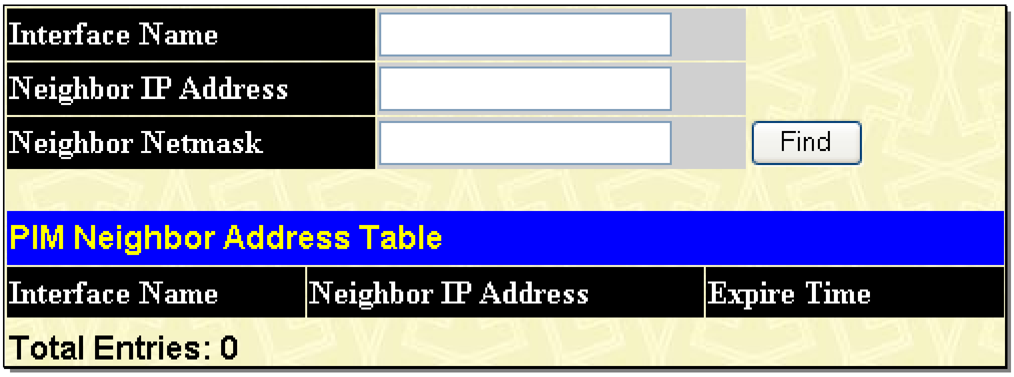
PIM Monitor

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 Address Table contains information regarding each of a router’s PIM neighbors. To search this table, enter an Interface Name, Neighbor Address or Neighbor Netmask into the respective field and click the **Find** button. PIM neighbors of that entry will appear in the PIM Neighbor Address Table below.

To view this window, click **Monitoring** > **PIM Monitor > Browse PIM Neighbor Table**, as shown below:



Interface Name	
Neighbor IP Address	
Neighbor Netmask	

PIM Neighbor Address Table

Interface Name	Neighbor IP Address	Expire Time

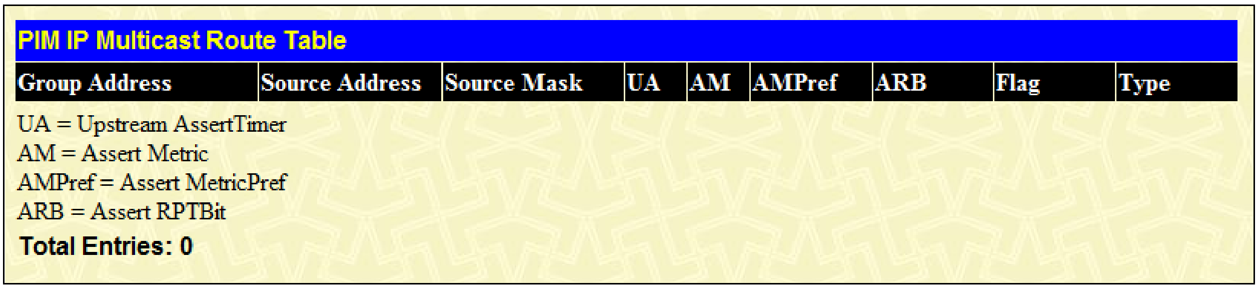
Total Entries: 0

Figure 8- 49. PIM Neighbor Address Table window

Browse PIM IP Multicast Route Table

The PIM IP Multicast Route Table is used to view information regarding the multicast data route entries in the Switch.

To view this window, click **Monitoring > PIM Monitor > Browse PIM IP Mutlicast Route Table**, as shown below:



PIM IP Multicast Route Table

Group Address	Source Address	Source Mask	UA	AM	AMPref	ARB	Flag	Type

UA = Upstream AssertTimer
AM = Assert Metric
AMPref = Assert MetricPref
ARB = Assert RPTBit

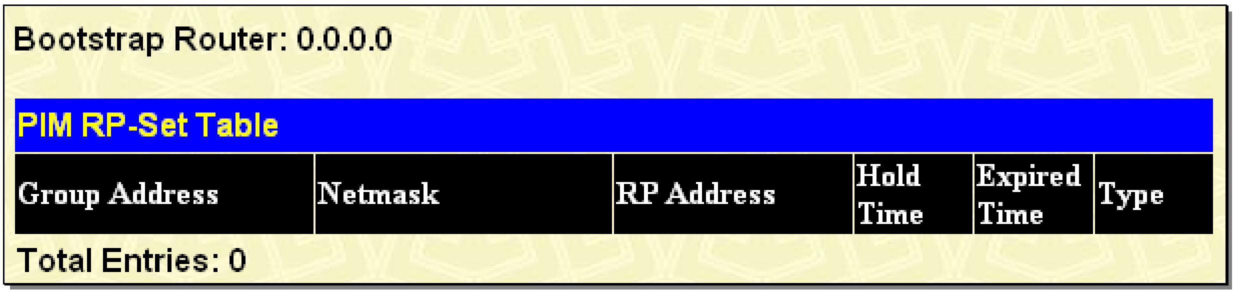
Total Entries: 0

Figure 8- 50. PIM IP Multicast Route Table window

Browse PIM RP-Set Table

The following window is used to assess information regarding the Rendezvous Point (RP) Set on the Switch.

To view this window, click **Monitoring** > **PIM Monitor** > **Browse PIM RP-Set Table**, as shown below:



Bootstrap Router: 0.0.0.0

PIM RP-Set Table

Group Address	Netmask	RP Address	Hold Time	Expired Time	Type

Total Entries: 0

Figure 8- 51. PIM RP Set Table window

OSPF Monitor

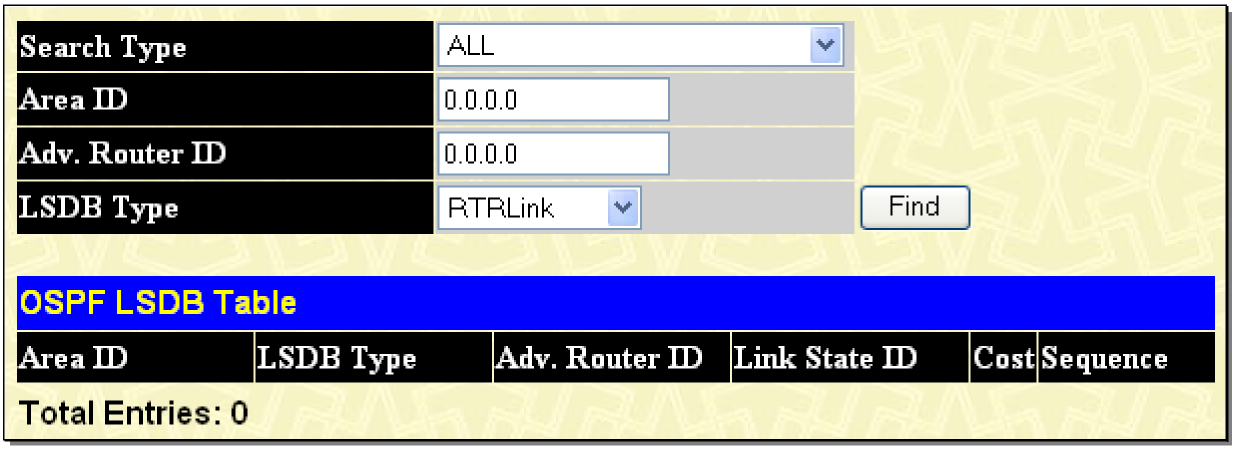
This section offers windows regarding OSPF (Open Shortest Path First) information on the Switch, including the OSPF LSDB Table, OSPF Neighbor Table and the OSPF Virtual Neighbor Table.

OSPF

Browse OSPF LSDB Table

The OSPF LSDB 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** > **OSPF** > **Browse OSPF LSDB Table**, as shown below:



Search Type	ALL
Area ID	0.0.0.0
Adv. Router ID	0.0.0.0
LSDB Type	RTRLink

OSPF LSDB Table

Area ID	LSDB Type	Adv. Router ID	Link State ID	Cost	Sequence

Total Entries: 0

Figure 8- 52. OSPF LSDB Table window

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** window, 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, users must enter the IP address in the Area ID field, and then click *Find*.

If *Adv. Router ID* is selected, users must enter the IP address in the Adv. Router ID field, and then click *Find*.

If *LSDB* is selected, users must select the type of link state (*RTRLink*, *NETLink*, *Summary*, *ASSummary*, *ASExtLink* and *NSSA_EXT*) in the LSDB Type field, and then click *Find*.

The following fields are displayed in the OSPF LSDB Table:

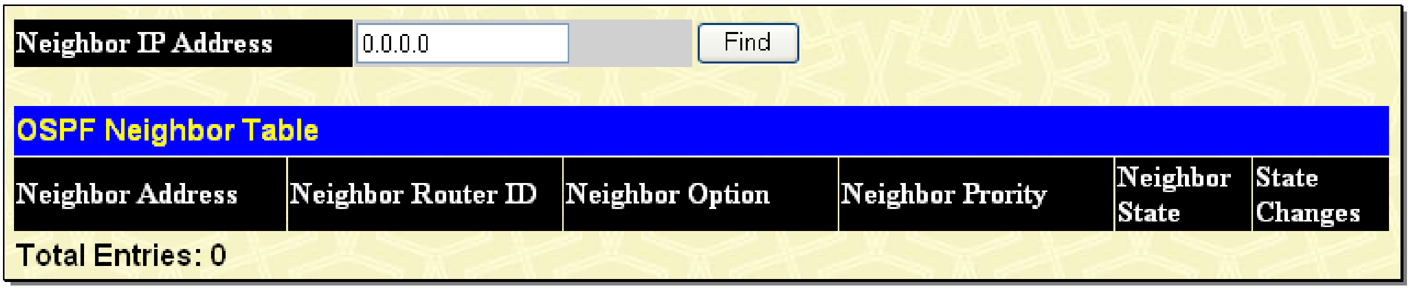
Parameter	Description
Area ID	Allows the entry of an OSPF Area ID. This Area ID will then be used to search the table, and display an entry – if there is one.
Adv. Router ID	Displays the Advertising Router's ID.

LSDB Type	Displays which one of six types of link advertisements by which the current link was discovered by the Switch: Router link (*RTRLink*), Network link (*NETLink*), Summary link (*Summary*), Autonomous System link (*ASSummary*), Autonomous System external link (*ASExternal)*, and NSSA_EXT (*Not So Stubby Area* external)
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 Monitor** > **OSPF > Browse OSPF Neighbor Table** as shown below.



Neighbor IP Address: 0.0.0.0

OSPF Neighbor Table

Neighbor Address	Neighbor Router ID	Neighbor Option	Neighbor Prority	Neighbor State	State Changes

Total Entries: 0

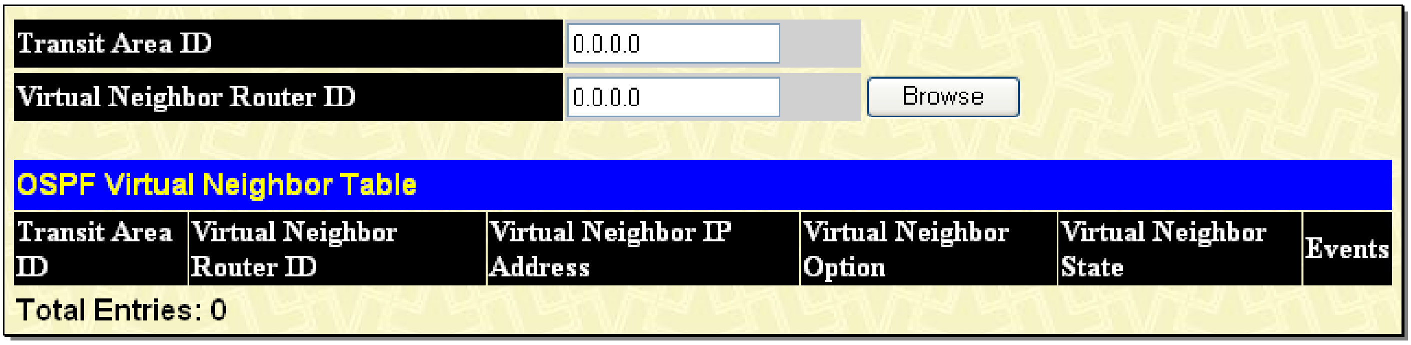
Figure 8- 53. OSPF Neighbor Table window

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 > OSPF Monitor** > **OSPF > Browse OSPF Virtual Neighbor Table**, as shown below:



Transit Area ID: 0.0.0.0

Virtual Neighbor Router ID: 0.0.0.0

OSPF Virtual Neighbor Table

Transit Area ID	Virtual Neighbor Router ID	Virtual Neighbor IP Address	Virtual Neighbor Option	Virtual Neighbor State	Events

Total Entries: 0

Figure 8- 54. OSPF Virtual Neighbor Table window

The user may choose specifically search a virtual neighbor by using one of the two search options at the top of the window, 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.

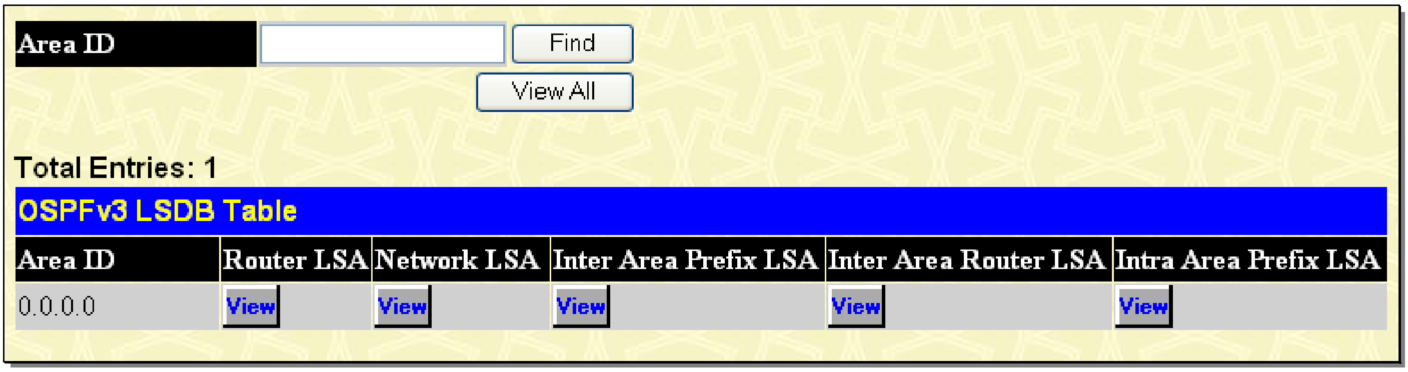
OSPFv3

This section offers windows regarding OSPF (Open Shortest Path First) Version 3 information on the Switch, including the OSPFv3 LSDB Table, OSPFv3 LSDB AS External LSA Table, OSPFV3 LSDB Link LSA Interface Table, OSPFv3 Neighbor Table, and the OSPFv3 Virtual Neighbor Table.

Browse OSPFv3 LSDB Table

The OSPFv3 LSDB Table displays the current link-state database in use by the OSPFv3 routing protocol on a per-OSPF area basis.

To view this table, click **Monitoring** > **OSPF Monitor** > **OSPFv3** > **Browse OSPFv3 LSDB Table**, as shown below:



Total Entries: 1

OSPFv3 LSDB Table

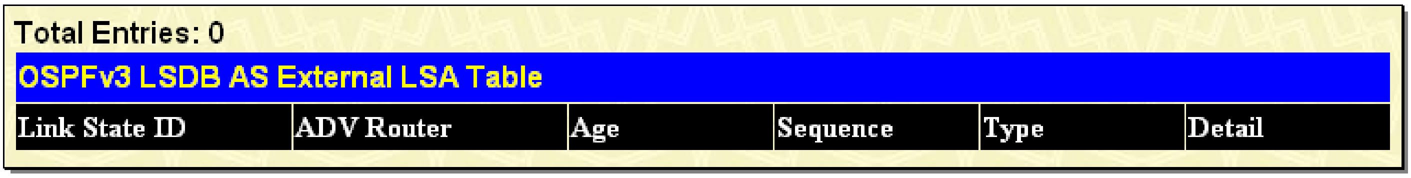
Area ID	Router LSA	Network LSA	Inter Area Prefix LSA	Inter Area Router LSA	Intra Area Prefix LSA
0.0.0.0	View	View	View	View	View

Figure 8- 55. OSPFv3 LSDB Table window

Browse OSPFv3 LSDB AS External LSA Table

This table displays a list of OSPFv3 LSDB AS External LSA Table entries of the Switch.

To view this table, click **Monitoring** > **OSPF Monitor** > **OSPFv3** > **Browse OSPFv3 LSDB AS External Table**, as shown below:



Total Entries: 0

OSPFv3 LSDB AS External LSA Table

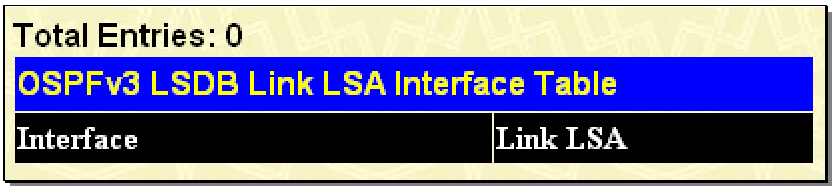
Link State ID	ADV Router	Age	Sequence	Type	Detail

Figure 8- 56. OSPFv3 LSDB AS External LSA Table window

Browse OSPFv3 LSDB Link LSA Interface Table

This table displays a list of OSPFv3 LSDB Link LSA Interfaces of the Switch.

To view this table, click **Monitoring** > **OSPF Monitor** > **OSPFv3** > **Browse OSPFv3 LSDB Link LSA Interface Table**, as shown below:



Total Entries: 0

OSPFv3 LSDB Link LSA Interface Table

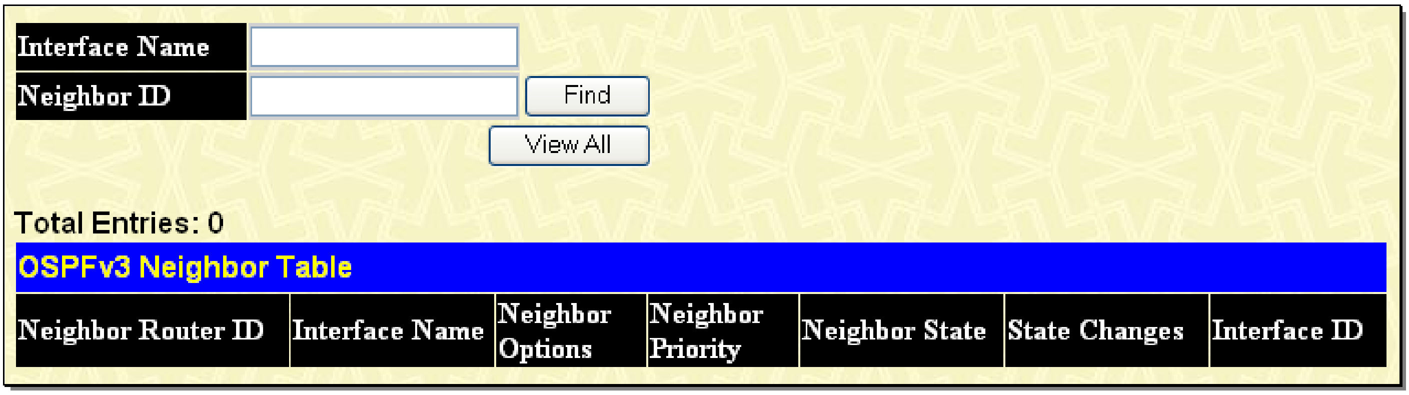
Interface	Link LSA

Figure 8- 57. OSPFv3 LSDB Link LSA Interface Table window

Browse OSPFv3 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 OSPFv3 neighbors of the Switch.

To view this table, click **Monitoring** > **OSPF Monitor** > **OSPFv3** > **Browse OSPFv3 Neighbor Table**, as shown below:



Interface Name	
Neighbor ID	

Total Entries: 0

OSPFv3 Neighbor Table

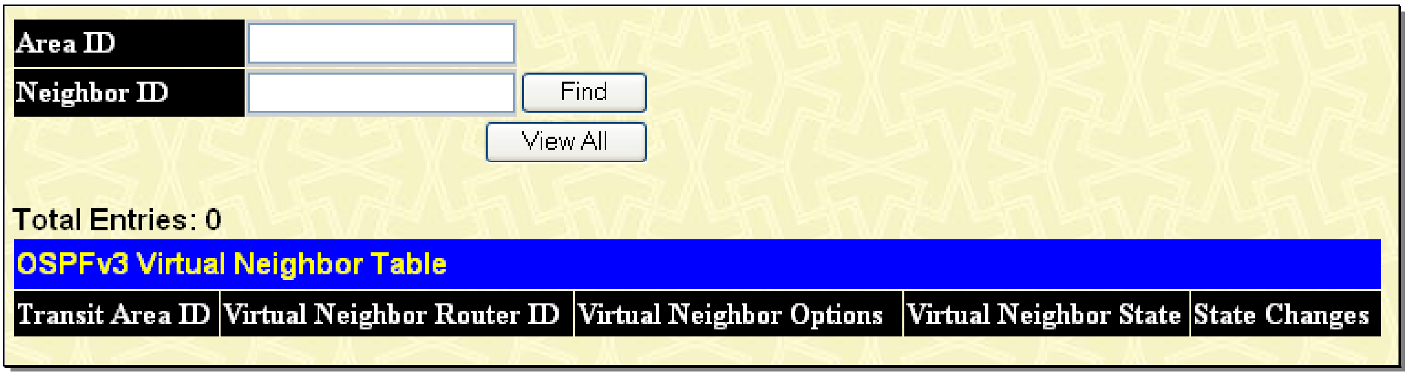
Neighbor Router ID	Interface Name	Neighbor Options	Neighbor Priority	Neighbor State	State Changes	Interface ID

Figure 8- 58. OSPFv3 Neighbor Table window

Browse OSPFv3 Virtual Neighbor Table

This table displays a list of OSPFv3 Virtual Neighbors of the Switch.

To view this table, click **Monitoring** > **OSPF Monitor** > **OSPFv3** > **Browse OSPFv3 Virtual Neighbor Table**, as shown below:



Area ID	
Neighbor ID	

Total Entries: 0

OSPFv3 Virtual Neighbor Table

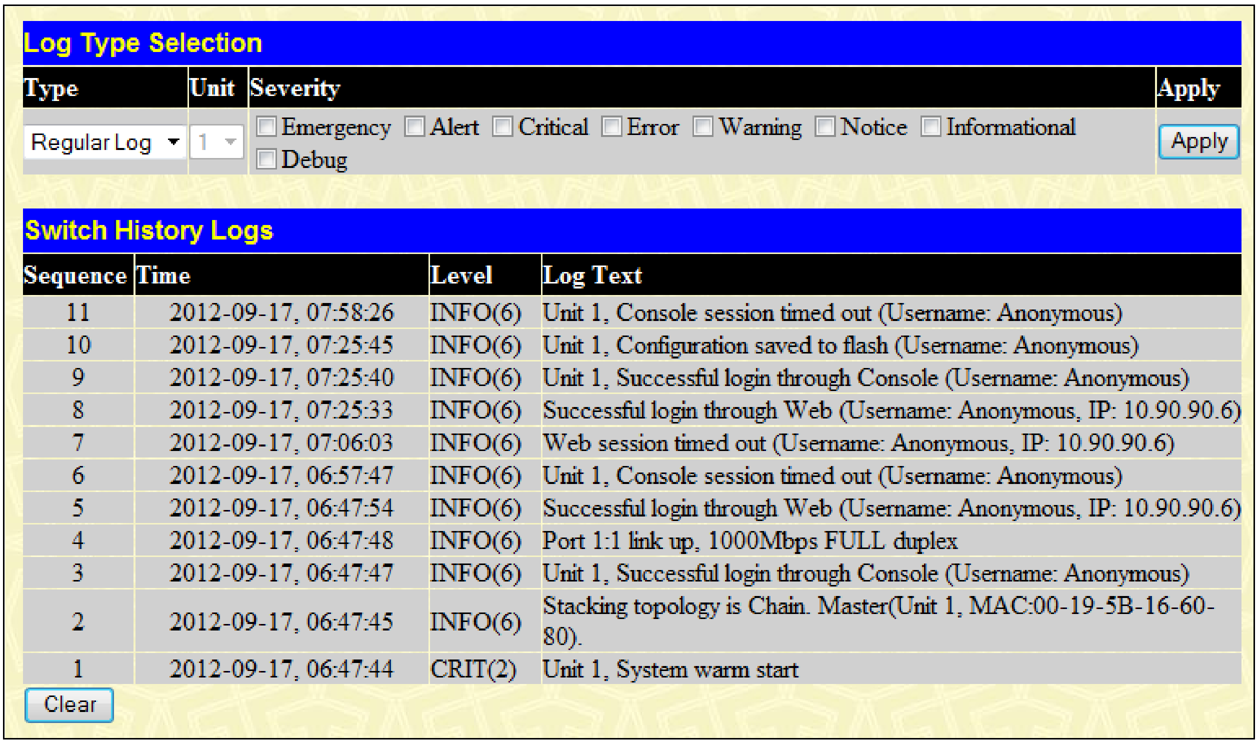
Transit Area ID	Virtual Neighbor Router ID	Virtual Neighbor Options	Virtual Neighbor State	State Changes

Figure 8- 59. OSPFv3 Virtual Neighbor Table window

Switch Logs

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 Logs**, as shown below:



Log Type Selection

Type	Unit	Severity	Apply
Regular Log ▾	1 ▾	□ Emergency □ Alert □ Critical □ Error □ Warning □ Notice □ Informational □ Debug	Apply

Switch History Logs

Sequence	Time	Level	Log Text
11	2012-09-17, 07:58:26	INFO(6)	Unit 1, Console session timed out (Username: Anonymous)
10	2012-09-17, 07:25:45	INFO(6)	Unit 1, Configuration saved to flash (Username: Anonymous)
9	2012-09-17, 07:25:40	INFO(6)	Unit 1, Successful login through Console (Username: Anonymous)
8	2012-09-17, 07:25:33	INFO(6)	Successful login through Web (Username: Anonymous, IP: 10.90.90.6)
7	2012-09-17, 07:06:03	INFO(6)	Web session timed out (Username: Anonymous, IP: 10.90.90.6)
6	2012-09-17, 06:57:47	INFO(6)	Unit 1, Console session timed out (Username: Anonymous)
5	2012-09-17, 06:47:54	INFO(6)	Successful login through Web (Username: Anonymous, IP: 10.90.90.6)
4	2012-09-17, 06:47:48	INFO(6)	Port 1:1 link up, 1000Mbps FULL duplex
3	2012-09-17, 06:47:47	INFO(6)	Unit 1, Successful login through Console (Username: Anonymous)
2	2012-09-17, 06:47:45	INFO(6)	Stacking topology is Chain. Master(Unit 1, MAC:00-19-5B-16-60-80).
1	2012-09-17, 06:47:44	CRIT(2)	Unit 1, System warm start

Figure 8- 60. Log Type Selection 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. Clicking **Clear** will allow the user to clear the Switch History Log.

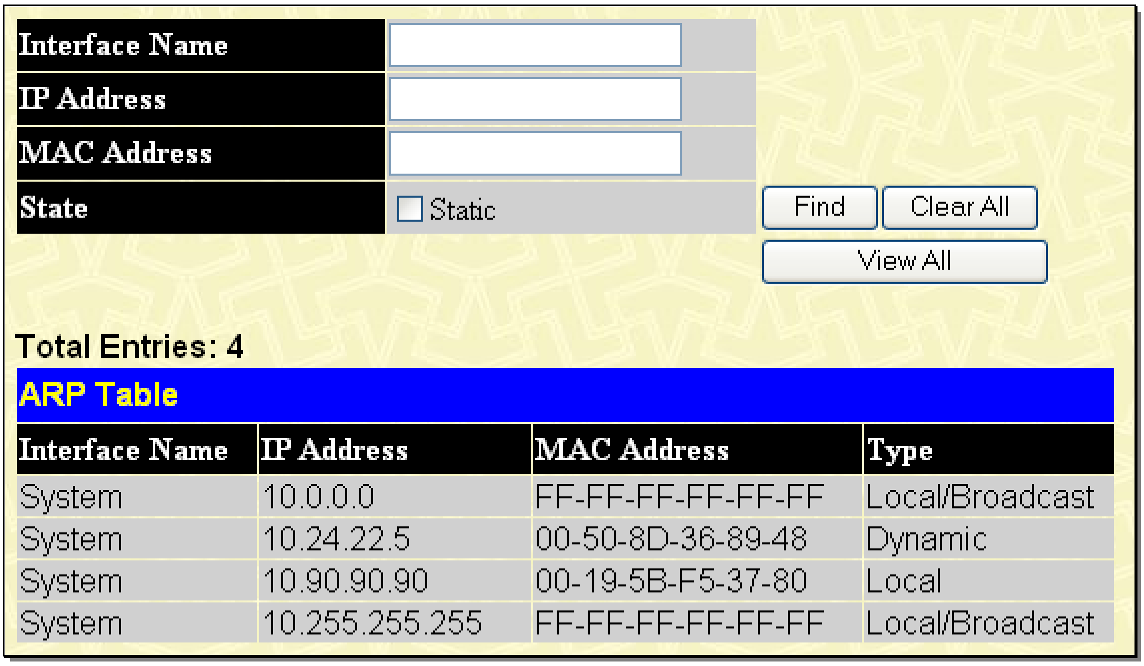
The information in the table is categorized as:

Parameter	Description
Type	Choose the type of log to view. There are two choices: *Regular Log* – Choose this option to view regular switch log entries, such as logins or firmware transfers. *Attack Log* – Choose this option to view attack log files, such as spoofing attacks.
Unit	Enter the unit you wish to view.
Severity	Specifies the severity to be displayed.
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 generated the log file.
Log Text	Displays text describing the event that triggered the history log entry.

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 a MAC address, and click **Find.** To clear the ARP Table, click **Clear All.**

To view the Browse ARP table, click **Monitoring** > **Browse ARP Table**, as shown below:



Interface Name	
IP Address	
MAC Address	
State	□ Static

Total Entries: 4

ARP Table

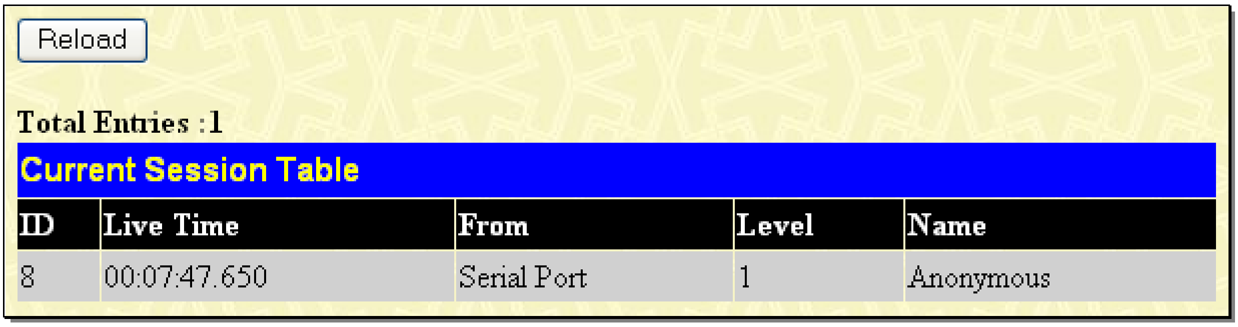
Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.24.22.5	00-50-8D-36-89-48	Dynamic
System	10.90.90.90	00-19-5B-F5-37-80	Local
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

Figure 8- 61. ARP Table window

Session Table

This window is used to display the current session table.

To view this window, click **Monitoring** > **Session Table**, as shown below:



Total Entries :1

Current Session Table

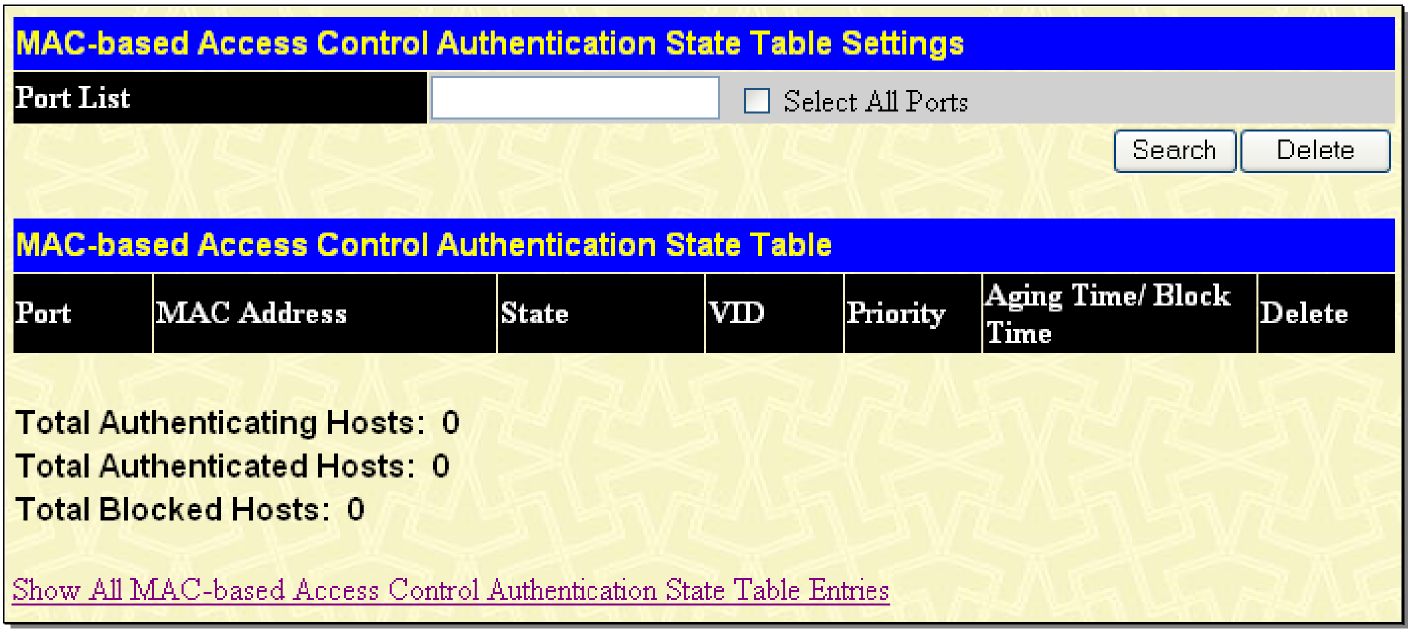
ID	Live Time	From	Level	Name
8	00:07:47.650	Serial Port	1	Anonymous

Figure 8- 62. Current Session Table window

MAC-based Access Control Authentication Status

This window is used to clear previously configured MAC Based Access Control Authentication entries.

To view the Browse ARP table, click **Monitoring** > **MAC Based Access Control Authentication**, as shown below:



MAC-based Access Control Authentication State Table Settings

Port List □ Select All Ports

MAC-based Access Control Authentication State Table

Port	MAC Address	State	VID	Priority	Aging Time/ Block Time	Delete

Total Authenticating Hosts: 0

Total Authenticated Hosts: 0

Total Blocked Hosts: 0

Show All MAC-based Access Control Authentication State Table Entries

Figure 8- 63. MAC-based Access Control Authentication State Table Settings window

The The following fields can be configured:

Parameter	Description
Ports (e.g:1,5,7-12)	Enter the range of ports you wish to clear and click **Clear**, to clear all ports check the **All Ports** check box before clicking **Clear**.
MAC Address	Enter the MAC Address of the entry you wish to clear, and click **Clear**.

Section 9

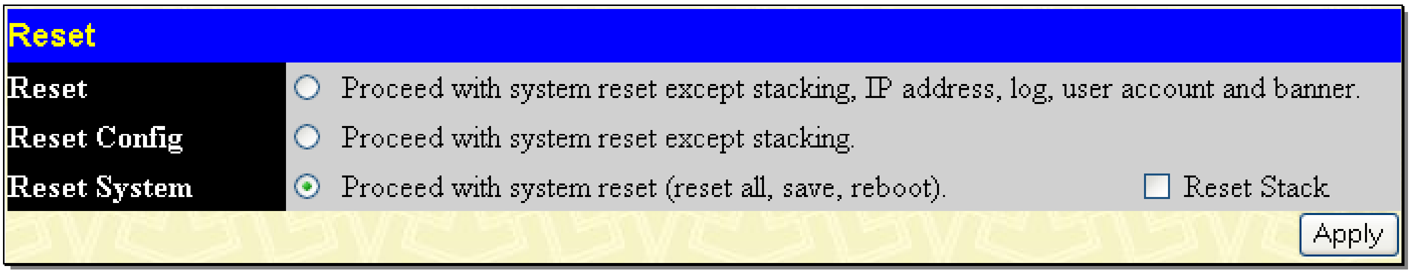
Switch Maintenance

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.



Reset

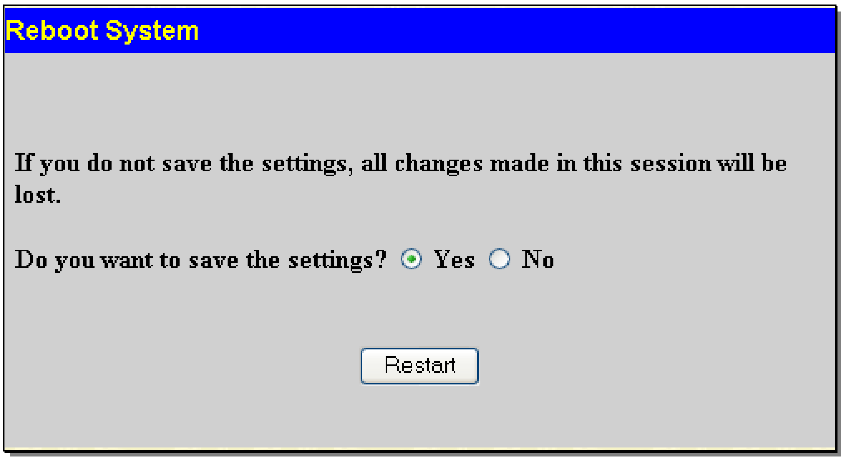
Reset	○ Proceed with system reset except stacking, IP address, log, user account and banner.
Reset Config	○ Proceed with system reset except stacking.
Reset System	● Proceed with system reset (reset all, save, reboot). □ Reset Stack

Figure 9- 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 **Restart** button to restart the Switch.



Reboot System

If you do not save the settings, all changes made in this session will be lost.

Do you want to save the settings? ● Yes ○ No

Figure 9- 2. Reboot System window

Save Services

The following three windows will aid the user in saving configurations to the Switch's memory.

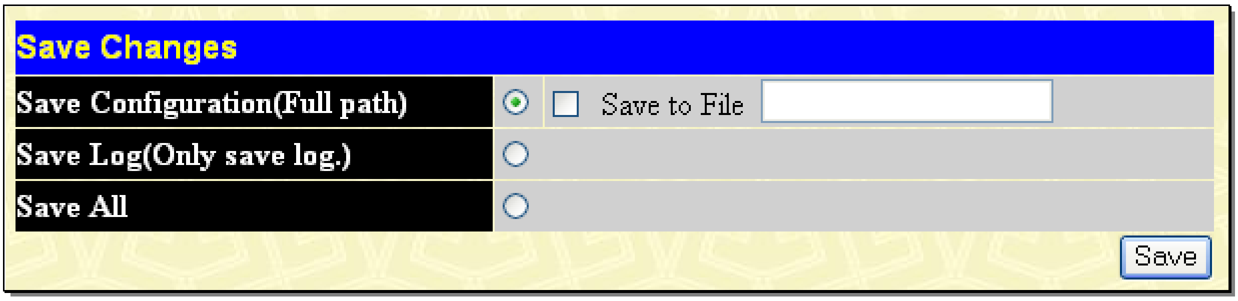
Save Changes

The Switch has two levels of memory, normal RAM and non-volatile or NV-RAM. Configuration changes are made effective clicking the **Save** 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** button in the **Save Changes** window. The save options allow one alternative configuration image to be stored.

To view this window, click **Save Services > Save Changes**, as shown beow.



Save Changes

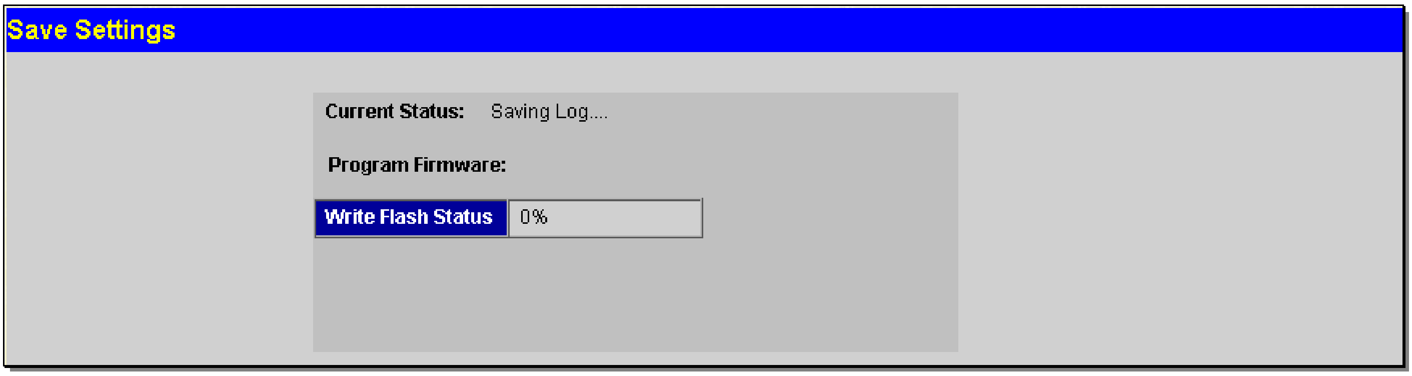
Save Configuration(Full path)	●	□ Save to File
Save Log(Only save log.)	○	
Save All	○	

Figure 9- 3. Save Changes window

The Save Changes options include:

- **Save Configuration (Full path) -** Users may save the configuration to the internal flash memory of the Switch. To name the file, click the check box and enter the path of the filename to nominate this file as. All configuration files should start with C:/ . To use this file for configuration it must be designated as the *Boot* configuration using the **Configuration Settings** window (**Save Services > Current Configuration Settings**).
- **Save Log (Only save log) -** To save only the current log.
- **Save All -** To save the current configuration file indexed as Image file 1 and save the current log.

Once the **Save** button has been clicked, the following window will appear, confirming that the settings have been saved.



Save Settings

Current Status: Saving Log....

Program Firmware:

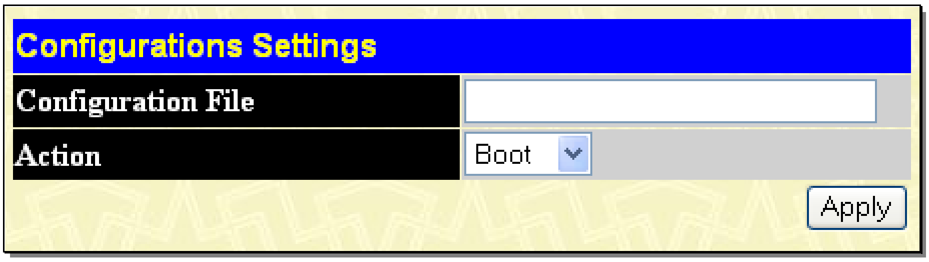
Write Flash Status 0%

Figure 9- 4. Save Settings window

Current Configuration Settings

The **Current Configuration Settings** window allows users to manipulate configuration images saved in the Flash memory of the Switch.

To view this window, click **Save Services > Current Configuration Settings**, as shown below:



Configurations Settings

Configuration File

Action: Boot

Figure 9- 5. Current Configuration Settings window

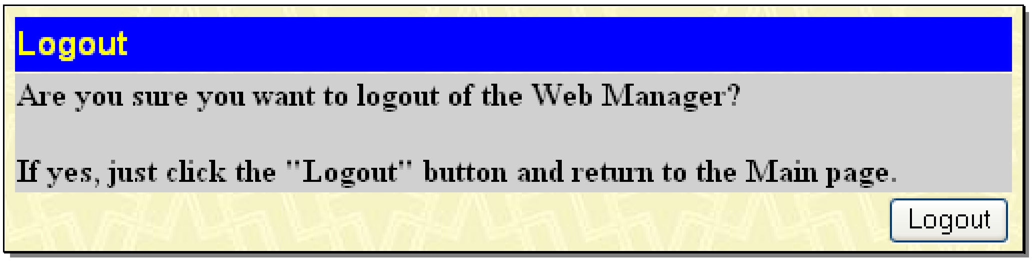
This window offers the following information:

Parameter	Description
Configuration File	Enter the configuration file located on the Flash drive to be altered.
Action	This field has two options for configuration. *Boot* – Select this option to set the configuration file specified above as the boot up configuration for the Switch. This saved configuration will be set as the boot up file after a switch reboot has been performed. The default setting has configuration file C:/STARTUP.CFG as the boot up configuration file for the Switch unless specified here. *Active* - Choosing this parameter will first load and then activate this configuration file on the Switch.

Click **Apply** to implement changes made.

Logout

Use the Logout page to logout of the Switch's Web-based management agent by clicking on the **Logout** button.



Logout

Are you sure you want to logout of the Web Manager?

If yes, just click the "Logout" button and return to the Main page.

Figure 9- 6. Logout window

Appendix A - Technical Specifications

General		
Protocols	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”) IEEE 802.1D Spanning Tree IEEE 802.1s Multiple Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1Q VLAN IEEE 802.1V Protocol VLAN IEEE 802.1p Priority Queues IEEE 802.1X Port Based Network Access Control IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation	
Fiber-Optic	SFP (Mini GBIC) Support IEEE 802.3u 100BASE-FX (DEM-210 transceiver) (DGS-3612/DGS-3612G only) IEEE 802.3u 100BASE-FX (DEM-211 transceiver) (DGS-3612/DGS-3612G only) IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-312GT2 transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver) IEEE 802.3z WDM Transceiver (DEM-330T transceiver) IEEE 802.3z WDM Transceiver (DEM-330R transceiver) IEEE 802.3z WDM Transceiver (DEM-331T transceiver) IEEE 802.3z WDM Transceiver (DEM-331R transceiver)	
XFP Support	IEEE 802.3ae 10G Fiber-Optic	
CX4 Support	IEEE 802.3ak 10G Copper	
Standards	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n/a	2000Mbps
Topology	Star	
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)	
Number of Ports	DGS-3627: 24 x 10/100/1000Mbps ports 4 x 1000Mbps Combo SFP ports 3 available slots for optional 10GE modules DGS-3627G: 24 x 1000Mbps SFP ports 4 x 10/100/1000Mbps Combo Ports 3 available slots for optional 10GE modules	

	DGS-3650: 48 x 10/100/1000 Mbps ports 4 x 1000Mbps Combo SFP Ports 2 available slots for optional 10GE modules DGS-3612G: 12 x 100/1000Mbps SFP ports 4 x Combo 10/100/1000Mbps ports DGS-3612: 12 x 10/100/1000Mbps copper ports 4 x Combo 100/1000Mbps SFP ports

Physical and Environmental

Internal Power Supply	Input: 100~240V, AC/1.3A, 50~60Hz Output: 12V, 10A (Max)
Power Consumption	DGS-3627 – 95W DGS-3627G – 77W DGS-3650 – 137W DGS-3612G – 50W DGS-3612 – 45W
DC Fans	DGS-3627 – Four 40mm x 40mm x 20mm; one 50mm x 50mm x 20mm; one 44mm x 44mm x 11mm DGS-3627G – Four 40mm x 40mm x 20mm; one 50mm x 50mm x 20mm fans DGS-3650 – Two 40mm x 40mm x 20mm; three 40mm x 40mm x 10mm; one 75.7mm x 75.7mm x 30mm fans; one 44mm x 44mm x 11mm DGS-3612G – Three 40mm x 40mm x 20mm; one 50mm x 50mm x 20mm fans DGS-3612 - Two 40mm x 40mm x 20mm fans
Operating Temperature	0 - 40°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	DGS-3627, DGS-3627G, DGS-3650, DGS-3612G – 441mm x 389mm x 44mm DGS-3612 - 441mm x 310mm x 44mm
Weight	DGS-3627, DGS-3627G – 5.5kg (12.13 lbs) DGS-3650 – 6kg (13.23 lbs) DGS-3612G – 5kg (11.02 lbs) DGS-3612 - 3.8kg (8.38 lbs)
EMI	CE Class A, FCC Class A, C-Tick, VCCI
Safety	CB Report, CUL

Performance

Transmission Method	Store-and-forward
Packet Buffer	2 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 - 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.

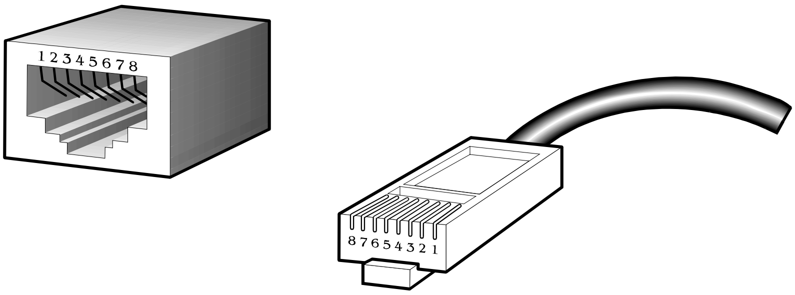


Figure B- 1. The standard RJ-45 port and connector

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 C - System Log Entries

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

Category	Event Description	Log Content	Severity	Remark
system	System started up	**System warm start**	Critical	
system	System started up	**System cold start**	Critical	
	Configuration saved to Flash	**Configuration and log saved to flash by console (Username: <username>)**	Informational	"by console" and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log strings, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	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	
up/down-load	Firmware successfully uploaded	**Firmware successfully uploaded by console (Username:<username>, IP:<ipaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in by console, there will be no IP and MAC information for logging.
	Firmware upload was unsuccessful	**Firmware upload by console was unsuccessful (Username:<username>, IP:<ipaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in by console, there will be no IP and MAC information for logging.
	Firmware upgraded successfully	**Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	Firmware upgrade was unsuccessful	**Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or

Category	Event Description	Log Content	Severity	Remark
				MAC address information will be included in the log.
	Configuration successfully downloaded	**Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	Configuration download was unsuccessful	**Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	Configuration successfully uploaded	**Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	Configuration upload was unsuccessful	**Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	Log message successfully uploaded	**Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
	Log message upload was unsuccessful	**Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if the user logs in through the console, no IP or MAC address information will be included in the log.
Interface	Port link up	**Port <portNum> link up**	Informational	Port link state (ex: , 100Mbps FULL duplex)
	Port link down	**Port <portNum> link down**	Informational	
Console	Successful login through Console	**Successful login through Console (Username: <username>)**	Informational	If the user logs in through the console, no IP or MAC address information will be

Category	Event Description	Log Content	Severity	Remark
				included in the log.
	Login failed through Console	**Login failed through Console (Username: <username>)**	Warning	If the user logs in through the console, no IP or MAC address information will be included in the log.
	Logout through Console	**Logout through Console (Username: <username>)**	Informational	If the user logs in through the console, no IP or MAC address information will be included in the log.
	Console session timed out	**Console session timed out (Username: <username>)**	Informational	If the user logs in through the console, no IP or MAC address information will be included in the log.
Web	Successful login through Web	**Successful login through Web (Username: <username>)**	Informational	
	Login failed through Web	**Login failed through Web (Username: <username>)**	Warning	
	Logout through Web	**Logout through Web (Username: <username>)**	Informational	
	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>)**	Informational	
	Login failed through Telnet	**Login failed through Telnet (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through Telnet	**Logout through Telnet (Username: <username>, IP: <ipaddr>)**	Informational	
	Telnet session timed out	**Telnet session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
SNMP	SNMP request received with invalid community string	**SNMP request received from <ipaddr> with invalid community string!**	Informational	

Category	Event Description	Log Content	Severity	Remark
STP	Topology changed	**Topology changed [([Instance:<InstanceID>], port:<[unitID:] portNum>, MAC: <macaddr>)**	Informational	
	New Root selected	**New root port selected [([Instance:<InstanceID>], port:<[unitID:] portNum>)]**	Notice	
	BPDU Loop Back on ports	**BPDU Loop Back on Ports <portNum>**	Warning	
	Spanning Tree Protocol is enabled	**Spanning Tree Protocol is enabled**	Informational	
	Spanning Tree Protocol is disabled	**Spanning Tree Protocol is disabled**	Informational	
	Spanning Tree port status changed	**Spanning Tree port status changed [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_status> -> <new_status>**	Notice	
	Spanning Tree port role changed	**Spanning Tree port status changed. [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_role> -> <new_role>**	Informational	
	Spannig Tree instance created	**Spanning Tree instance created. Instance:<InstanceID>**	Informational	
	Spannig Tree instance deleted	**Spanning Tree instance deleted. Instance:<InstanceID>**	Informational	
	Spanning Tree Version changed	**Spanning Tree version changed. New version:<new_version>**	Informational	
	Spanning Tree MST configuration ID name and revision level changed	**Spanning Tree MST configuration ID name and revision level changed (name:<name>, revision level <revision_level>)**	Informational	
	Spanning Tree MST configuration ID VLAN mapping table deleted	**Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>])**	Informational	
	Spanning Tree MST configuration ID VLAN mapping	**Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID>**	Informational	

Category	Event Description	Log Content	Severity	Remark
	table added	**add vlan <startvlanid> [-<endvlanid>])**		
	Spanning Tree MST configuration ID VLAN mapping table added	**Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [-<endvlanid>])**	Informational	
SSH	Successful login through SSH	**Successful login through SSH (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through SSH	**Login failed through SSH (Username: <username>, IP: <ipaddr)**	Warning	
	Logout through SSH	**Logout through SSH (Username: <username>, IP: <ipaddr>)**	Informational	
	SSH session timed out	**SSH session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
	Enable SSH server	**SSH server is enabled**	Informational	
	Disable SSH server	**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>)**	Informational	
	Login failed through Web authenticated by AAA local method	**Login failed through Web from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	

Category	Event Description	Log Content	Severity	Remark
	Successful login through Web (SSL) authenticated by AAA local method	**Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Web (SSL) authenticated by AAA local method	**Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Telnet authenticated by AAA local method	**Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Telnet authenticated by AAA local method	**Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through SSH authenticated by AAA local method	**Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through SSH authenticated by AAA local method	**Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Console authenticated by AAA none method	**Successful login through Console authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Web authenticated by AAA none method	**Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Web (SSL) authenticated by AAA none method	**Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Telnet authenticated by AAA none method	**Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	

Category	Event Description	Log Content	Severity	Remark
	Successful login through SSH authenticated by AAA none method	**Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Console authenticated by AAA server	**Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational	If the user logs in through the console, no IP or MAC address information will be included in the log.
	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>)**	Informational	
	Login failed through Web authenticated by AAA server	**Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	**Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through Web (SSL) authenticated by AAA server	**Successful login through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Web (SSL) authenticated by AAA server	**Login failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Web (SSL) due to AAA server timeout or improper configuration	**Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	

Category	Event Description	Log Content	Severity	Remark
	Successful login through Telnet authenticated by AAA server	**Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Telnet authenticated by AAA server	**Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Telnet due to AAA server timeout or improper configuration	**Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through SSH authenticated by AAA server	**Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through SSH authenticated by AAA server	**Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through SSH due to AAA server timeout or improper configuration	**Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Console authenticated by AAA 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>)**	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	**Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	

Category	Event Description	Log Content	Severity	Remark
	Successful Enable Admin through Web (SSL) authenticated by AAA local_enable method	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA local_enable method	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through Telnet authenticated by AAA local_enable method	**Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	**Enable Admin failed through <Telnet or Web or SSH> from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Console authenticated by AAA none method	**Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web authenticated by AAA none method	**Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web (SSL) authenticated by AAA none method	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Telnet authenticated by AAA none method	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	

Category	Event Description	Log Content	Severity	Remark
	Successful Enable Admin through SSH authenticated by AAA none method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Console authenticated by AAA server	**Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Console authenticated by AAA server	**Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	**Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Web authenticated by AAA server	**Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Web authenticated by AAA server	**Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	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>)**	Warning	
	Successful Enable Admin through Web (SSL) authenticated by AAA server	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA server	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	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>)**	Warning	

Category	Event Description	Log Content	Severity	Remark
	Successful Enable Admin through Telnet authenticated by AAA server	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Telnet authenticated by AAA server	**Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	**Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	**Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA server	**Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	**Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	AAA server timed out	**AAA server <serverIP> (Protocol: <protocol>) connection failed**	Warning	<protocol> is one of TACACS, XTACACS, TACACS+ or RADIUS
Port Security	port security has reached its maximum learning size and will not learn any new addresses	**Port security violation (Port: <portNum>, MAC: <macaddr>)**	Warning	
IP-MAC-Port Binding	Unauthenticated IP address discarded by IP mac port binding	**Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
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	

Category	Event Description	Log Content	Severity	Remark
Packet Storm	Broadcast storm occurrence	**Port <unitID:portNum> Broadcast storm is occurring**	Warning	
	Broadcast storm cleared	**Port <unitID:portNum> Broadcast storm has cleared**	Informational	
	Multicast storm occurrence	**Port <unitID:portNum> Multicast storm is occurring**	Warning	
	Multicast storm cleared	**Port <unitID:portNum> Multicast storm has cleared**	Informational	
	Port shut down due to a packet storm	**Port <unitID:portNum> is currently shut down due to a packet storm**	Warning	
Security	Packet received containing a MAC address identical to the MAC address of the device’s interface	**Possible spoofing attack from (IP <ipaddr> MAC <macaddr> port <id>)**	Critical	
MAC-based Access Control	A host failed to pass authentication.	**MBAC unauthenticated host(MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>)**	Critical	
	The authorized number of users on a port has reached the maximum user limit.	**Port < [unitID:]portNum> has entered the MBAC stop learning state.**	Warning	
	The authorized number of users on a port is below the maximum user limit in a time interval.	**Port <[unitID:]portNum> recovered from MBAC stop learning state.**	Warning	
	The authorized number of users on the whole device has reached the maximum user limit.	**MBAC has entered the stop learning state.**	Warning	
	The authorized number of users on the whole device is below the maximum user limit in a time interval.	**MBAC recovered from stop learning state.**	Warning	

Category	Event Description	Log Content	Severity	Remark
JWAC	When a client host has authenticated successfully.	**JWAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)**	Warning	
	When a client host fails to authenticate.	**JWAC unauthenticated user (User Name: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)**	Warning	
	This log will be triggered when the number of authorized users reaches the maximum user limit on thewhole device.	**JWAC enters stop learning state.**	Warning	
	This log will be triggered when the number of authorized users is below the maximum user limit on the whole device in a time interval.	**JWAC recovered from stop learning state.**	Warning	
WAC	When a client host fails to authenticate.	**WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)**	Warning	
	This log will be triggered when the authorized user number reaches the max user limit on whole device.	**WAC enters stop learning state.**	Warning	
	This log will be triggered when the authorized user number is below the max user limit on whole device in a time interval (interval is project dependent)	**WAC recovers from stop learning state.**	Warning	
IP-MAC-Port Binding	Unauthenticated IP address discarded by IP mac port binding	**Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	

Category	Event Description	Log Content	Severity	Remark
	Dynamic IMPB entry is in conflict with static FDB	**Dynamic IMPB entry is conflict with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)**	Warning	
	Dynamic IMPB entry is in conflict with static ARP	**Dynamic IMPB entry is conflict with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)**	Warning	
	Dynamic IMPB entry conflicts with static IMPB	**Dynamic IMPB entry conflicts with static IMPB: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>**	Warning	
	IMPB entry cannot be created in ACL mode due to no ACL rules	**Creating IMPB entry Failed due to no ACL rule available <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>**	Warning	
	Port enter stop learning state	**Port <[unitID:]portNum> IMPB stop learning state**	Information	
	Port recover normal state	**Port <[unitID:]portNum> IMPB normal state**	Information	
DHCP Server Screen	Detected untrusted DHCP server	**Detected untrusted DHCP server (IP:<ipaddr>, Port: <[unitID:]portNum>)**	Information	
DULD	A unidirectional link has been detected on this port	**Port: <[unitID:]portNum> is unidirectional**	Warning	
DDM	DDM exceeded or recover from DDM alarm threshold	**Port <[unitID:]portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] alarm threshold**	Critical	
	DDM exceeded or recover from DDM warning threshold	**Port <[unitID:]portNum> SFP [thresholdType] [exceedType] the %s warning threshold**	Warning	

Category	Event Description	Log Content	Severity	Remark
Voice VLAN	When a new voice device is detected in the port.	**New voice device detected (Port <portNum>, MAC <macaddr>)**	Informational	
	When a port which is in auto Voice VLAN mode joins the Voice VLAN	**Port < portNum > add into Voice VLAN <vid >**	Informational	
	When a port leaves the Voice VLAN and at the same time, no voice device is detected in the aging interval for that port, the log message will be sent.	**Port < portNum > remove from Voice VLAN <vid >**	Informational	
LLDP (MED)	LLDP-MED topology change detected	**LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)**	Notice	
	Conflict LLDP-MED device type detected	**Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)**	Notice	
	Incompatible LLDP-MED TLV set detected	**Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)**	Notice	

Appendix D - Module Specs and Cable Lengths

Use the following table to as a guide for the module specs and maximum cable lengths.

Standard	Media Type	Maximum Distance
Mini-GBIC	1000BASE-LX, Single-mode fiber module 1000BASE-SX, Multi-mode fiber module 1000BASE-LH, Single-mode fiber module 1000BASE-ZX, Single-mode fiber module	10km 550m / 2km 50km 80km
1000BASE-T	Category 5e UTP Cable	100m
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3, 4 or 5 UTP Cable (10 Mbps)	100m
DEM-310GT	1000Base-LX, Single-mode	10km
DEM-311GT	1000ase-SX, Multi-mode	500m
DEM-312GT2	1000Base-SX, Multi-mode	2km
DEM-314GT	1000BASE-LH, Single-mode	50km
DEM-315GT	1000BASE-ZX, Single-mode	80km
DEM-210	100BASE-FX, Single-mode	15km
DEM-211	100BASE-FX, Multi-mode	2km
DEM-330T	TX-1550/RX-1310nm, Single-mode	up to 10km
DEM-330R	TX-1310/RX-1550 nm, Single-mode	up to 10km
DEM-331T	TX-1550/RX-1310 nm, Single-mode	up to 40km
DEM-331R	TX-1310/RX-1550 nm, Single-mode	up to 40km
DEM-410CX	10-Gigabit CX4 module, Infiniband 4X latch-type cable	1 and 3 meters
DEM-410X	10-Gigabit XFP module	*distance depends on transceiver type
DEM-421	850mn Multi-mode XFP transceiver	
DEM-422	1310mn, Single-mode XFP transceiver	

Network pluggable optical modules meet the following regulatory requirements:

- Class 1 Laser Product
- EN60825-1+A2:2001 or later, European laser standard
- FCC 21 CFR Chapter 1, Subchapter J in accordance with FDA & CDRH requirements

Appendix E - Password Recovery Procedure

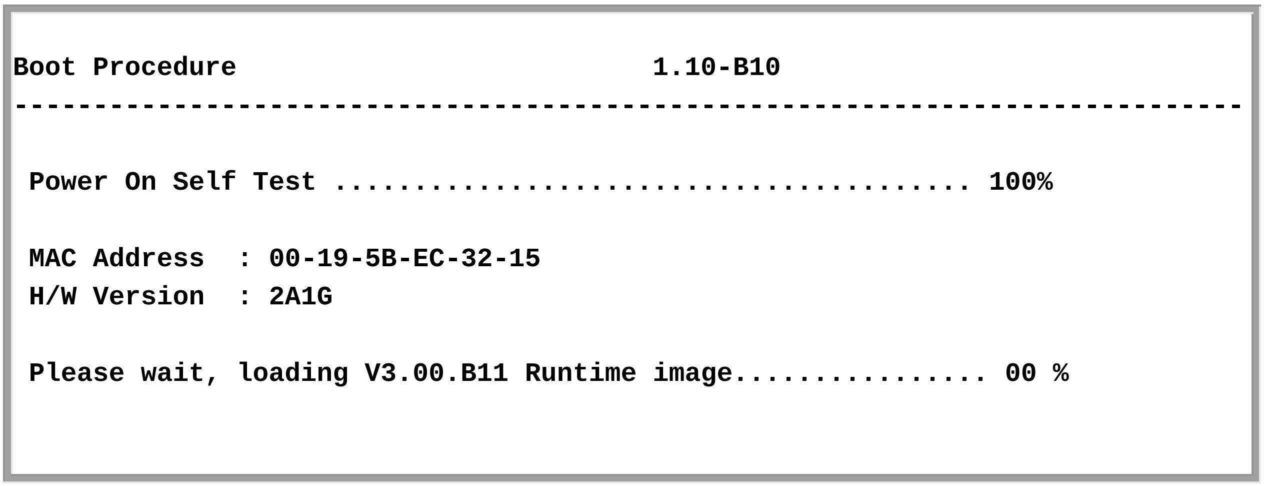
This section describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode”. Once the Switch enters the “Password Recovery Mode”, all ports on the Switch will be disabled.

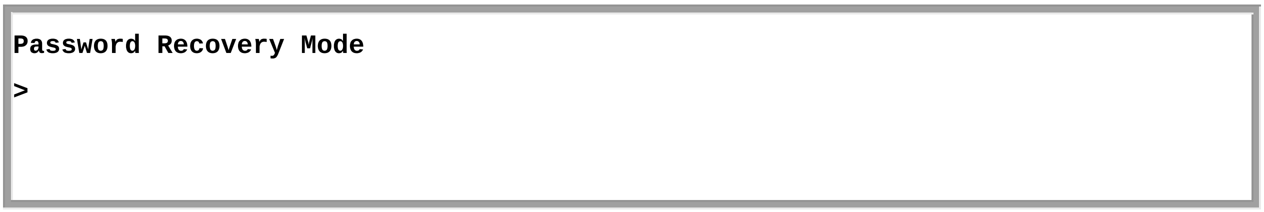


```
Boot Procedure                          1.10-B10
-----------------------------------------------------------------------------


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

 MAC Address  : 00-19-5B-EC-32-15
 H/W Version  : 2A1G

 Please wait, loading V3.00.B11 Runtime image................ 00 %
```



```
Password Recovery Mode
>
```

3. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config	This command resets the whole configuration back to the default values.
reboot	This command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reboot force_agree	This command forces the switch to restart.
reset account	This command deletes all the previously created accounts.
reset password	This command resets the password of the specified user. If a username is not specified,

Command	Parameters
{<username>}	the password of all users will be reset.
show account	This command displays all previously created accounts.

Appendix F - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: 802.1X (Port-based and MAC-based), Web-based Access Control (WAC), Japanese Web-based Access Control (JWAC), and MAC-based Access Control.

The description that follows explains the following RADIUS Attributes Assignment types:

- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN

To assign Ingress/Egress bandwidth by RADIUS Server, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0” or more, than the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to no_limited.

To assign **802.1p default priority by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or Host-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign VLAN by RADIUS Server, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminatior).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC-based Access Control authentication is successful, the port will be added to VLAN 3. However, if the user does not configure the VLAN attribute and authenticates successfully, the port will be kept in its original VLAN. If the VLAN attribute configured on the RADIUS server does not exist, the port will not be assigned to the requested VLAN.

To assign ACL by RADIUS Server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for an ACL. The RADIUS ACL assignment is only used in MAC-based Access Control.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	12 (for ACL profile) 13 (for ACL rule)	Required
Attribute-Specific Field	Used to assign the ACL profile or rule.	ACL Command For example: ACL profile: **create access_profile ethernet vlan 0xFFF profile_id 100**; ACL rule: **config access_profile profile_id 100 add access_id auto_assign ethernet vlan_id default port all deny**;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: create access_profile ethernet vlan 0xFFF profile_id 100; ACL rule: config access_profile profile_id 100 add access_id auto_assign ethernet), and the MAC-based Access Cotntrol authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to the Access Control List (ACL) chapter in the DGS-3600 Series CLI Reference Guide.

Glossary

1000BASE-SX: A short laser wavelength on multimode fiber optic cable for a maximum length of 2000 meters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

line speed: See baud rate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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