User's Manual

WGS3-24000

24-Port 10/100/1000Mbps Layer 3 Managed Ethernet Switch

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

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 the Instruction 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 whose own expense.

CE Mark Warning

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

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET 24-Port 10/100/1000Mbps with 4 Gigabit SFP Layer 3 Managed Ethernet Switch User's Manual

FOR MODEL: WGS3-24000

REVISION: 1.1 (May.2007)

Part No. EM-WGS3-24000_v1.1 (2081-A96020-001)

Table of Contents

1. INTRODUCTION

1.1 Packet Contents

Thank you for purchasing PLANET 24-Port 10/100/1000Mbps wtih 4 shared SFP Layer 3 Managed Switch- WGS3-24000. Terms of **“WGS3-Layer 3 Switch”** means the Switches mentioned titled in the cover page of this User’s manual, i.e.WGS3-24000.

Check the contents of your package for following parts:

- The WGS3 Layer 3 Switch x1
- CD-ROM user’s manual x1
- Quick installation guide x1
- 19” rack mounting kit x1
- Power cord x1
- Rubber feet x 4
- RS-232 Console x 1

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.

1.2 How to Use This Manual

This User Manual is structured as follows:

Section 2, **Installation**

The section explains the functions of the Switch and how to physically install the Switch.

Section 3, **Configuration**

The section contains the information about the software function of the Switch.

Section 4, **Web Configuration**

The section explains how to manage the switch by Web interface.

Section 5, **Command Structure**

The section explains how to manage the switch by Console interface..

Section 6, **Quick Start Up**

Section 7, **Mode-Base CLI**

Section 8, **CLI Command:-Base**

Section 9, **CLI Command: Quality of Service**

Section 10, **CLI Command: Security**

Section 11, **CLI Commands: Switching**

Section 12, **CLI Commands: Routing**

Appendex A

The section contains cable information of the Switch.

In the following section, terms with lower case "switch" means other Ethernet switch devices.

1.3 Product Feature

- **Physical Ports**
  - □ 24 RJ-45 ports for 10/100/1000Base-T
  - □ 4 shared SFP mini-GBIC interfaces (Shared with Port-12 and Port-24)
  - □ One DB9 male/RS-232 console port
  - □ One DB9 male/RS-232 console port
  - □ One DB9 male/RS-232 console port

- **Layer 2 Features**
  - □ Supports auto MDI/MDI-X on all 10/100/1000Base-T ports
  - □ The 10/100/1000Base-TX ports support auto-sensing, auto-negotiation
  - □ Supports Jumbo frame up to 9KB
  - □ Provides wire speed of L2 switching performance
  - □ Supports up to 16K MAC address entries
  - □ Supports Flow Control
    - IEEE 802.1x for Full-Duplex mode
    - Back-Pressure Flow Control in Half-Duplex mode
  - □ Provides Store-and-Forward forwarding scheme
  - □ Provides Broadcast storm protection
  - □ Supports IGMP snooping v1, v2
  - □ Supports VLAN
    - IEEE 802.1Q VLAN
    - GARP/GVRP/GMRP
    - Up to 4041 VLANs, out of 4041 VLAN IDs
    - Protocol-Based VLAN
  - □ Supports Spanning Tree Protocol
    - STP, IEEE 802.1d
    - RSTP, IEEE 802.1w
    - MSTP, IEEE 802.1s
  - □ Supports Link Aggregation
    - up to 8 trunk groups
    - up to 8 ports per trunk group
    - 802.3ad Link Aggregation and LACP
    - Cisco ether-channel (Static Trunk)
  - □ Provides Port Mirror (many-to-1)

- **Routing Features**
  - □ Supports RIP v1 and v2
  - □ Supports OSPF v1/v2
  - □ Supports router discovery (IRDP)

□ Supports VLAN routing

□ Supports VRRP

□ Supports IP routing

□ Supports route redistribution

□ Supports route preferences

► **Multicast**

□ Supports PIM-DM and PIM-SM

□ Supports DVMRP

□ Supports IGMP v1/v2/v3

► **Security**

□ User/Password protected system management

□ L2/L3/L4 ACL (access control list)

□ RADIUS client

□ TACACS client

□ SSH v1/v2

□ SSL v3/TLS v1

□ IEEE 802.1x Port-Based Autentication

□ Port MAC lock

► **Quality of Service**

□ IEEE 802.1p based CoS

□ 8 priority queues per port

□ IP TOS/Precedence based Cos

□ DSCP based CoS

□ Policy based DiffServ

► **Management**

□ Provides 1 male DB9 RS-232C console interface

□ Supports BOOTP and DHCP for IP address assignment

□ Supports DHCP relay function

□ Supports software upload/download via XMODEM or TFTP

□ Supports configuration upload/download via XMODEM or TFTP

□ Supports up to three configuration files including factory default

□ Supports SSH v1/v2 switch management

□ Supports SSH/SSL/TLS keys download via XMODEM or TFTP

□ Supports SNTP (Simple Network Time Protocol)

□ Supports Ping function

□ Supports telnet function

□ Supports message/event/error/trap logs

- □ Supports logging to local file and syslog server
- □ Supports Command Line Interface switch management
- □ Supports Web switch management
- □ Supports SNMP v1, v2c, and v3 switch management
- □ Supports Private Enterprise MIB
- □ Supports RMON groups 1, 2, 3, 9
- □ Supports port mirror (many-to-1)

1.4 Product Specification

Product	**WGS3-24000** 24-Port 10/100/1000Mbps TP with 4-Port mini-GBIC Layer 3 Managed Ethernet Switch
Hardware Specification	
10/100/1000Base-T Ports	24 RJ-45 Auto-MDI/MDI-X ports
SFP/mini-GBIC slots	4 SFP interfaces
Switch Architecture	Store-and-Forward
Switch Fabric	48Gbps Capacity
Switch throughput	35.7Mpps
Address Table	16K MAC address table with Auto learning function
Layer 3 Routing Table	2048
Buffer Memory	2Mbits for packet buffer
Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex
LED	Power, Link/Act, FDX/COL
Layer 2 function	
Management Interface	Console. Telnet, SSH, Web, SSL, SNMP
Port configuration	Port disable/enable. Auto-negotiation 10/100Mbps full and half duplex mode selection. Flow Control disable / enable. Bandwidth control on each port.
Port Status	Display each port’s speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.
VLAN	IEEE 802.1Q Tagged Based VLAN ,up to 4041 VLAN groups
Port trunking	Support 8 groups of 8-Port trunk
QoS	Traffic classification based on Port Number, 802.1p priority, DS/TOS field in IP Packet
IGMP Snooping	Allow to disable or enable.

IP Routing Protocol	Static Route, RIPv1/v2, OSPFv2,IRDP, VRRP
Multicast Routing Protocol	DVMRP, PIM-DM/SM
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid Spanning tree protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging

2. INSTALLATION

This section describes the functionalities of the Switch's components and guides how to install it on the desktop or shelf. Basic knowledge of networking is assumed. Please read this chapter completely before continuing.

2.1 Product Description

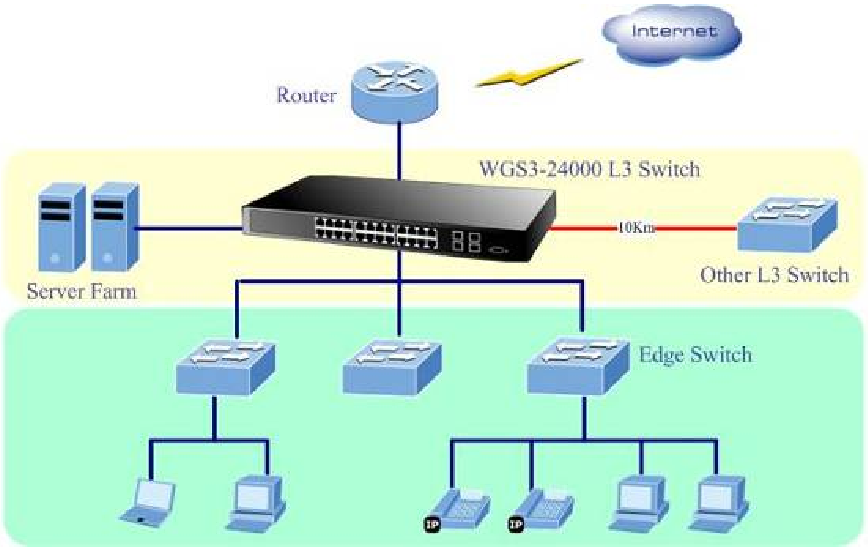
The PLANET WGS3-24000 is a 24-Port 10/100/1000Mbps with 4 shared SFP/copper GbE interface Gigabit Ethernet Switch. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 48Gbps. Its two built-in GbE uplink ports also offer incredible extensibility, flexibility and connectivity to the Core switch or Servers.

2.1.1 Product Overview

PLANET WGS3-24000 is loaded with powerful traffic management and QoS features to enhance services offered by telcos. It provides 4 priority queues per port for different types of traffics, allowing administrators to set policies for classified filtering and rule-based rate limitation. The WGS3-24000 prioritizes applications with WFQ (Weighted Fair Queuing) scheduling algorithm to allocate more bandwidth to key traffics such as voice transmission, empowering the enterprise to take full advantages of the limited network resources and guarantee the best performance.

PLANET WGS3-24000 offers comprehensive Access Control List (ACL) for enforcing security to the edge. Its protection mechanisms comprised of port-based 802.1x user and device authentication. The administrators can now construct highly secured corporate networks with time and effort considerably less then before.

With its built-in web-based management, the PLANET WGS3-24000 offers an easy-to-use, platform-independent management and configuration facility. The PLANET WGS3-24000 supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. For text-based management, the WGS3-24000 can also be accessed via Telnet and the console port. For secure remote management, the WGS3-24000 support SSL and SSH connection which encrypt the packet content at each session.



2.1.2 Switch Front Panel

Figure 2-1 shows the front panel of the switch.

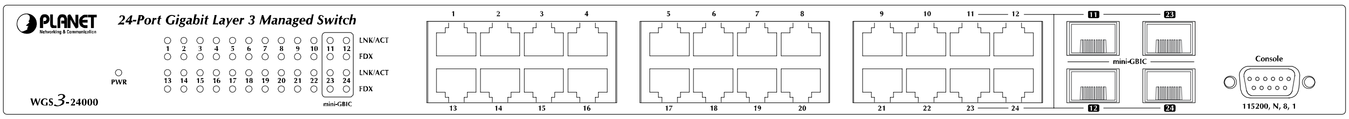


Figure 2-1 WGS3-24000 front panel.

2.1.3 LED Indications

Network:

LED	Color	Function
PWR	Green	Lights to indicate that the Switch is powered on.
LNK/ACT	Green	Lights to indicate the link through that port is successfully established.
FDX	Green	Blink to indicate the switch is actively sending or receiving data over that port.

Gigabit:

LED	Color	Function
LNK/ACT	Green	Lights to indicate the link through that port is successfully established.
FDX/COL	Green	Blink to indicate the switch is actively sending or receiving data over that port.

2.1.4 Switch Rear Panel

Figure 2-2 shows the rear panel of the switch

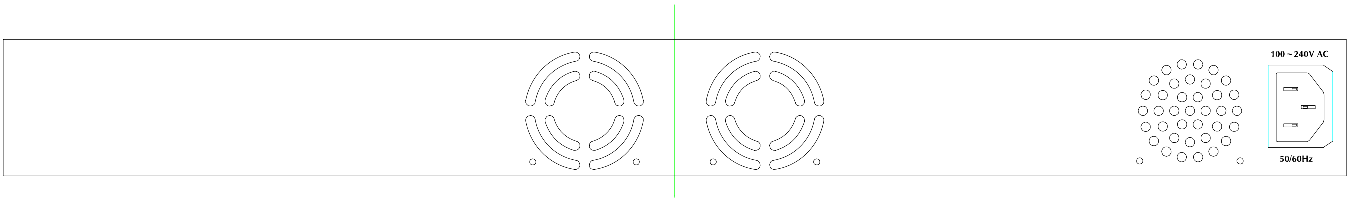


Figure 2-2 WGS3-24000 rear panel.

Power Notice:

1. The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.
2. In some area, installing a surge suppression device may also help to protect your switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Install the Switch

This section describes how to install the Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.2.1 Desktop Installation

To install the Switch on desktop or shelf, please follows these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the switch.

Step2: Place the switch on the desktop or the shelf near an AC power source.

Step3: Keep enough ventilation space between the switch and the surrounding objects.

Note: When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, in Specification.

Step4: Connect the Switch to network devices.

A. Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Switch

B. Connect the other end of the cable to the network devices such as printer servers, workstations or routers…etc.

Note: Connection to the Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the switch.

A. Connect one end of the power cable to the switch.

B. Connect the power plug of the power cable to a standard wall outlet.

When the switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the switch in a 19-inch standard rack, please follows the instructions described below.

Step1: Place the switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the switch with supplied screws attached to the package.

Figure 2-5 shows how to attach brackets to one side of the switch.

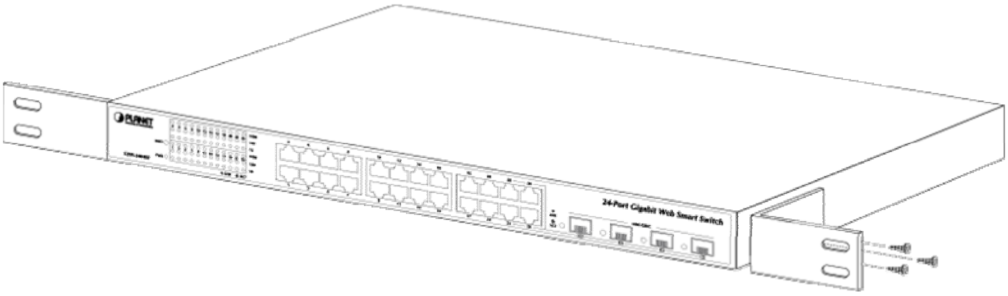


Figure 2-5 Attach brackets to the switch.

Caution:

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6

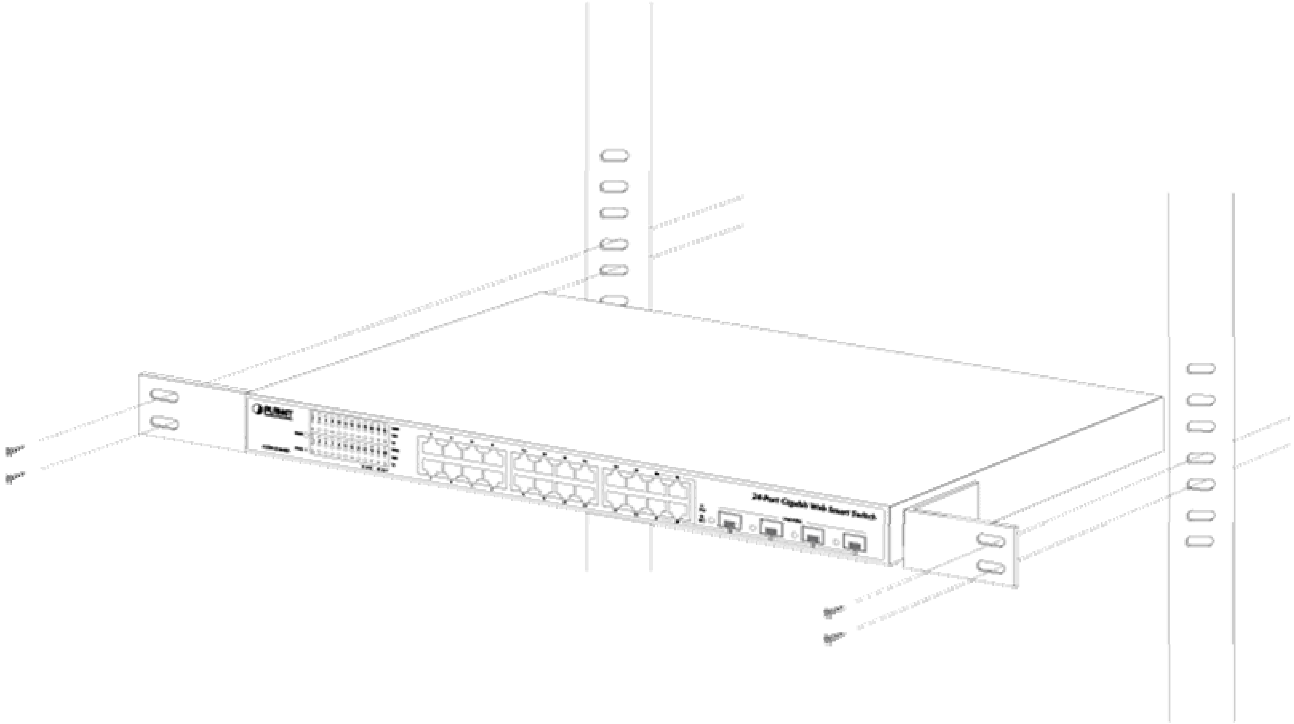


Figure 2-6 Mounting the Switch in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the switch.

2.2.3 Installing the SFP transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Switch. As the Figure 2-7 appears.

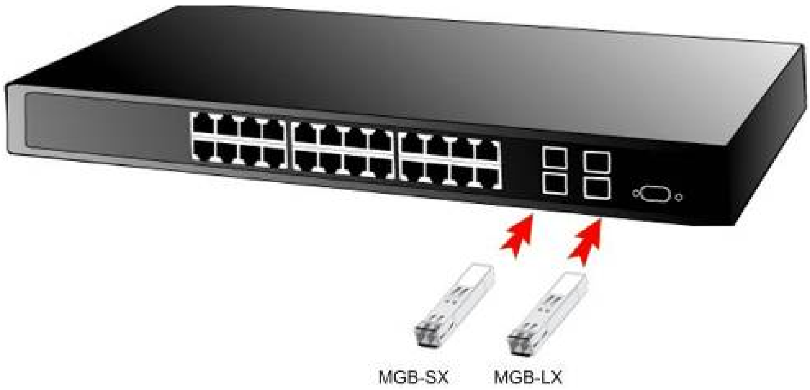


Figure 2-7 Plug-in the SFP transceiver

Approved PLANET SFP Transceivers

PLANET WGS3-24000 support both single mode and multi mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

■MGB-SX SFP (1000BASE-SX SFP transceiver)

■MGB-LX SFP (1000BASE-LX SFP transceiver)

Note: It recommends using PLANET SFPs on the Switch. If you insert a SFP transceiver that is not supported, the Switch will not recognize it.

Before connect the other switches, workstation or Media Converter.

1. Make sure both side of the SFP transfer are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type match the SFP transfer model.
   - To connect to **1000Base-SX** SFP transfer, use the **multi-mode** fiber cable- with one side must be male duplex LC connector type.
   - To connect to **1000Base-LX** SFP transfer, use the **single-mode** fiber cable-with one side must be male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter..
3. Check the LNK/ACT LED of the SFP slot on the front of the Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to “1000 Force” is needed.

Remove the transceiver module

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MGB/MFB module to horizontal.
4. Pull out the module gently through the handle.

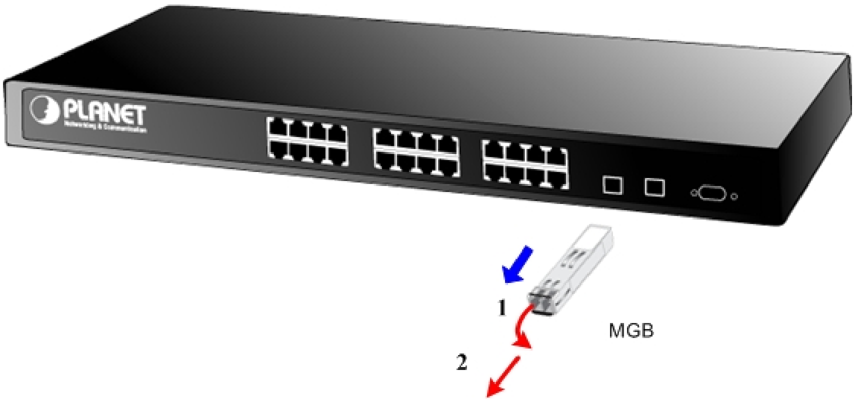


Figure 2-8 Pull Out the SFP transceiver

Note: Never pull out the module without pull the handle or the push bolts on the module. Direct pull out the module with violent could damage the module and SFP module slot of the device.

---

3. CONFIGURATION

This chapter explains the methods that you can use to configure management access to the switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (work-station or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Management Access Overview
- Key Concepts
- Key Guidelines for Implementation
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Management Access Overview

The switch gives you the flexibility to access and manage the switch using any or all of the following methods:

- An administration console
- Web browser interface
- An external SNMP-based network management application

The administration console and Web browser interface support are embedded in the switch software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

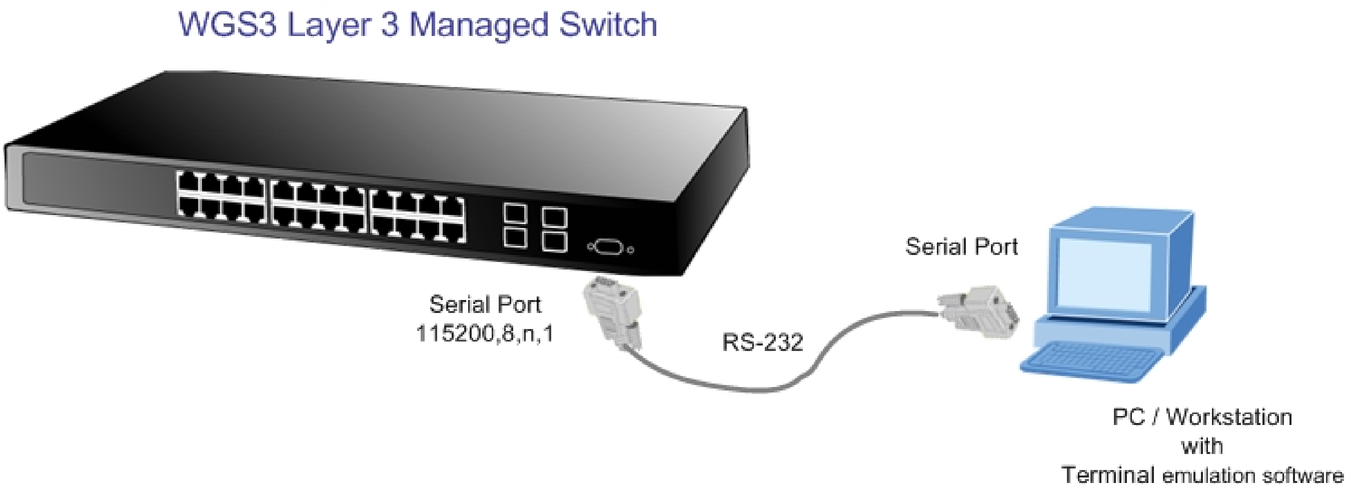
Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure	• Must be near switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level	• Requires SNMP manager software • Least visually appealing of all three methods

	• Based on open standards	• Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1 Management Methods Comparison

3.1.1 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console (serial) port. There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 4 Command Line Interface Console Management**.



3.1.2 Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console (serial) port.

When using this management method, a null-modem cable is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **115,200 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

3.2 Web Management

The switch provides a browser interface that lets you configure and manage the switch remotely. After you set up your IP address for the switch, you can access the switch's Web interface applications directly in your Web browser by entering the IP address of the switch. You can then use your Web browser to list and manage switch configuration parameters from one central location, just as if you were directly connected to the switch's console port.

Web Management requires either Microsoft Internet Explorer 6.0 or later or Mozilla Firefox 1.5 or later.

3.3 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the switch. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the get community string and the set community string. If the SNMP Net-work management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default gets and sets community strings for the switch are public.

3.4 Protocols

The switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- Simple Network Management Protocol (SNMP)

3.4.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the switch before you can establish access to it with a virtual terminal protocol.

✍ ***Note:*** Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal directly to the console (serial) port.

3.4.2 SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

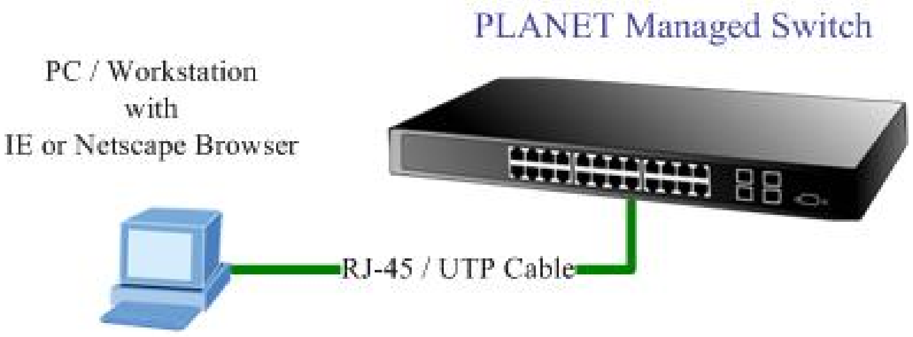
3.4.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent of Web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. Web Configuration

The WGS3-24000 can be configured through an Ethernet connection, make sure the manager PC must be set on same the **IP subnet address** with the switch. For example, if you have changed the default IP address of the Switch to **192.168.1.1** with subnet mask **255.255.255.0** via console, then the manager PC should be set at **192.168.1.x** (where x is a number between 2 and 254) with subnet mask **255.255.255.0**. Or you can use the factory default IP address **192.168.1.254** to do the relative configuration on manager PC.



- **Logging on the switch**

1. Use Internet Explorer 6.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address as following:

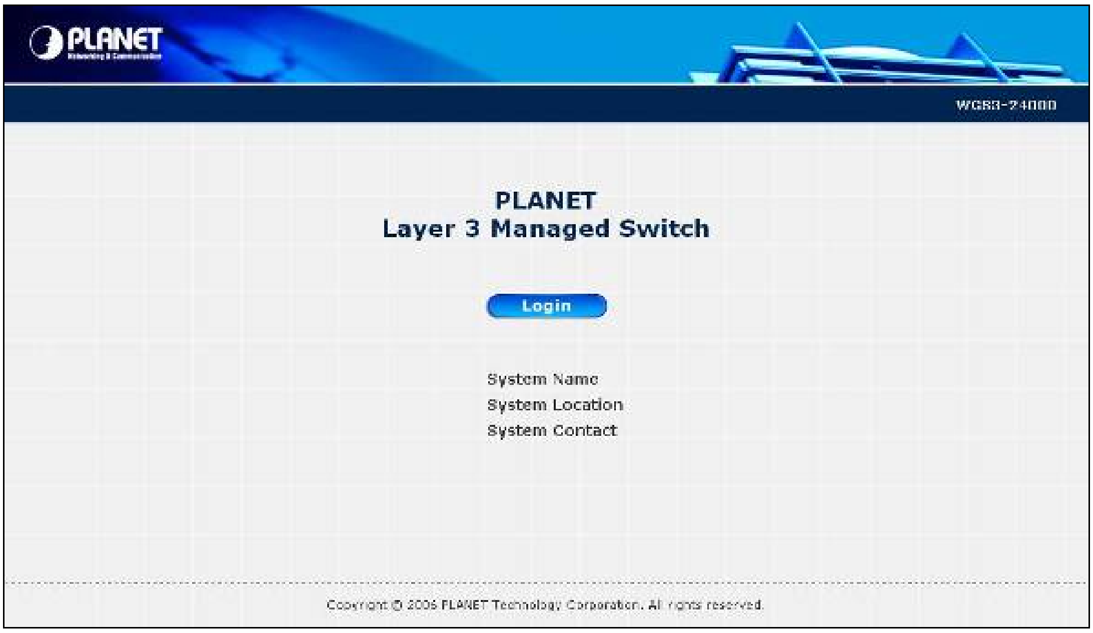
http://192.168.1.254

2. When the following login screen appears, the system will ask you to enter the username and password.

Default User name: **admin**

Default Password: **admin**

The login screen in Figure 4-2 appears.

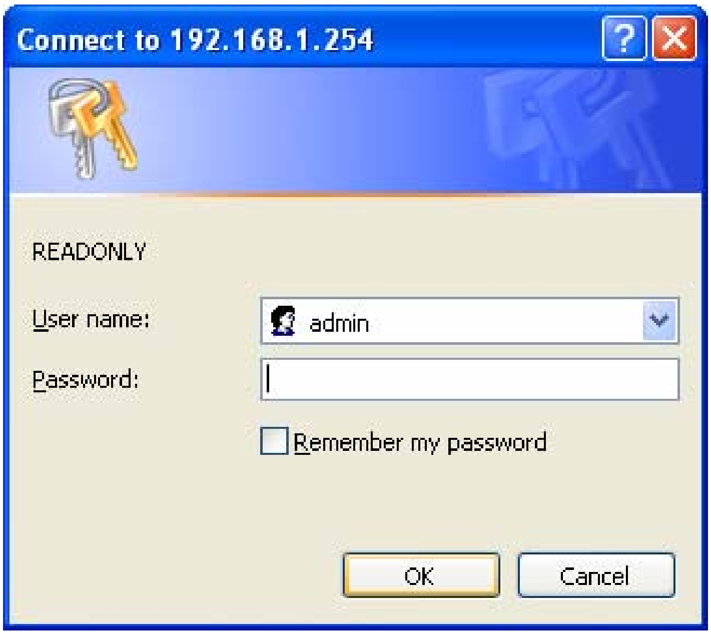


PLANET
Layer 3 Managed Switch

System Name
System Location
System Contact

Copyright © 2006 PLANET Technology Corporation. All rights reserved.

3. When the following login screen appears, please enter the default username **"admin"** with password “**admin**” (or the username/password you have changed via console) to login the main screen of Switch. The login screen in Figure 4-1 appears.



Connect to 192.168.1.254

READONLY

User name: admin

Password:

□ Remember my password

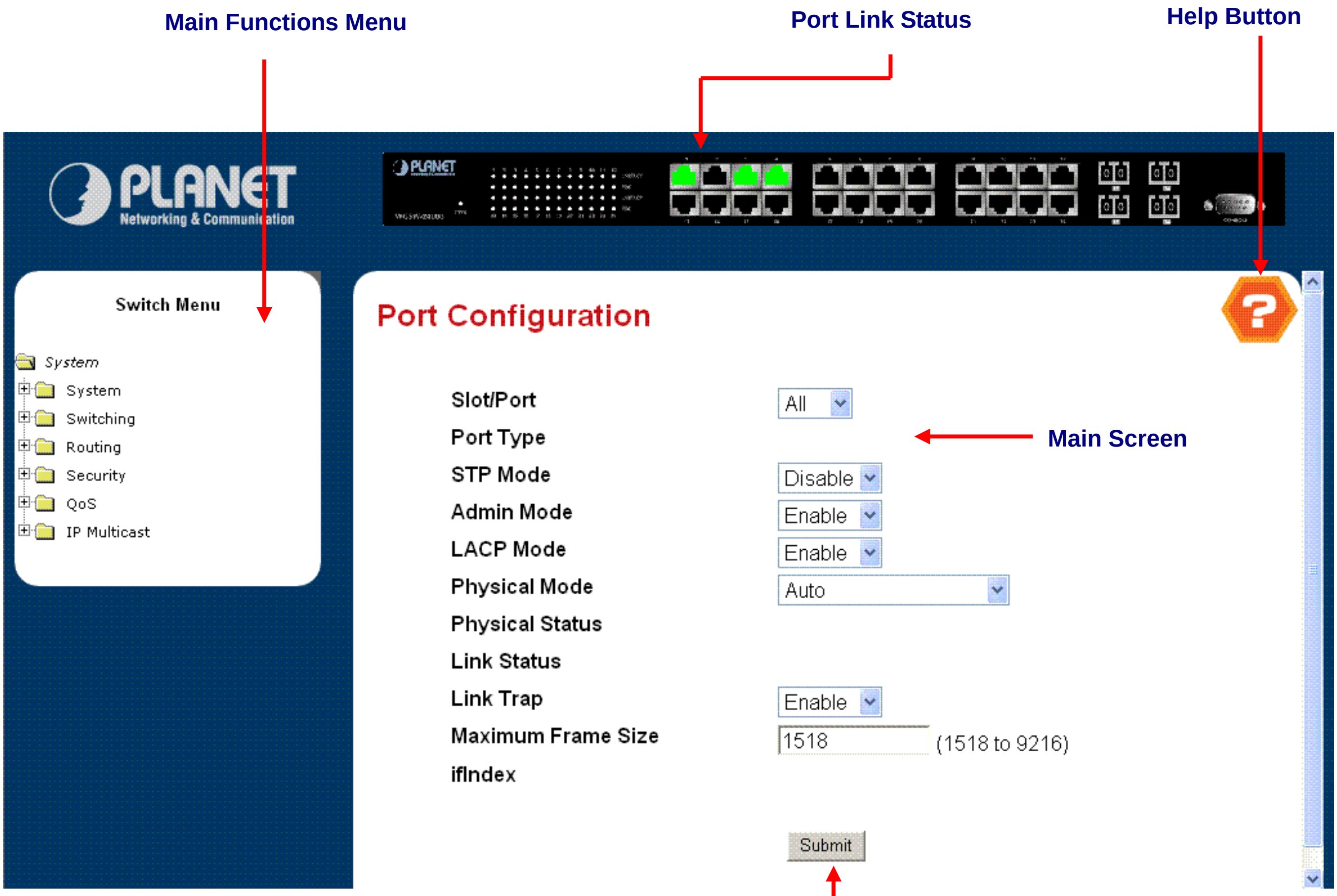
Figure 4-1 Login screen

Now, you can use the Web management interface to continue the switch management or manage the switch by console interface.

Note: It is recommended to use Internet Explore 6.0 or above to access WGS3-24000.

4.1 Main Menu

The Switch provides a Web-based browser interface for configuring and managing the Switch. This interface allows you to access the switch using the Web browser of your choice. This chapter describes how to use the switch's Web browser interface to con-figure and manage the switch.



Port Configuration

Slot/Port	All
Port Type	
STP Mode	Disable
Admin Mode	Enable
LACP Mode	Enable
Physical Mode	Auto
Physical Status	
Link Status	
Link Trap	Enable
Maximum Frame Size	1518 (1518 to 9216)
ifIndex	

Submit

Figure 4-1-1 Main Page

Via the Web-Management, the administrator can setup the WGS3-24000 by select the functions those listed in the Main Function. The screen in Figure 4-2 appears.

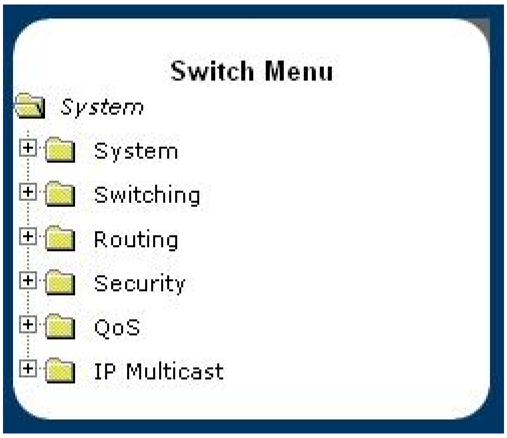


Figure 4-1-2 WGS3-24000 Main Funcrions Menu

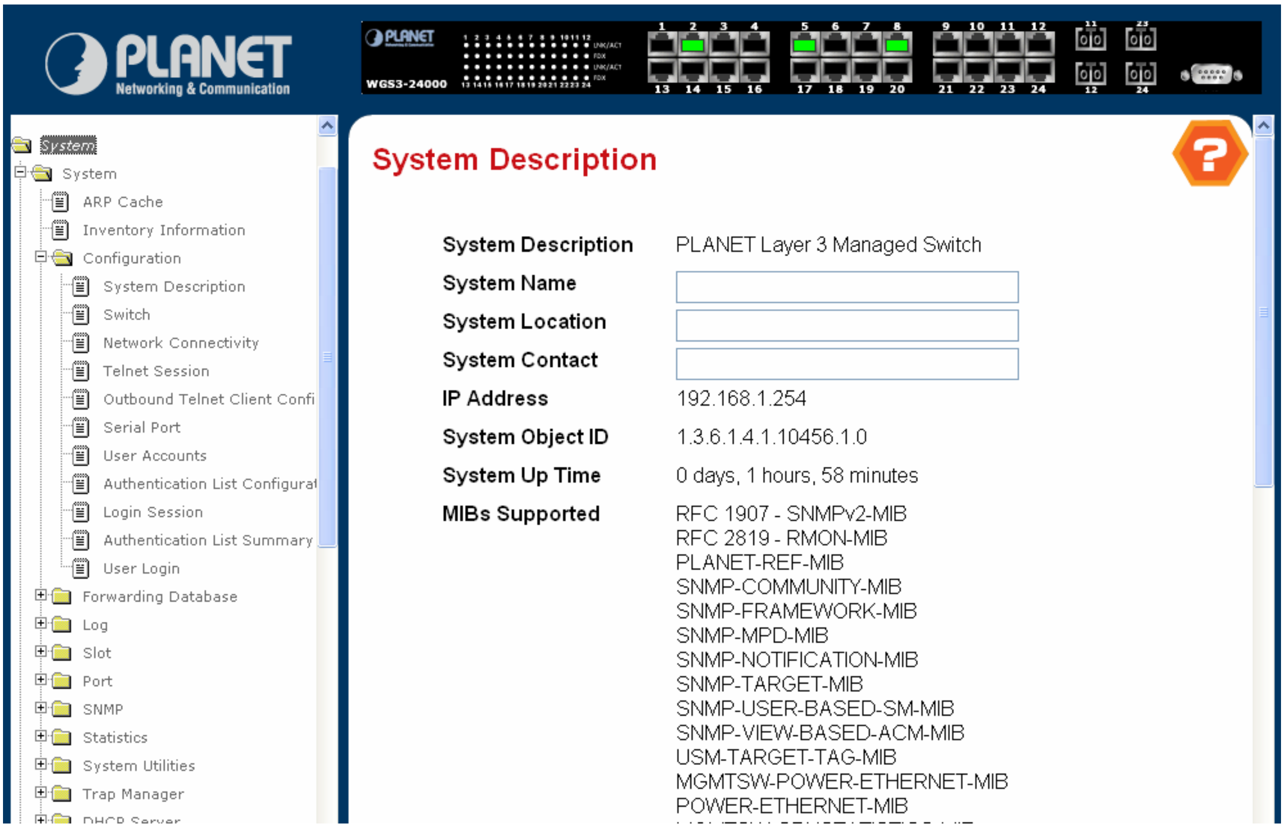
The following functions can be configured here:

- **System**
- **Switching**
- **Routing**
- **Security**
- **QoS**
- **IP Multicast**

System Description

After a successful login, the main screen appears, the main screen displays the port status and a list of System section and the topics it provide. As showed in Figure 4-2.

- **System Name -** Enter the name you want to use to identify this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
- **System Location -** Enter the location of this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
- **System Contact -** Enter the contact person for this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.



System Description

System Description	PLANET Layer 3 Managed Switch
System Name	
System Location	
System Contact	
IP Address	192.168.1.254
System Object ID	1.3.6.1.4.1.10456.1.0
System Up Time	0 days, 1 hours, 58 minutes
MIBs Supported	RFC 1907 - SNMPv2-MIB RFC 2819 - RMON-MIB PLANET-REF-MIB SNMP-COMMUNITY-MIB SNMP-FRAMEWORK-MIB SNMP-MPD-MIB SNMP-NOTIFICATION-MIB SNMP-TARGET-MIB SNMP-USER-BASED-SM-MIB SNMP-VIEW-BASED-ACM-MIB USM-TARGET-TAG-MIB MGMTSW-POWER-ETHERNET-MIB POWER-ETHERNET-MIB

Figure 4-1-3 main menu screen

4.2 Configure System

The System section provides information for configuring system parameters. Under system the following topics are provided to configure and view the system information:

- **ARP Cache**
- **Inventory Information**
- **System Loading**
- **Configuration**
- **Forward Database**
- **Log**
- **Port**
- **SNMP**
- **Statistics**
- **System Utilities**
- **Trap Manager**
- **DHCP Server**
- **SNTP**

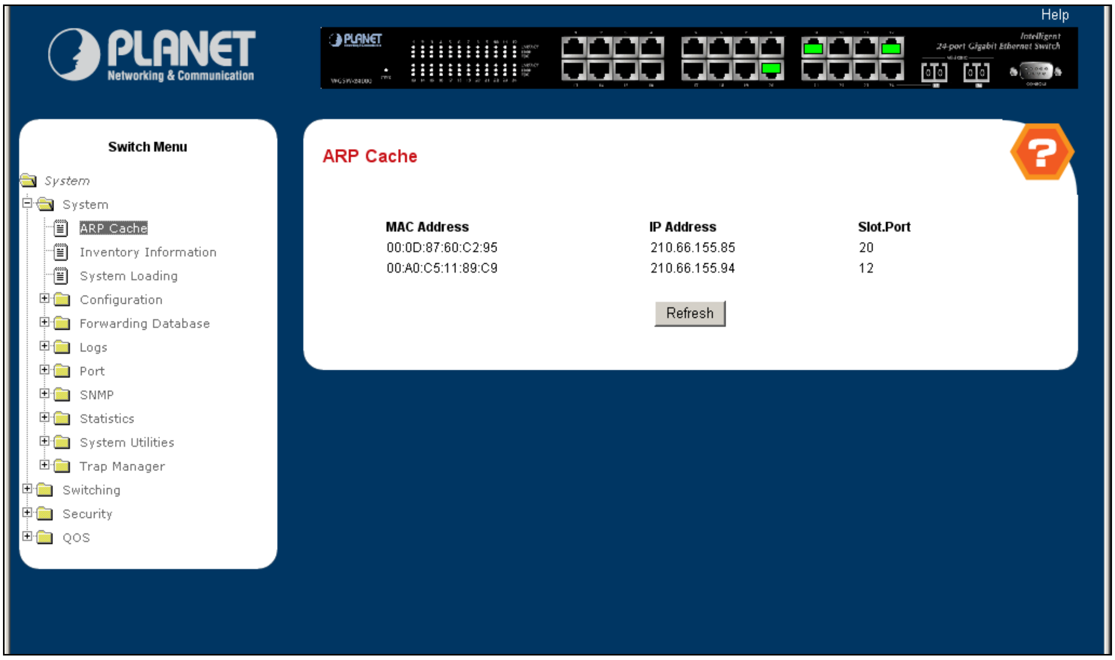
4.2.1 ARP Cache

The Address Resolution Protocol (ARP) dynamically maps physical (MAC) addresses to Internet (IP) addresses. This panel displays the current contents of the ARP cache.

For each connection, the following information is displayed:

- **The physical (MAC) Address**
- **The associated IP address**
- **The identification of the port being used for the connection**

As shows in figure 4-3:



ARP Cache

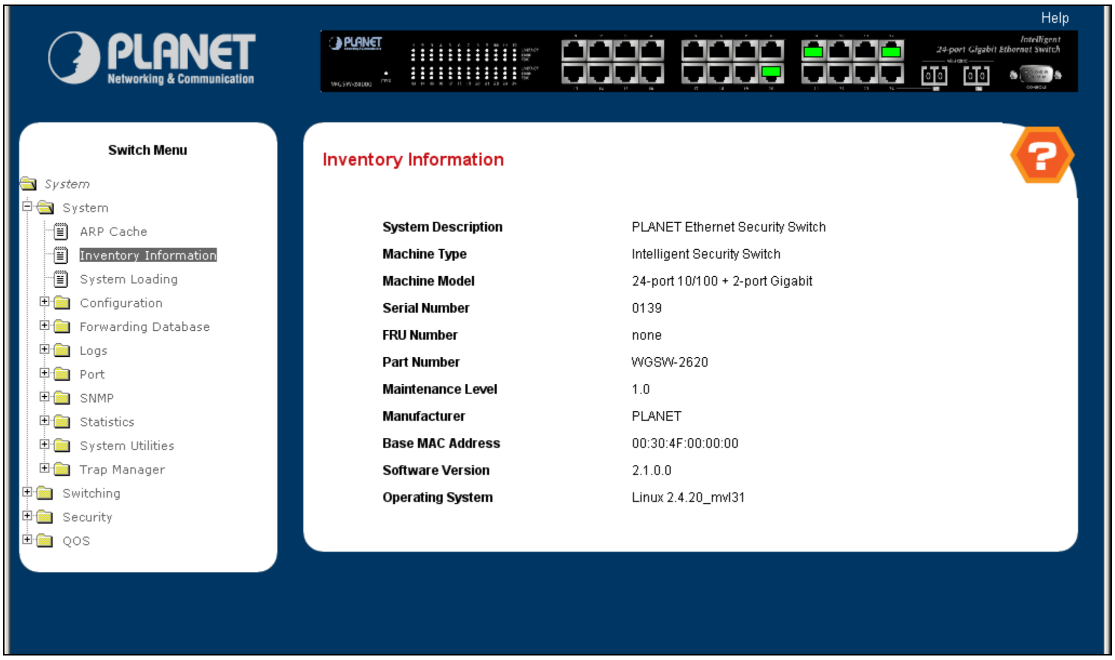
MAC Address	IP Address	Slot.Port
00:0D:87:60:C2:95	210.66.155.85	20
00:A0:C5:11:89:C9	210.66.155.94	12

Figure 4-2-1 ARP Cache

4.2.2 Inventory Information

Use this panel to display the switch's Vital Product Data, stored in non-volatile memory at the factory. The page includes the following fields:

- **System Description -** The product name of this switch.
- **Machine Type -** The machine type of this switch.
- **Machine Model -** The model within the machine type.
- **Serial Number -** The unique box serial number for this switch.
- **FRU Number -** The field replaceable unit number.
- **Part Number -** The manufacturing part number.
- **Maintenance Level -** The identification of the hardware change level.
- **Manufacturer -** The two-octet code that identifies the manufacturer.
- **Base MAC Address -** The burned-in universally administered MAC address of this switch.
- **Software Version -** The release version maintenance number of the code currently running on the switch. For example, if the release was 1, the version was 2 and the maintenance number was 4, the format would be '1.2.4'.
- **Operating System -** The operating system currently running on the switch.
- **Network Processing Device -** Identifies the network processor hardware.
- **Additional Packages -** A list of the optional software packages installed on the switch, if any. For example, FASTPATH BGP-4, or FASTPATH Multicast.



Inventory Information

System Description	PLANET Ethernet Security Switch
Machine Type	Intelligent Security Switch
Machine Model	24-port 10/100 + 2-port Gigabit
Serial Number	0139
FRU Number	none
Part Number	WGSW-2620
Maintenance Level	1.0
Manufacturer	PLANET
Base MAC Address	00:30:4F:00:00:00
Software Version	2.1.0.0
Operating System	Linux 2.4.20_mvl31

Figure 4-2-2 Inventory Information

4.2.3 Configuration

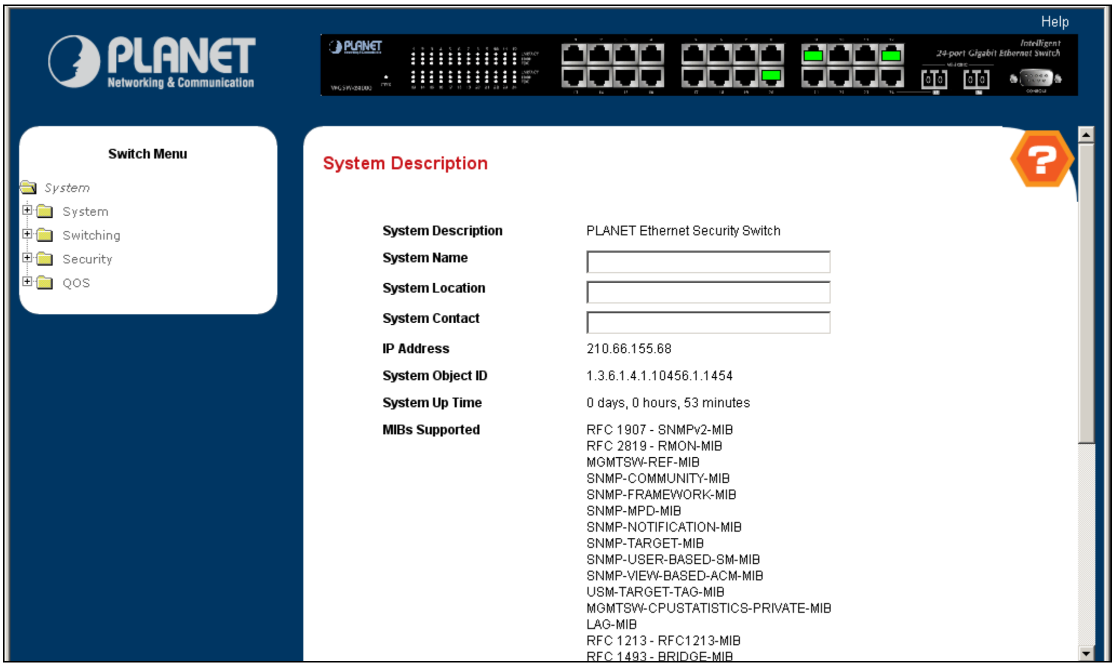
Use this page to configure the parameters for system management, including the following fields:

- **System Description**
- **Switch**
- **Network Connectivity**
- **Telnet Session**
- **Outbound Telnet Client Configuration**
- **Serial Port**
- **User Account**
- **Authentication List Configuration**
- **Login Session**
- **Authentication List Summary**
- **User Login**

4.2.3.1 System Description

This page shows the basic system information and is available to define the system name, location and contact person. Includes the following fields:

- **System Name -** Enter the name you want to use to identify this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
- **System Location -** Enter the location of this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
- **System Contact -** Enter the contact person for this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
- **System Description -** The product name of this switch.
- **System Object ID -** The base object ID for the switch's enterprise MIB.
- **System IP Address -** The IP Address assigned to the network interface.
- **System Up time -** The time in days, hours and minutes since the last switch reboot.
- **MIBs Supported -** The list of MIBs supported by the management agent running on this switch.



System Description

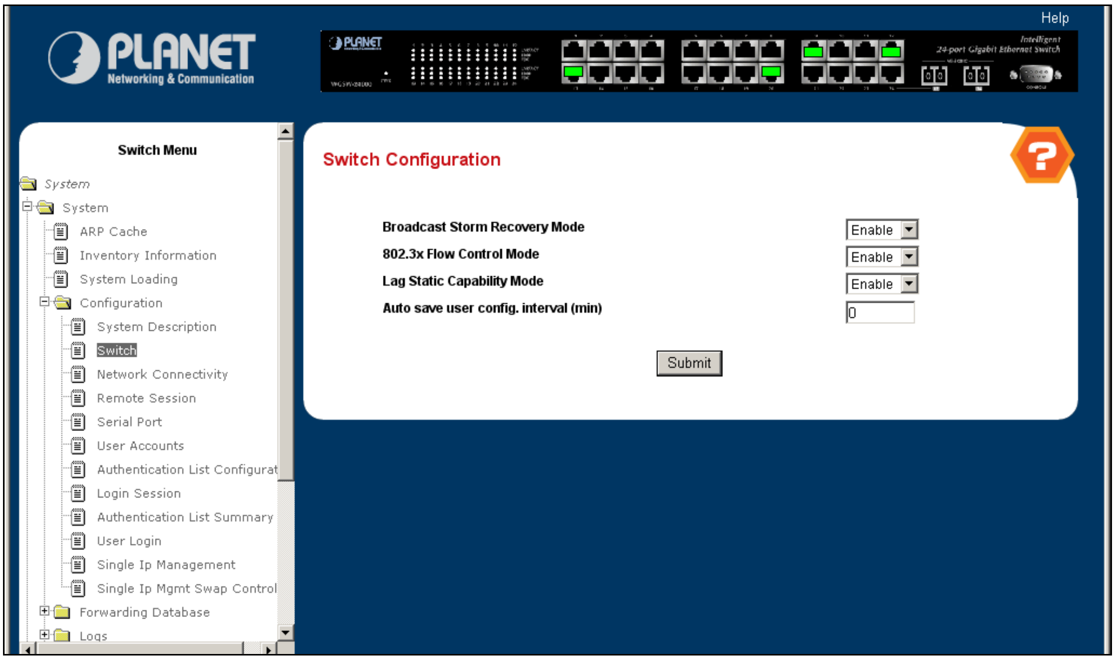
System Description	PLANET Ethernet Security Switch
System Name	
System Location	
System Contact	
IP Address	210.66.155.68
System Object ID	1.3.6.1.4.1.10456.1.1454
System Up Time	0 days, 0 hours, 53 minutes
MIBs Supported	RFC 1907 - SNMPv2-MIB RFC 2819 - RMON-MIB MGMTSW-REF-MIB SNMP-COMMUNITY-MIB SNMP-FRAMEWORK-MIB SNMP-MPD-MIB SNMP-NOTIFICATION-MIB SNMP-TARGET-MIB SNMP-USER-BASED-SM-MIB SNMP-VIEW-BASED-ACM-MIB USM-TARGET-TAG-MIB MGMTSW-CPUSTATISTICS-PRIVATE-MIB LAG-MIB RFC 1213 - RFC1213-MIB RFC 1493 - BRIDGE-MIB

Figure 4—2-3 System Description

4.2.4.2 Switch Configuration

This page includes the following fields:

- **Broadcast Storm Recovery Mode -** Enable or disable this option by selecting the corresponding line on the pull-down entry field. The factory default is disabled.
- **IEEE 802.3x Flow Control Mode -** Enable or disable this option by selecting the corresponding line on the pull-down entry field. The factory default is disabled.
- **Lag Static Capability Mode -** May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is disabled.



Switch Configuration

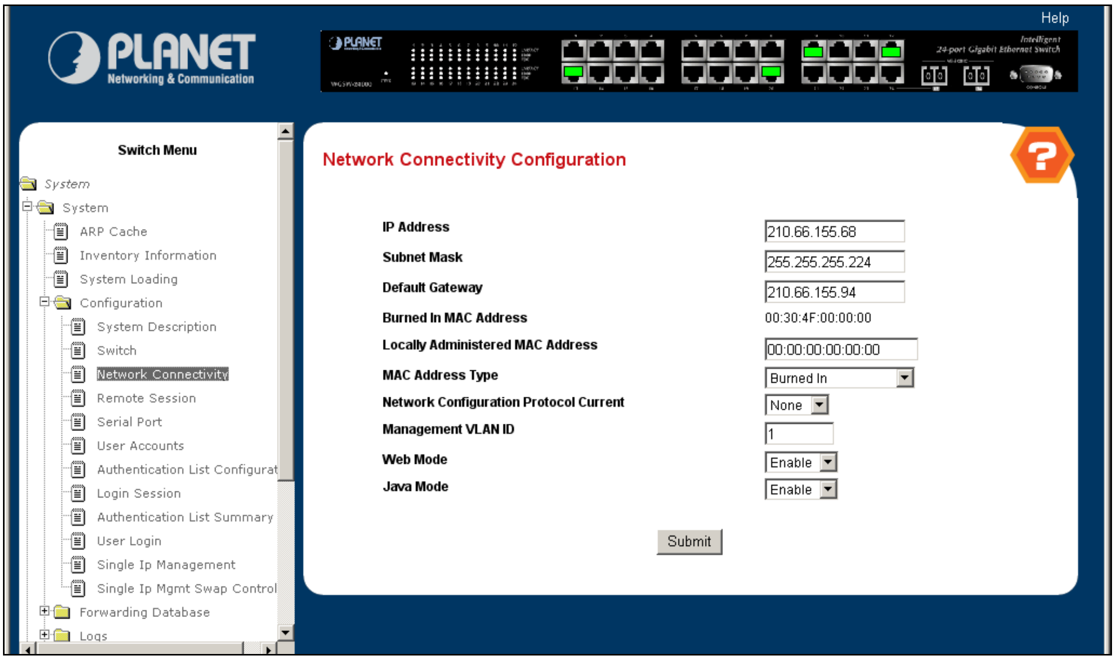
Broadcast Storm Recovery Mode	Enable
802.3x Flow Control Mode	Enable
Lag Static Capability Mode	Enable
Auto save user config. interval (min)	0

Submit

Figure 4-2-4 Switch Configuration

4.2.3.3 Network Connectivity

The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.



Network Connectivity Configuration

IP Address	210.66.155.68
Subnet Mask	255.255.255.224
Default Gateway	210.66.155.94
Burned In MAC Address	00:30:4F:00:00:00
Locally Administered MAC Address	00:00:00:00:00:00
MAC Address Type	Burned In
Network Configuration Protocol Current	None
Management VLAN ID	1
Web Mode	Enable
Java Mode	Enable

Submit

Figure 4-2-5 Network Connectivity Configuration

To access the switch over a network you must first configure it with IP information (IP address, subnet mask, and default gateway). You can configure the IP information using any of the following:

- **BOOTP**
- **DHCP**
- **Terminal interface via the EIA-232 port**

Once you have established in-band connectivity, you can change the IP information using any of the following:

- **Terminal interface via the EIA-232 port**
- **Terminal interface via telnet**
- **SNMP-based management**
- **Web-based management**

The page includes the following configurable data:

- **IP Address -** The IP address of the interface. The factory default value is 0.0.0.0
- **Subnet Mask -** The IP subnet mask for the interface. The factory default value is 0.0.0.0
- **Default Gateway -** The default gateway for the IP interface. The factory default value is 0.0.0.0
- **Locally Administered MAC Address -** You may configure a locally administered MAC address for in-band connectivity instead of using the burned-in universally administered MAC address. In addition to entering an address in this field, you must also set the MAC address type to locally administered. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 must have a value between x'40' and x'7F'.
- **MAC Address type -** Specify whether the burned-in or the locally administered MAC address should be used for in-band connectivity. The factory default is to use the burned-in MAC address

- **Network Configuration Protocol Current -** Choose what the switch should do following power-up: transmit a Bootp request, transmit a DHCP request, or do nothing (none). The factory default is DHCP.
- **Management VLAN ID -** Specifies the management VLAN ID of the switch. It may be configured to any value in the range of 1 - 4093. The management VLAN is used for management of the switch. This field is configurable for administrative users and read-only for other users.
- **Web Mode -** Specify whether the switch may be accessed from a web browser. If you choose to enable web mode you will be able to manage the switch from a web browser. The factory default is enabled.
- **Java Mode -** Enable or disable the java applet that displays a picture of the switch at the top right of the screen. If you run the applet you will be able to click on the picture of the switch to select configuration screens instead of using the navigation tree at the left side of the screen. The factory default is disabled.

The following data are non-configurable:

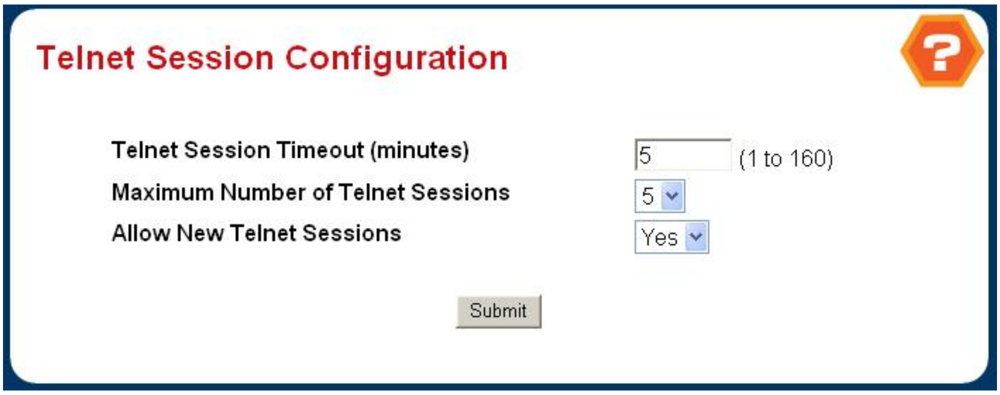
- **Burned-in MAC Address -** The burned-in MAC address used for in-band connectivity if you choose not to configure a locally administered address.
- **Network Configuration Protocol Current -** Indicates what network protocol was used on the last, or current power-up cycle, if any.

4.2.3.4 Telnet Session

This page includes the following fields:

Configurable Data

- **Telnet Session Timeout (minutes)** - Specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5.
- **Maximum Number of Telnet Sessions** - Use the pulldown menu to select how many simultaneous telnet sessions will be allowed. The maximum is 5, which is also the factory default.
- **Allow New Telnet Sessions** - If you set this to no, new telnet sessions will not be allowed. The factory default is yes.



Telnet Session Configuration

Telnet Session Timeout (minutes) 5 (1 to 160)

Maximum Number of Telnet Sessions 5

Allow New Telnet Sessions Yes

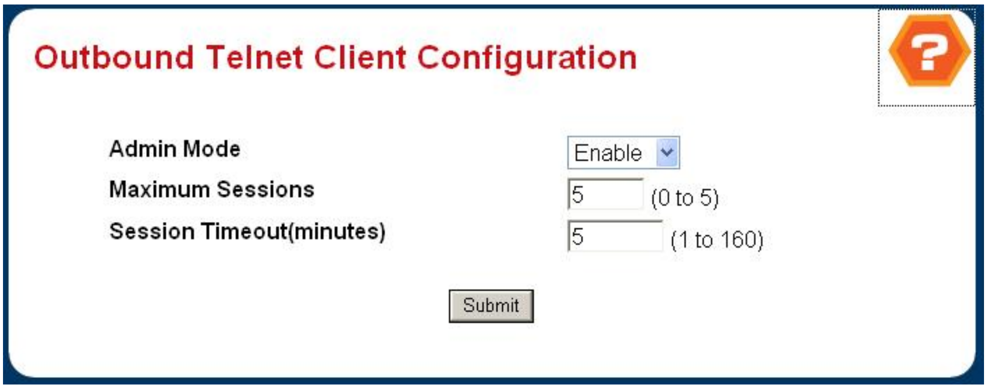
Figure 4-2-6 Telnet Session Configuration

4.2.3.5 Outbound Telnet Client Configuration

This page includes the following fields:

Configurable Data

- **Admin Mode** - Specifies if the Outbound Telnet service is Enabled or Disabled. Default value is Enabled.
- **Maximum Sessions** - Specifies the maximum number of Outbound Telnet Sessions allowed. Default value is 5. Valid Range is (0 to 5).
- **Session Timeout** - Specifies the Outbound Telnet login inactivity timeout. Default value is 5. Valid Range is (1 to 160).



Outbound Telnet Client Configuration

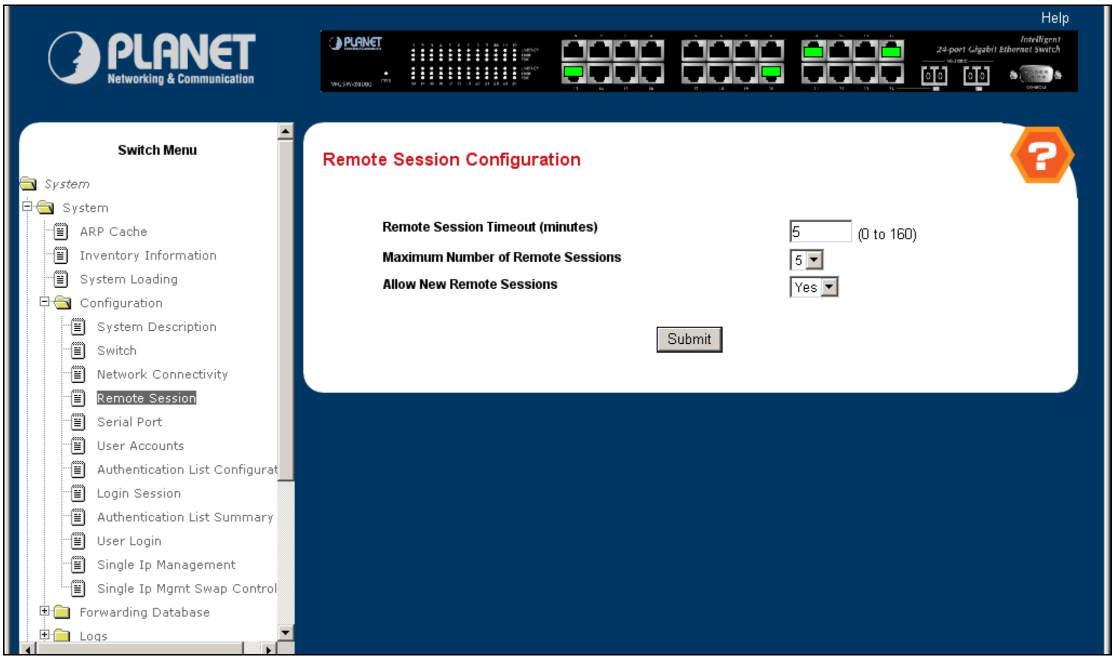
Admin Mode	Enable	
Maximum Sessions	5	(0 to 5)
Session Timeout(minutes)	5	(1 to 160)

Figure 4-2-7 OutboundTelnet Client Configuration

4.2.3. Remote Session

This page includes the following fields:

- **Remote Login Timeout (minutes) -** Specify how many minutes of inactivity should occur on a telnet or SSH session before the switch logs off. A zero means there will be no timeout. You may enter any number from 0 to 160. The factory default is 5.
- **Maximum Number of Remote Sessions -** Use the pull-down menu to select how many simultaneous telnet or SSH sessions will be allowed. The maximum is 5, which is also the factory default.
- **Allow New Remote Sessions -** If you set this to no, new telnet sessions will not be allowed. The factory default is yes.



Remote Session Configuration

Remote Session Timeout (minutes) 5 (0 to 160)

Maximum Number of Remote Sessions 5

Allow New Remote Sessions Yes

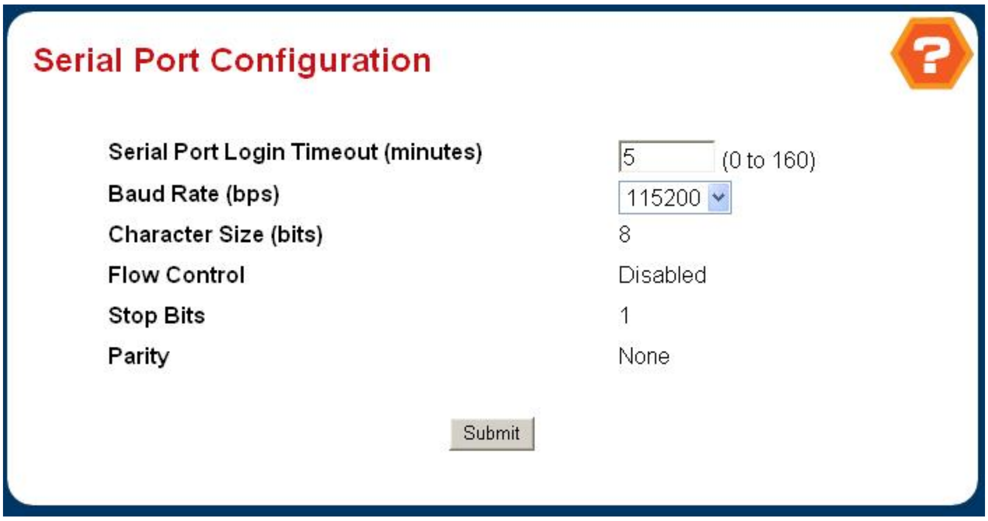
4.2.3.7 Serial Port

Use this page to define the parameters of console connectivity. The configurable data are:

- **Serial Port Login Timeout (minutes) -** Specify how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160: the factory default is 5. Entering 0 disables the timeout.
- **Baud Rate (bps) -** Select the default baud rate for the serial port connection from the pull-down menu. You may choose from 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 115200 baud.

And the non-configurable data:

- **Character Size (bits) -** The number of bits in a character. This is always 8.
- **Flow Control -** Whether hardware flow control is enabled or disabled. It is always disabled.
- **Parity -** The parity method used on the serial port. It is always None.
- **Stop Bits -** The number of stop bits per character. The value is always 1.



Serial Port Configuration

Serial Port Login Timeout (minutes)	5 (0 to 160)
Baud Rate (bps)	115200
Character Size (bits)	8
Flow Control	Disabled
Stop Bits	1
Parity	None

Figure 4-2-8 Serial Port Configuration

4.2.3.8 User Accounts

By default, two user accounts exist:

- **admin**, with 'Read/Write' privileges
- **guest**, with 'Read Only' privileges

By default, both of these accounts have blank passwords. The names are not case sensitive.

If you logon with a user account with 'Read/Write' privileges (i.e. as admin) you can use the User Accounts screen to assign passwords and set security parameters for the default accounts, and to add and delete accounts (other than admin) up to the maximum of six. Only a user with 'Read/Write' privileges may alter data on this screen, and only one account may be created with 'Read/Write' privileges.

Selection Criteria

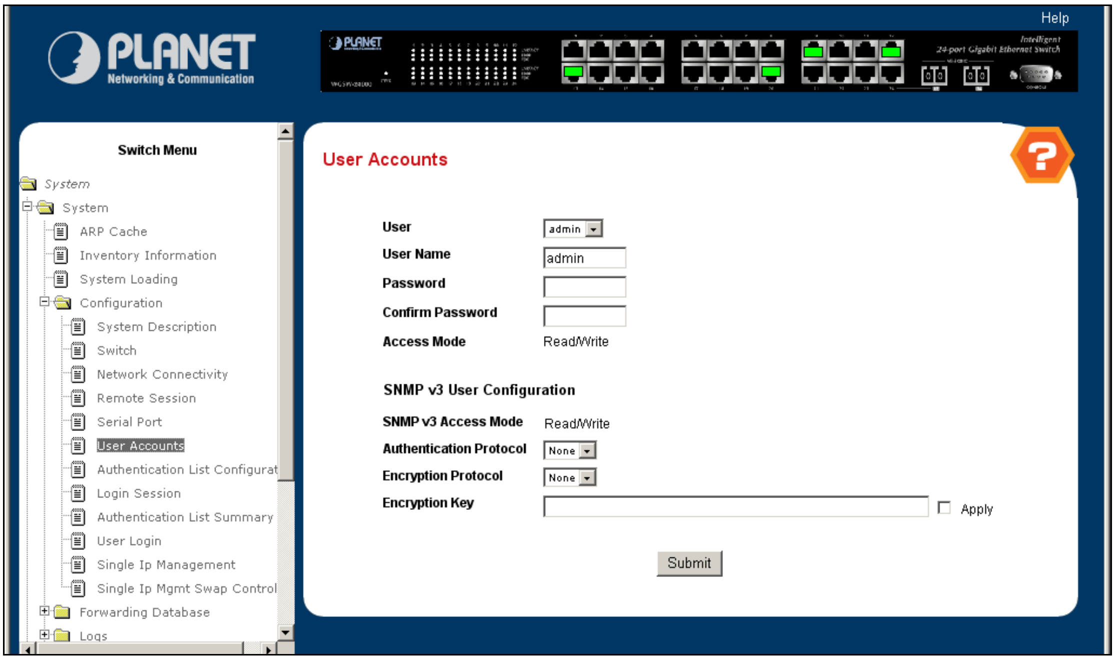
- **User Name Selector -** You can use this screen to reconfigure an existing account, or to create a new one. Use this pull-down menu to select one of the existing accounts, or select 'Create' to add a new one, provided the maximum of five 'Read Only' accounts has not been reached.

Configurable Data

- **User Name -** Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to eight characters in length and are not case sensitive. Valid characters include all the alphanumeric characters as well as the dash ('-') and underscore ('_') characters.
- **Password -** Enter the optional new or changed password for the account. It will not display as it is typed, only asterisks(*) will show. Passwords are up to eight alpha numeric characters in length, and are case sensitive.
- **Confirm Password -** Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*)
- **Authentication Protocol -** Specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are None, MD5 or SHA. If you select None, the user will be unable to access the SNMP data from an SNMP browser. If you select MD5 or SHA, the user login password will be used as the SNMPv3 authentication password, and you must therefore specify a password, and it must be eight characters long.
- **Encryption Protocol -** Specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are None or DES. If you select the DES Protocol you must enter a key in the Encryption Key field. If None is specified for the Protocol, the Encryption Key is ignored.
- **Encryption Key -** If you selected DES in the Encryption Protocol field enter the SNMPv3 Encryption Key here. Otherwise this field is ignored. Valid keys are 0 to 15 characters long. The Apply checkbox must be checked in order to change the Encryption Protocol and Encryption Key.

Non-Configurable Data

- **Access Mode -** Indicates the user's access mode. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.
- **SNMP v3 Access Mode -** Indicates the SNMPv3 access privileges for the user account. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.



User Accounts

User admin

User Name admin

Password

Confirm Password

Access Mode Read/Write

SNMP v3 User Configuration

SNMP v3 Access Mode Read/Write

Authentication Protocol None

Encryption Protocol None

Encryption Key □ Apply

Submit

Figure 4-2-9 User Accounts

4.2.3.9 Authentication List Configuration

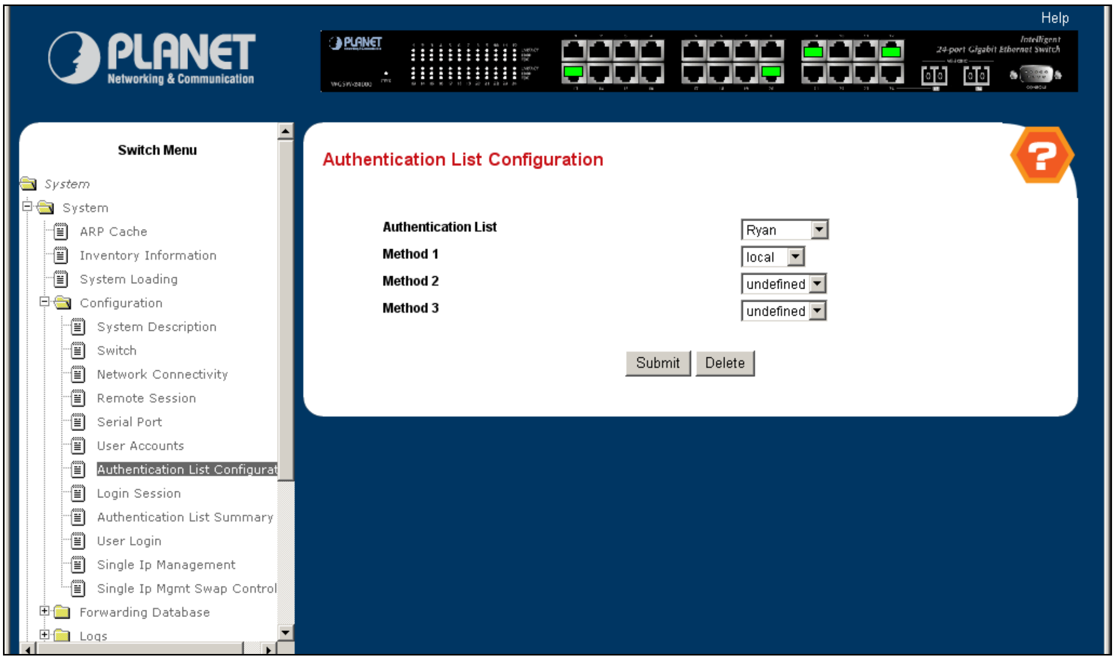
Use this screen to configure login lists. A login list specifies the authentication method(s) you want used to validate switch or port access for the users associated with the list. The pre-configured users, admin and guest, are assigned to a pre-configured list named **defaultList**, which you may not delete. All newly created users are also assigned to the **defaultList** until you specifically assign them to a different list

Selection Criteria

- **Authentication List -** Select the authentication login list you want to configure. Select 'create' to define a new login list. When you create a new login list, 'local' is set as the initial authentication method.

Configurable Data

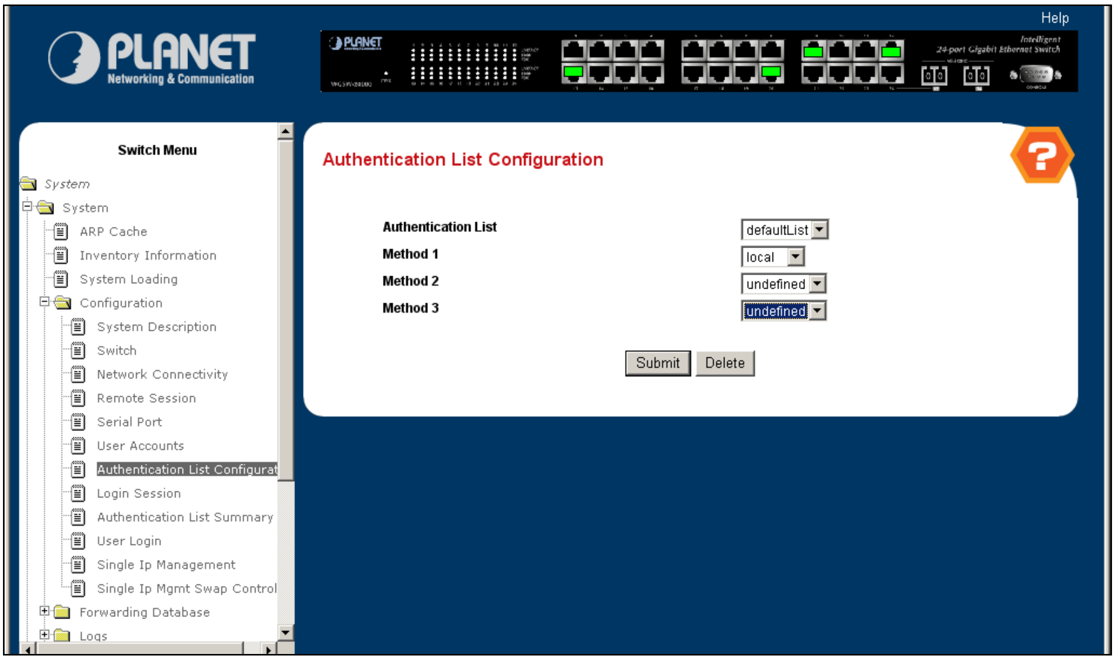
- **Authentication List Name -** If you are creating a new login list, enter the name you want to assign. It can be up to 15 alphanumeric characters long and is not case sensitive.
- **Method 1 -** Use the dropdown menu to select the method that should appear first in the selected authentication login list. If you select a method that does not time out as the first method, such as 'local' no other method will be tried, even if you have specified more than one method. Note that this parameter will not appear when you first create a new login list. The options are:
  - **Local-** the user's locally stored ID and password will be used for authentication
  - **Radius-** the user's ID and password will be authenticated using the RADIUS server instead of locally
  - **Reject-** the user is never authenticated
  - **Undefined-** the authentication method is unspecified (this may not be assigned as the first method)
- **Method 2 -** Use the dropdown menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
- **Method 3 -** Use the dropdown menu to select the method, if any, that should appear third in the selected authentication login list. Note that this parameter will not appear when you first create a new login list.



Authentication List Configuration

Authentication List	Ryan
Method 1	local
Method 2	undefined
Method 3	undefined

Figure 4-2-10 Authentication List Configuration – Create User



Authentication List Configuration

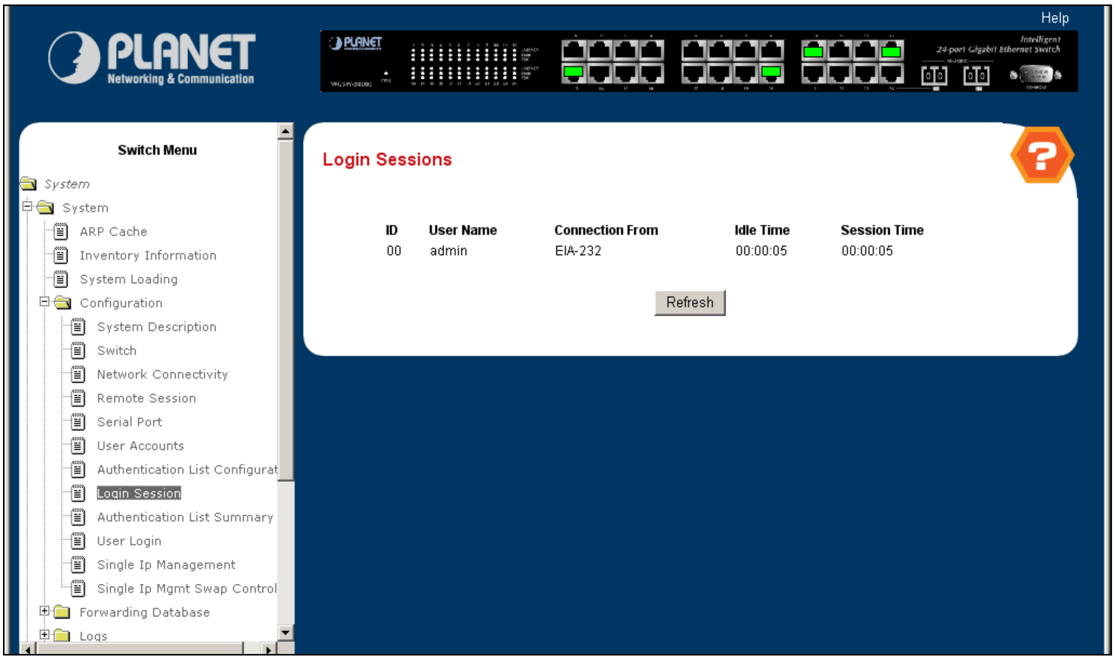
Authentication List	defaultList
Method 1	local
Method 2	undefined
Method 3	undefined

Figure 4-2-11 Authentication List Configuration – DefaultList

4.2.3.10 Login Session

This page shows the information of login session, including:

- **ID -** Identifies the ID of this row.
- **User Name -** Shows the user name of user made the session.
- **Connection From -** Shows the user is connected from which machine.
- **Idle Time -** Shows the idle session time.
- **Session Time -** Shows the total session time.



Login Sessions

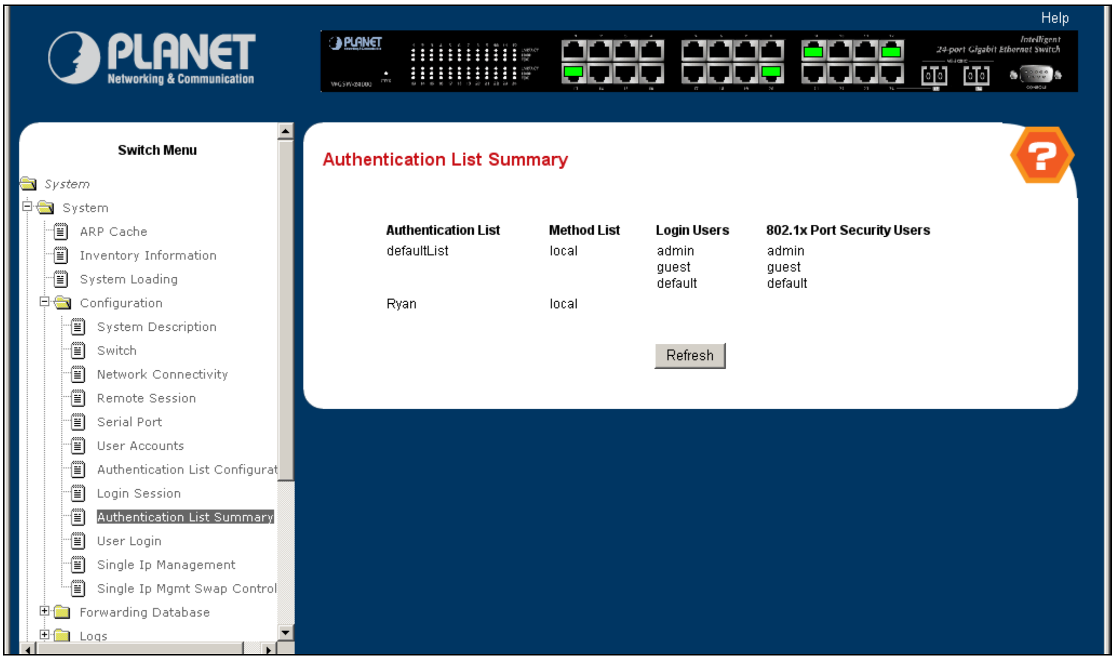
ID	User Name	Connection From	Idle Time	Session Time
00	admin	EIA-232	00:00:05	00:00:05

Figure 4-2-12 Login Sessions

4.2.3.11 Authentication List Summary

This page lists the authenticate user, the information fields include:

- **Authentication List -** Identifies the authentication login list summarized in this row.
- **Method List -** The ordered list of methods configured for this login list.
- **Login Users -** The users you assigned to this login list on the User Login Configuration screen. This list is used to authenticate the users for system login access.
- **802.1x Port Security Users** - The users you assigned to this login list on the Port Access Control User Login Configuration screen - This list is used to authenticate the users for port access, using the IEEE 802.1x protocol.



Authentication List Summary

Authentication List	Method List	Login Users	802.1x Port Security Users
defaultList	local	admin guest default	admin guest default
Ryan	local		

Figure 4-2-13 Authentication List Summary

4.2.3.12 User Login

Each configured user is assigned to a login list that specifies how the user should be authenticated when attempting to access the switch or a port on the switch. After creating a new user account on the User Account screen, you should assign that user to a login list for the switch using this screen and, if necessary, to a login list for the ports using the Port Access Control User Login Configuration screen. If you need to create a new login list for the user, you would do so on the Login Configuration screen. The pre-configured users, admin and guest, are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list.

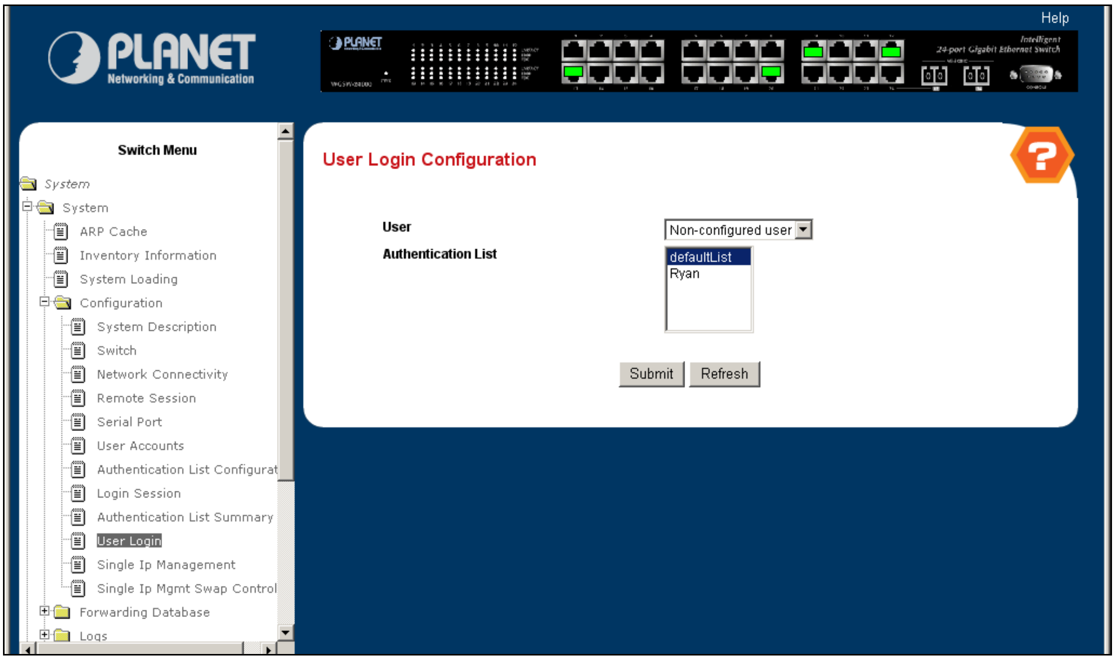
A user that does not have an account configured on the switch is termed the **'default'** or **'non-configured'** user. If you assign the 'non-configured user' to a login list that specifies authentication via the RADIUS server, you will not need to create an account for all users on each switch. However, by default the **'non-configured user'** is assigned to **'defaultList'**, which by default uses local authentication.

Selection Criteria

- **User -** Select the user you want to assign to a login list. Note that you must always associate the admin user with the default list. This forces the admin user to always be authenticated locally to prevent full lockout from switch configuration. If you assign a user to a login list that requires remote authentication, the user's access to the switch from all CLI, web, and telnet sessions will be blocked until the authentication is complete. Refer to the discussion of maximum delay in the RADIUS configuration help.

Configurable Data

- **Authentication List -** Select the authentication login list you want to assign to the user for system login.



User Login Configuration

User: Non-configured user

Authentication List: defaultList, Ryan

Submit Refresh

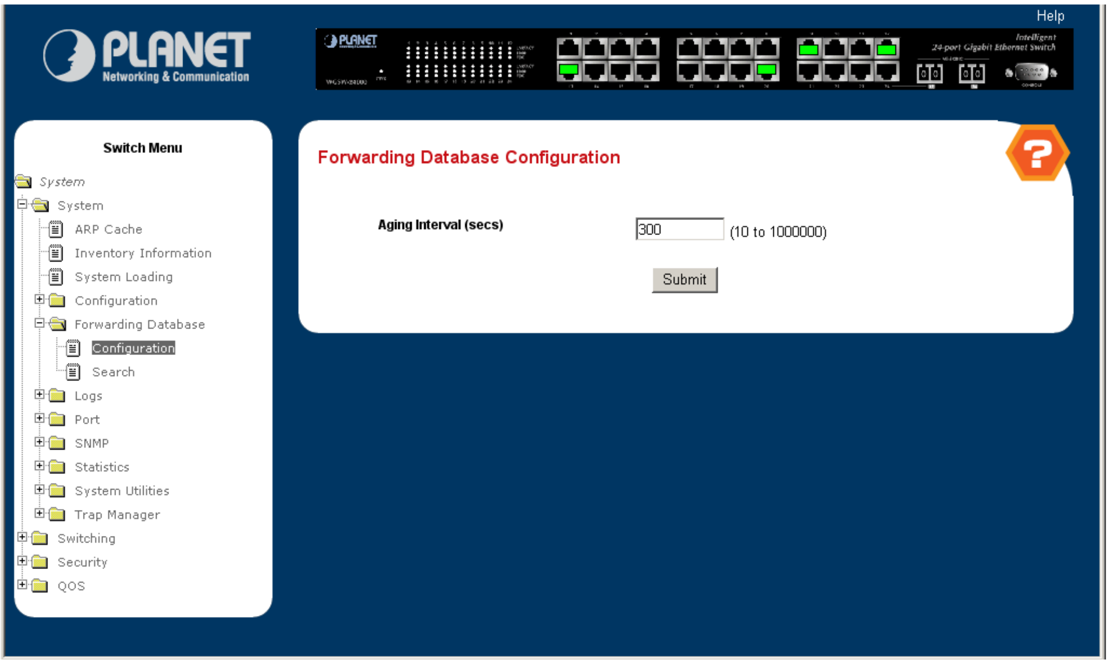
Figure 4-2-14 User Login Configuration

4.2.4 Forwarding Database

4.2.4.1 Configuration

Use this panel to set the Address Ageing Timeout for the forwarding database.

- **Address Ageing Timeout (seconds) -** The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time. You specify that time by entering a value for the Address Ageing Timeout. You may enter any number of seconds between 10 and 1000000. IEEE 802.1D recommends a default of 300 seconds, which is the factory default.



Forwarding Database Configuration

Aging Interval (secs) 300 (10 to 1000000)

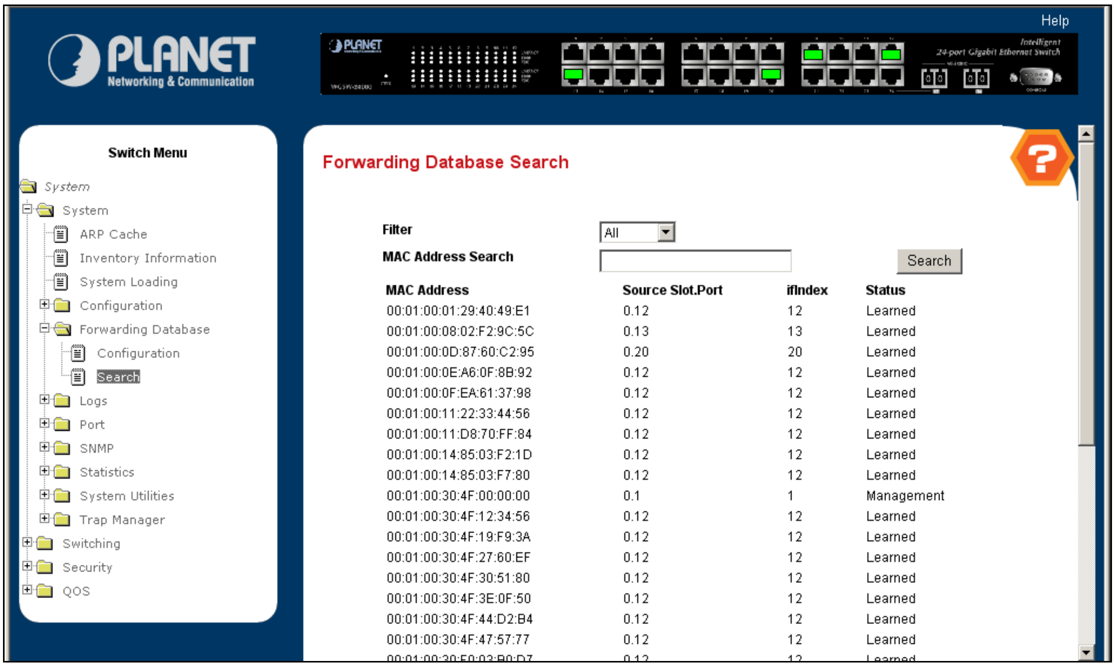
Figure 4-2-15 Forwarding Database

4.2.4.2 Search

Use this panel to display information about entries in the forwarding database. These entries are used by the transparent bridging function to determine how to forward a received frame.

Configurable Data

- **Filter -** Specify the entries you want displayed.
  - **Learned:** If you choose "learned" only MAC addresses that have been learned will be displayed.
  - **All:** If you choose "all" the whole table will be displayed.
- **MAC Address Search -** You may also search for an individual MAC address. Enter the two byte hexadecimal VLAN ID followed by the six byte hexadecimal MAC address in two-digit groups separated by colons, for example 01:23:45:67:89:AB:CD:EF where 01:23 is the VLAN ID and 45:67:89:AB:CD:EF is the MAC address. Then click on the search button. If the address exists, that entry will be displayed as the first entry followed by the remaining (greater) MAC addresses. An exact match is required.



Forwarding Database Search

Filter: All

MAC Address Search:

Search

MAC Address	Source Slot.Port	ifIndex	Status
00:01:00:01:29:40:49:E1	0.12	12	Learned
00:01:00:08:02:F2:9C:5C	0.13	13	Learned
00:01:00:0D:87:60:C2:95	0.20	20	Learned
00:01:00:0E:A6:0F:8B:92	0.12	12	Learned
00:01:00:0F:EA:61:37:98	0.12	12	Learned
00:01:00:11:22:33:44:56	0.12	12	Learned
00:01:00:11:D8:70:FF:84	0.12	12	Learned
00:01:00:14:85:03:F2:1D	0.12	12	Learned
00:01:00:14:85:03:F7:80	0.12	12	Learned
00:01:00:30:4F:00:00:00	0.1	1	Management
00:01:00:30:4F:12:34:56	0.12	12	Learned
00:01:00:30:4F:19:F9:3A	0.12	12	Learned
00:01:00:30:4F:27:60:EF	0.12	12	Learned
00:01:00:30:4F:30:51:80	0.12	12	Learned
00:01:00:30:4F:3E:0F:50	0.12	12	Learned
00:01:00:30:4F:44:D2:B4	0.12	12	Learned
00:01:00:30:4F:47:57:77	0.12	12	Learned
00:01:00:30:F0:03:B0:D7	0.12	12	Learned

Figure 4-2-16 Forwarding Database Search

4.2.5 Log

- **Buffered Log Configuration**
- **Buffered Log**
- **Command Logger Configuration**
- **Console Log Configuration**
- **Event Log**
- **Hosts Configuration**
- **Persistent Log Configuration**
- **Persistent Log**
- **Syslog Configuration**

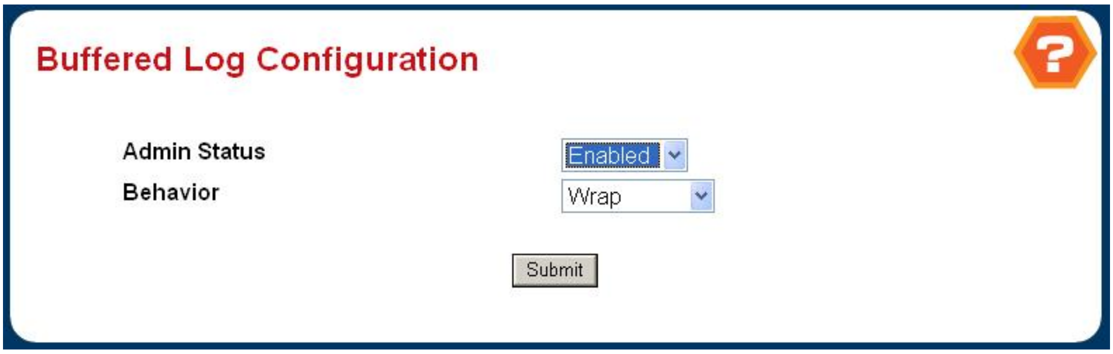
4.2.5.1 Buffered Log Configuration

This log stores messages in memory based upon the settings for message component and severity. On stackable systems, this log exists only on the top of stack platform. Other platforms in the stack forward their messages to the top of stack log.

Configurable Data

- **Admin Status** - A log that is "Disabled" shall not log messages. A log that is "Enabled" shall log messages. Enable or Disable logging by selecting the corresponding line on the pulldown entry field.

- **Behavior** Indicates the behavior of the log when it is full. It can either wrap around or stop when the log space is filled.



Buffered Log Configuration

Admin Status: Enabled

Behavior: Wrap

Figure 4-2-17 Buffered Log Configuration

4.2.5.2 Buffered Log

This help message applies to the format of all logged messages which are displayed for the buffered log, persistent log or console log.

Format of the messages

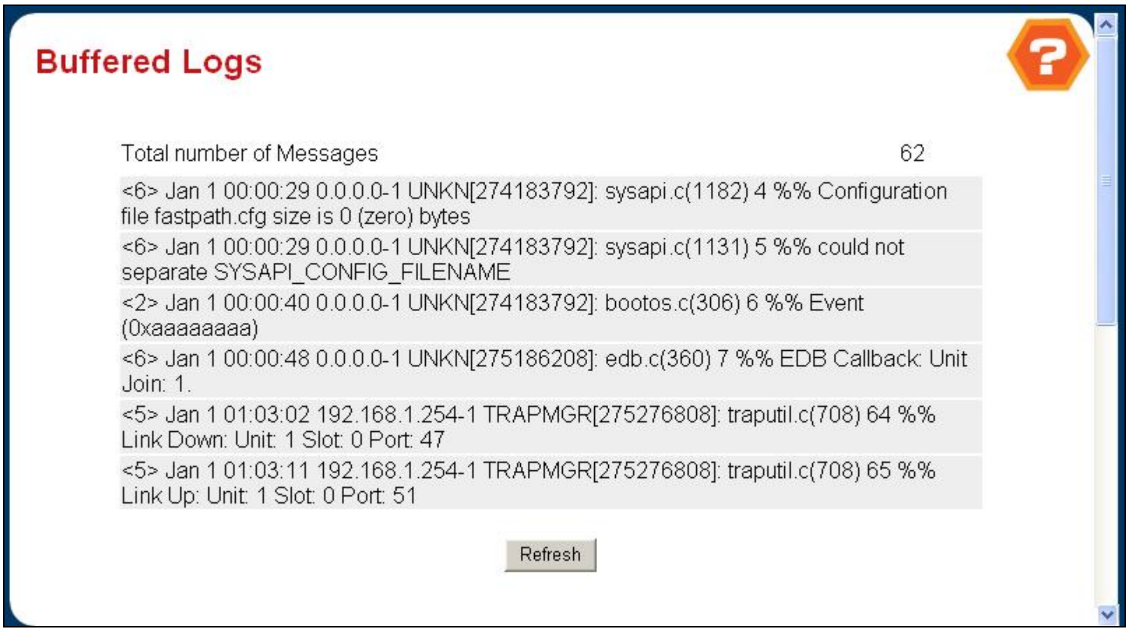
Messgges logged to a collector or relay via syslog have an identical format of either type

- **<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry**

  -The above example indicates a message with severity 7(15 mod 8) (debug) on a system that is not stack and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged.

Command Buttons

- **Refresh** - Refresh the page with the latest log entries.



Buffered Logs

Total number of Messages	62

```
<6> Jan 1 00:00:29 0.0.0.0-1 UNKN[274183792]: sysapi.c(1182) 4 %% Configuration file fastpath.cfg size is 0 (zero) bytes
<6> Jan 1 00:00:29 0.0.0.0-1 UNKN[274183792]: sysapi.c(1131) 5 %% could not separate SYSAPI_CONFIG_FILENAME
<2> Jan 1 00:00:40 0.0.0.0-1 UNKN[274183792]: bootos.c(306) 6 %% Event (0xaaaaaaaa)
<6> Jan 1 00:00:48 0.0.0.0-1 UNKN[275186208]: edb.c(360) 7 %% EDB Callback: Unit Join: 1.
<5> Jan 1 01:03:02 192.168.1.254-1 TRAPMGR[275276808]: traputil.c(708) 64 %% Link Down: Unit: 1 Slot: 0 Port: 47
<5> Jan 1 01:03:11 192.168.1.254-1 TRAPMGR[275276808]: traputil.c(708) 65 %% Link Up: Unit: 1 Slot: 0 Port: 51
```

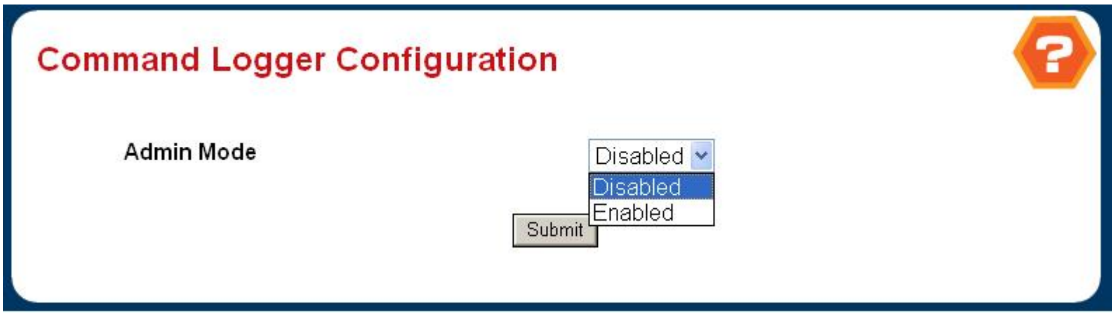
Figure 4-2-18 Buffered Logs

44.2.5.3 Command Logger Configuration

This page includes the following fields:

Configurable Data

- **Admin Mode** - Enable/Disable the operation of the CLI Command logging by selecting the corresponding pulldown field and clicking Submit.



Command Logger Configuration

Admin Mode: Disabled

Figure 4-2-19 Command Logger Configuration

4.2.5.4 Console Log Configuration

This allows logging to any serial device attached to the host.

Configurable Data

- **Admin Status** -A log that is "Disabled" shall not log messages. A log that is "Enabled" shall log messages. Enable or Disable logging by selecting the corresponding line on the pulldown entry field.
- **Severity Filter** - A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pulldown entry field. These severity levels have been enumerated below:

  -**Emergency (0)**: system is unusable

  -**Alert (1)**: action must be taken immediately

  -**Critical (2)**: critical conditions

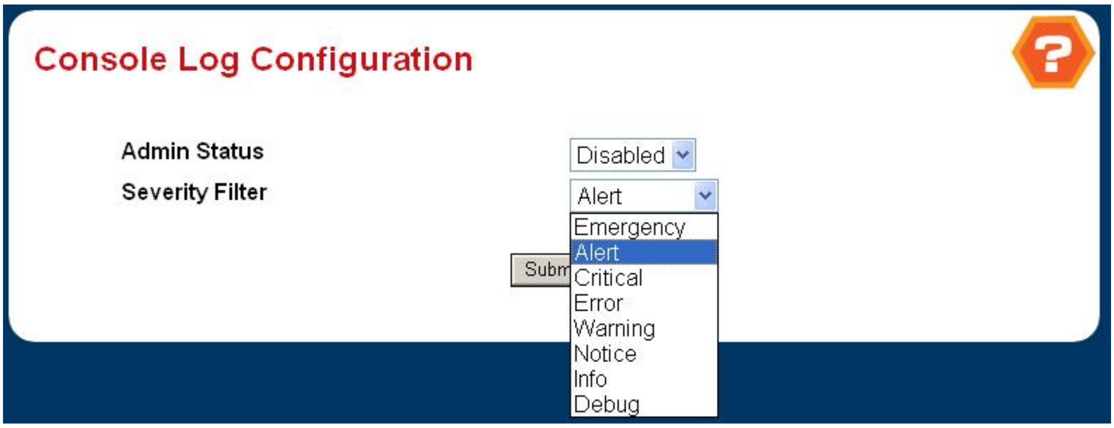
  -**Error (3)**: error conditions

  -**Warning (4)**: warning conditions

  -**Notice(5)**: normal but significant conditions

  -**Informational(6)**: informational messages

  -**Debug(7)**: debug-level messages



Console Log Configuration

Admin Status: Disabled

Severity Filter: Alert

Figure 4-2-20 Console Log Configuration

4.2.5.5 Event Log

This allows logging to any serial device attached to the host.

Configurable Data

- **Admin Status** -A log that is "Disabled" shall not log messages. A log that is "Enabled" shall log messages. Enable or Disable logging by selecting the corresponding line on the pulldown entry field.
- **Severity Filter** - A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pulldown entry field. These severity levels have been enumerated below:

  -**Emergency (0)**: system is unusable

  -**Alert (1)**: action must be taken immediately

  -**Critical (2)**: critical conditions

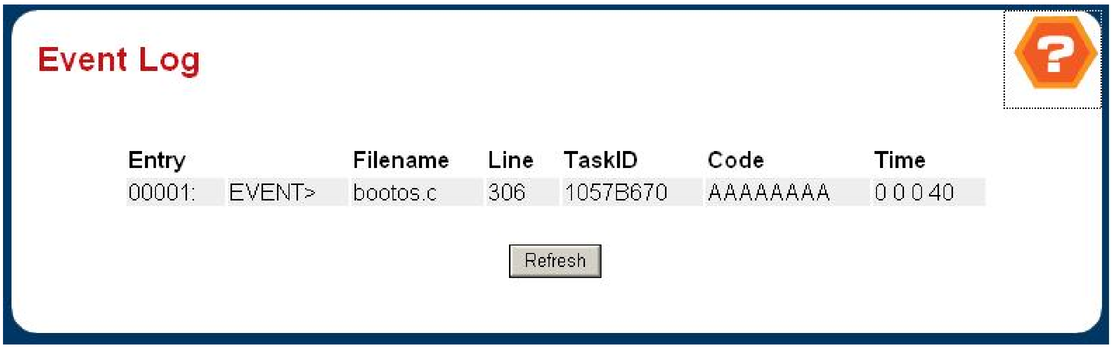
  -**Error (3)**: error conditions

  -**Warning (4)**: warning conditions

  -**Notice(5)**: normal but significant conditions

  -**Informational(6)**: informational messages

  -**Debug(7)**: debug-level messages

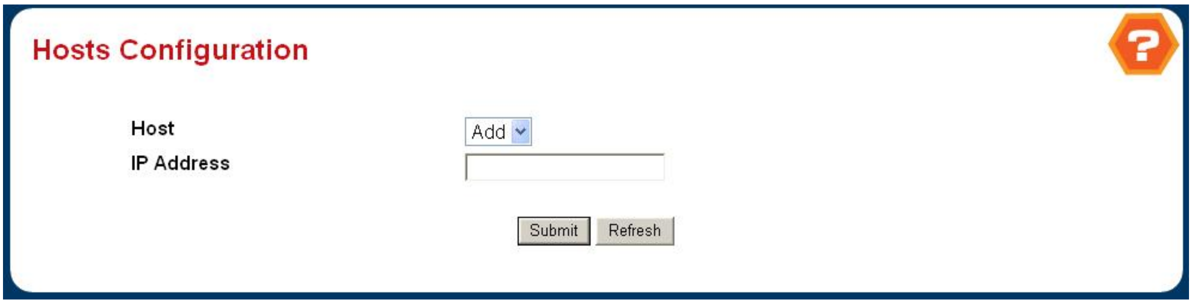


Event Log

Entry		Filename	Line	TaskID	Code	Time
00001:	EVENT>	bootos.c	306	1057B670	AAAAAAAA	0 0 0 40

Figure 4-2-21 Event Log

4.2.5.6 Hosts Configuration



Hosts Configuration

Host	Add ▾
IP Address	

Figure 4-2-22 Host Configuration

Configurable Data

- **Host** - This is a list of the hosts that have been configured for syslog. Select a host for changing the configuration or choose to add a new hosts from the drop down list.
- **IP Address** - This is the ip address of the host configured for syslog.

- **Port** -This is the port on the host to which syslog messages are sent. The default port is 514. The default port is 514. Specify the port in the text field.
- **Severity Filter** -A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pulldown entry field. These severity levels have been enumerated below:

  -Emergency (0): system is unusable

  -Alert (1): action must be taken immediately

  -Critical (2): critical conditions

  -Error (3): error conditions

  -Warning (4): warning conditions

  -Notice(5): normal but significant conditions

  -Informational(6): informational messages

  -Debug(7): debug-level messages

Non Configurable Data

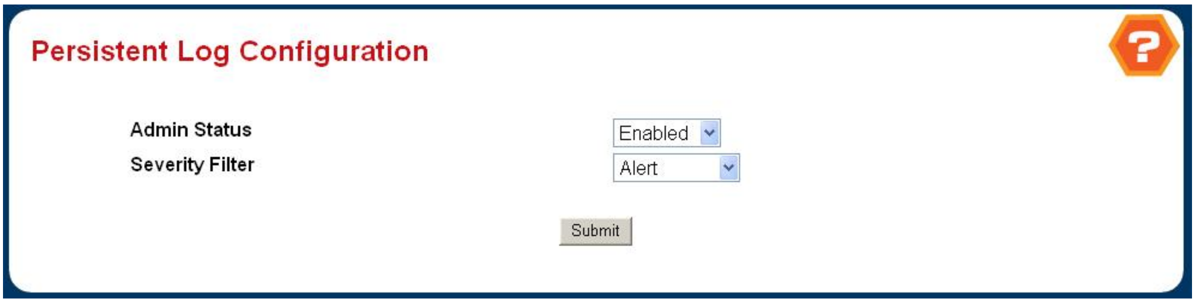
- **Status** -This specifies wether the host has been configured to be actively logging or not.

Command Buttons

- **Submit** - Update the switch with the values you entered.
- **Refresh** - Refetch the database and display it again starting with the first entry in the table.
- **Delete** - Delete a configured host.

4.2.5.7 Persistent Log Configuration

A persistent log is a log that is stored in persistent storage. Persistent storage survives across platform reboots. The first log type is the system startup log. The system startup log stores the first N messages received after system reboot. The second log type is the system operation log. The system operation log stores the last N messages received during system operation.



Persistent Log Configuration

Admin Status: Enabled

Severity Filter: Alert

Figure 4-2-23 Persistent Log Configuration

Configurable Data

- **Admin Status** - A log that is "Disabled" shall not log messages. A log that is "Enabled" shall log messages. Enable or Disable logging by selecting the corresponding line on the pulldown entry field.

- **Severity Filter** - A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pulldown entry field. These severity levels have been enumerated below:

  -**Emergency (0)**: system is unusable

  -**Alert (1)**: action must be taken immediately

  -**Critical (2)**: critical conditions

  -**Error (3)**: error conditions

  -**Warning (4)**: warning conditions

  -**Notice(5)**: normal but significant conditions

  -**Informational(6)**: informational messages

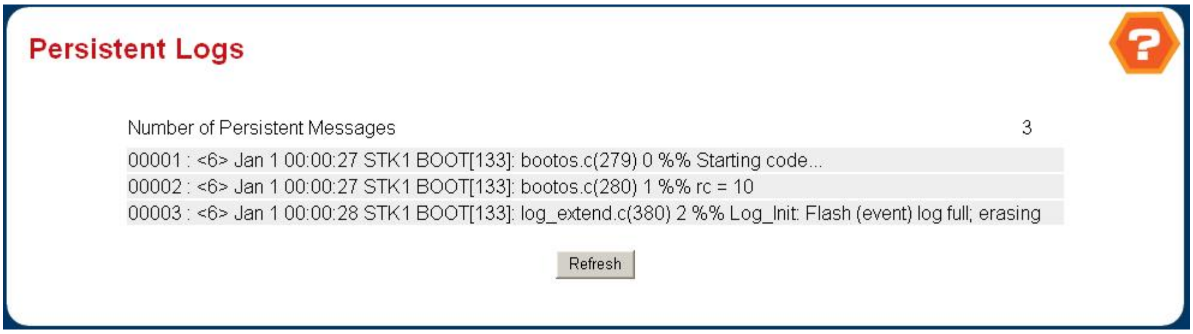
  -**Debug(7)**: debug-level messages

Command Buttons

- **Submit** - Update the switch with the values you entered.

4.2.5.8 Persistent Log

This help message applies to the format of all logged messages which are displayed for the buffered log, persistent log or console log.



Persistent Logs

Number of Persistent Messages 3

```
00001 : <6> Jan 1 00:00:27 STK1 BOOT[133]: bootos.c(279) 0 %% Starting code...
00002 : <6> Jan 1 00:00:27 STK1 BOOT[133]: bootos.c(280) 1 %% rc = 10
00003 : <6> Jan 1 00:00:28 STK1 BOOT[133]: log_extend.c(380) 2 %% Log_Init: Flash (event) log full; erasing
```

Figure 4-2-24 Persistent Logs

Format of the messages

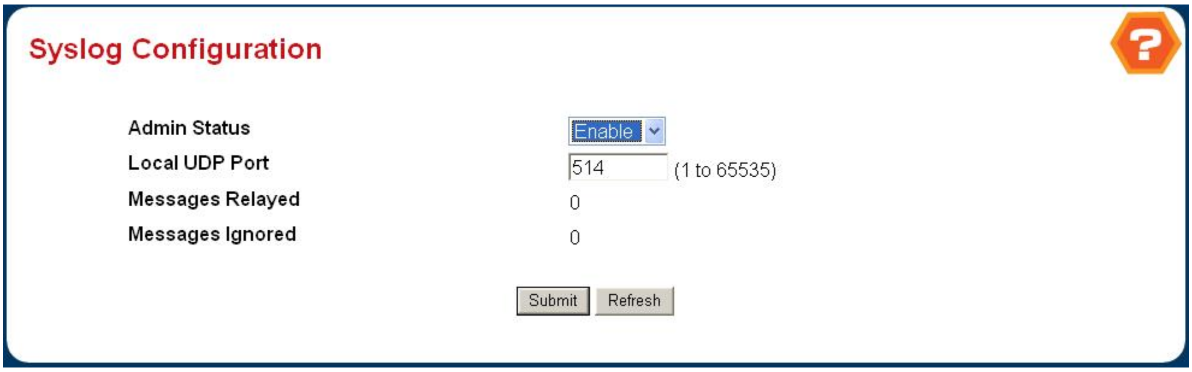
- **<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry**

  -The above example indicates a user-level message (1) with severity 7 (debug) on a system that is not stack and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog have an identical format to the above message.

Command Buttons

- **Refresh** - Refresh the page with the latest log entries.

4.2.5.9 Syslog Configuration



Syslog Configuration

Admin Status: Enable

Local UDP Port: 514 (1 to 65535)

Messages Relayed: 0

Messages Ignored: 0

Figure 4-2-25 Syslog Configuration

Configurable Data

- **Admin Status** -For Enabling and Disabling logging to configured syslog hosts. Setting this to disable stops logging to all syslog hosts. Disable means no messages will be sent to any collector/relay. Enable means messages will be sent to configured collector/relays using the values configured for each collector/relay. Enable/Disable the operation of the syslog function by selecting the corresponding line on the pulldown entry field.
- **Local UDP Port** This is the port on the local host from which syslog messages are sent. The default port is XXX. The default port is 514. Specify the local port in the text field.

Non-Configurable Data

- **Messages Relayed** - The count of syslog messages relayed.
- **Messages Ignored** - The count of syslog messages ignored.

Command Buttons

- **Submit** - Update the switch with the values you entered.

Refresh - Refetch the database and display it again starting with the first entry in the table.

4.2.6 Port

4.2.7.1 Configuration

Use this page to configure the parameters of the distinct port.

Selection Criteria

- **Slot.Port -** Selects the interface for which data is to be displayed or configured.

Configurable Data

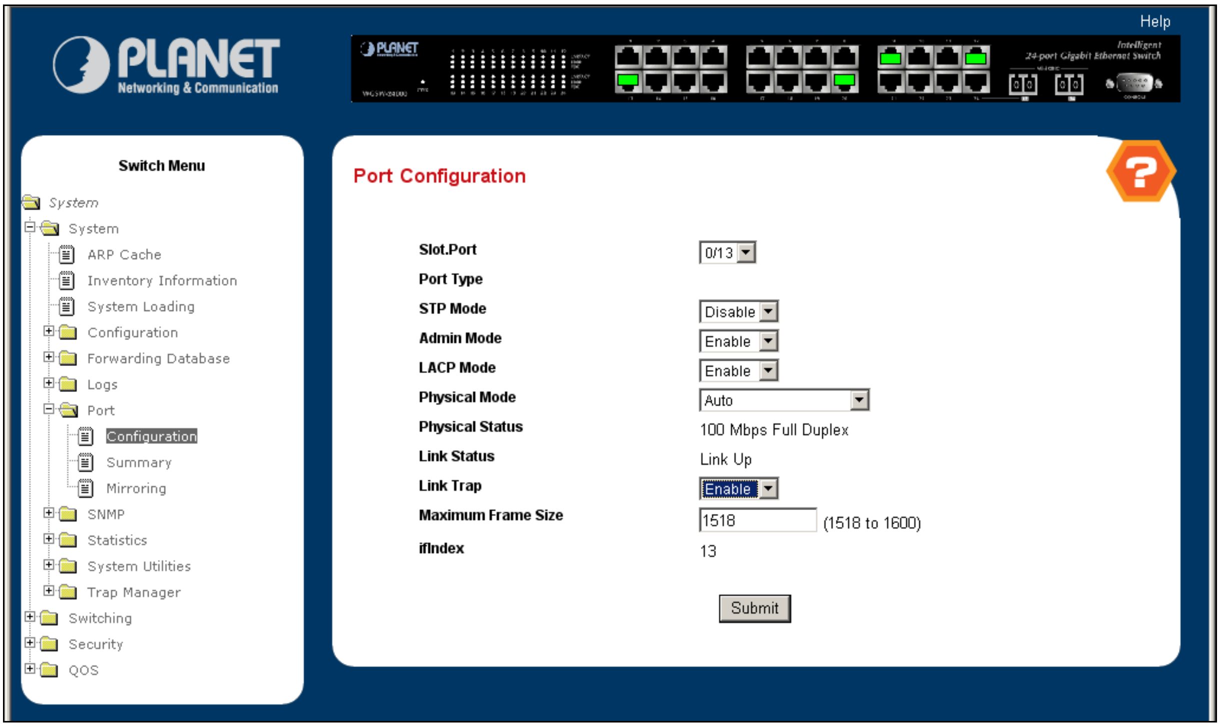
- **STP Mode -** The Select the Spanning Tree Protocol Administrative Mode for the port or LAG. The possible values are:
  - **Enable -** select this to enable the Spanning Tree Protocol for this port.
  - **Disable -** select this to disable the Spanning Tree Protocol for this port.
- **Admin Mode -** Use the pull-down menu to select the Port control administration state. You must select enable if

you want the port to participate in the network. The factory default is enabled.

- **LACP Mode -** Selects the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
- **Physical Mode -** Use the pull-down menu to select the port's speed and duplex mode. If you select auto the duplex mode and speed will be set by the auto-negotiation process. Note that the port's maximum capability (full duplex and 100 Mbps) will be advertised. Otherwise, your selection will determine the port's duplex mode and transmission rate. The factory default is auto. The selection when applied against the **"All"** option in Slot.Port is applied to all applicable interfaces only.
- **Link Trap -** This object determines whether or not to send a trap when link status changes. The factory default is enabled.
- **Maximum Frame Size** - The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. (1518 to 1600). The default maximum frame size is 1518.

Non-Configurable Data

- **Port Type -** For normal ports this field will be blank. Otherwise the possible values are:
  - **Mon -** the port is a monitoring port. Look at the Port Monitoring screens for more information.
  - **LAG -** the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.
- **Physical Status -** Indicates the port speed and duplex mode.
- **Link Status -** Indicates whether the Link is up or down.
- **ifIndex -** The ifIndex of the interface table entry associated with this port.



Port Configuration

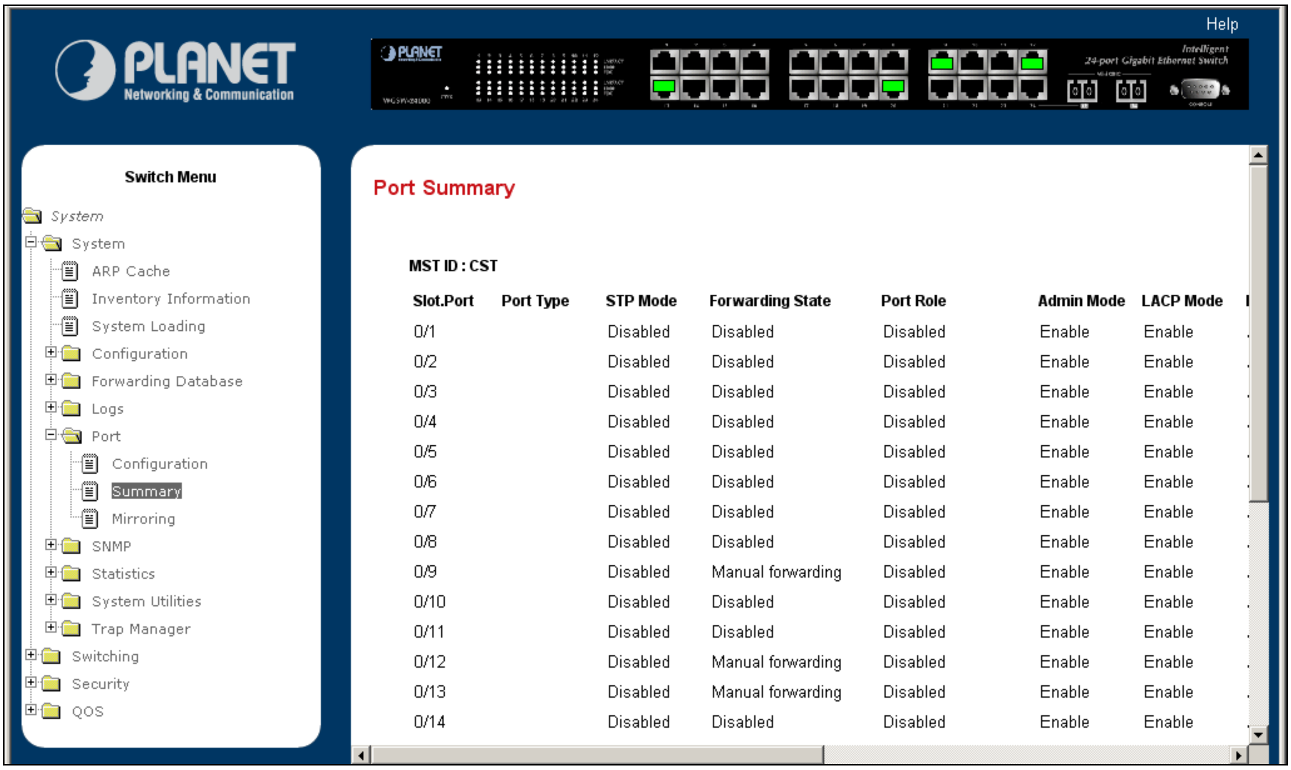
Slot.Port	0/13
Port Type	
STP Mode	Disable
Admin Mode	Enable
LACP Mode	Enable
Physical Mode	Auto
Physical Status	100 Mbps Full Duplex
Link Status	Link Up
Link Trap	Enable
Maximum Frame Size	1518 (1518 to 1600)
ifIndex	13

Submit

Figure 4-2-26 Port Configuration

4.2.6.2 Summary

This screen displays the status for all ports in the box.



Port Summary

MST ID : CST

Slot.Port	Port Type	STP Mode	Forwarding State	Port Role	Admin Mode	LACP Mode
0/1		Disabled	Disabled	Disabled	Enable	Enable
0/2		Disabled	Disabled	Disabled	Enable	Enable
0/3		Disabled	Disabled	Disabled	Enable	Enable
0/4		Disabled	Disabled	Disabled	Enable	Enable
0/5		Disabled	Disabled	Disabled	Enable	Enable
0/6		Disabled	Disabled	Disabled	Enable	Enable
0/7		Disabled	Disabled	Disabled	Enable	Enable
0/8		Disabled	Disabled	Disabled	Enable	Enable
0/9		Disabled	Manual forwarding	Disabled	Enable	Enable
0/10		Disabled	Disabled	Disabled	Enable	Enable
0/11		Disabled	Disabled	Disabled	Enable	Enable
0/12		Disabled	Manual forwarding	Disabled	Enable	Enable
0/13		Disabled	Manual forwarding	Disabled	Enable	Enable
0/14		Disabled	Disabled	Disabled	Enable	Enable

Figure 4-2-27 Port Summary

Selection Criteria

- **MST ID -** Select the Multiple Spanning Tree instance ID from the list of all currently configured MST ID's to determine the values displayed for the Spanning Tree parameters. Changing the selected MST ID will generate a screen refresh. If Spanning Tree is disabled this will be a static value, CST, instead of a selector.

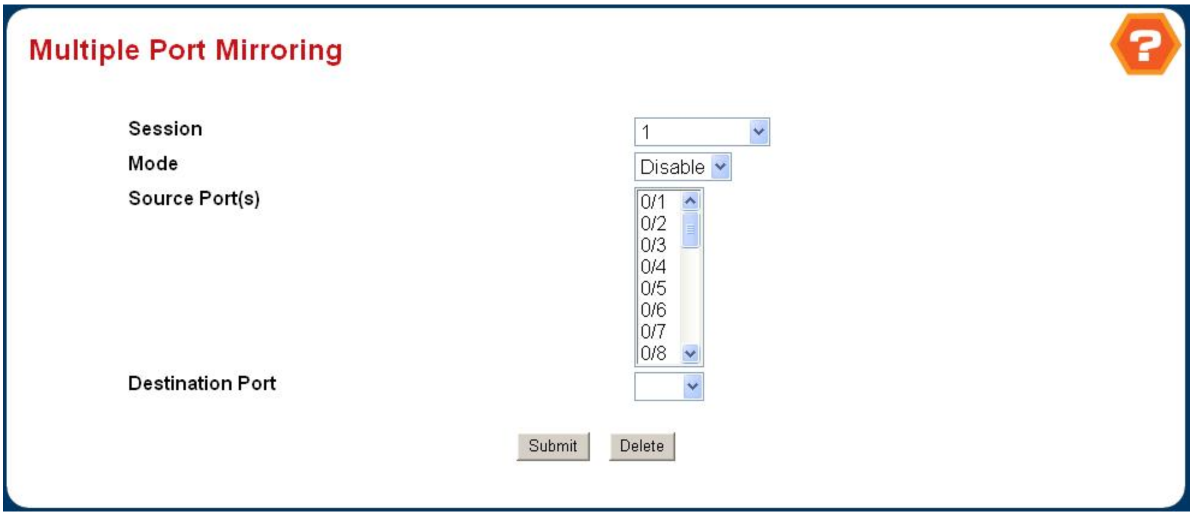
Non-Configurable Port Status Data

- **Slot.Port -** Identifies the port
- **Port Type -** For normal ports this field will be blank. Otherwise the possible values are:
  - **Mon -** this port is a monitoring port. Look at the Port Monitoring screens for more information.
  - **LAG -** the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.
- **STP Mode -** The Spanning Tree Protocol Administrative Mode associated with the port or LAG. The possible values are:
  - **Enable -** spanning tree is enabled for this port.
  - **Disable -** spanning tree is disabled for this port.
- **Forwarding State -** The port's current state Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it will place that port into the broken state. The other five states are defined in IEEE 802.1D:
  - **Disabled**
  - **Blocking**
  - **Listening**
  - **Learning**
  - **Forwarding**
  - **Broken**

- **Port Role -** Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
- **Admin Mode -** The Port control administration state. The port must be enabled in order for it to be allowed into the network. The factory default is enabled.
- **LACP Mode -** Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation.
- **Physical Mode -** Indicates the port speed and duplex mode. In auto-negotiation mode the duplex mode and speed are set from the auto-negotiation process.
- **Physical Status -** Indicates the port speed and duplex mode.
- **Link Status -** Indicates whether the Link is up or down.
- **Link Trap -** Indicates whether or not the port will send a trap when link status changes.
- **ifIndex -** Indicates the ifIndex of the interface table entry associated with this port.

4.2.6.3 Port Mirroring

Use this page to configure the port mirror function.



Multiple Port Mirroring

Session: 1
Mode: Disable
Source Port(s): 0/1, 0/2, 0/3, 0/4, 0/5, 0/6, 0/7, 0/8
Destination Port:

Figure 4-2-29 Multiple Port Mirroring

Configurable Data

- **Session ID** - A session ID or "All Sessions" option may be selected. By default the First Session is selected.
- **Session Mode** - Specifies the Session Mode for a selected session ID. By default Session Mode is enabled.
- **Source Port(s)** - Specifies the configured port(s) as mirrored port(s). Traffic of the configured port(s) is sent to the probe port.
- **Destination Port** - Acts as a probe port and will recieve all the traffic from configured mirrored port(s). Default value is blank.

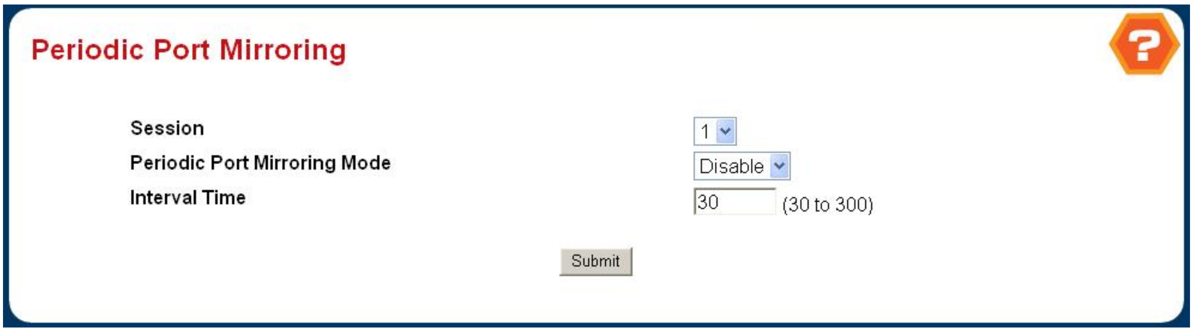
Command Buttons

- **Submit** - Send the updated screen to the switch and cause the changes to take effect on the switch.

- **Delete** - Remove the selected session configuration.

4.2.6.4 Periodic Port Mirroring

Use this page to configure the periodic port mirroring.



Periodic Port Mirroring

Session	1
Periodic Port Mirroring Mode	Disable
Interval Time	30 (30 to 300)

Figure 4-2-30 Periodic Port Mirroring

Selection Criteria

- **Session ID** - A session ID can be selected. By default the First Session is selected.

Configurable Data

- **Peroidic Port Mirroring Mode** - Specifies the Periodic Port Mirroring Mode for a selected session ID. By default Periodic Port Mirroring Mode is Disabled.
- **Interval Time** - Specifies the periodic port mirroring time interval in seconds.Default value is 30. Valid Range is (30 to 300).

Non-Configurable Data

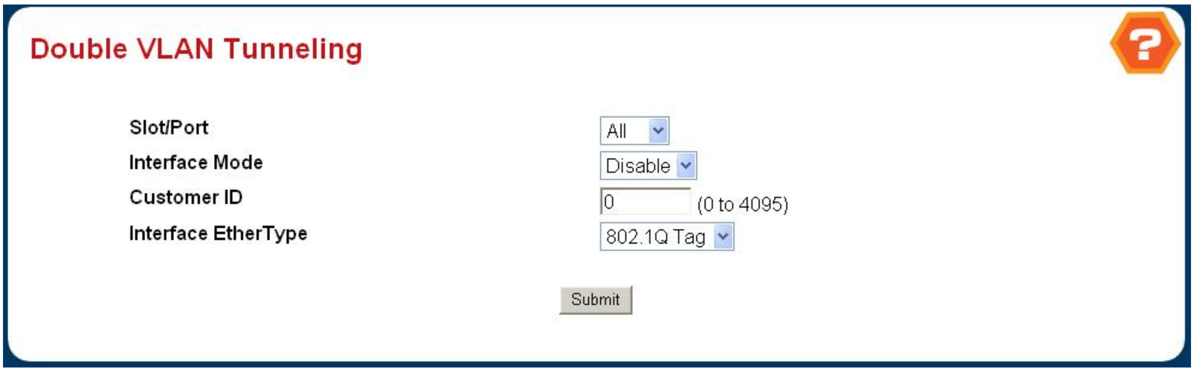
- **Source Port** - Specifies the mirrored port. This field is only visible when periodic port mirroring mode is enabled. Source port changes periodically as per specified Interval Time.

Command Buttons

- **Submit** - Send the updated screen to the switch and cause the changes to take effect on the switch.

4.2.6.5 Double VLAN Tunneling

Use this page to configure the Doubble VLAN Tunneling.



Double VLAN Tunneling

Slot/Port	All
Interface Mode	Disable
Customer ID	0 (0 to 4095)
Interface EtherType	802.1Q Tag

Figure 4-2-31 Double VLAN Tunneling

Selection Criteria

- **Slot/Port** - Select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to same values.

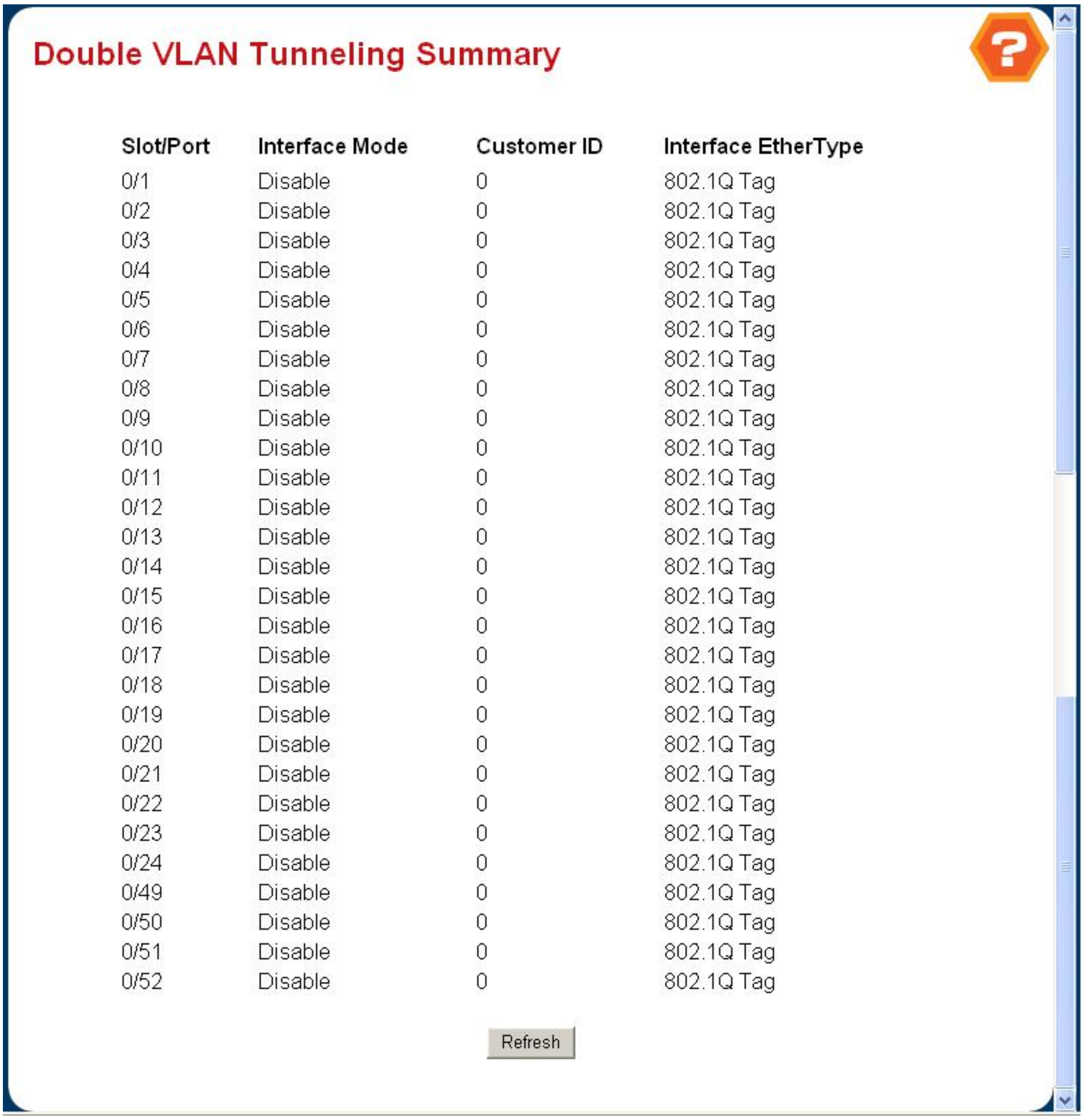
Configurable Data

- **Mode** - This specifies the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disabled.
- **Customer ID** - This is a 12 bit customer ID which will be used as the last 12 bits of the DVlan tag. The valid range for a customer Id is (0 to 4095). The default customer Id is 0 .
- **EtherType** - The two-byte hex EtherType to be used as the first 16 bits of the DVlan tag.
    - ***802.1Q Tag*** - Commonly used tag representing 0x8100
    - ***vMAN Tag*** - Commonly used tag representing 0x88A8
    - ***Custom Tag*** - Configure the EtherType in any range from (0 to 65535)

Command Buttons

- **Submit** - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.

4.2.6.7 Double VLAN Tunneling Summary



Double VLAN Tunneling Summary

Slot/Port	Interface Mode	Customer ID	Interface EtherType
0/1	Disable	0	802.1Q Tag
0/2	Disable	0	802.1Q Tag
0/3	Disable	0	802.1Q Tag
0/4	Disable	0	802.1Q Tag
0/5	Disable	0	802.1Q Tag
0/6	Disable	0	802.1Q Tag
0/7	Disable	0	802.1Q Tag
0/8	Disable	0	802.1Q Tag
0/9	Disable	0	802.1Q Tag
0/10	Disable	0	802.1Q Tag
0/11	Disable	0	802.1Q Tag
0/12	Disable	0	802.1Q Tag
0/13	Disable	0	802.1Q Tag
0/14	Disable	0	802.1Q Tag
0/15	Disable	0	802.1Q Tag
0/16	Disable	0	802.1Q Tag
0/17	Disable	0	802.1Q Tag
0/18	Disable	0	802.1Q Tag
0/19	Disable	0	802.1Q Tag
0/20	Disable	0	802.1Q Tag
0/21	Disable	0	802.1Q Tag
0/22	Disable	0	802.1Q Tag
0/23	Disable	0	802.1Q Tag
0/24	Disable	0	802.1Q Tag
0/49	Disable	0	802.1Q Tag
0/50	Disable	0	802.1Q Tag
0/51	Disable	0	802.1Q Tag
0/52	Disable	0	802.1Q Tag

Figure 4-2-32 Double VLAN Tunneling Summary

Non-Configurable Data

- **Slot/Port** - The physical interface for which data is being displayed.
- **Mode** - This specifies the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disabled.
- **Customer ID** - This is the 12 bit customer ID which will be used as the last 12 bits of the DVlan tag. The valid range for a customer Id is (0 to 4095). The default customer Id is 0 .
- **EtherType** - The two-byte hex EtherType to be used as the first 16 bits of the DVlan tag.
  - ***802.1Q Tag*** - Commonly used tag representing 0x8100
  - ***vMAN Tag*** - Commonly used tag representing 0x88A8
  - ***Custom Tag*** - Configure the EtherType in any range from (0 to 65535)

Command Buttons

Refresh - Refresh the data on the screen with the present state of the data in the switch.

4.2.7 SNMP

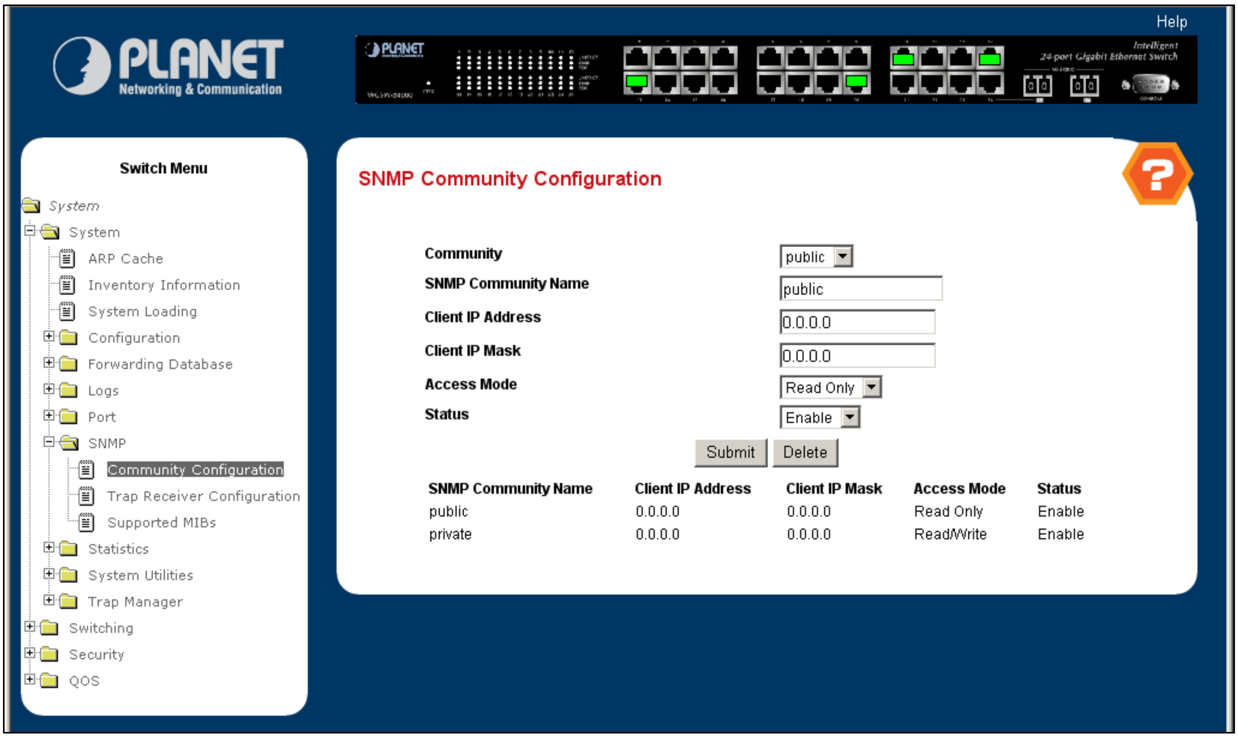
4.2.7.1 Community Configuration

By default, two SNMP Communities exist:

- **private**, with 'Read/Write' privileges and status set to enable
- **public**, with 'Read Only' privileges and status set to enable

These are well-known communities; you can use this menu to change the defaults or to add other communities. Only the communities that you define using this menu will have access to the switch using the SNMPv1 and SNMPv2c protocols. Only those communities with read-write level access will have access to this menu via SNMP.

You should use this menu when you are using the SNMPv1 and SNMPv2c protocol: if you want to use SNMP v3 you should use the User Accounts menu.



SNMP Community Configuration

Community	public
SNMP Community Name	public
Client IP Address	0.0.0.0
Client IP Mask	0.0.0.0
Access Mode	Read Only
Status	Enable

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
private	0.0.0.0	0.0.0.0	Read/Write	Enable

Figure 4-2-33 SNMP Community

Configurable Data

- **SNMP Community Name -** You can use this screen to reconfigure an existing community, or to create a new one. Use this pull-down menu to select one of the existing community names, or select **'Create'** to add a new one. A valid entry is a case-sensitive string of up to 16 characters.
- **Client IP Address -** Taken together, the Client IP Address and Client IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.
- **Client IP Mask -** Taken together, the Client IP Address and Client IP Mask denote a range of IP addresses from

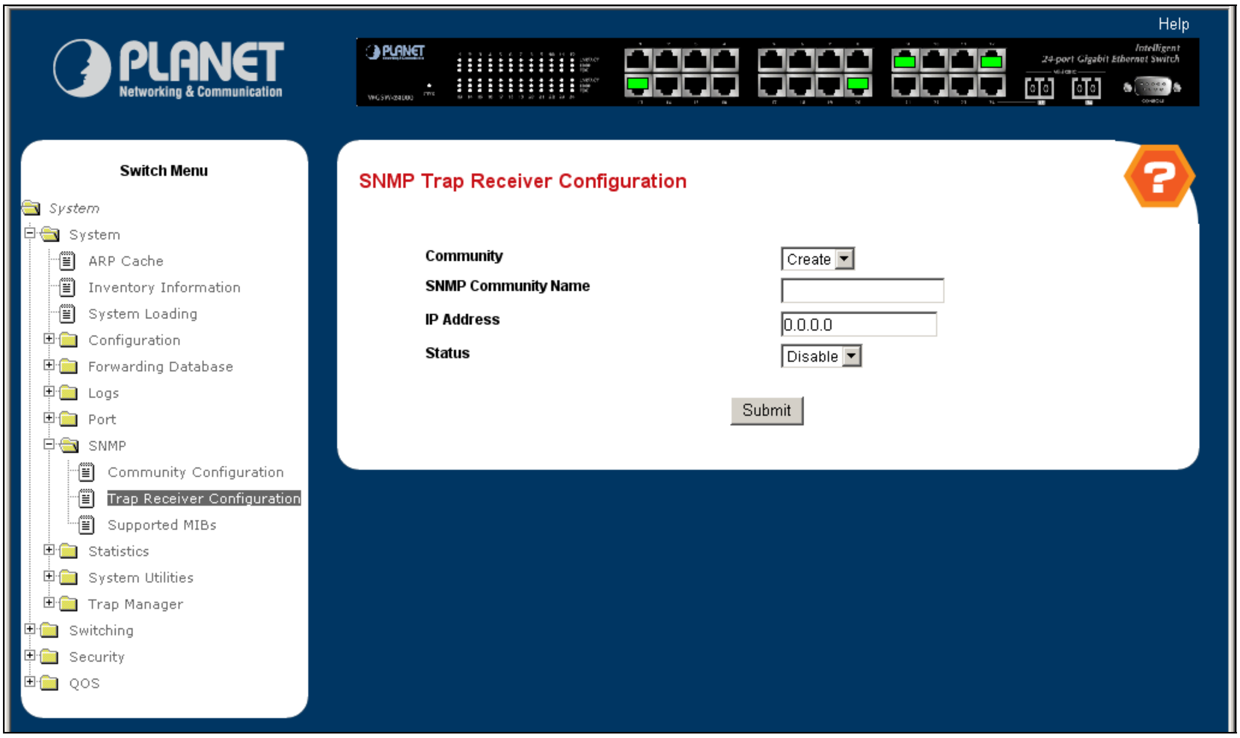
which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.

◦ **Access Mode -** Specify the access level for this community by selecting **Read/Write** or **Read Only** from the pull-down menu.

◦ **Status -** Specify the status of this community by selecting Enable or Disable from the pull-down menu. If you select enable, the Community Name must be unique among all valid Community Names or the set request will be rejected. If you select disable, the Community Name will become invalid.

4.2.7.2 Trap Receiver Configuration

This menu will display an entry for every active Trap Receiver.



SNMP Trap Receiver Configuration

Community	Create
SNMP Community Name	
IP Address	0.0.0.0
Status	Disable

Figure 4-2-34 SNMP Trap Receiver

◦ **SNMP Community Name -** Enter the community string for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.

◦ **IP Address -** Enter the IP address to receive SNMP traps from this device. Enter 4 numbers between 0 and 255 separated by periods.

◦ **Status -** Select the receiver's status from the pulldown menu:

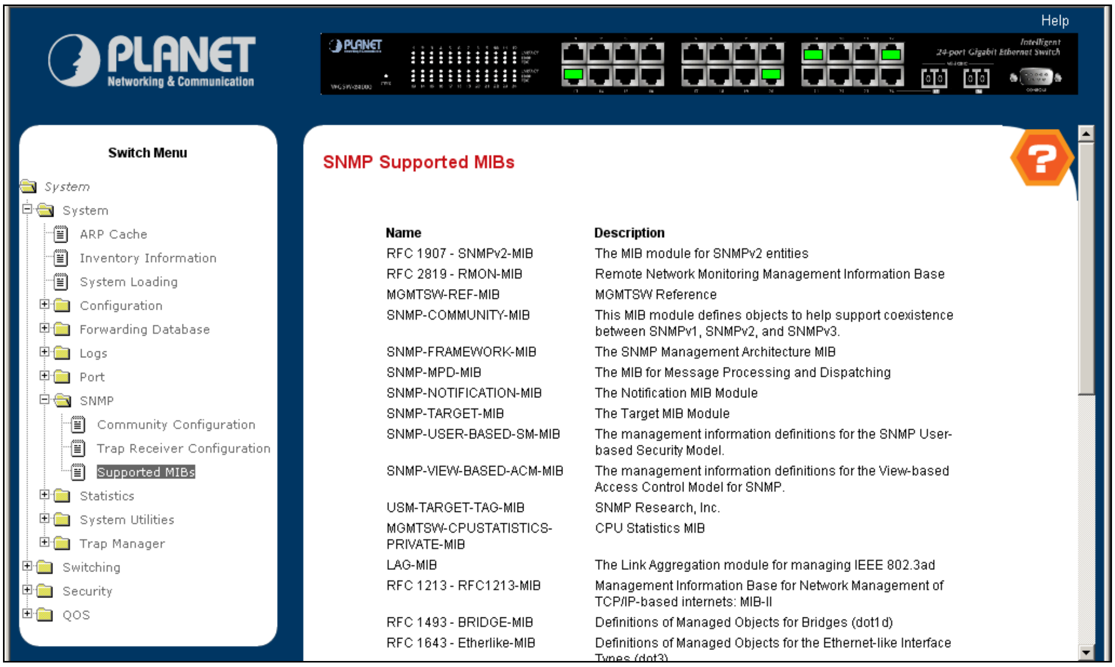
◦ **Enable -** send traps to the receiver

◦ **Disable -** do not send traps to the receiver.

4.2.7.3 Supported MIBS

This is a list of all the MIBs supported by the switch.

- **Name -** The RFC number if applicable and the name of the MIB.
- **Description -** The RFC title or MIB description.
- **Refresh -** Update the data.



SNMP Supported MIBs

Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
MGMTSW-REF-MIB	MGMTSW Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
MGMTSW-CPUSTATISTICS-PRIVATE-MIB	CPU Statistics MIB
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB	Definitions of Managed Objects for Bridges (dot1d)
RFC 1643 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types (dot3)

Figure 4-2-35 SNMP Supported MIBs

4.2.9 Statistics

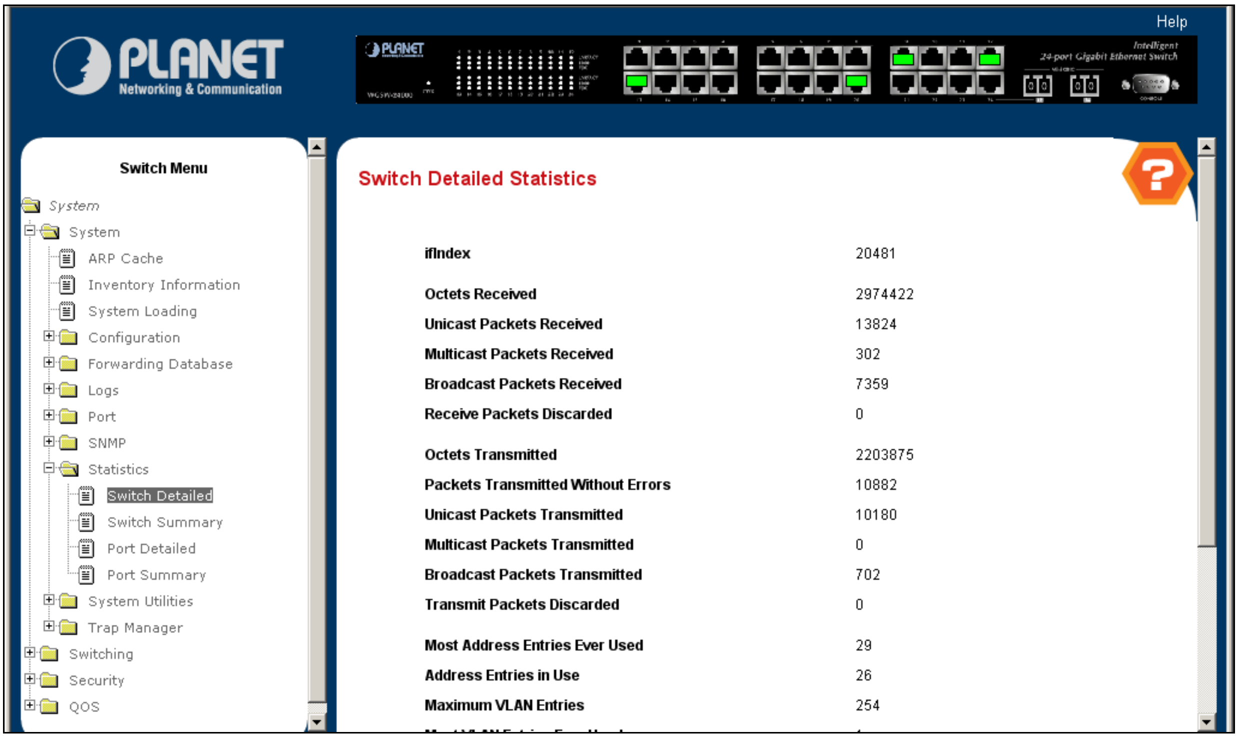
4.2.9.1 Switch Detail

This page shows the detail information of the switch, including the following data:

- **ifIndex -** This object indicates the ifIndex of the interface table entry associated with the Processor of this switch.
- **Octets Received -** The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
- **Unicast Packets Received -** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Multicast Packets Received -** The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
- **Broadcast Packets Received -** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Receive Packets Discarded -** The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
- **Octets Transmitted -** The total number of octets transmitted out of the interface, including framing characters.
- **Packets Transmitted Without Errors -** The total number of packets transmitted out of the interface.
- **Unicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Multicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted

to a Multicast address, including those that were discarded or not sent.

- **Broadcast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
- **Transmit Packets Discarded -** The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
- **Most Address Entries Ever Used -** The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
- **Address Entries in Use -** The number of Learned and static entries in the Forwarding Database Address Table for this switch.
- **Maximum VLAN Entries -** The maximum number of Virtual LANs (VLANs) allowed on this switch.
- **Most VLAN Entries Ever Used -** The largest number of VLANs that have been active on this switch since the last reboot.
- **Static VLAN Entries -** The number of presently active VLAN entries on this switch that have been created statically.
- **Dynamic VLAN Entries -** The number of presently active VLAN entries on this switch that have been created by GVRP registration.
- **VLAN Deletes -** The number of VLANs on this switch that have been created and then deleted since the last reboot.
- **Time Since Counters Last Cleared -** The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.



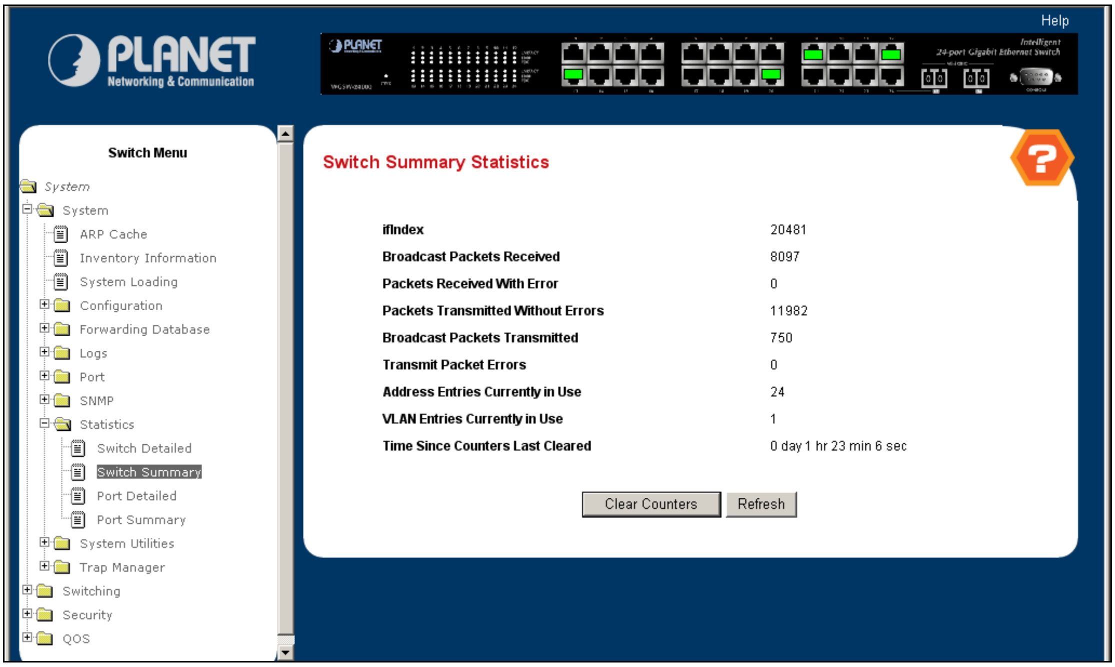
Switch Detailed Statistics

ifIndex	20481
Octets Received	2974422
Unicast Packets Received	13824
Multicast Packets Received	302
Broadcast Packets Received	7359
Receive Packets Discarded	0
Octets Transmitted	2203875
Packets Transmitted Without Errors	10882
Unicast Packets Transmitted	10180
Multicast Packets Transmitted	0
Broadcast Packets Transmitted	702
Transmit Packets Discarded	0
Most Address Entries Ever Used	29
Address Entries in Use	26
Maximum VLAN Entries	254

Figure 4-2-36 Switch Detailed Statistics

4.2.9.2 Switch Summary

- **ifIndex -** This object indicates the ifIndex of the interface table entry associated with the Processor of this switch.
- **Broadcast Packets Received -** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Packets Received With Error -** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Packets Transmitted Without Errors -** The total number of packets transmitted out of the interface.
- **Broadcast Packets Transmitted -** The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
- **Transmit Packet Errors -** The number of outbound packets that could not be transmitted because of errors.
- **Address Entries Currently in Use -** The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
- **VLAN Entries Currently in Use -** The number of VLAN entries presently occupying the VLAN table.
- **Time Since Counters Last Cleared -** The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.



Switch Summary Statistics

ifIndex	20481
Broadcast Packets Received	8097
Packets Received With Error	0
Packets Transmitted Without Errors	11982
Broadcast Packets Transmitted	750
Transmit Packet Errors	0
Address Entries Currently in Use	24
VLAN Entries Currently in Use	1
Time Since Counters Last Cleared	0 day 1 hr 23 min 6 sec

Figure 4-2-37 Switch Summary Statistics

4.2.8.3 Port Detailed

Selection Criteria

- **Slot.Port -** Selects the interface for which data is to be displayed or configured.

Non-Configurable Data

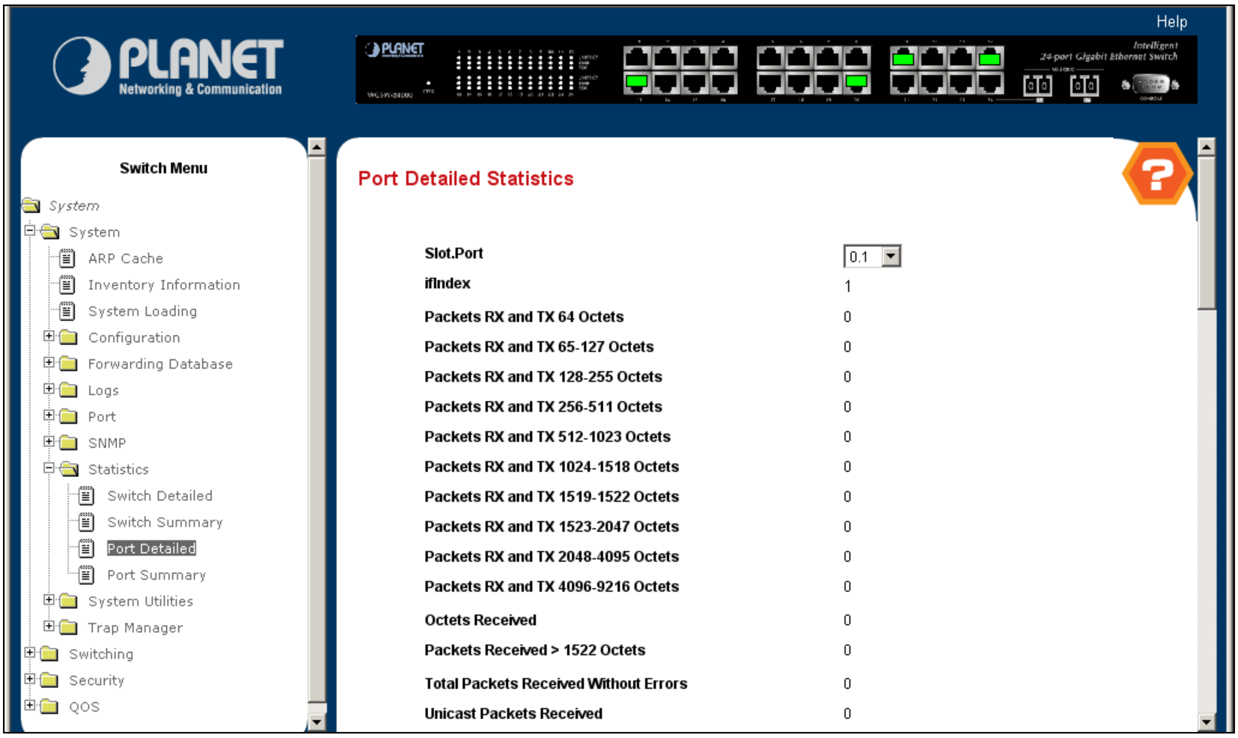
- **ifIndex -** This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
- **Packets RX and TX 64 Octets -** The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
- **Packets RX and TX 65-127 Octets -** The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 128-255 Octets -** The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 256-511 Octets -** The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 512-1023 Octets -** The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 1024-1518 Octets -** The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 1519-1522 Octets -** The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 1523-2047 Octets -** The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 2048-4095 Octets -** The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets RX and TX 4096-9216 Octets -** The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
- **Octets Received -** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
- **Packets Received > 1522 Octets -** The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Total Packets Received Without Errors -** The total number of packets received that were without errors.
- **Unicast Packets Received -** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Multicast Packets Received -** The total number of good packets received that were directed to a multicast

address. Note that this number does not include packets directed to the broadcast address.

- **Broadcast Packets Received -** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Total Packets Received with MAC Errors -** The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Jabbers Received -** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
- **Fragments/Undersize Received -** The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- **Alignment Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
- **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
- **Overruns -** The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
- **Total Received Packets Not Forwarded -** A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.
- **Local Traffic Frames -** The total number of frames dropped in the forwarding process because the destination address was located off of this port.
- **802.3x Pause Frames Received -** A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
- **Unacceptable Frame Type -** The number of frames discarded from this port due to being an unacceptable frame type.
- **Multicast Tree Viable Discards -** The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.
- **Reserved Address Discards -** The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
- **Broadcast Storm Recovery -** The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.
- **CFI Discards -** The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
- **Upstream Threshold -** The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

- **Total Packets Transmitted (Octets) -** The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
- **Packets Transmitted 1523-2047 Octets -** The total number of packets (including bad packets) received that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted 2048-4095 Octets -** The total number of packets (including bad packets) received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted 4096-9216 Octets -** The total number of packets (including bad packets) received that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
- **Maximum Frame Size -** The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. (1518 to 1600). The default maximum frame size is 1518.
- **Total Packets Transmitted Successfully -** The number of frames that have been transmitted by this port to its segment.
- **Unicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Multicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
- **Broadcast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
- **Total Transmit Errors -** The sum of Single, Multiple, and Excessive Collisions.
- **Tx FCS Errors -** The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
- **Tx Oversized -** The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.
- **Underrun Errors -** The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
- **Total Transmit Packets Discarded -** The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
- **Single Collision Frames -** A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
- **Multiple Collision Frames -** A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
- **Excessive Collision Frames -** A count of frames for which transmission on a particular interface fails due to excessive collisions.
- **Port Membership Discards -** The number of frames discarded on egress for this port due to egress filtering being enabled.
- **STP BPDUs Received -** Number of STP BPDUs received at the selected port.
- **STP BPDUs Transmitted -** Number of STP BPDUs transmitted from the selected port.

- **RSTP BPDUs Received -** Number of RSTP BPDUs received at the selected port.
- **RSTP BPDUs Transmitted -** Number of RSTP BPDUs transmitted from the selected port.
- **MSTP BPDUs Received -** Number of MSTP BPDUs received at the selected port.
- **MSTP BPDUs Transmitted -** Number of MSTP BPDUs transmitted from the selected port.
- **802.3x Pause Frames Transmitted -** A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
- **GVRP PDUs Received -** The count of GVRP PDUs received in the GARP layer.
- **GVRP PDUs Transmitted -** The count of GVRP PDUs transmitted from the GARP layer.
- GVRP Failed Registrations - The number of times attempted GVRP registrations could not be completed.
- **GMRP PDUs Received -** The count of GMRP PDUs received from the GARP layer.
- **GMRP PDUs Transmitted -** The count of GMRP PDUs transmitted from the GARP layer.
- **GVRP Failed Registrations -** The number of times attempted GMRP registrations could not be completed.
- **Time Since Counters Last Cleared -** The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.



Port Detailed Statistics

Slot.Port	0.1
ifIndex	1
Packets RX and TX 64 Octets	0
Packets RX and TX 65-127 Octets	0
Packets RX and TX 128-255 Octets	0
Packets RX and TX 256-511 Octets	0
Packets RX and TX 512-1023 Octets	0
Packets RX and TX 1024-1518 Octets	0
Packets RX and TX 1519-1522 Octets	0
Packets RX and TX 1523-2047 Octets	0
Packets RX and TX 2048-4095 Octets	0
Packets RX and TX 4096-9216 Octets	0
Octets Received	0
Packets Received > 1522 Octets	0
Total Packets Received Without Errors	0
Unicast Packets Received	0

Figure 4-2-38 Port Detailed Statistic

4.2.8.4 Port Summary

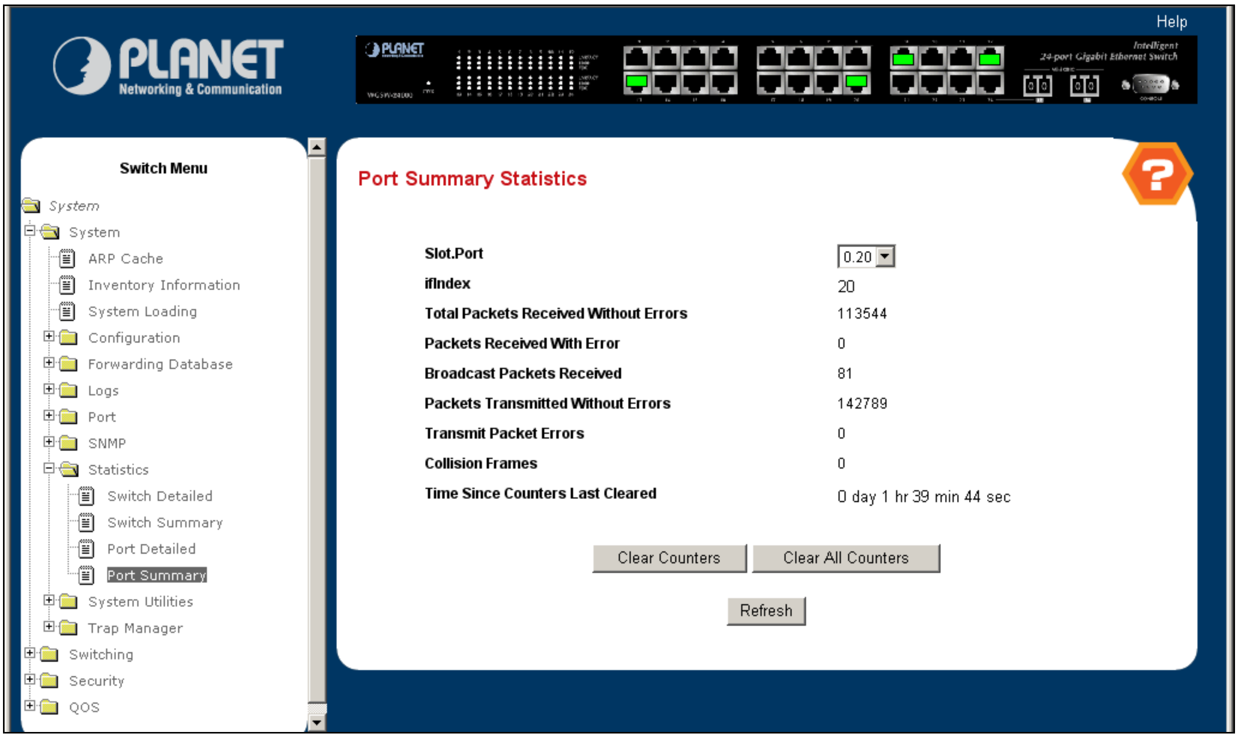
Selection Criteria

- **Slot.Port -** Selects the interface for which data is to be displayed or configured.

Non-Configurable Data

- **ifIndex -** This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
- **Total Packets Received Without Errors -** The total number of packets received that were without errors.
- **Packets Received With Error -** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

- **Broadcast Packets Received -** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Packets Transmitted Without Errors -** The number of frames that have been transmitted by this port to its segment.
- **Transmit Packet Errors -** The number of outbound packets that could not be transmitted because of errors.
- **Collision Frames -** The best estimate of the total number of collisions on this Ethernet segment.
- **Time Since Counters Last Cleared -** The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.



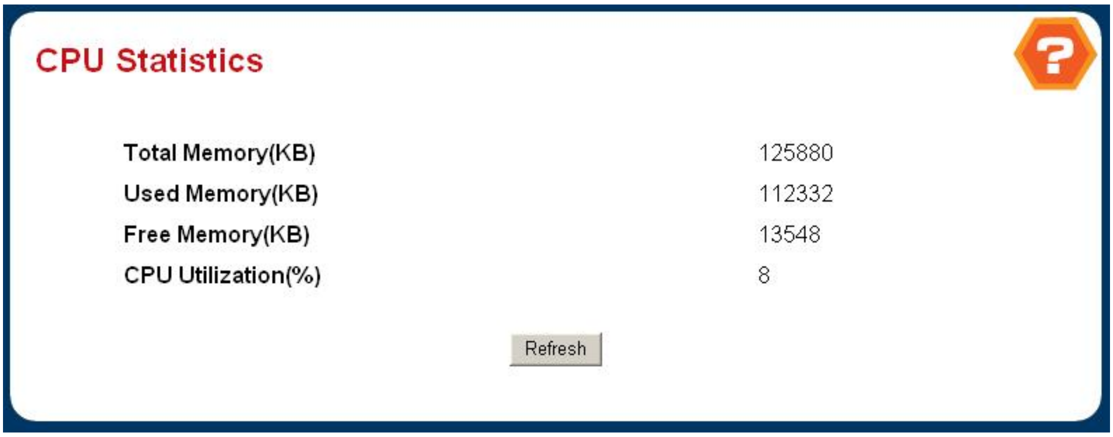
Port Summary Statistics

Slot.Port	0.20
ifIndex	20
Total Packets Received Without Errors	113544
Packets Received With Error	0
Broadcast Packets Received	81
Packets Transmitted Without Errors	142789
Transmit Packet Errors	0
Collision Frames	0
Time Since Counters Last Cleared	0 day 1 hr 39 min 44 sec

Figure 4-2-39 Port Summary Statistics

4.2.8.5 CPU Statistics

This page shows the system loading information, including the following fields:



CPU Statistics

Total Memory(KB)	125880
Used Memory(KB)	112332
Free Memory(KB)	13548
CPU Utilization(%)	8

Figure 4-2-40 CPU Statistics

Non-Configurable Data

- **Total Memory** - The total RAM memory available with the CPU.
- **Used Memory** - The RAM memory already used by CPU.
- **Free Memory** - The free memory available with the CPU.
- **% CPU Utilization** - % of CPU capacity used over time.

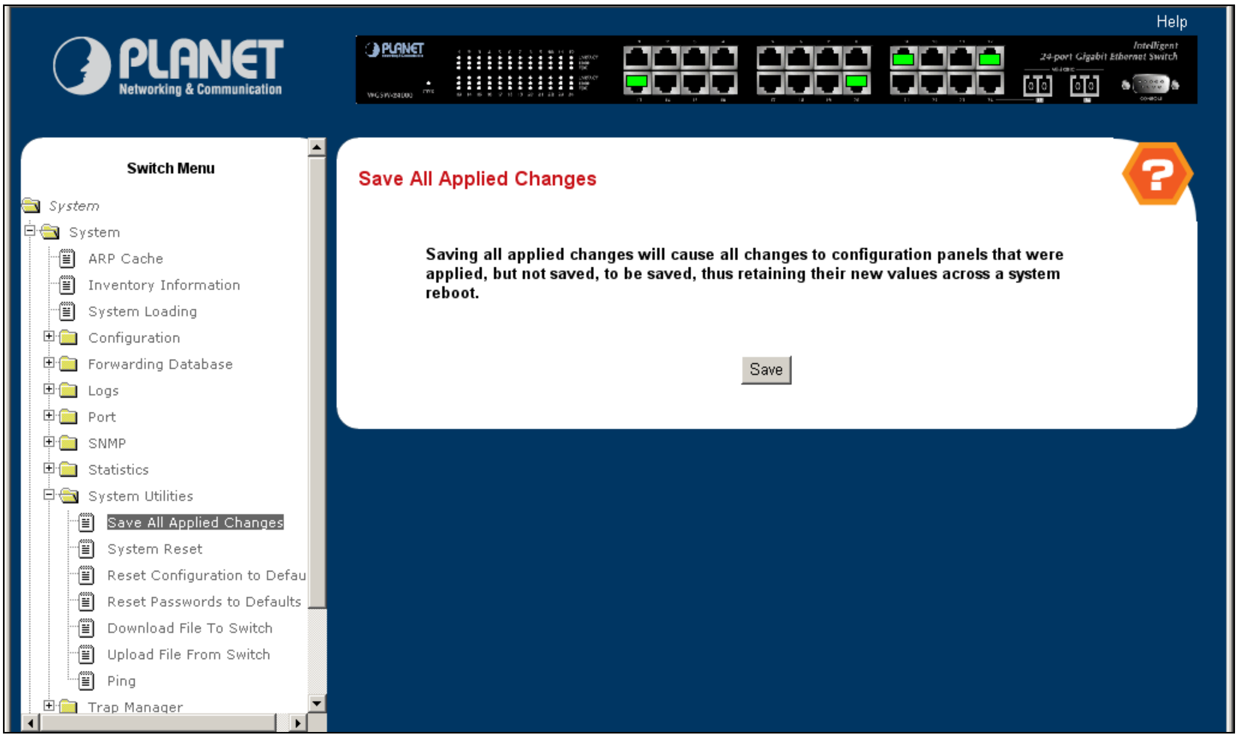
Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.2.9 System Utilities

4.2.9.1 Save All Applied Changes

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved, thus retaining their new values across a system reboot.



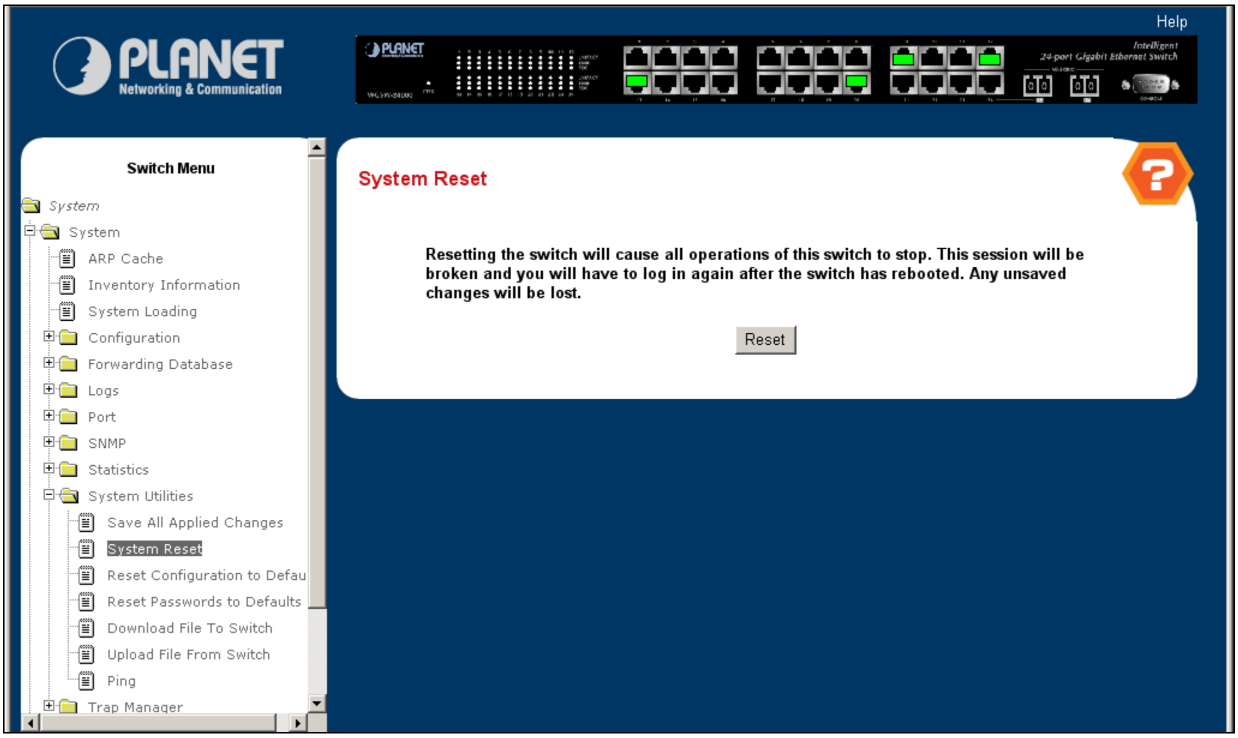
Save All Applied Changes

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved, thus retaining their new values across a system reboot.

Figure 4-2-41 Save All Applied Changes

4.2.9.2 System Reset

Reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost. You will be shown a confirmation screen after you select the button.



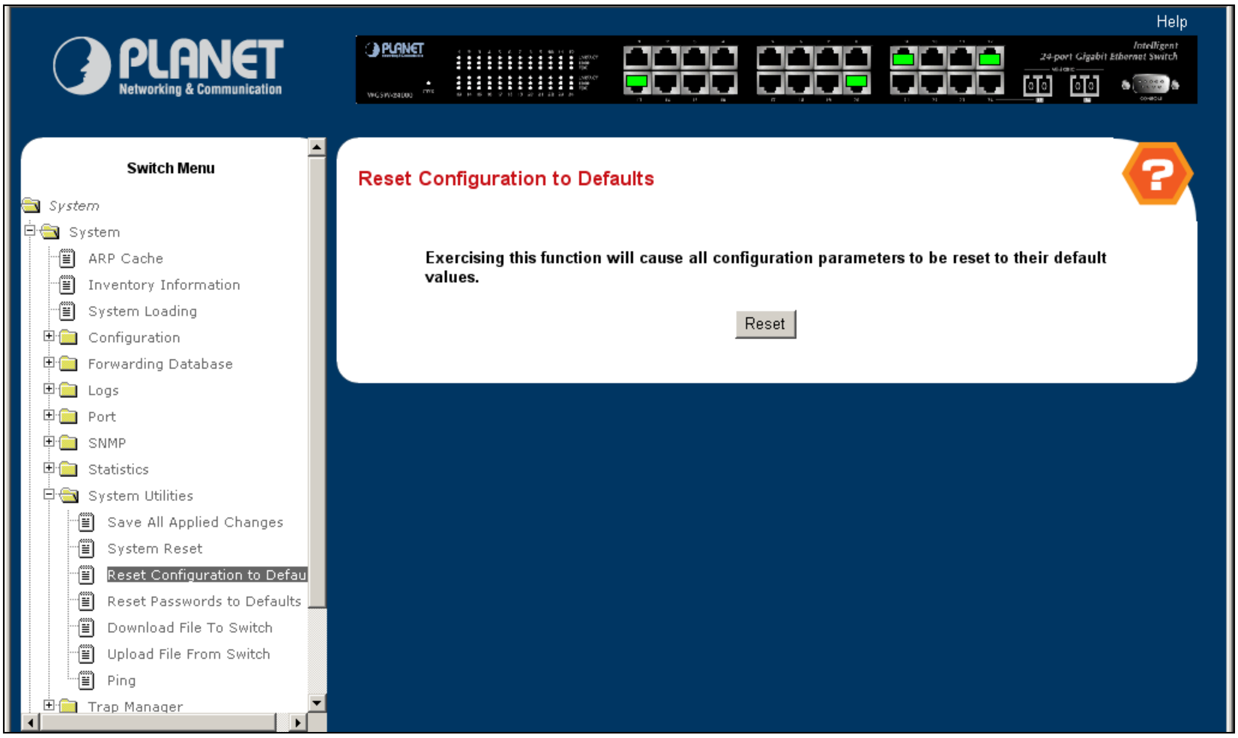
System Reset

Resetting the switch will cause all operations of this switch to stop. This session will be broken and you will have to log in again after the switch has rebooted. Any unsaved changes will be lost.

Figure 4-2-42 System Reset

4.2.9.3 Reset Configuration to Default

Have all configuration parameters reset to their factory default values. All changes you have made will be lost, even if you have issued a save. You will be shown a confirmation screen after you select the button.



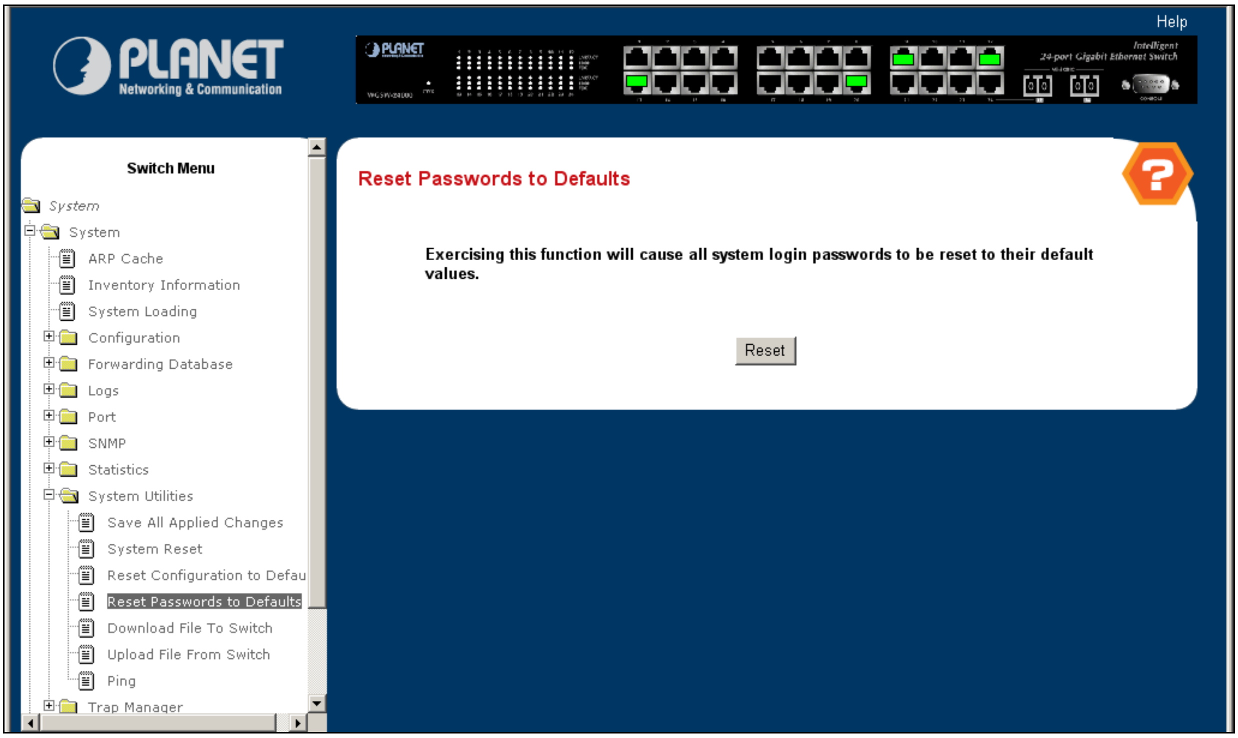
Reset Configuration to Defaults

Exercising this function will cause all configuration parameters to be reset to their default values.

Figure 4-2-43 Reset Configuration to Default

4.2.9.4 Reset Password to Default

Reset all of the system login passwords to their default values. If you want the switch to retain the new values across a power cycle, you must perform a save.



Reset Passwords to Defaults

Exercising this function will cause all system login passwords to be reset to their default values.

Reset

Figure 4-2-44 Reset Password to Default

4.2.9.5 Download File To Switch

Use this menu to download a file to the switch.

Configurable Data

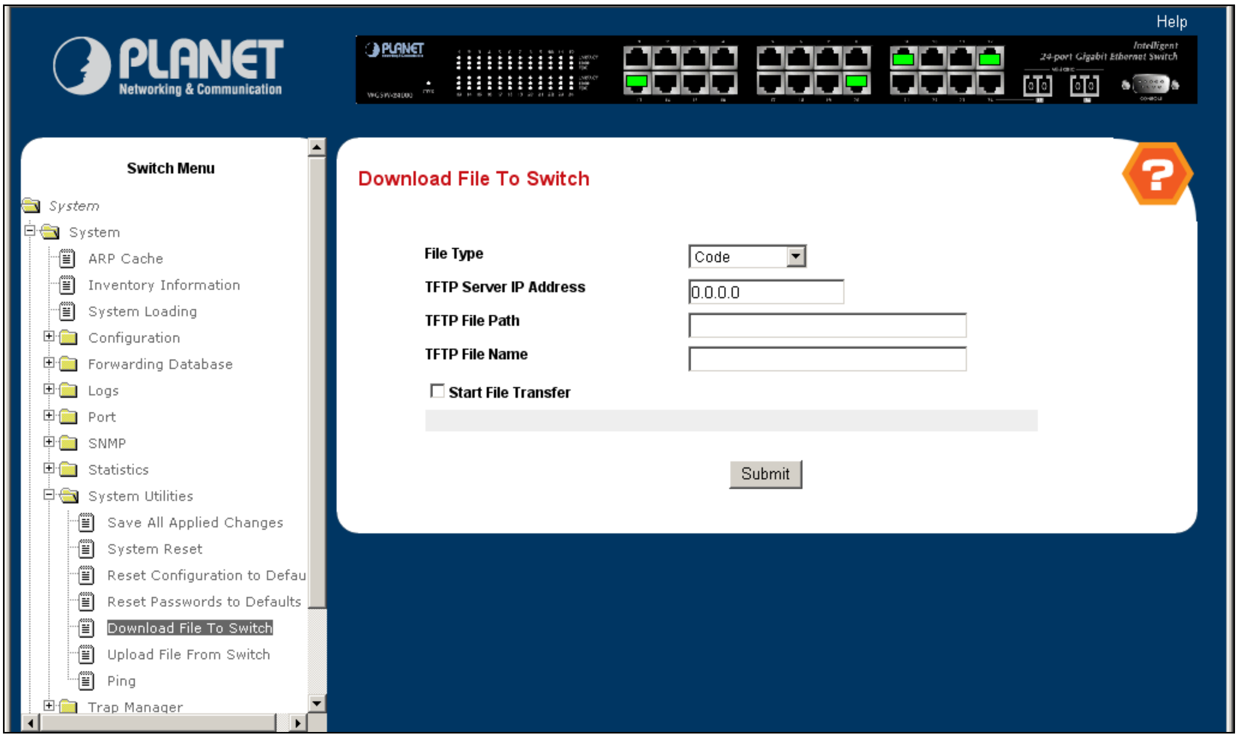
- **File Type -** Specify what type of file you want to download:
  - **Code -** specify code when you want to upgrade the operational flash.
  - **Configuration -** specify configuration when you want to update the switch's configuration. If the file has errors the update will be stopped.
  - **SSH-1 RSA Key File -** SSH-1 Rivest-Shamir-Adleman (RSA) Key File
  - **SSH-2 RSA Key PEM File -** SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)
  - **SSH-2 DSA Key PEM File -** SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded)
  - **SSL Trusted Root Certificate PEM File -** SSL Trusted Root Certificate File (PEM Encoded)
  - **SSL Server Certificate PEM File -** SSL Server Certificate File (PEM Encoded)
  - **SSL DH Weak Encryption Parameter PEM File -** SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded)
  - **SSL DH Strong Encryption Parameter PEM File -** SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)

The factory default is code.

Note that to download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

- **TFTP Server IP Address -** Enter the IP address of the TFTP server. The factory default is 0.0.0.0.

- **TFTP File Path -** Enter the path on the TFTP server where the selected file is located. You may enter up to 32 characters. The factory default is blank.
- **TFTP File Name -** Enter the name on the TFTP server of the file you want to download. You may enter up to 32 characters. The factory default is blank.
- **Start File Transfer -** To initiate the download you need to check this box and then select the submit button.



Download File To Switch

File Type	Code
TFTP Server IP Address	0.0.0.0
TFTP File Path	
TFTP File Name	

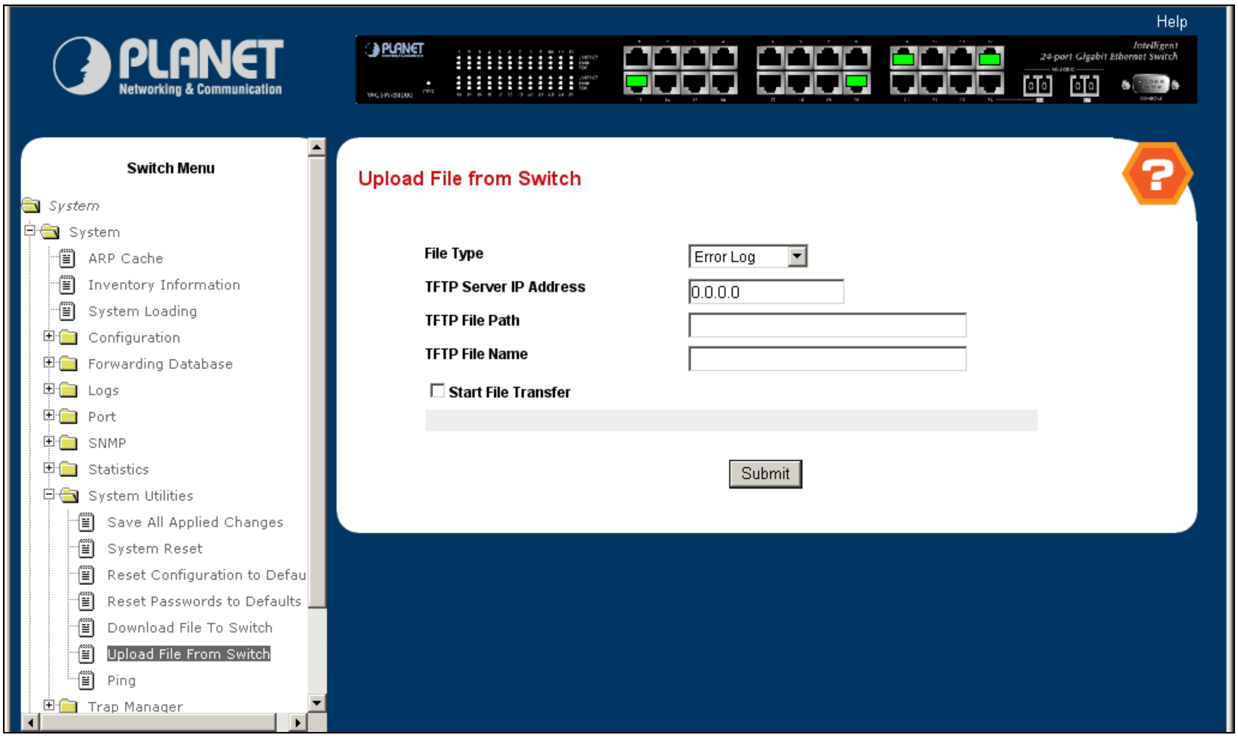
□ Start File Transfer

Submit

Figure 4-2-45 Download File To Switch

4.2.9.6 Upload File From Switch

Use this menu to upload a configuration or log file from the switch.



Upload File from Switch

File Type	Error Log
TFTP Server IP Address	0.0.0.0
TFTP File Path	
TFTP File Name	

□ Start File Transfer

Submit

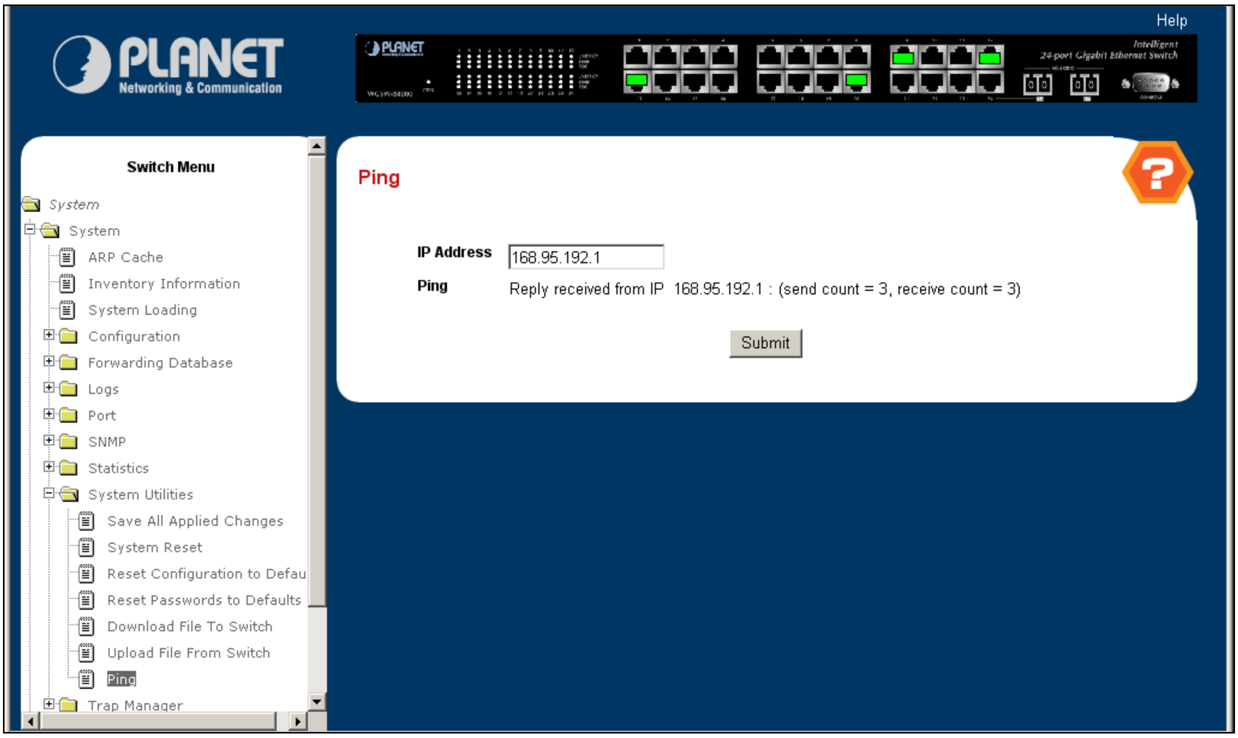
Figure 4-2-46 Upload File from Switch

Configurable Data

- **File Type -** Specify the type of file you want to upload. The available options are Configuration, Error Log, System Trace, and Trap Log. The factory default is Error Log.
- **TFTP Server IP Address -** Enter the IP address of the TFTP server. The factory default is 0.0.0.0
- **TFTP File Path -** Enter the path on the TFTP server where you want to put the file being uploaded. You may enter up to 32 characters. The factory default is blank.
- **TFTP File Name -** Enter the name you want to give the file being uploaded. You may enter up to 32 characters. The factory default is blank.
- **Start File Transfer -** To initiate the upload you need to check this box and then select the submit button.

4.2.9.7 Ping

Use this screen to tell the switch to send a Ping request to a specified IP address. You can use this to check whether the switch can communicate with a particular IP station. Once you click the Submit button, the switch will send three pings and the results will be displayed below the configurable data. If a reply to the ping is not received, you will see **No Reply Received from IP xxx.xxx.xxx.xxx**, otherwise you will see **Reply received from IP xxx.xxx.xxx.xxx : (send count = 3, receive count = n)**.



Ping

IP Address: 168.95.192.1

Ping: Reply received from IP 168.95.192.1 : (send count = 3, receive count = 3)

Figure 4-2-47 Ping

Configurable Data

- **IP Address -** Enter the IP address of the station you want the switch to ping. The initial value is blank. The IP Address you enter is not retained across a power cycle.

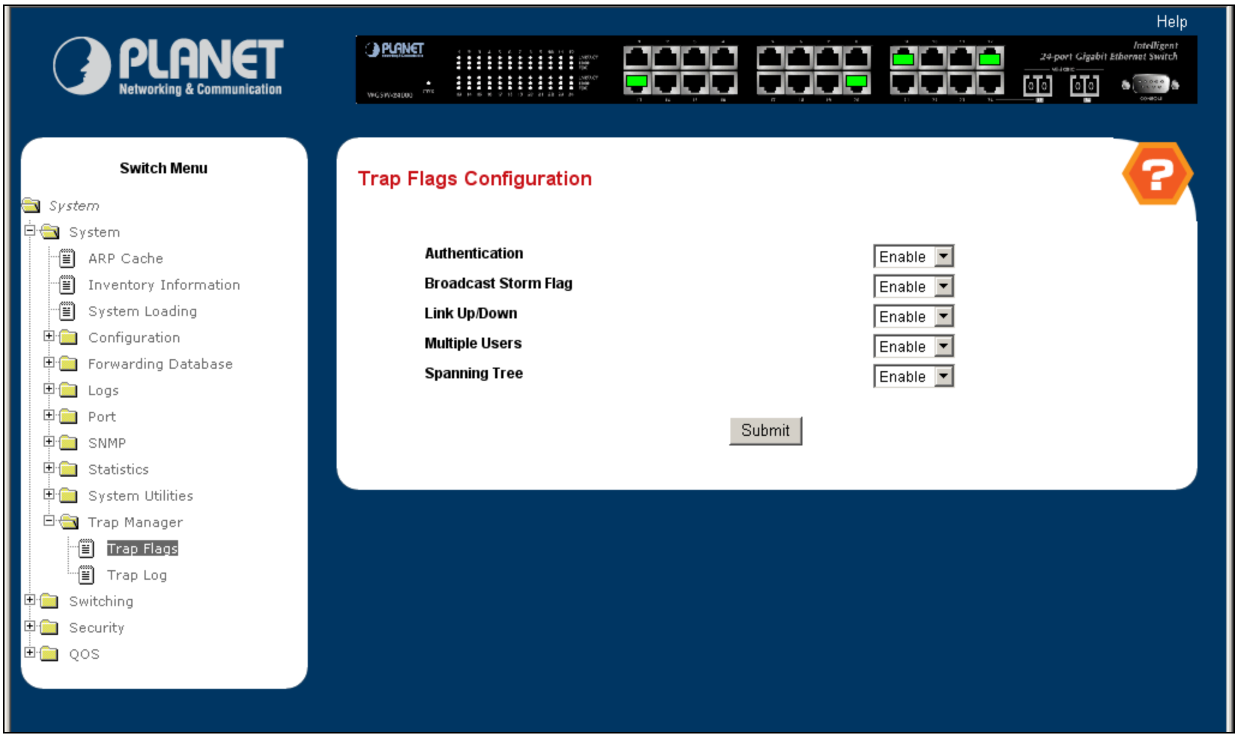
4.2.10 Trap Management

4.2.10.1 Trap Flags

Use this menu to specify which traps you want to enable. When the condition identified by an active trap is encountered by the switch a trap message will be sent to any enabled SNMP Trap Receivers, and a message will be written to the trap log.

Configurable Data

- **Authentication -** Enabled or disable activation of authentication failure traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
- **Broadcast Storm Flag -** This field will only be displayed if Broadcast storm feature is supported. Enabled or disable activation of broadcast storm traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
- **Link Up/Down -** Enabled or disable activation of link status traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
- **Multiple Users -** Enabled or disable activation of multiple user traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either via telnet or the serial port).
- **Spanning Tree -** Enabled or disable activation of spanning tree traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.



Trap Flags Configuration

Authentication	Enable
Broadcast Storm Flag	Enable
Link Up/Down	Enable
Multiple Users	Enable
Spanning Tree	Enable

Figure 4-2-48 Trap Flags

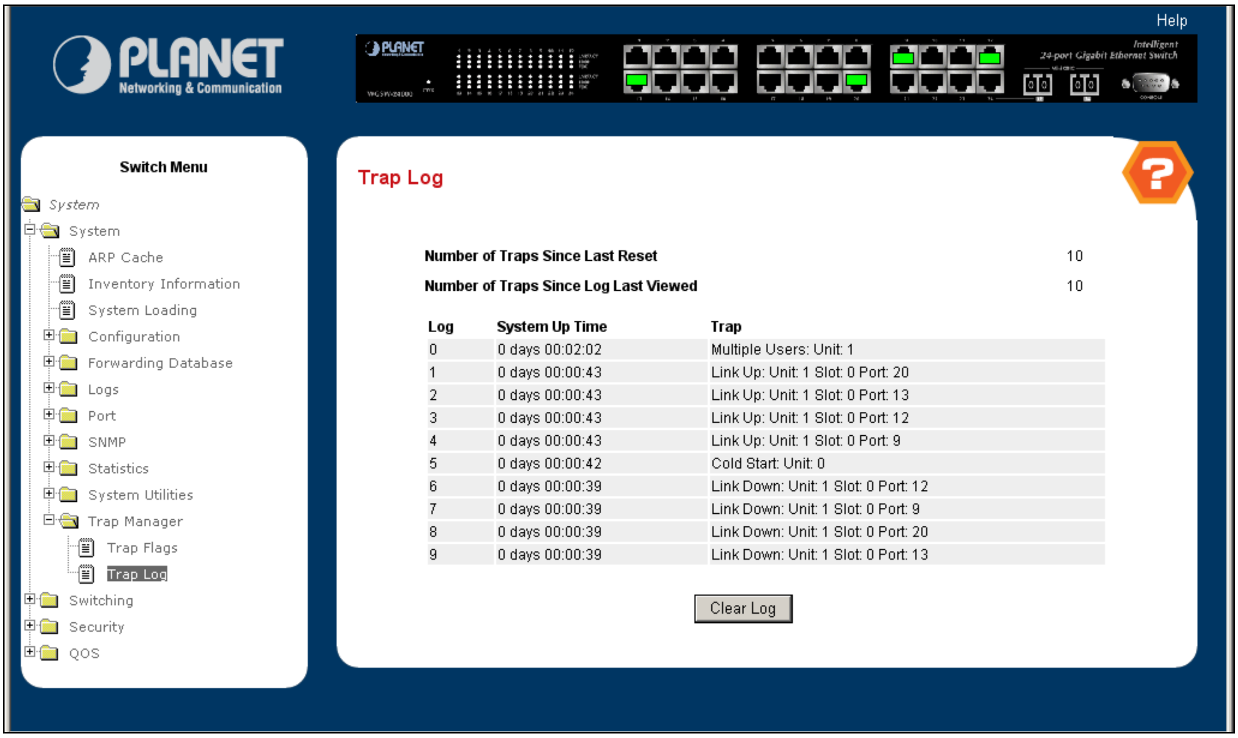
4.2.10.2 Trap Log

This screen lists the entries in the trap log. The information can be retrieved as a file by using System Utilities, Upload File from Switch.

Non-Configurable Data

- **Number of Traps since last reset -** The number of traps that have occurred since the last time the switch was reset.

- **Number of Traps since log last viewed -** The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch etc.) will cause this counter to be cleared to 0.
- **Log -** The sequence number of this trap.
- **System Up Time -** The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.
- **Trap -** Information identifying the trap.



Trap Log

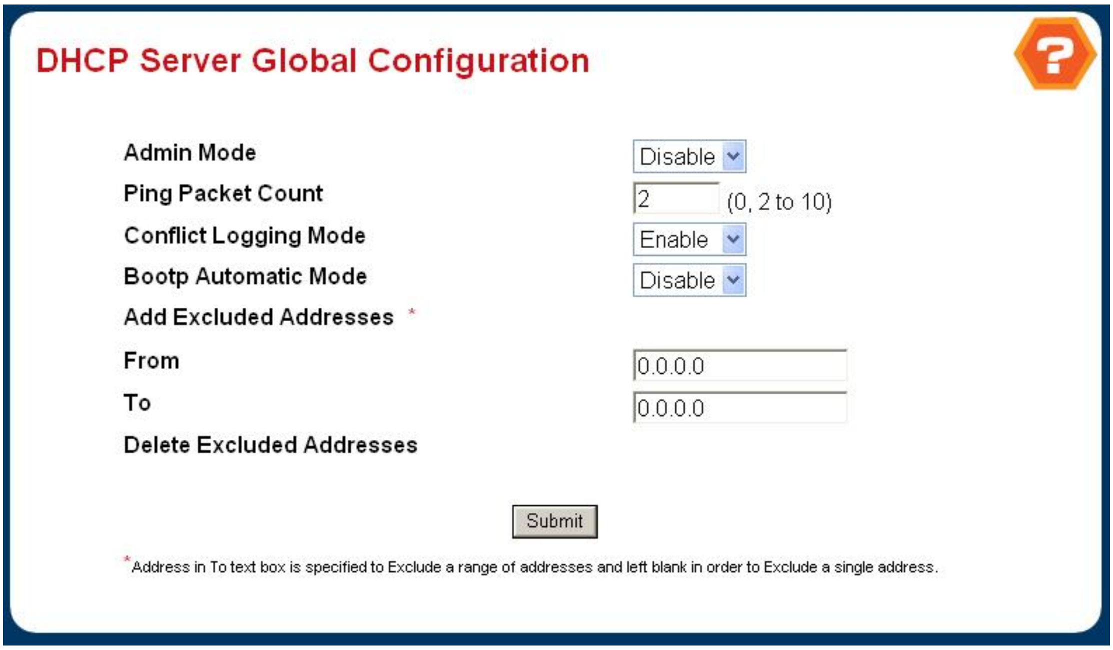
Number of Traps Since Last Reset	10
Number of Traps Since Log Last Viewed	10

Log	System Up Time	Trap
0	0 days 00:02:02	Multiple Users: Unit: 1
1	0 days 00:00:43	Link Up: Unit: 1 Slot: 0 Port: 20
2	0 days 00:00:43	Link Up: Unit: 1 Slot: 0 Port: 13
3	0 days 00:00:43	Link Up: Unit: 1 Slot: 0 Port: 12
4	0 days 00:00:43	Link Up: Unit: 1 Slot: 0 Port: 9
5	0 days 00:00:42	Cold Start: Unit: 0
6	0 days 00:00:39	Link Down: Unit: 1 Slot: 0 Port: 12
7	0 days 00:00:39	Link Down: Unit: 1 Slot: 0 Port: 9
8	0 days 00:00:39	Link Down: Unit: 1 Slot: 0 Port: 20
9	0 days 00:00:39	Link Down: Unit: 1 Slot: 0 Port: 13

Figure 4-2-49 Trap Log

4.2.11 DHCP Server

4.2.11.1 Global Configuration



DHCP Server Global Configuration

Admin Mode: Disable

Ping Packet Count: 2 (0, 2 to 10)

Conflict Logging Mode: Enable

Bootp Automatic Mode: Disable

Add Excluded Addresses *

From: 0.0.0.0

To: 0.0.0.0

Delete Excluded Addresses

*Address in To text box is specified to Exclude a range of addresses and left blank in order to Exclude a single address.

Figure 4-2-50 DHCP Server Global Configuration

Configurable Data

- **Admin Mode** - Specifies if the DHCP Service is to be Enabled or Disabled. Default value is Disable.
- **Ping Packet Count** - Specifies the number of packets a server sends to a Pool address to check for duplication as part of a ping operation. Default value is 2. Valid Range is (0, 2 to 10). Setting the value to 0 will disable the function.
- **Conflict Logging Mode** - Specifies if conflict logging on a DHCP Server is to be Enabled or Disabled. Default value is Enable.
- **Bootp Automatic Mode** - Specifies if Bootp for dynamic pools is to be Enabled or Disabled. Default value is Disable.
- **Add Excluded Addresses** - Specifies the IP addresses that the server should not assign to the client.

  - ***From*** - Specifies the low address in case the user wants to exclude a range of addresses. Specifies the address to be Excluded in case the user wants to exclude a single address.
  - ***To*** - Specifies the high address in case the user wants to exclude a range of addresses. To exclude a single addres you may enter the same IP address as specified in From or leave as 0.0.0.0.

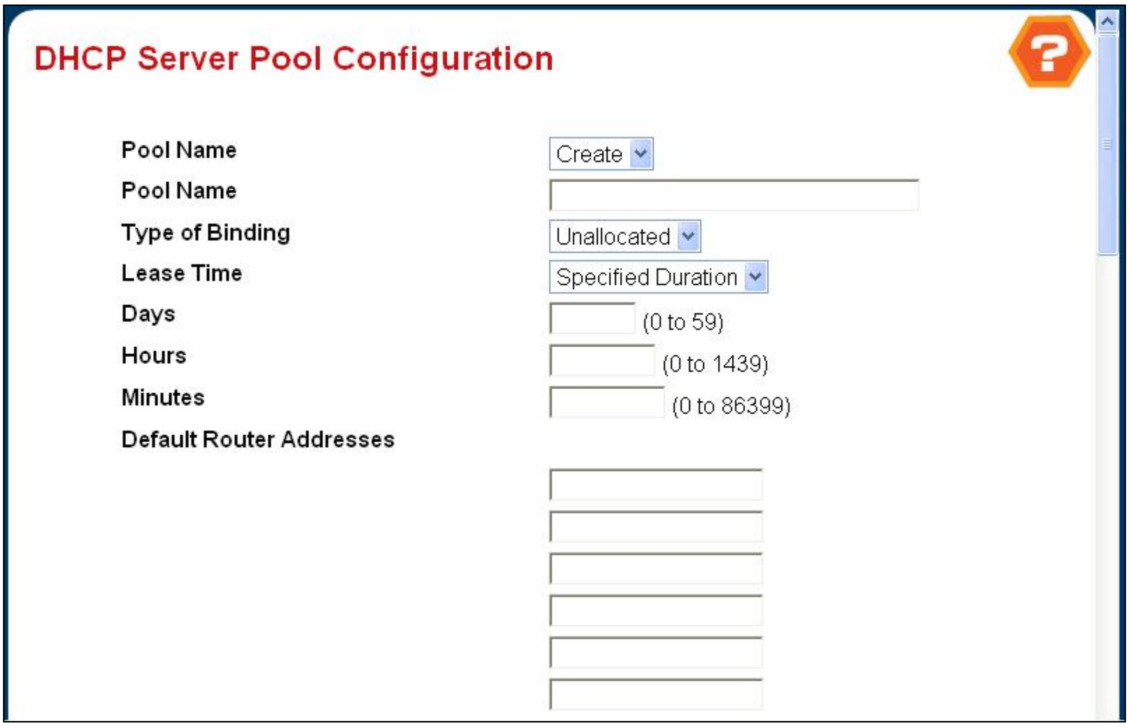
- **Delete Excluded Addresses** - Lists the Excluded Address ranges with a checkbox against each. One or more checkbox(es) can be selected (checked) in order to delete the listed Excluded Addresses.

Command Buttons

- **Submit** - Sends the updated configuration to the switch. Configuration changes take effect immediately.

4.2.11.2 Pool Configuration

DHCP Server Pool Configuration



DHCP Server Pool Configuration

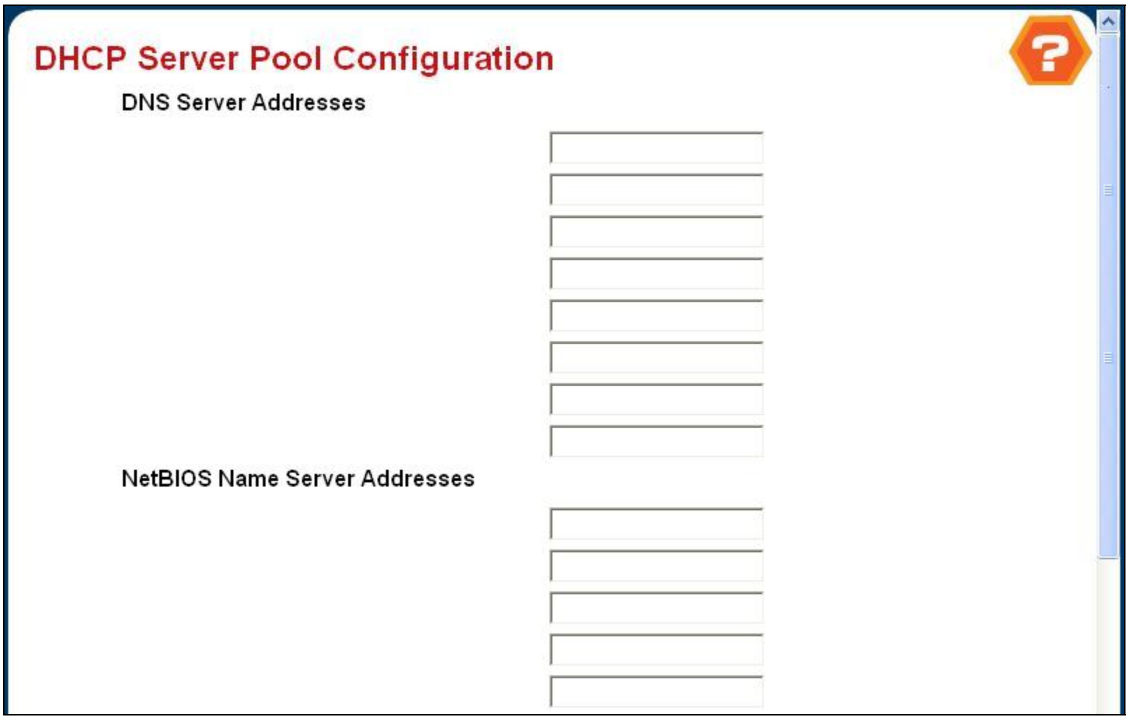
Pool Name	Create
Pool Name	
Type of Binding	Unallocated
Lease Time	Specified Duration
Days	(0 to 59)
Hours	(0 to 1439)
Minutes	(0 to 86399)
Default Router Addresses	

Figure 4-2-51 DHCP Server Pool Configuration

Configurable Data

- **Pool Name*** - For a user with readwrite permission, this field would show names of all the existing pools along with an additional option "Create". When the user selects "Create" another text box "Pool Name" appears where the user may enter name for the Pool to be created.For a user with readonly permission, this field would show names of the existing pools only.
- **Pool Name** - This field appears when the user with read-write permission has selected "Create" in the Drop Down list against Pool Name*.Specifies the Name of the Pool to be created. Pool Name can be upto 31 characters in length.
- **Type of Binding** - Specifies the type of binding for the pool.
    - ***Unallocated***
    - ***Dynamic***
    - ***Manual***
- **Network Number** - Specifies the subnet number for a DHCP address of a dynamic pool.
- **Network Mask** - Specifies the subnet number for a DHCP address of a dynamic pool. Either Network Mask or Prefix Length can be configured to specify the subnet mask but not both.
- **Prefix Length** - Specifies the subnet number for a DHCP address of a dynamic pool. Either Network Mask or Prefix Length can be configured to specify the subnet mask but not both. Valid Range is (0 to 32)
- **Client Name** - Specifies the Client Name for DHCP manual Pool.

- **Hardware Address** - Specifies the MAC address of the hardware platform of the DHCP client.
- **Hardware Address Type** - Specifies the protocol of the hardware platform of the DHCP client. Valid types are ethernet and ieee802. Default value is ethernet.
- **Client ID** - Specifies the Client Identifier for DHCP manual Pool.
- **Host Number** - Specifies the IP address for a manual binding to a DHCP client. Host can be set only if at least one among of Client Identifier or Hardware Address is specified. Deleting Host would delete Client Name, Client ID, Hardware Address for the Manual Pool and set the Pool Type to Unallocated.
- **Host Mask** - Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both.
- **Prefix Length** - Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both. Valid Range is (0 to 32)
- **Lease Time** - Can be selected as "Infinite" to specify lease time as Infinite or "Specified Duration" to enter a specific lease period. In case of dynamic binding infinite implies a lease period of 60 days and In case of manual binding infinite implies indefinite lease period. Default Value is "Specified Duration".
- **Days** - Specifies the Number of Days of Lease Period. This field appears only if the user has specified "Specified Duration" as the Lease time. Default Value is 1. Valid Range is (0 to 59)
- **Hours** - Specifies the Number of Hours of Lease Period. This field appears only if the user has specified "Specified Duration" as the Lease time. Valid Range is (0 to 1439)
- **Minutes** - Specifies the Number of Minutes of Lease Period. This field appears only if the user has specified "Specified Duration" as the Lease time. Valid Range is (0 to 86399)
- **Default Router Addresses** - Specifies the list of Default Router Addresses for the pool. The user may specify upto 8 Default Router Addresses in order of preference.



DHCP Server Pool Configuration

DNS Server Addresses

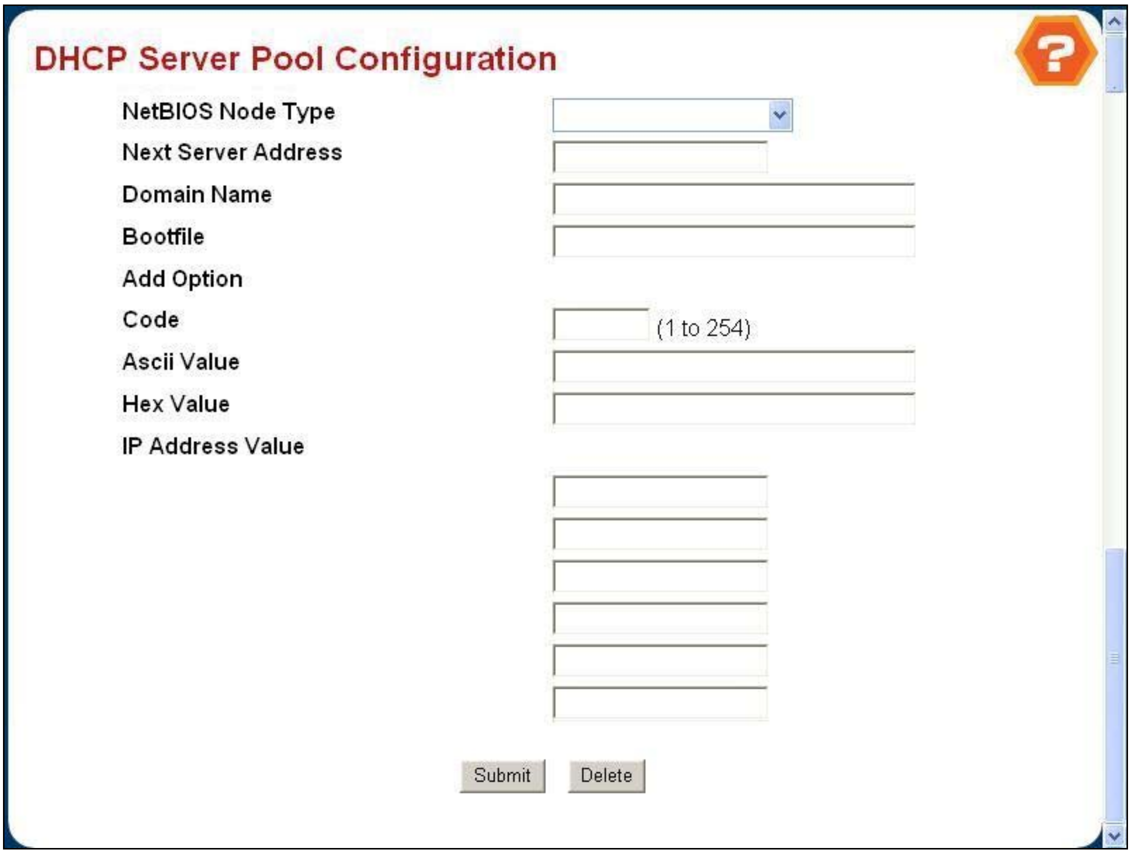
NetBIOS Name Server Addresses

Figure 4-2-52 DHCP Server Pool Configuration

- **DNS Server Addresses** - Specifies the list of DNS Server Addresses for the pool. The user may specify upto 8 DNS Server Addresses in order of preference.
- **NetBIOS Name Server Addresses** - Specifies the list of NetBIOS Name Server Addresses for the pool. The user may specify upto 8 NetBIOS Name Server Addresses in order of preference.
- **NetBIOS Node Type** - Specifies the NetBIOS node type for DHCP clients.

  - ***b-node Broadcast***
  - ***p-node Peer-to-Peer***
  - ***m-node Mixed***
  - ***h-node Hybrid***

- **Next Server Address** - Specifies the Next Server Address for the pool.
- **Domain Name** - Specifies the domain name for a DHCP client. Domain Name can be upto 255 characters in length.
- **Boot File** - Specifies the name of the default boot image for a DHCP client. File Name can be upto 128 characters in length.
- **Option Code** - Specifies the DHCP option code. Valid Range is (1 to 254)
- **Option Ascii** - Specifies an NVT ASCII character string.
- **Option Hex** - Specifies dotted hexadecimal data. Each byte in hexadecimal character strings is 2 hexadecimal digits. Each byte can be separated by a colon or white space. A period separates 2 bytes/4 hexadecimal digits.
- **Option IP Address** - Specifies the Option IP addresses.



DHCP Server Pool Configuration

NetBIOS Node Type

Next Server Address

Domain Name

Bootfile

Add Option

Code (1 to 254)

Ascii Value

Hex Value

IP Address Value

Figure 4-2-53 DHCP Server Pool Configuration

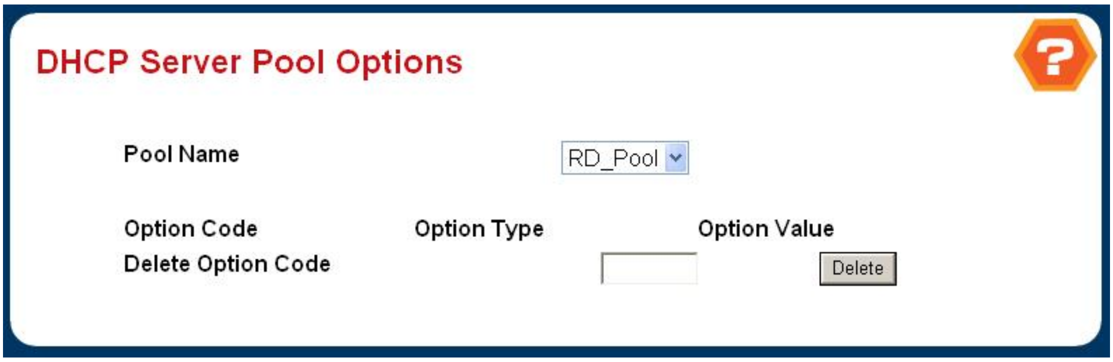
Command Buttons

- **Submit** - Creates/Modifies the Pool Configuration. Sends the updated configuration to the switch. Configuration changes take effect immediately.
- **Delete** - Deletes the Pool. This field is not visible to a user with readonly permission.

Note: The network ip address/mask of the switch shall be within the same as ip pool.

4.2.11.3 Pool Options

DHCP Server Pool Options



DHCP Server Pool Options

Pool Name RD_Pool

Option Code	Option Type	Option Value

Delete Option Code

Figure 4-2-54 DHCP Server Pool Options

Selection Criteria

- **Pool Name** - Shows all the existing Pool Names.

Non-Configurable Data

- **Option Code** - Specifies the Option Code configured for the selected Pool.
- **Option Type** - Specifies the Option Type against the Option Code configured for the selected pool.
  - ***Ascii***
  - ***Hex***
  - ***IP Address***
- **Option Value** - Specifies the Value against the Option Code configured for the selected pool.

Configurable Data

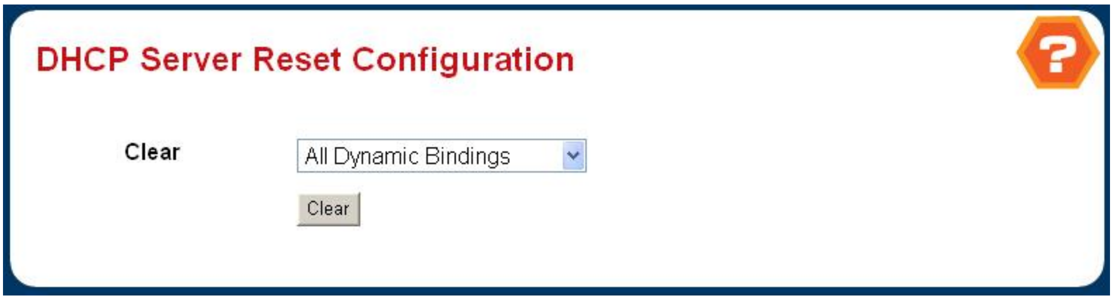
- **Delete Option Code** - Specifies the Option Code to be deleted for the selected Pool. This field is not visible to a user with readonly permission.

Command Buttons

- **Delete** - Deletes the Option Code for the selected Pool. This field is not visible to a user with readonly permission.

4.2.11.4 Reset Configuration

DHCP Server Reset Configuration



DHCP Server Reset Configuration

Clear: All Dynamic Bindings

Figure 4-2-55 DHCP Server Reset Configuration

Selection Criteria

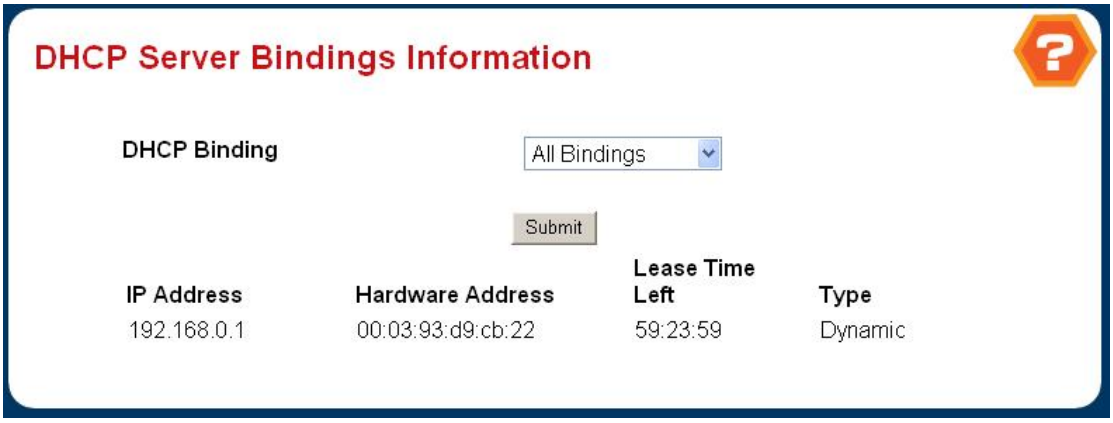
- **Clear** - Specifies whether All Dynamic Bindings/Specific Dynamic Binding/All Address Conflicts/Specific Address Conflict is to be deleted.
- **Clear IP Address** - IP Address against the Binding/Address Conflict to be cleared.This field appears only if the user has selected "Specific Dynamic Binding/Specific Address Conflict" in Clear.

Command Buttons

- **Clear** - Clears/Removes the Dynamic Binding/Address Conflict.

4.2.11.5 Bindings Information

DHCP Server Bindings Information



DHCP Server Bindings Information

DHCP Binding: All Bindings

IP Address	Hardware Address	Lease Time Left	Type
192.168.0.1	00:03:93:d9:cb:22	59:23:59	Dynamic

Figure 4-2-56 DHCP Server Bindings Information

Selection Criteria

- **DHCP Binding** - Specifies whether information is to be displayed for All/Specific Binding.
- **Binding IP Address** - IP Address against the Binding for which information is to be displayed. This field appears only if the user has selected "Specific Binding" in DHCP Binding.

Non-Configurable Data

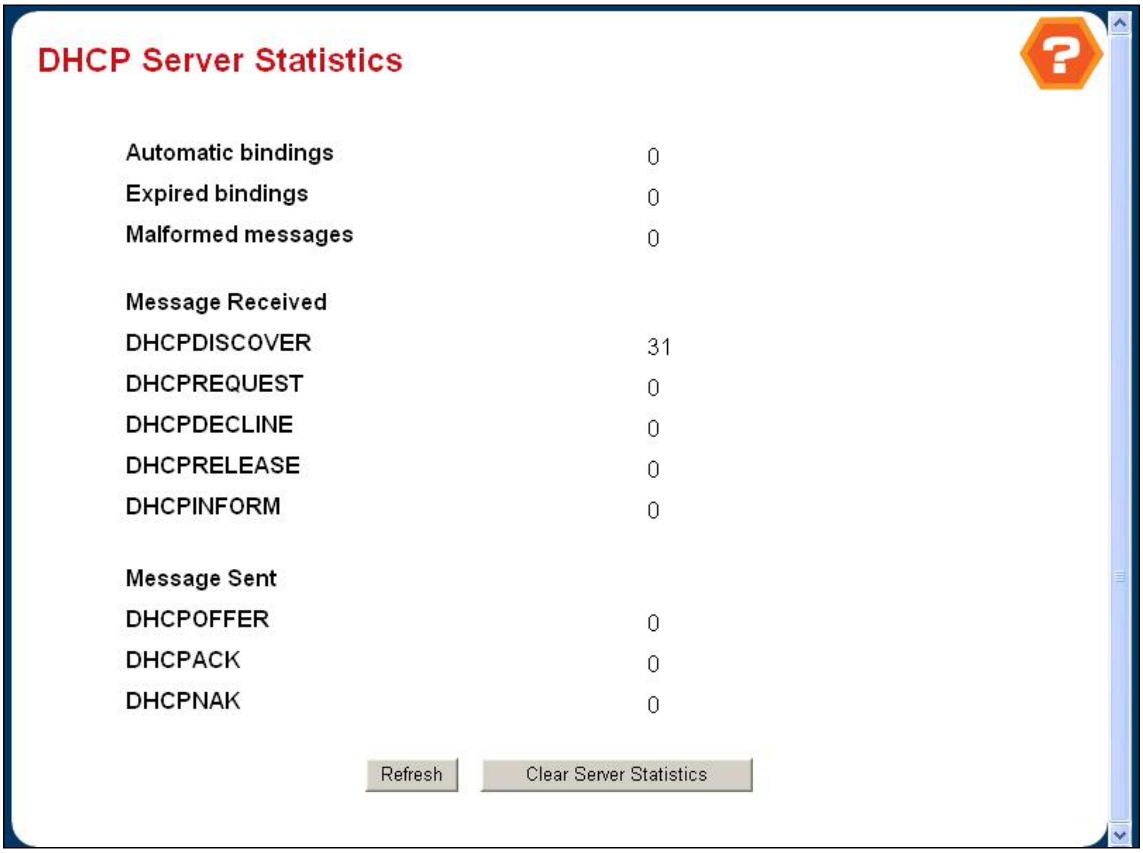
- **IP Address** - Specifies the Client's IP Address.
- **Hardware Address** - Specifies the Client's Hardware Address.
- **Lease Time** - Specifies the Lease time left in Days, Hours and Minutes dd:hh:mm format.
- **Type** - Specifies the Type of Binding: Dynamic / Manual.

Command Buttons

- **Submit** - Displays information for chosen Bindings.

4.2.11.6 Server Statistics

DHCP Server Statistics



DHCP Server Statistics

Automatic bindings	0
Expired bindings	0
Malformed messages	0
Message Received	
DHCPDISCOVER	31
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Message Sent	
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

Figure 4-2-57 Server Statistics

Non-Configurable Data

- **Automatic Bindings** - Specifies the number of Automatic Bindings on the DHCP Server.
- **Manual Bindings** - Specifies the number of Manual Bindings on the DHCP Server.
- **Expired Bindings** - Specifies the number of Expired Bindings on the DHCP Server.
- **Malformed Messages** - Specifies the number of the malformed messages.
- **DHCPDISCOVER** - Specifies the number of DHCPDISCOVER messages received by the DHCP Server.

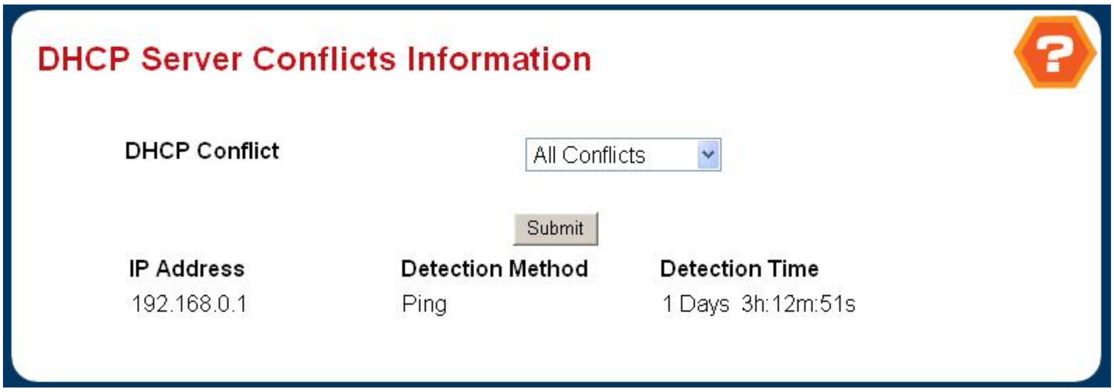
- **DHCPREQUEST** - Specifies the number of DHCPREQUEST messages received by the DHCP Server.
- **DHCPDECLINE** - Specifies the number of DHCPDECLINE messages received by the DHCP Server.
- **DHCPRELEASE** - Specifies the number of DHCPRELEASE messages received by the DHCP Server.
- **DHCPINFORM** - Specifies the number of DHCPINFORM messages received by the DHCP Server.
- **DHCPOFFER** - Specifies the number of DHCPOFFER messages sent by the DHCP Server.
- **DHCPACK** - Specifies the number of DHCPACK messages sent by the DHCP Server.
- **DHCPNAK** - Specifies the number of DHCPNAK messages sent by the DHCP Server.

Command Buttons

- **Refresh** - Refresh the data on the screen to the latest state.
- **Clear Server Statistics** - Reset DHCP Server Statistics.

4.2.11.7 Conflicts Information

DHCP Server Conflicts Information



DHCP Server Conflicts Information

DHCP Conflict: All Conflicts

IP Address	Detection Method	Detection Time
192.168.0.1	Ping	1 Days 3h:12m:51s

Figure 4-2-58 DHCP Server Conflicts Information

Selection Criteria

- **DHCP Conflict** - Specifies whether information is to be displayed for a Specific Address Conflict or for All Address Conflicts.
- **Conflict IP Address** - IP Address of the conflict to be shown. This field appears only if the user has selected "Specific Address Conflict" in DHCP Conflict.

Non-Configurable Data

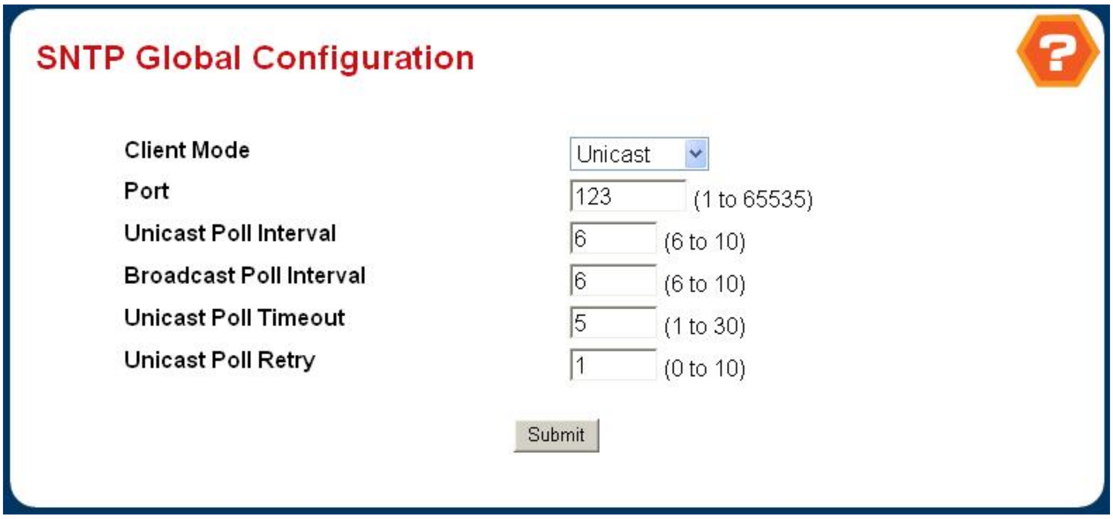
- **IP Address** - Specifies the IP Address of the host as recorded on the DHCP server.
- **Detection Method** - Specifies the manner in which the IP address of the hosts were found on the DHCP Server.
- **Detection Time** - Specifies the time when the conflict was detected in N days NNh:NNm:NNs format with respect to the system up time.

Command Buttons

- **Submit** - Displays information about the chosen conflict(s).

4.2.12 SNTP

4.2.12.1 Global Configuration



SNTP Global Configuration

Client Mode	Unicast
Port	123 (1 to 65535)
Unicast Poll Interval	6 (6 to 10)
Broadcast Poll Interval	6 (6 to 10)
Unicast Poll Timeout	5 (1 to 30)
Unicast Poll Retry	1 (0 to 10)

Figure 4-2-59 SNTP Global Configuration

Configurable Data

◦ **Client Mode** - Specifies the mode of operation of SNTP Client. An SNTP client may operate in one of the following modes.

- ***Disable***- SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed.
- ***Unicast***- SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server.
- ***Broadcast*** - SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope.

Default value is **Disable.**

◦ **Port** - Specifies the local UDP port to listen for responses/broadcasts. Allowed range is (1 to 65535). Default value is 123.

◦ **Unicast Poll Interval** - Specifies the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. Allowed range is (6 to 10). Default value is 6.

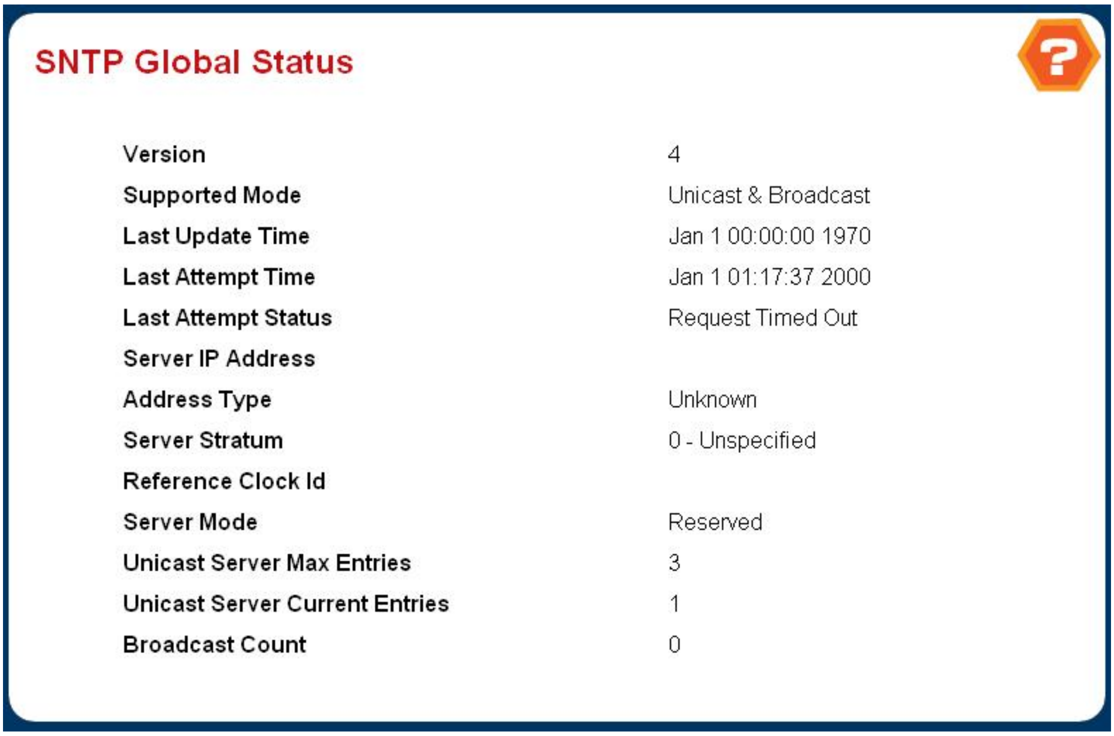
◦ **Broadcast Poll Interval** - Specifies the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. Allowed range is (6 to 10). Default value is 6.

- **Unicast Poll Timeout** - Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.
- **Unicast Poll Retry** - Specifies the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. Allowed range is (0 to 10). Default value is 1.

Command Buttons

- **Submit** - Sends the updated configuration to the switch. Configuration changes take effect immediately.

4.2.12.2 Global Status



SNTP Global Status

Version	4
Supported Mode	Unicast & Broadcast
Last Update Time	Jan 1 00:00:00 1970
Last Attempt Time	Jan 1 01:17:37 2000
Last Attempt Status	Request Timed Out
Server IP Address	
Address Type	Unknown
Server Stratum	0 - Unspecified
Reference Clock Id	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	1
Broadcast Count	0

Figure 4-2-60 SNTP Global Status

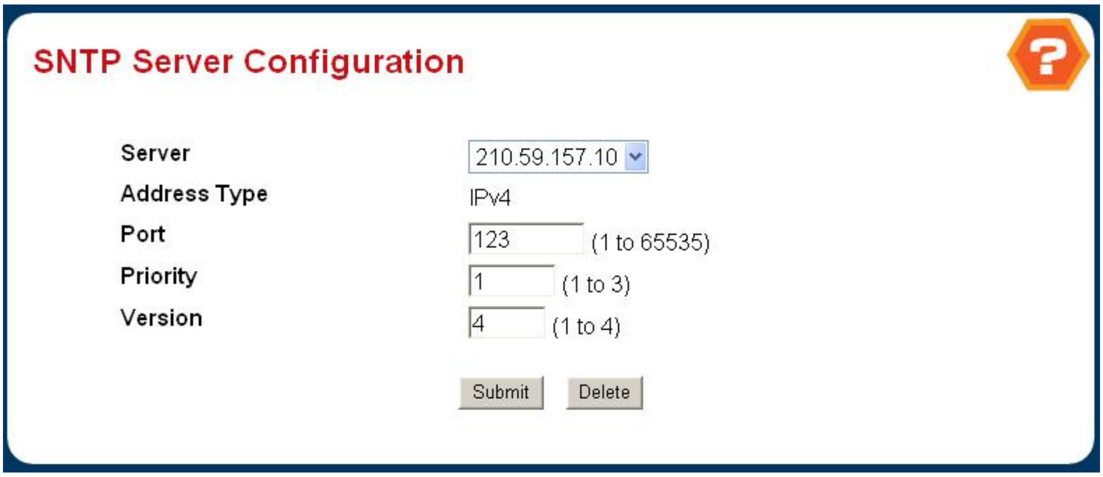
Non-Configurable Data

- **Version** - Specifies the SNTP Version the client supports.
- **Supported Mode** - Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.
- **Last Update Time** - Specifies the local date and time (UTC) the SNTP client last updated the system clock.
- **Last Attempt Time** - Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
- **Last Attempt Status** - Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes.

- ***Other***None of the following enumeration values.
- ***Success***The SNTP operation was successful and the system time was updated.
- ***Request Timed Out***A directed SNTP request timed out without receiving a response from the SNTP server.
- ***Bad Date Encoded***The time provided by the SNTP server is not valid.
- ***Version Not Supported***TheSNTP version supported by the server is not compatible with the version supported by the client.
- ***Server Unsychronized***The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.
- ***Server Kiss Of Death***The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.

- **Server IP Address** - Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.
- **Address Type** - Specifies the address type of the SNTP Server address for the last received valid packet.
- **Server Stratum** - Specifies the claimed stratum of the server for the last received valid packet.
- **Reference Clock Id** - Specifies the reference clock identifier of the server for the last received valid packet.
- **Server Mode** - Specifies the mode of the server for the last received valid packet.
- **Unicast Sever Max Entries** - Specifies the maximum number of unicast server entries that can be configured on this client.
- **Unicast Server Current Entries** - Specifies the number of current valid unicast server entries configured for this client.
- **Broadcast Count** - Specifies the number of unsolicited broadcast SNTP messages that have been received and processed by the SNTP client since last reboot.

4.2.12.3 Server Configuration



SNTP Server Configuration

Server	210.59.157.10
Address Type	IPv4
Port	123 (1 to 65535)
Priority	1 (1 to 3)
Version	4 (1 to 4)

Figure 4-2-61 SNTP Server Configuration

Configurable Data

- **Server** - Specifies all the existing Server Addresses along with an additional option "Create". When the user selects "Create" another text box "Address" appears where the user may enter Address for Server to be configured.
- **Address** - Specifies the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
- **Address Type** - Specifies the address type of the configured SNTP Server address. Allowed type is :

  - ***IPV4***

  Default value is **Unknown**

- **Port** - Specifies the port on the server to which SNTP requests are to be sent. Allowed range is (1 to 65535). Default value is 123.
- **Priority** - Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests will be sent. The client continues sending requests to different servers until a successful response is received or all servers are exhausted. This object indicates the order in which to query the servers. A server entry with a precedence of 1 will be queried before a server with a priority of 2, and so forth. If more than one server has the same priority then the requesting order will follow the lexicographical ordering of the entries in this table. Allowed range is (1 to 3). Default value is 1.
- **Version** - Specifies the NTP Version running on the server. Allowed range is (1 to 4). Default value is 4.

Command Buttons

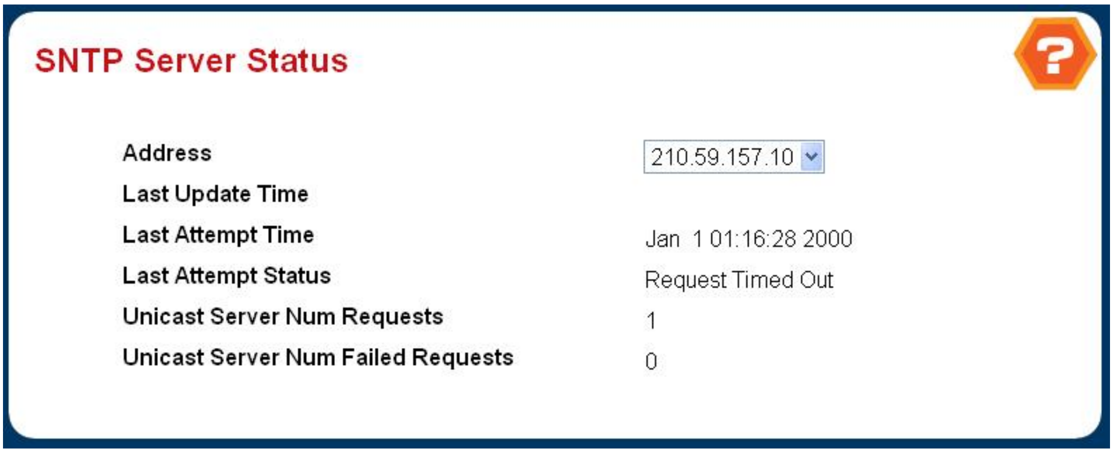
- **Submit** - Sends the updated configuration to the switch. Configuration changes take effect immediately.
- **Delete** - Deletes the SNTP Server entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Notice: It is recommended that you research any time server selection to ensure that it can meet your specific time server requirements. Any NTP time server selection should be evaluated to determine if the server in question meets your specific time server requirements.

For more detail about the Time Server and Time Server List, please refer to the following URL:

http://ntp.isc.org/bin/view/Servers/WebHome
http://ntp.isc.org/bin/view/Servers/NTPPoolServers
http://support.microsoft.com/kb/262680/en-us

4.2.12.4 Server Status



SNTP Server Status

Address	210.59.157.10
Last Update Time	
Last Attempt Time	Jan 1 01:16:28 2000
Last Attempt Status	Request Timed Out
Unicast Server Num Requests	1
Unicast Server Num Failed Requests	0

Figure 4-2-62 SNTP Server Status

Non-Configurable Data

- **Address** - Specifies all the existing Server Addresses. If no Server configuration exists, a message saying "No SNTP server exists" flashes on the screen.
- **Last Update Time** - Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
- **Last Attempt Time** - Specifies the local date and time (UTC) that this SNTP server was last queried.
- **Last Attempt Status** - Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed.

  - ***Other***None of the following enumeration values.
  - ***Success***The SNTP operation was successful and the system time was updated.
  - ***Request Timed Out***A directed SNTP request timed out without receiving a response from the SNTP server.
  - ***Bad Date Encoded***The time provided by the SNTP server is not valid.
  - ***Version Not Supported***TheSNTP version supported by the server is not compatible with the version supported by the client.
  - ***Server Unsychronized***The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.
  - ***Server Kiss Of Death***The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.

- **Unicast Server Num Requests** - Specifies the number of SNTP requests made to this server since last agent reboot.
- **Unicast Server Num Failed Requests** - Specifies the number of failed SNTP requests made to this server since last reboot.

4.3 Switching

This page provides all system operation for configuring VLAN, Port-based VLAN, Spanning Tree, Port Aggregation, and Multicast Support.

The Switch page contains links to the following topics:

- **VLAN**
- **Protocol-based VLAN**
- **Filters**
- **GARP**
- **IGMP Snooping**
- **Port Channel**
- **Multicast Forwarding Database**
- **Spanning Tree**
- **Class of Service**
- **Port Security**

4.3.1 VLAN

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN 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.

VLAN 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.

Notice:

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
3. The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

IEEE 802.1Q VLANs

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

VLAN 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.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN 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 VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN 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.

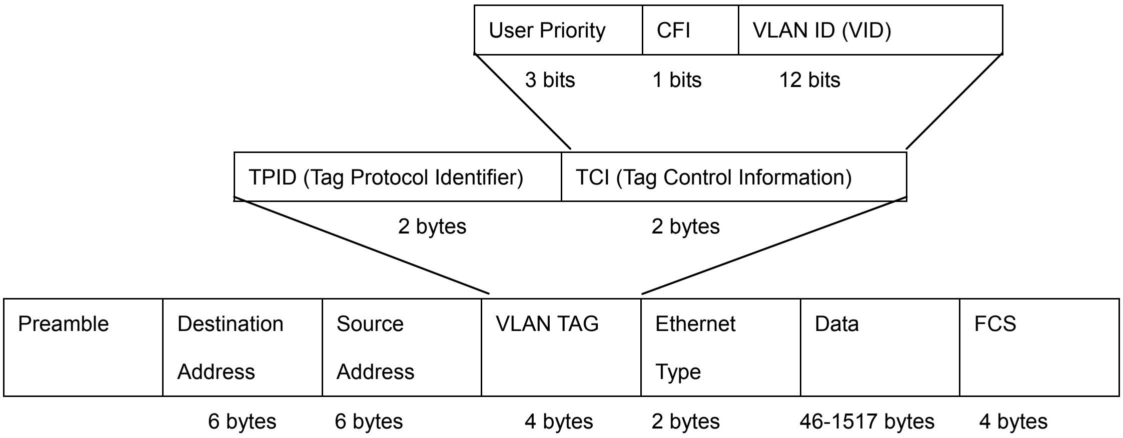
Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allow VLAN to work with legacy switches that don’t recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection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

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.

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 Ether Type field. When a packet's Ether Type 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 VLAN 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.

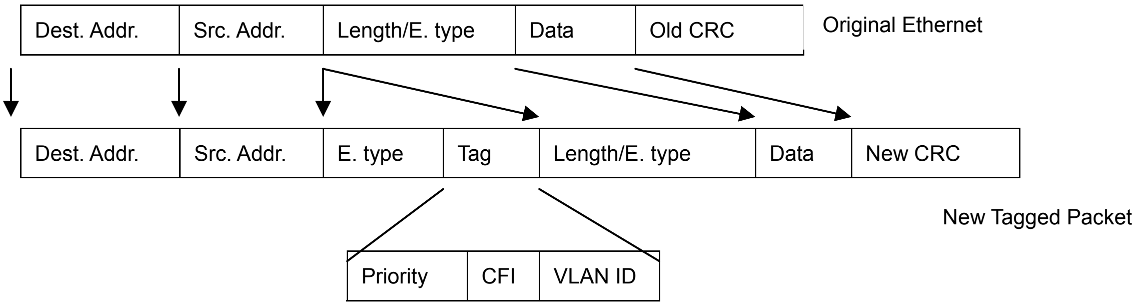
802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/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.

Adding an IEEE802.1Q 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 VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN 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 VLAN 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 PVID within the switch to VID 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 VID 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 VID 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.

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 VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

VLAN and Link aggregation Groups

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

4.3.1.1 VLAN Configuration

802.1Q VLAN Configuration

There are up to 4041 configurable VLAN groups. By default when 802.1Q is enabled, all ports on the switch belong to default VLAN (VID 1). The default VLAN cannot be deleted.

Understand nomenclature of the Switch

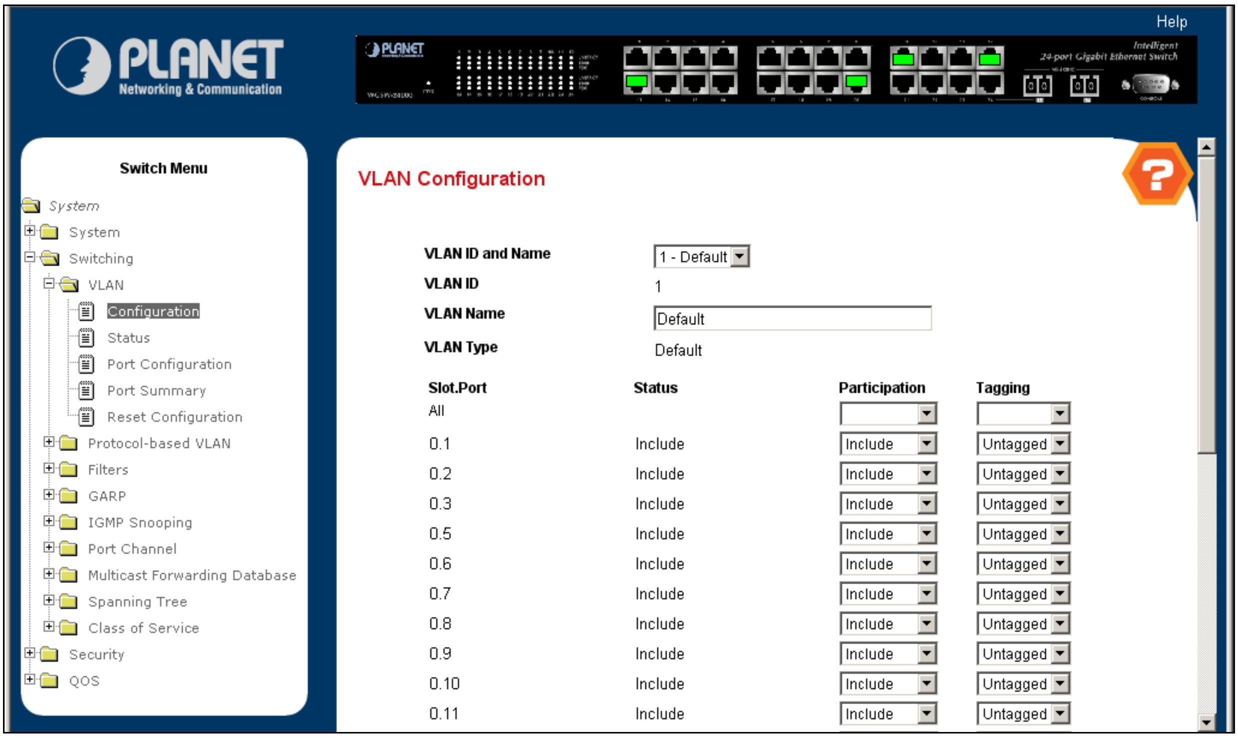
Tagging and Untagging

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

◦ **Tagging:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

◦ **Untagging:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into 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.

Frame Income Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged



VLAN Configuration

VLAN ID and Name: 1 - Default

VLAN ID: 1

VLAN Name: Default

VLAN Type: Default

Slot.Port	Status	Participation	Tagging
All			
0.1	Include	Include	Untagged
0.2	Include	Include	Untagged
0.3	Include	Include	Untagged
0.5	Include	Include	Untagged
0.6	Include	Include	Untagged
0.7	Include	Include	Untagged
0.8	Include	Include	Untagged
0.9	Include	Include	Untagged
0.10	Include	Include	Untagged
0.11	Include	Include	Untagged

Figure 4-3-1 VLAN Configuration

Selection Criteria

- **VLAN ID and Name -** You can use this screen to reconfigure an existing VLAN, or to create a new one. Use this pulldown menu to select one of the existing VLANs, or select 'Create' to add a new one.

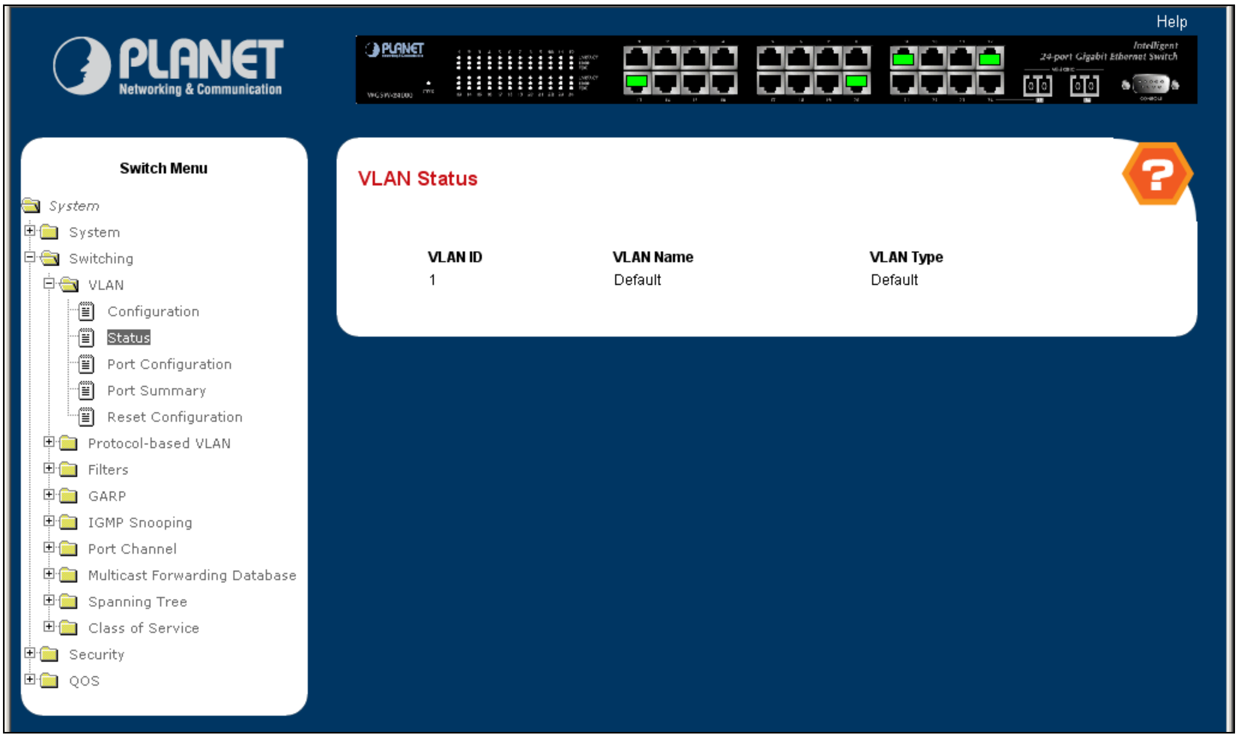
Configurable Data

- **VLAN ID -** Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is (1 to 4093).
- **VLAN Name -** Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of 'Default'.
- **VLAN Type -** This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type 'Default'. When you create a VLAN, using this screen, its type will always be 'Static'. A VLAN that is created by GVRP registration initially has a type of 'Dynamic'. You may use this pull-down menu to change its type to 'Static'.
- **Participation -** Use this field to specify whether a port will participate in this VLAN. The factory default is **'Autodetect'**. The possible values are:
- **Include -** This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.
- **Exclude -** This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.
- **Autodetect -** Specifies that port may be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless it receives a GVRP request. This is equivalent to registration normal in the IEEE 802.1Q standard.
- **Tagging -** Select the tagging behavior for this port in this VLAN. The factory default is **'Untagged'**. The possible values are:
- **Tagged -** all frames transmitted for this VLAN will be tagged.
- **Untagged -** all frames transmitted for this VLAN will be untagged.

4.3.1.2 VLAN Status

This page displays the status of all currently configured VLANs.

- **VLAN ID -** The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is (1 to 4093) .
- **VLAN Name -** The name of the VLAN. VLAN ID 1 is always named `Default`.
- **VLAN Type -** The VLAN type:
  - **Default** (VLAN ID = 1) -- always present
  - **Static** -- a VLAN you have configured
  - **Dynamic** -- a VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove



VLAN Status

VLAN ID	VLAN Name	VLAN Type
1	Default	Default

Figure 4-3-2 VLAN Status

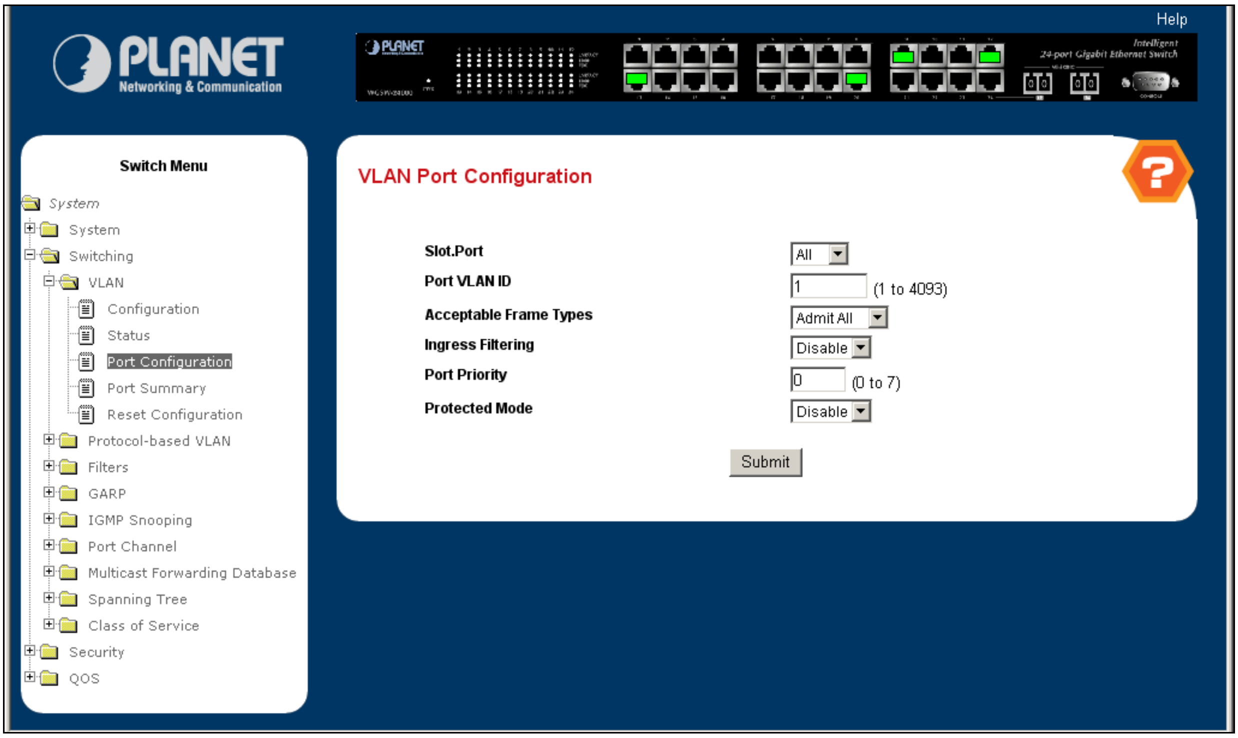
4.3.1.3 VLAN Port Configuration

Selection Criteria

- **Slot.Port -** Select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to same values.

Configurable Data

- **Port VLAN ID -** Specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The factory default is 1.
- **Acceptable Frame Types -** Specify how you want the port to handle untagged and priority tagged frames. If you select 'VLAN only', the port will discard any untagged or priority tagged frames it receives. If you select 'Admit All', untagged and priority tagged frames received on the port will be accepted and assigned the value of the Port VLAN ID for this port. Whichever you select, VLAN tagged frames will be forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is 'Admit All'.
- **Ingress Filtering -** Specify how you want the port to handle tagged frames. If you enable Ingress Filtering on the pulldown menu, a tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. If you select disable from the pulldown menu, all tagged frames will be accepted. The factory default is disable.
- **Port Priority - S**pecify the default 802.1p priority assigned to untagged packets arriving at the port.



VLAN Port Configuration

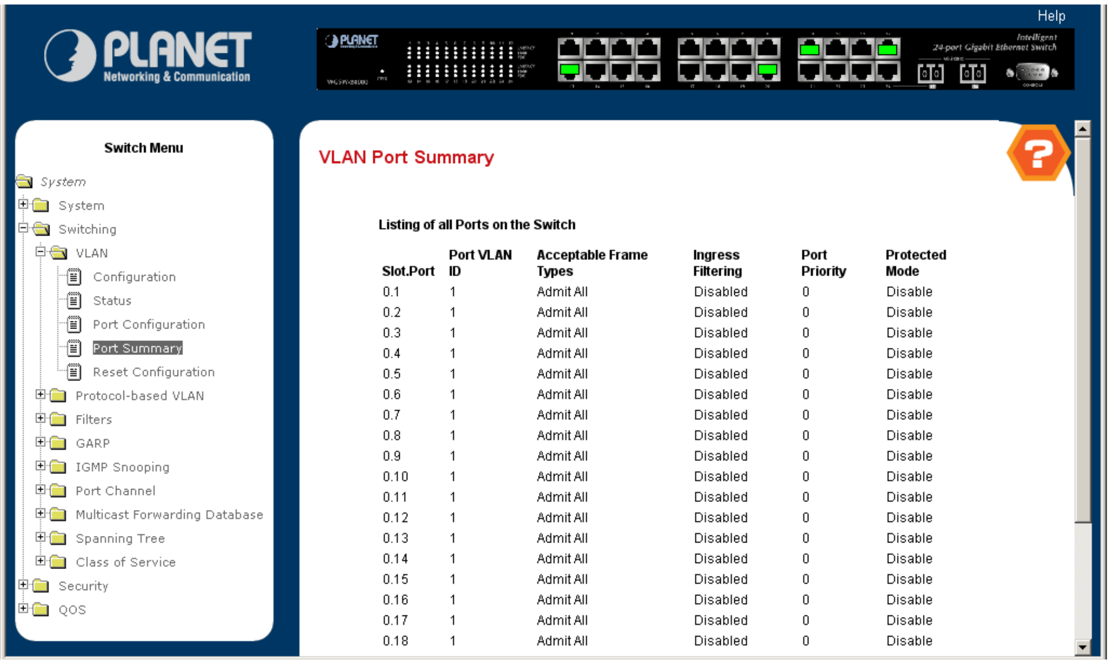
Slot.Port	All
Port VLAN ID	1 (1 to 4093)
Acceptable Frame Types	Admit All
Ingress Filtering	Disable
Port Priority	0 (0 to 7)
Protected Mode	Disable

Figure 4-3-3 VLAN Port Configuration

4.3.1.4 VLAN Port Summary

This page shows the configured VLAN parameters.

- **Slot.Port -** The interface.
- **Port VLAN ID -** The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port.
- **Acceptable Frame Types -** Specifies the types of frames that may be received on this port. The options are **'VLAN only'** and **'Admit All'**. When set to **'VLAN only'**, untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
- **Ingress Filtering -** When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.



VLAN Port Summary

Listing of all Ports on the Switch

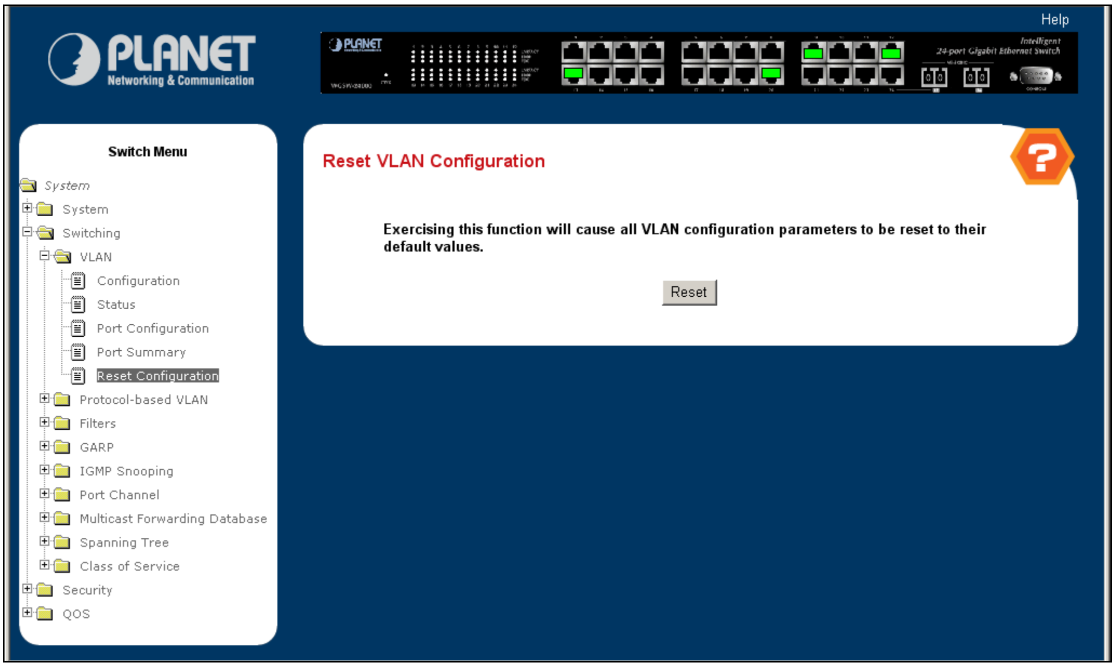
Slot.Port	Port VLAN ID	Acceptable Frame Types	Ingress Filtering	Port Priority	Protected Mode
0.1	1	Admit All	Disabled	0	Disable
0.2	1	Admit All	Disabled	0	Disable
0.3	1	Admit All	Disabled	0	Disable
0.4	1	Admit All	Disabled	0	Disable
0.5	1	Admit All	Disabled	0	Disable
0.6	1	Admit All	Disabled	0	Disable
0.7	1	Admit All	Disabled	0	Disable
0.8	1	Admit All	Disabled	0	Disable
0.9	1	Admit All	Disabled	0	Disable
0.10	1	Admit All	Disabled	0	Disable
0.11	1	Admit All	Disabled	0	Disable
0.12	1	Admit All	Disabled	0	Disable
0.13	1	Admit All	Disabled	0	Disable
0.14	1	Admit All	Disabled	0	Disable
0.15	1	Admit All	Disabled	0	Disable
0.16	1	Admit All	Disabled	0	Disable
0.17	1	Admit All	Disabled	0	Disable
0.18	1	Admit All	Disabled	0	Disable

Figure 4-3-4 VLAN Port Summary

4.3.1.5 VLAN Reset Configuration

If you select this button and confirm your selection on the next screen, all VLAN configuration parameters will be reset to their factory default values. Also, all VLANs, except for the default VLAN, will be deleted. The factory default values are:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with Ingress Filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.
- GVRP is disabled for the switch and all dynamic entries are cleared.



Reset VLAN Configuration

Exercising this function will cause all VLAN configuration parameters to be reset to their default values.

Figure 4-3-5 Reset VLAN Configuration

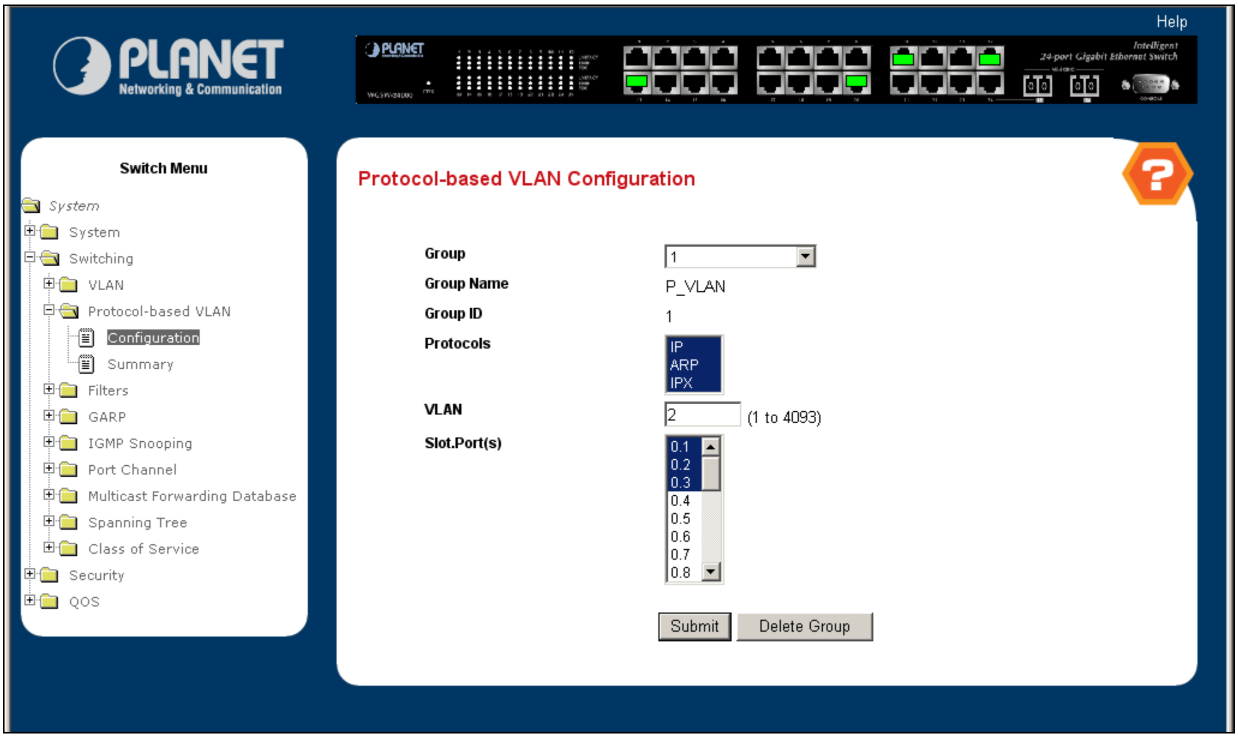
4.3.2 Protocol-based VLAN

4.3.2.1 Configuration

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port- (IEEE 802.1Q) or protocol-based VLANs, untagged packets will be assigned to VLAN 1. You can override this behavior by defining either port-based VLANs or protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard, and are not included in protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol will be assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID - either the default PVID (1) or a PVID you have specifically assigned to the port using the Port VLAN Configuration screen.

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group you will choose a name and a Group ID will be assigned automatically.



Protocol-based VLAN Configuration

Group	1
Group Name	P_VLAN
Group ID	1
Protocols	IP ARP IPX
VLAN	2 (1 to 4093)
Slot.Port(s)	0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8

Figure 4-3-6 Protocol-based VLAN Configuration

Selection Criteria

- **Group ID -** You can use this screen to reconfigure or delete an existing protocol-based VLAN, or create a new one. Use this pulldown menu to select one of the existing PBVLANs, or select 'Create' to add a new one. A Group ID number will be assigned automatically when you create a new group. You can create up to 128 groups.

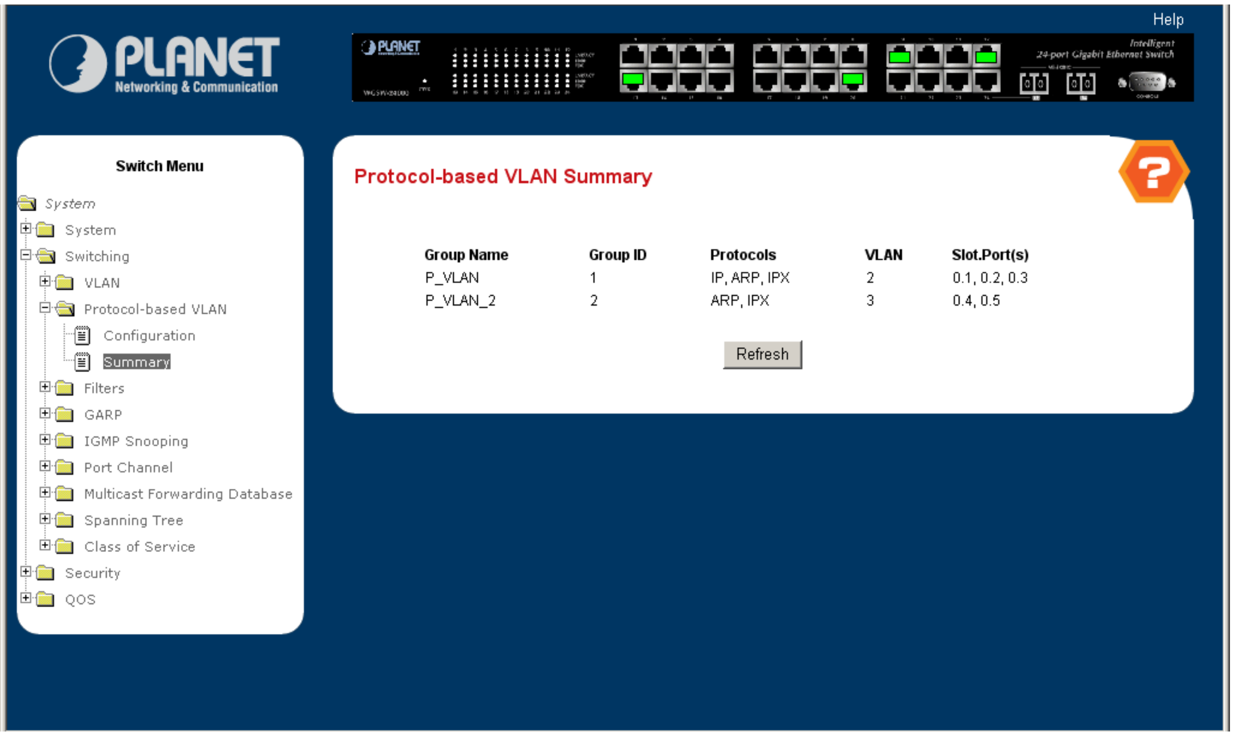
Configurable Data

- **Group Name -** Use this field to assign a name to a new group. You may enter up to 16 characters.
- **Protocol(s) -** Select the protocols you want to be associated with the group. There are three configurable protocols: IP, IPX, ARP. Hold down the control key to select more than one protocol.

- **IP -** IP is a network layer protocol that provides a connectionless service for the delivery of data.
- **ARP -** Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses
- **IPX -** The Internetwork Packet Exchange (IPX) is a connectionless datagram Network-layer protocol that forwards data over a network.
- **VLAN -** VLAN can be any number in the range of (1 to 4093) . All the ports in the group will assign this VLAN ID to untagged packets received for the protocols you included in this group.
- **Slot.Port(s) -** Select the interface(s) you want to be included in the group. Note that a given interface can only belong to one group for a given protocol. If you have already added interface 0.1 to a group for IP, you cannot add it to another group that also includes IP, although you could add it to a new group for IPX.

4.3.2.2 Protocol-based VLAN Summary

- **Group Name -** The name associated with the group. Group names can be up to 16 characters long. The maximum number of groups allowed is 128.
- **Group ID -** The number used to identify the group. It was automatically assigned when you created the group.
- **Protocol(s) -** The protocol(s) that belongs to the group. There are three configurable protocols: IP, IPX, ARP.
- **IP -** IP is a network layer protocol that provides a connectionless service for the delivery of data.
- **ARP -** Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses
- **IPX -** The Internetwork Packet Exchange (IPX) is a connectionless datagram Network-layer protocol that forwards data over a network.
- **VLAN -** The VLAN ID associated with the group.
- **Slot.Port(s) -** The interfaces associated with the group.



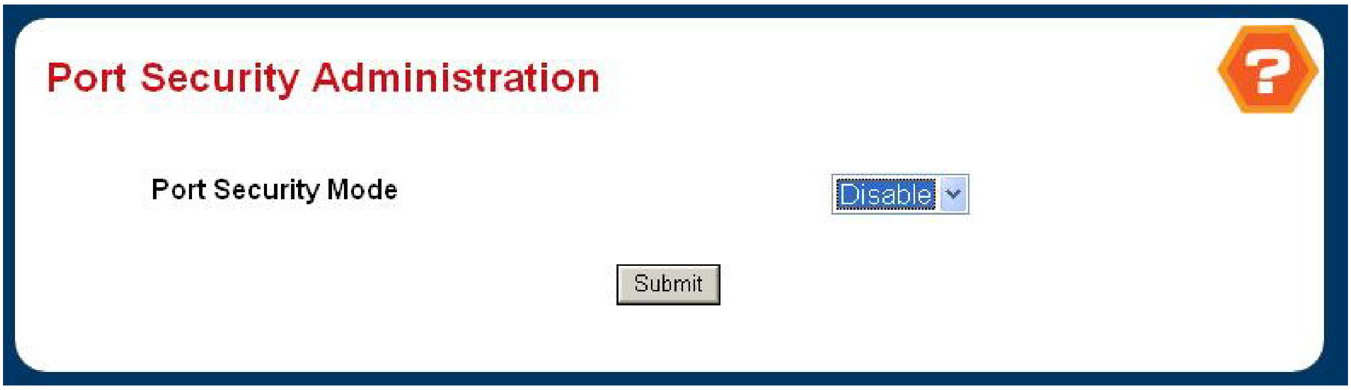
Protocol-based VLAN Summary

Group Name	Group ID	Protocols	VLAN	Slot.Port(s)
P_VLAN	1	IP, ARP, IPX	2	0.1, 0.2, 0.3
P_VLAN_2	2	ARP, IPX	3	0.4, 0.5

Figure 4-3-7 Protocol-based VLAN Summary

4.3.3 Port Security

4.3.3.1 Port Security Administration



Port Security Administration

Port Security Mode: Disable

Figure 4-3-8 Port Security Administration

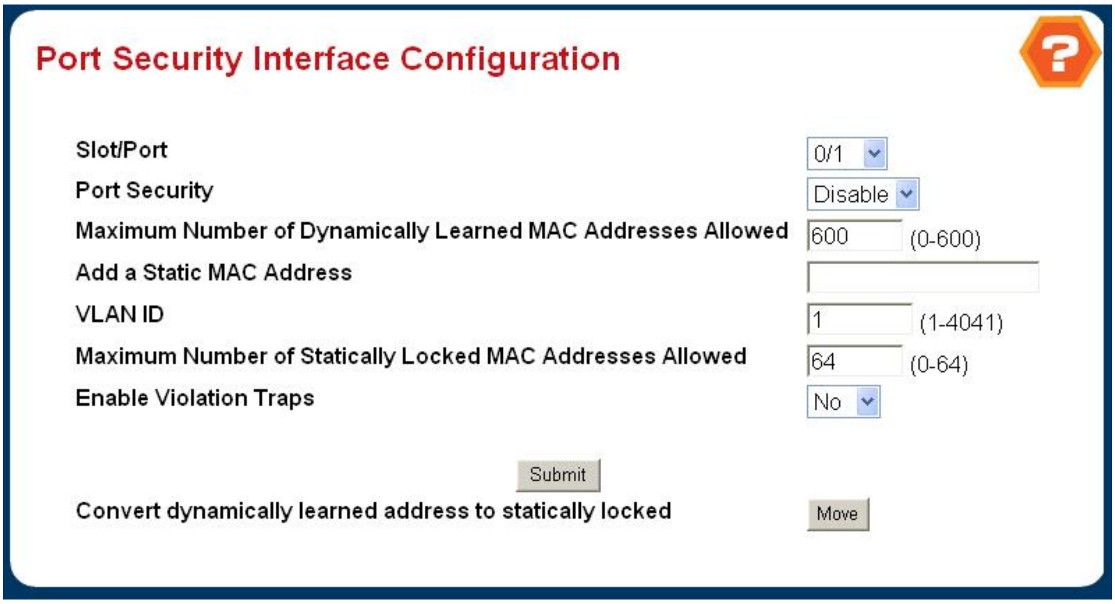
Configurable Data

- **Port Security Mode** - Enables or disables the Port Security feature.

Command Buttons

- **Submit** - Applies the new configuration and causes the changes to take effect. These changes will not be retained across a power cycle unless a save configuration is performed.

4.3.3.2 Port Security Interface Configuration



Port Security Interface Configuration

Slot/Port	0/1	
Port Security	Disable	
Maximum Number of Dynamically Learned MAC Addresses Allowed	600	(0-600)
Add a Static MAC Address		
VLAN ID	1	(1-4041)
Maximum Number of Statically Locked MAC Addresses Allowed	64	(0-64)
Enable Violation Traps	No	

Convert dynamically learned address to statically locked

Figure 4-3-9 Port Security Interface Configuration

Selection Criteria

- **Unit/Slot/Port** - Selects the interface to be configured.

Configurable Data

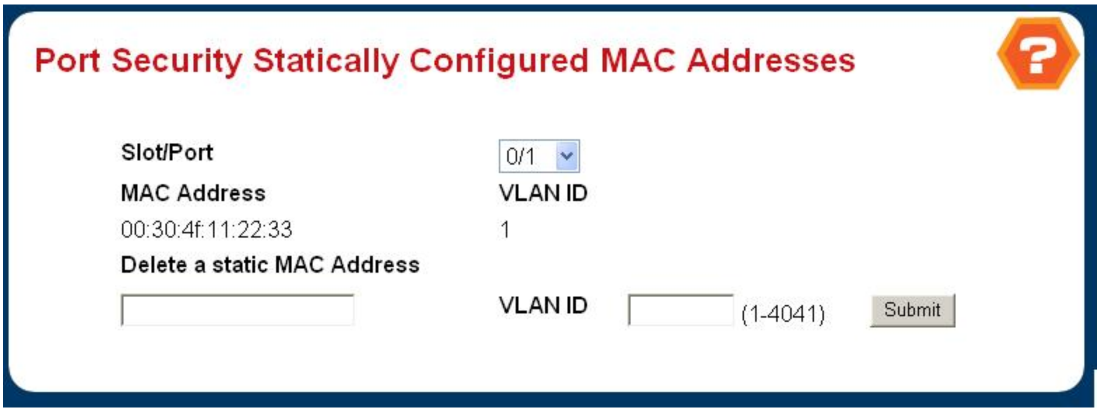
- **Port Security** - Enables or disables the Port Security feature for the selected interface.
- **Maximum Dynamic MAC Addresses allowed** - Sets the maximum number of dynamically learned MAC addresses on the selected interface.
- **Add a static MAC address** - Adds a MAC address to the list of statically locked MAC addresses for the selected interface.
- **VLAN ID** - Adds a corresponding VLAN ID for the MAC Address being added to the list of statically locked MAC addresses for the selected interface.
- **Maximum static MAC Addresses allowed** - Sets the maximum number of statically locked MAC addresses on the selected interface.
- **Enable violation traps** - Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Command Buttons

- **Submit** - Applies the new configuration and causes the changes to take effect. These changes will not be retained across a power cycle unless a save configuration is performed.
- **Move** - Converts a dynamically learned MAC address to a statically locked address. The Dynamic MAC address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.

Notice: The format of entering MAC Address should be ***xx : xx : xx : xx : xx : xx***

4.3.3.3 Port Security Static



Port Security Statically Configured MAC Addresses

Slot/Port	0/1
MAC Address	VLAN ID
00:30:4f:11:22:33	1

Delete a static MAC Address

VLAN ID (1-4041)

Figure 4-3-10 Port Security Statically Configured MAC Address

Port Security Statically Configured MAC Addresses

Selection Criteria

- **Unit/Slot/Port** - Select the physical interface for which you want to display data.
- **VLAN ID** - selects the VLAN ID corresponding to the MAC address being deleted.

Configurable data

- **MAC Address** - Accepts user input for the MAC address to be deleted.

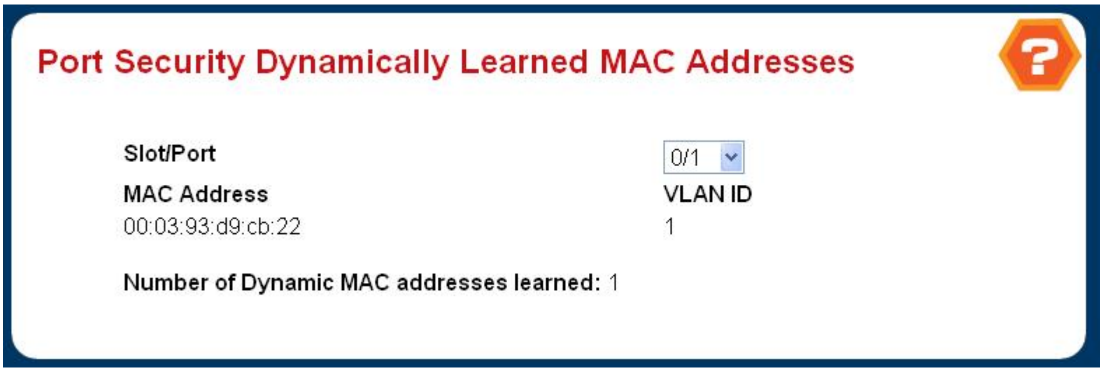
Non-configurable data

- **MAC Address** - Displays the user specified statically locked MAC address.
- **VLAN ID** - Displays the VLAN ID corresponding to the MAC address.
- **Delete a Static MAC Address** - Deletes the MAC address from the Port-Security Static MAC address table.
- **VLAN ID** - Displays the VLAN ID corresponding to the MAC address to be deleted from the Static list.

Command Buttons

- **Submit** - Applies the new configuration and causes the changes to take effect. These changes will not be retained across a power cycle unless a save configuration is performed.

4.3.3.4 Port Security Dynamic



Port Security Dynamically Learned MAC Addresses

Slot/Port 0/1

MAC Address	VLAN ID
00:03:93:d9:cb:22	1

Number of Dynamic MAC addresses learned: 1

Figure 4-3-11 Port Security Dynamically Learned MAC Address

Port Security Dynamically Learned MAC Addresses.

Selection Criteria

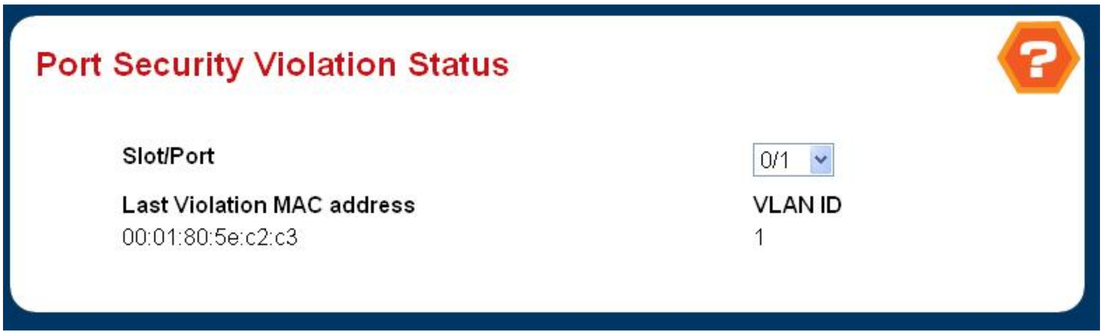
◦ **unit/slot/port** - Select the physical interface for which you want to display data.

Non-configurable data

◦ **MAC Address** - Displays the allowable MAC address learned on a specific port.

◦ **VLAN id** - Displays the VLAN id corresponding to the MAC address.

4.3.3.5 Port Security Violation Status



Port Security Violation Status

Slot/Port 0/1

Last Violation MAC address	VLAN ID
00:01:80:5e:c2:c3	1

Figure 4-3-12 Port Security Violation Status

Selection Criteria

◦ **Unit/Slot/Port** - Select the physical interface for which you want to display data.

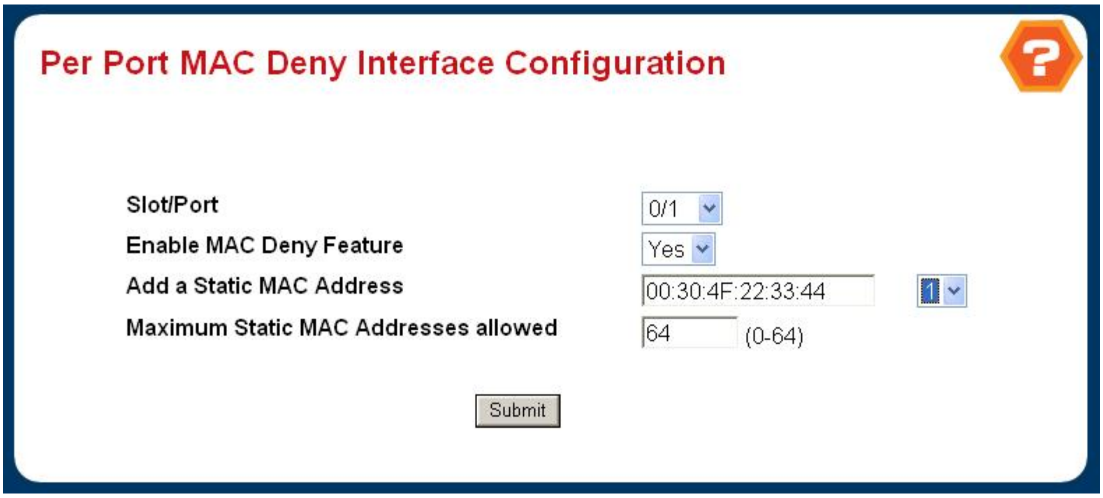
Non-configurable data

◦ **Last Violation MAC Address** - Displays the source MAC address of the last packet that was discarded at a locked port.

◦ **VLAN ID** - Displays the VLAN ID corresponding to the Last Violation MAC address.

4.3.3.6 Port MAC Deny

This page allows setting up per Port Mac Deny Interface Configuration



Per Port MAC Deny Interface Configuration

Slot/Port 0/1

Enable MAC Deny Feature Yes

Add a Static MAC Address 00:30:4F:22:33:44 1

Maximum Static MAC Addresses allowed 64 (0-64)

Figure 4-3-13 Per Port MAC Deny Interface Configuration

Selection Criteria

- **unit/slot/port** - Selects the interface to be configured.

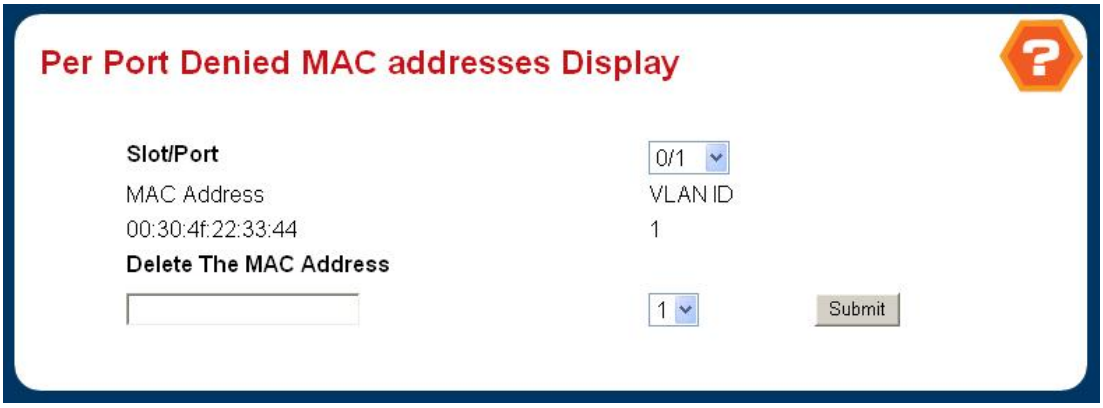
Configurable Data

- **Enable MAC Deny Feature** - Used to enable or disable the MAC Deny Fe ature for the selected interface.
- **Add a static MAC address and vlan id**- Adds a MAC address and a corr esonding vid to the list of statically locked MAC addresses for the selected int erface.
- **Maximum static MAC Addresses allowed**- Sets the maximum number of dy namically locked MAC addresses on the selected interface.

Command Buttons

- **Submit** - Applies the new configuration and causes the changes to take effect.These changes will not be retained across a pow er cycle unless a save configuration is performed.

4.3.3.7 Port MAC Deny Listing



Per Port Denied MAC addresses Display

Slot/Port 0/1

MAC Address	VLAN ID
00:30:4f:22:33:44	1

Delete The MAC Address

Figure 4-3-14 Per Port Denied MAC Address Display

Selection Criteria

◦ **unit/slot/port** - Selects the interface to be configured.

Non-configurable data

◦ **MAC Address** - Displays the MAC addresses learned on a specific port.

◦ **VLAN ID** - Displays the VLAN ID corresponding to the MAC address.

◦ **Number of Dynamic MAC addresses learned** - Displays the number of dynamically learned MAC addresses on a specific port.

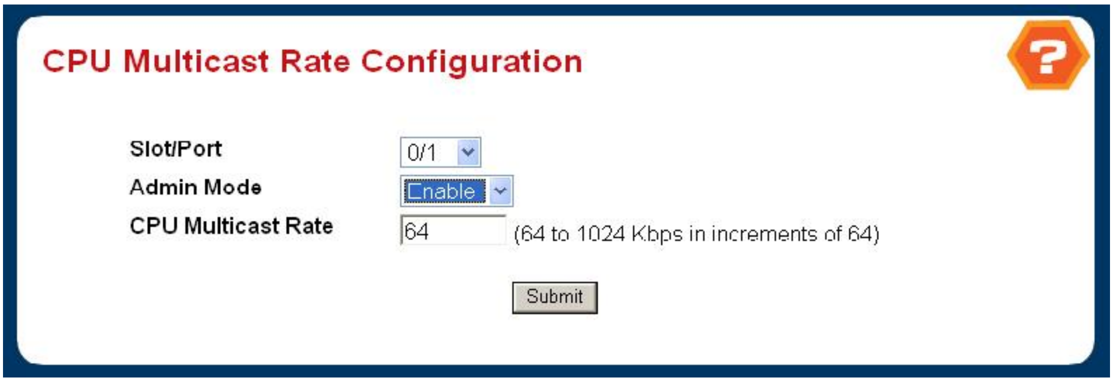
Configurable Data

◦ **Delete the MAC address and vlan id**- Deletes a MAC address and the c orresonding vid from the list of denied MAC addresses for the selected interface .

Command Buttons

◦ **Submit** - Applies the new configuration and causes the changes to ta ke effect.These changes will not be retained across a power cycle unless a save configuration is performed.

4.3.3.8 CPU Multicast Configuration



CPU Multicast Rate Configuration

Slot/Port: 0/1

Admin Mode: Enable

CPU Multicast Rate: 64 (64 to 1024 Kbps in increments of 64)

Figure 4-3-15 CPU Multicast Rate Configuration

Selection Criteria

◦ **unit/slot/port** - Selects the interface to be configured.

Configurable Data

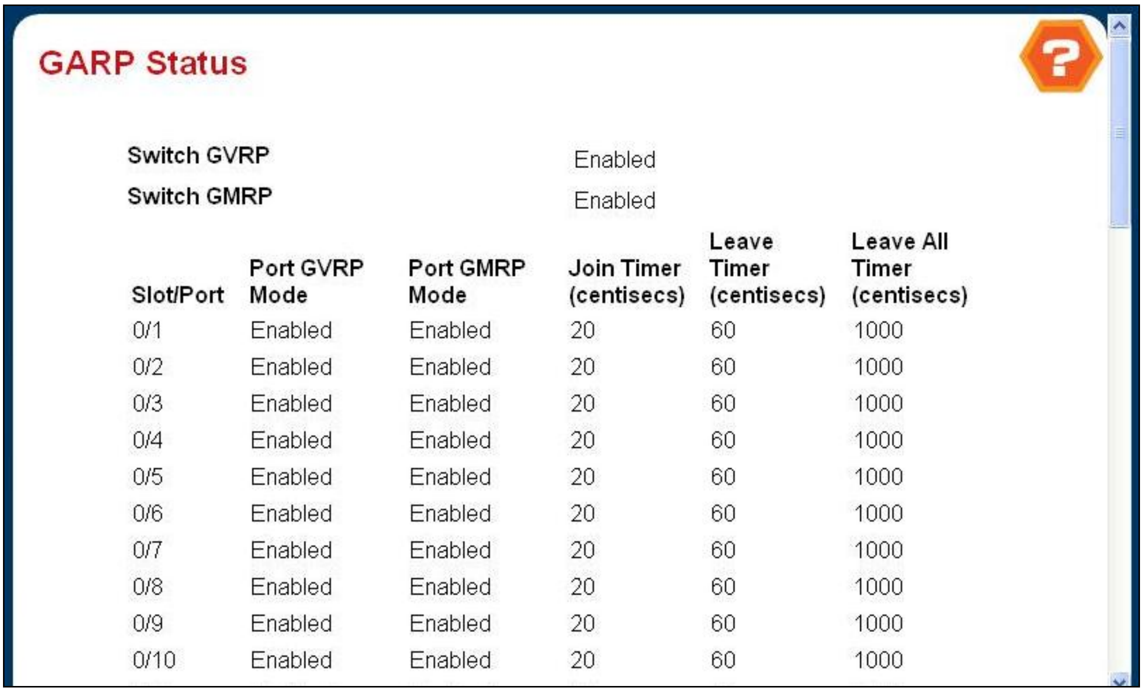
◦ **Admin Mode** - Specifies whether Admin mode is enabled on the switch. Value is enabled or disabled.

◦ **CPU Multicast Rate**- Sets the CPU Multicast Rate.

4.3.4 GARP

4.3.4.1 GARP Status

This screen shows the GARP Status for the switch and for the individual ports. Note that the timers are only relevant when the status for a port shows as enabled.



GARP Status

Switch GVRP	Enabled
Switch GMRP	Enabled

Slot/Port	Port GVRP Mode	Port GMRP Mode	Join Timer (centisecs)	Leave Timer (centisecs)	Leave All Timer (centisecs)
0/1	Enabled	Enabled	20	60	1000
0/2	Enabled	Enabled	20	60	1000
0/3	Enabled	Enabled	20	60	1000
0/4	Enabled	Enabled	20	60	1000
0/5	Enabled	Enabled	20	60	1000
0/6	Enabled	Enabled	20	60	1000
0/7	Enabled	Enabled	20	60	1000
0/8	Enabled	Enabled	20	60	1000
0/9	Enabled	Enabled	20	60	1000
0/10	Enabled	Enabled	20	60	1000

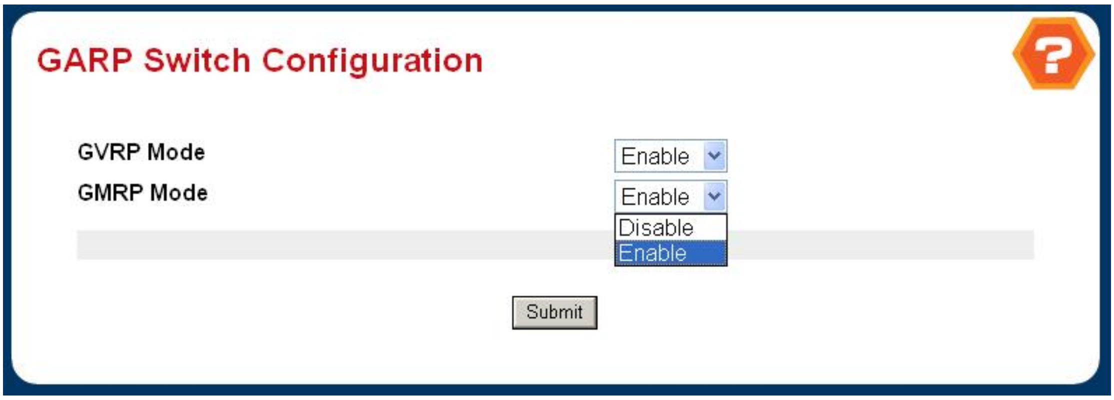
Figure 4-3-16 GARP Status

- **Switch GVRP -** Indicates whether the GARP VLAN Registration Protocol administrative mode for this switch is enabled or disabled. The factory default is disabled.
- **Switch GMRP -** Indicates whether the GARP Multicast Registration Protocol administrative mode for this switch, enabled or disabled. The factory default is disabled.
- **Slot.Port -** Slot.Port of the interface.
- **Port GVRP Mode -** Indicates whether the GVRP administrative mode for the port is enabled or disabled. The factory default is disabled.
- **Port GMRP Mode -** Indicates whether the GMRP administrative mode for the port is enabled or disabled. The factory default is disabled.
- **Join Time (centiseconds) -** Specifies the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. An instance of this timer exists for each GARP participant for each port. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds).
- **Leave Time (centiseconds) -** Specifies the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. An instance of this timer exists for each GARP participant for each port. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
- **Leave All Time (centiseconds) -**This Leave All Time controls how frequently LeaveAll PDUs are generated. A

LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. An instance of this timer exists for each GARP participant for each port. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).

4.3.4.2 GARP Switch Configuration

This page is to Enable/Disable GVRP and GMRP mode. Note that it can take up to 10 seconds for GARP configuration changes to take effect.



GARP Switch Configuration

GVRP Mode: Enable

GMRP Mode: Enable

Figure 4-3-17 GARP Switch Configuration

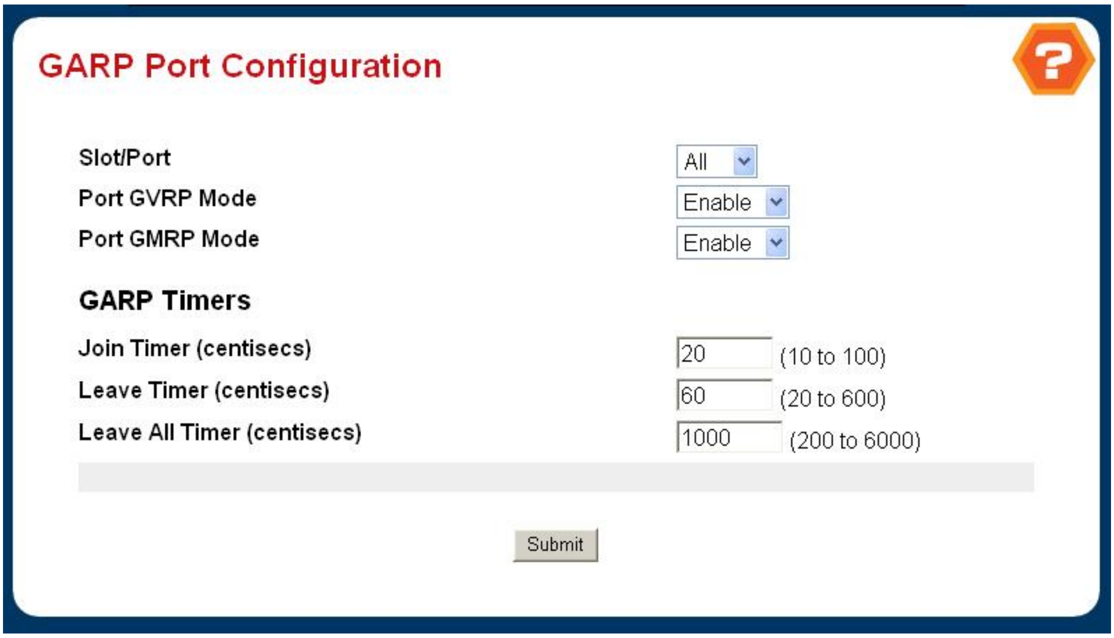
- **GVRP Mode -** Choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled.
- **GMRP Mode -** Choose the GARP Multicast Registration Protocol administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled.

4.3.4.3 GARP Port Configuration

Use this page to configure the GVRP/GMRP mode and GARP Timers on the ports. Note that it can take up to 10 seconds for GARP configuration changes to take effect.

- **Slot.Port -** Select the physical interface for which data is to be displayed or configured. It is possible to set the parameters for all ports by selecting 'All'.
- **Port GVRP Mode -** Choose the GARP VLAN Registration Protocol administrative mode for the port by selecting enable or disable from the pull-down menu. If you select disable, the protocol will not be active and the Join Time, Leave Time and Leave All Time will have no effect. The factory default is disabled.
- **Port GMRP Mode -** Choose the GARP Multicast Registration Protocol administrative mode for the port by selecting enable or disable from the pull-down menu. If you select disable, the protocol will not be active, and Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.
- **Join Time (centiseconds) -** Specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.

- **Leave Time (centiseconds) -** Specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
- **Leave All Time (centiseconds) -** The Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.



GARP Port Configuration

Slot/Port	All
Port GVRP Mode	Enable
Port GMRP Mode	Enable

GARP Timers

Join Timer (centisecs)	20 (10 to 100)
Leave Timer (centisecs)	60 (20 to 600)
Leave All Timer (centisecs)	1000 (200 to 6000)

Figure 4-3-18 GARP Port Configuration

4.3.5 IGMP Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The Internet Group Management Protocol (IGMP) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the ‘queried’. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

IGMP Versions 1 and 2

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

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

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16 31
Type	Response Time	Checksum
Group Address (all zeros if this is a query)		

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)

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

A host sends an IGMP **“report”** to join a group

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

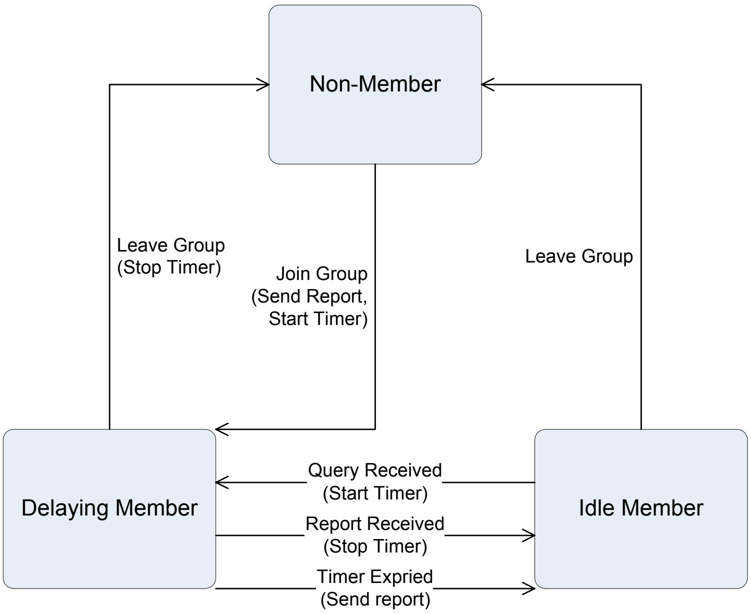
A host will send a **“leave”** report when it wants to leave a group (for version 2).

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

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

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

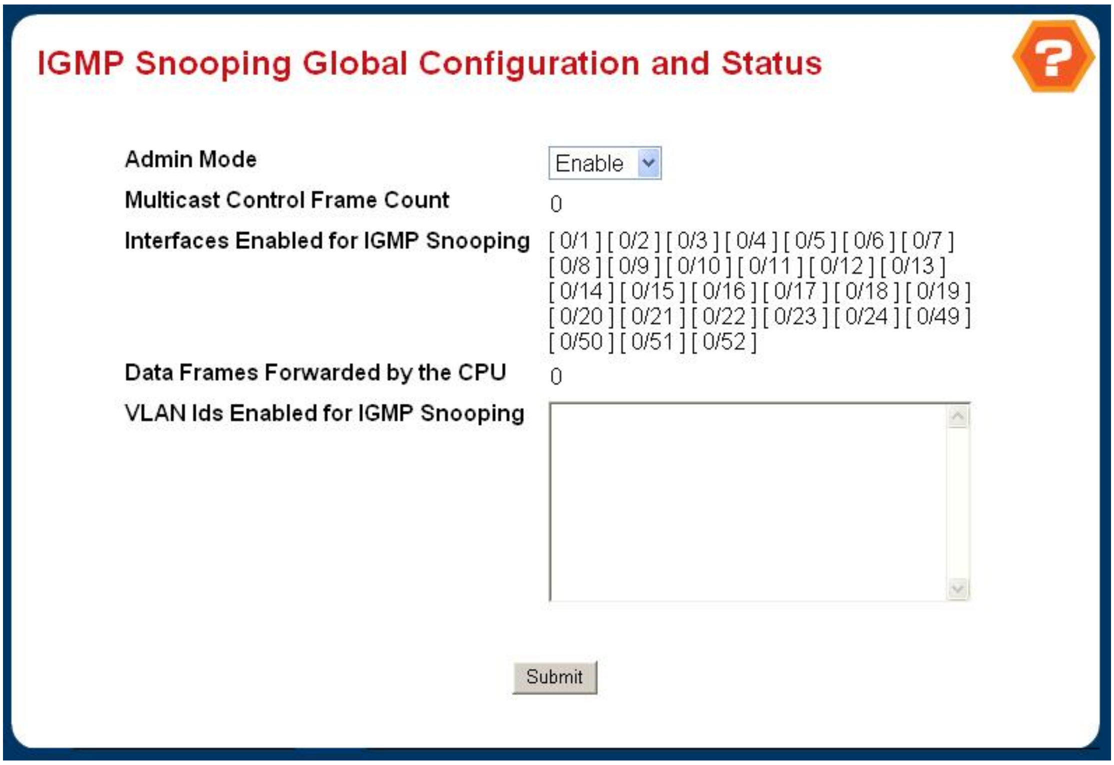
The states a computer will go through to join or to leave a multicast group are shown below:



IGMP State Transitions

4.3.5.1 IGMP Snooping Configuration and Status

Use this menu to configure the parameters for IGMP Snooping, which is used to build forwarding lists for multicast traffic. Note that only a user with Read/Write access privileges may change the data on this screen.



IGMP Snooping Global Configuration and Status

Admin Mode: Enable

Multicast Control Frame Count: 0

Interfaces Enabled for IGMP Snooping: [0/1] [0/2] [0/3] [0/4] [0/5] [0/6] [0/7] [0/8] [0/9] [0/10] [0/11] [0/12] [0/13] [0/14] [0/15] [0/16] [0/17] [0/18] [0/19] [0/20] [0/21] [0/22] [0/23] [0/24] [0/49] [0/50] [0/51] [0/52]

Data Frames Forwarded by the CPU: 0

VLAN Ids Enabled for IGMP Snooping:

Figure 4-3-19 IGMP Snooping Configuration and Status

Configurable Data

- **Admin Mode** - Select the administrative mode for IGMP Snooping for the switch from the pulldown menu. The default is disable.

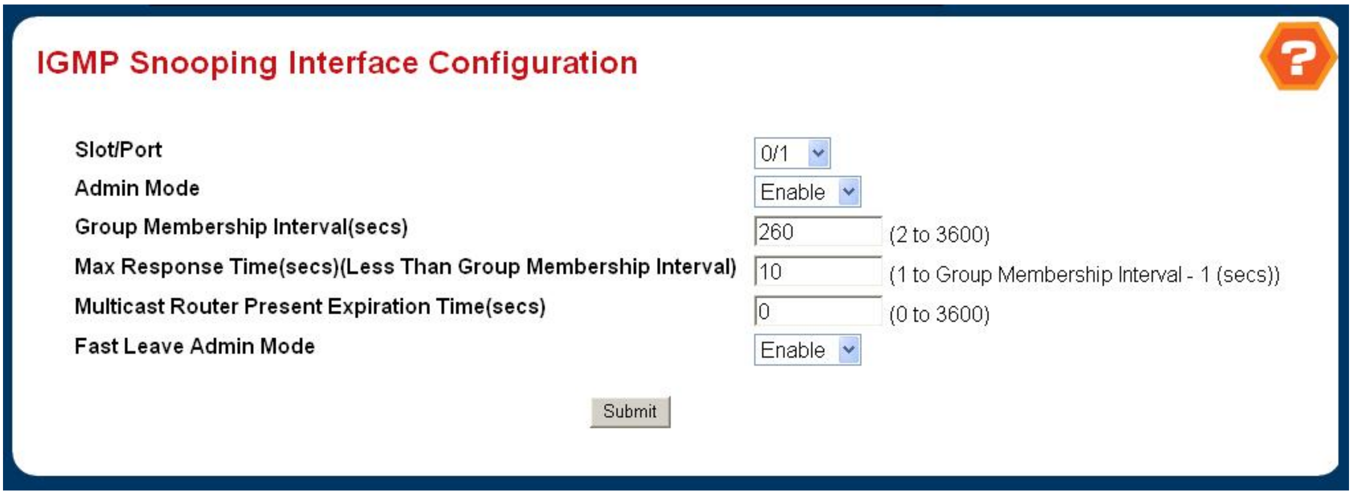
Non-Configurable Data

- **Multicast Control Frame Count** - The number of multicast control frames that are processed by the CPU.
- **Interfaces Enabled for IGMP Snooping** - A list of all the interfaces currently enabled for IGMP Snooping.
- **Data Frames Forwarded by the CPU** - The number of data frames forwarded by the CPU.
- **VLAN Ids Enabled For IGMP Snooping** - Displays VLAN Ids enabled for IGMP snooping.

Command Buttons

- **Submit** - Update the switch with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save. You will only see this button if you have Read/Write access privileges.

4.3.5.2 IGMP Snooping Interface Configuration



IGMP Snooping Interface Configuration

Slot/Port	0/1	
Admin Mode	Enable	
Group Membership Interval(secs)	260	(2 to 3600)
Max Response Time(secs)(Less Than Group Membership Interval)	10	(1 to Group Membership Interval - 1 (secs))
Multicast Router Present Expiration Time(secs)	0	(0 to 3600)
Fast Leave Admin Mode	Enable	

Figure 4-3-20 IGMP Snooping Interface Configuration

Configurable Data

- **Slot/Port** - The single select box lists all physical ,VLAN and LAG interfaces. Select the interface you want to configure.
- **Admin Mode** - Select the interface mode for the selected interface for IGMP Snooping for the switch from the pulldown menu.

  The default is **disable**.
- **Group Membership Interval** - Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. Enter a value between 1 and 3600 seconds.

  The default is 260 seconds.
- **Max Response Time** - Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds.

  The default is **10 seconds**. The configured value must be less than the Group Membership Interval.
- **Multicast Router Present Expiration Time** - Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds.

  The default is **0 seconds**. A value of zero indicates an infinite timeout, i.e. no expiration.
- **Fast Leave Admin mode** - Select the Fast Leave mode for the a particular interface from the pulldown menu.

  The default is **disable**.

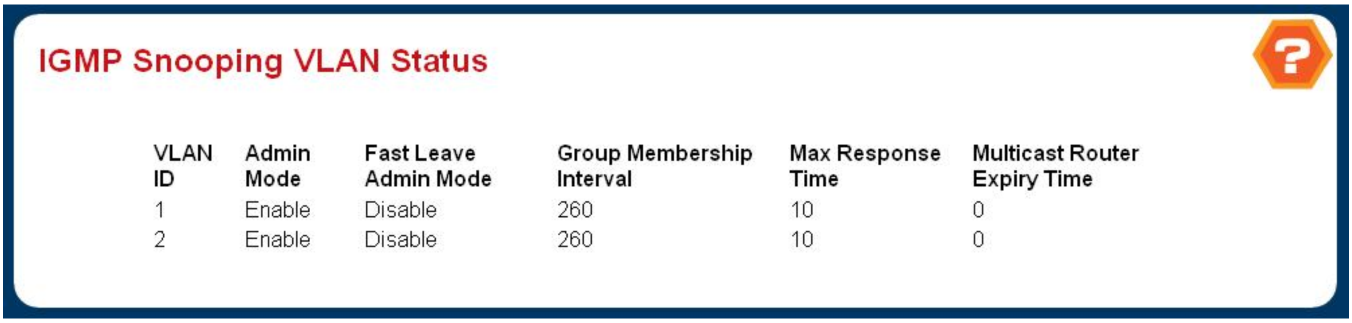
Command Buttons

- **Submit** - Update the switch with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save. You will only see this button if you have Read/Write access privileges.

Notice: This could take up to 10 to 30 seconds to become effective

4.3.5.3 VLAN Status

Use this page to display the IGMP Snooping VLAN status.



IGMP Snooping VLAN Status

VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Max Response Time	Multicast Router Expiry Time
1	Enable	Disable	260	10	0
2	Enable	Disable	260	10	0

Figure 4-3-21 IGMP Snooping VLAN Status

Non-Configurable Data

- **VLAN ID** - All Vlan Ids for which the IGMP Snooping mode is Enabled.
- **Admin Mode** - Igmp Snooping Mode for Vlan ID.
- **Fast Leave Admin Mode** - Fast Leave Mode for Vlan ID.
- **Group Membership Interval** - Group Membership Interval of IGMP Snooping for the specified VLAN ID.

  Valid range is **2 to 3600**.
- **Maximum Response Time** - Maximum Response Time of IGMP Snooping for the specified VLAN ID.

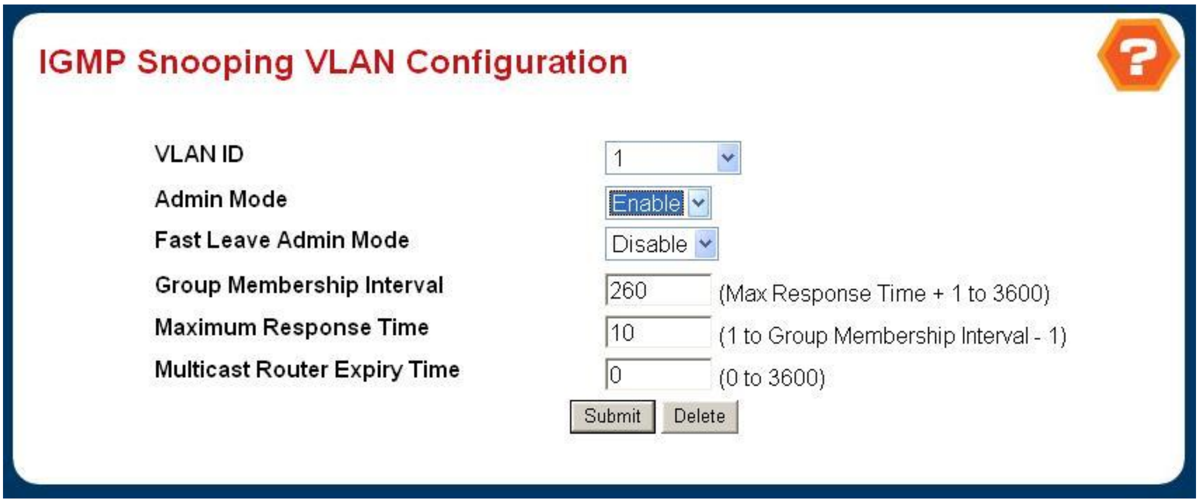
  Valid range is **1 to 3599**.

  Its value should be greater than group membership interval value.
- **Multicast Router Expiry Time** - Multicast Router Expiry Time of IGMP Snooping for the specified VLAN ID.

  Valid range is **0 to 3600**.

4.3.5.4 VLAN Configuration

Use this page to setup the IGMP Snooping VLAN configuration.



IGMP Snooping VLAN Configuration

VLAN ID: 1

Admin Mode: Enable

Fast Leave Admin Mode: Disable

Group Membership Interval: 260 (Max Response Time + 1 to 3600)

Maximum Response Time: 10 (1 to Group Membership Interval - 1)

Multicast Router Expiry Time: 0 (0 to 3600)

Figure 4-3-22 IGMP Snooping VLAN Configuration

Configurable Data

- **VLAN ID** - Specifies list of VLAN IDs for which IGMP Snooping is enabled.
- **VLAN ID** - Appears when "New Entry" is selected in VLAN ID combo box. Specifies VLAN ID for which pre-configurable Snooping parameters are to be set.
- **Admin Mode** - Enable Igmp Snooping for the specified VLAN ID.
- **Fast Leave Admin Mode** - Enable or disable the Igmp Snooping Fast Leave Mode for the specified VLAN ID.
- **Group Membership Interval** - Sets the value for group membership interval of IGMP Snooping for the specified VLAN ID.

  Valid range is **(Maximum Response Time + 1) to 3600**.
- **Maximum Response Time** - Sets the value for maximum response time of IGMP Snooping for the specified VLAN ID.

  Valid range is **1 to (Group Membership Interval - 1)**.

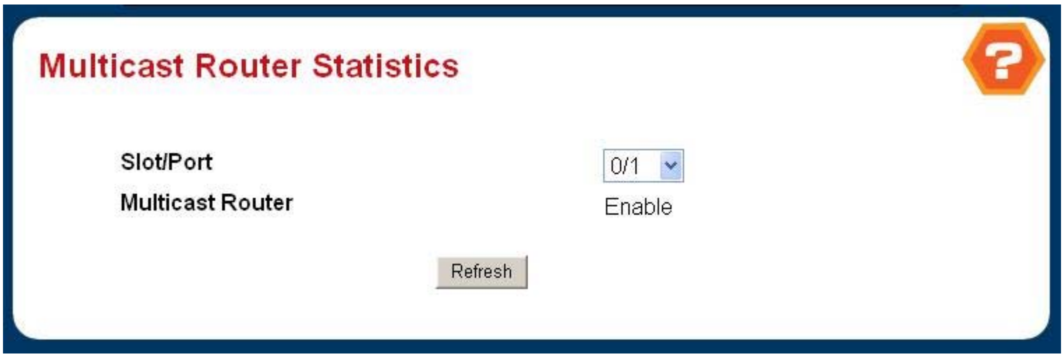
  Its value should be greater than group membership interval value.
- **Multicast Router Expiry Time** - Sets the value for multicast router expiry time of IGMP Snooping for the specified VLAN ID.

  Valid range is **0 to 3600**.

Command Buttons

- **Submit** - Update the switch with the values you entered.
- **Delete** - Update the switch with the default values.

4.3.5.5 Multicast Router Statistics



Multicast Router Statistics

Slot/Port 0/1

Multicast Router Enable

Figure 4-3-23 Multicast Router Statistics

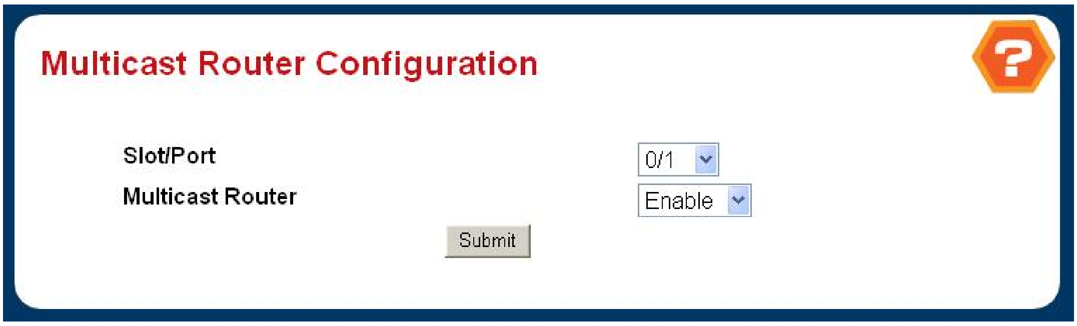
Non-Configurable Data

- **Slot/Port** - The single select box lists all physical and LAG interfaces. Select the interface for which you want to display the statistics.
- **Multicast Router** - Specifies for the selected interface whether multicast router is enable or disabled.

Command Buttons

- **Refresh** - Refetch the database and display it again starting with the first entry in the table.

4.3.5.6 Multicast Router Configuraton



Multicast Router Configuration

Slot/Port 0/1

Multicast Router Enable

Figure 4-3-24 Multicast Router Configuration

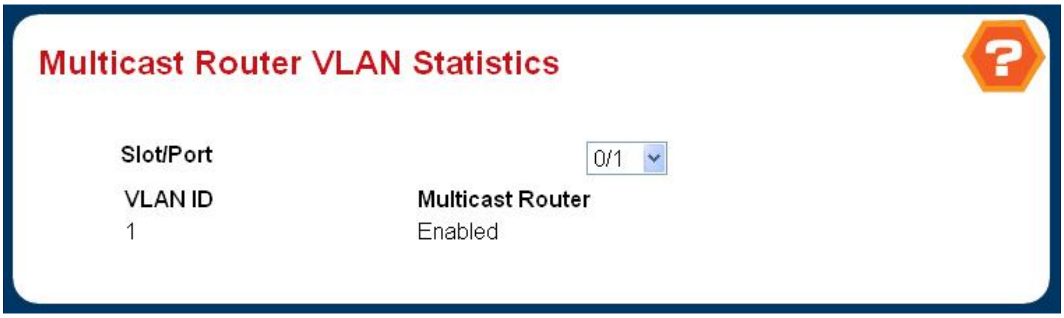
Configurable Data

- **Slot/Port** - The select box lists all Slot/Ports. Select the interface for which you want Multicast Router to be enabled .
- **Multicast Router** - Enable or disable Multicast Router on the selected Slot/Port.

Command Buttons

- **Submit** - Update the switch with the values you entered.

4.3.5.7 Multicast Router VLAN Statistics



Multicast Router VLAN Statistics

Slot/Port 0/1

VLAN ID	Multicast Router
1	Enabled

Figure 4-3-25 Multicast Router VLAN Statistics

Selection Criteria

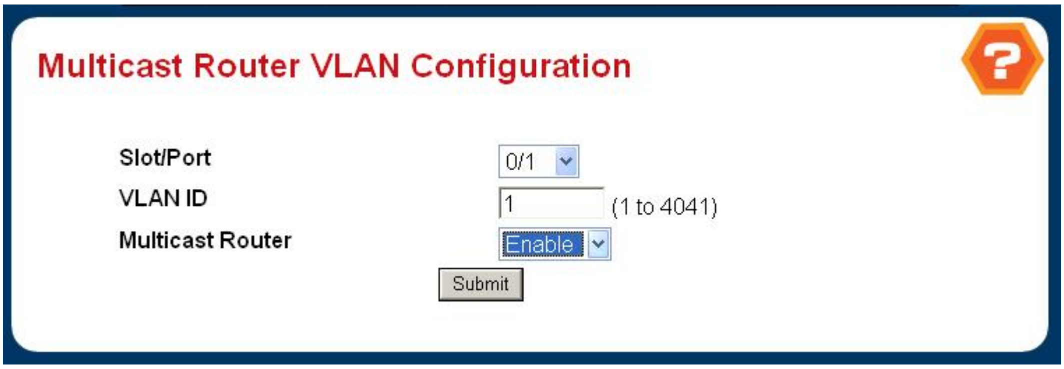
◦ **Slot/Port** - The select box lists all Slot/Ports.Select the interface for which you want to display the statistics.

Non-Configurable Data

◦ **VLAN ID** - All Vlan Ids for which the Multicast Router Mode is Enabled

◦ **Multicast Router** - Multicast Router Mode for Vlan ID.

4.3.5.8 Multicast Router VLAN Configuration



Multicast Router VLAN Configuration

Slot/Port 0/1

VLAN ID 1 (1 to 4041)

Multicast Router Enable

Figure 4-3-26 Multicast Router VLAN Configuration

Selection Criteria

- **Slot/Port** - The select box lists all Slot/Ports.Select the interface for which you want to display the statistics.

Non-Configurable Data

- **VLAN ID** - All Vlan Ids for which the Multicast Router Mode is Enabled
- **Multicast Router** - Multicast Router Mode for Vlan ID.

4.3.6 Port Channel

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

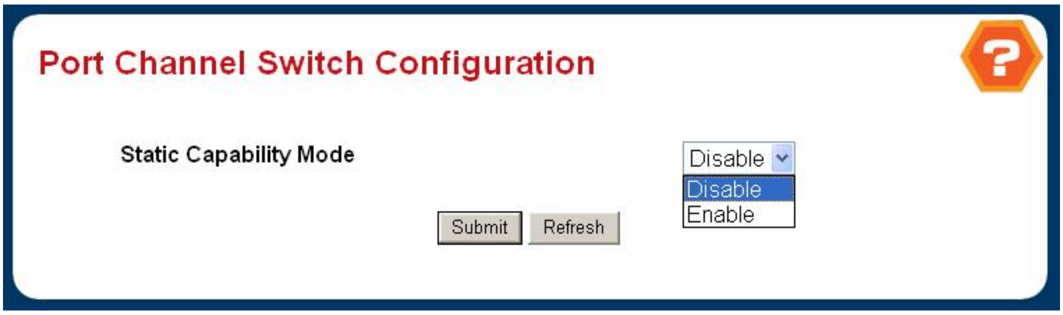
Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ-45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of eight ports to be aggregated at the same time. The Switch support Gigabit Ethernet ports (up to 12 groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

4.3.6.1 Switch Configuration

Use this page to setup the port channel switch configuration.



Port Channel Switch Configuration

Static Capability Mode: Disable

Figure 4-3-27 Port Channel Switch Configuration

Configurable Data

- **Static Capability Mode** - May be enabled or disabled by selecting the corresponding line on the pulldown entry field. The factory default is disabled. This field is non-configurable for read-only users.

Command Buttons

- **Submit** - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.
- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.3.6.2 Port Channel Configuration

Use this page to configure the link aggregation for gathering bandwidth.

Selection Criteria

- **Port Channel Name –** You can use this screen to reconfigure an existing Port Channel, or to create a new one. Use this pull-down menu to select one of the existing Port Channels, or select 'Create' to add a new one. There can be a maximum of 6 Port Channels.

Configurable Data

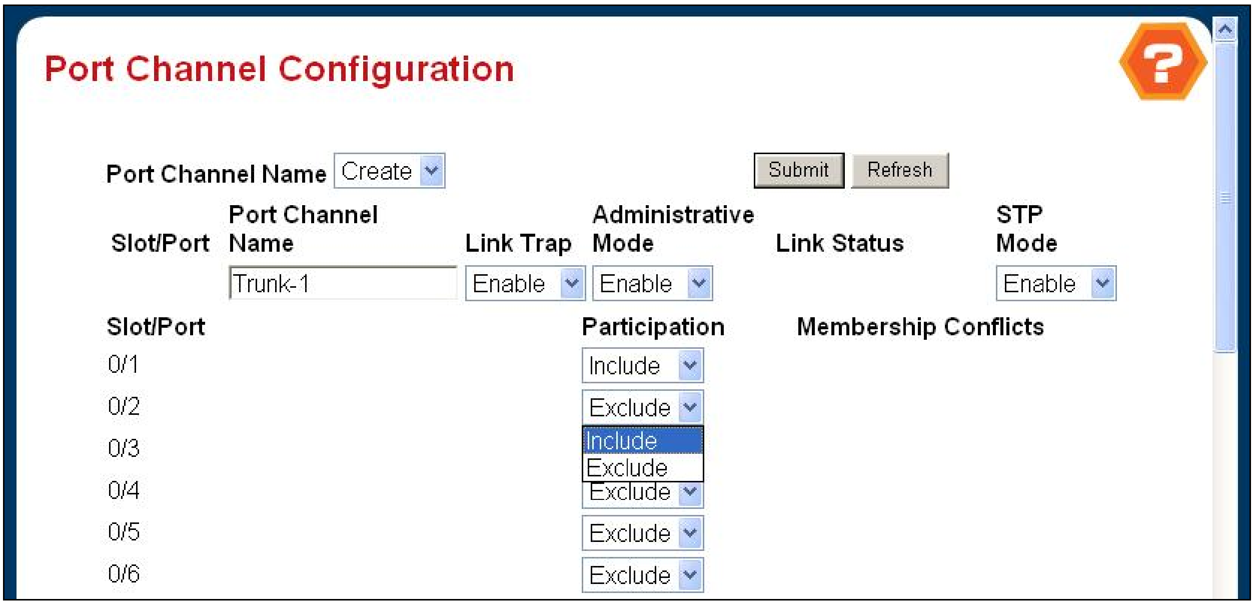
- **Port Channel Name -** Enter the name you want assigned to the Port Channel. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the Port Channel.
- **Link Trap -** Specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.
- **Administrative Mode -** Select enable or disable from the pull-down menu. When the Port Channel is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the Port Channel will not be released. The

factory default is enable.

- **STP Mode -** The Spanning Tree Protocol Administrative Mode associated with the Port Channel. The possible values are:
- **Disable -** spanning tree is disabled for this Port Channel.
- **Enable -** spanning tree is enabled for this Port Channel.
- **Participation -** For each port specify whether it is to be included as a member of this Port Channel or not. The default is exclude. There can be a maximum of 8 ports assigned to a Port Channel.

Non-Configurable Data

- **Slot.Port -** Slot.Port identification of the Port Channel being configured. This field will not appear when a new Port Channel is being created.
- **Link Status -** Indicates whether the Link is up or down.
- **Port Channel Members -** List of members of the Port Channel in slot.port form.
- **Membership Conflicts -** Shows ports that are already members of other Port Channels. A port may only be a member of one Port Channel at a time. If the entry is blank, it is not currently a member of any Port Channel.



Port Channel Configuration

Port Channel Name: Create

Slot/Port	Port Channel Name	Link Trap	Administrative Mode	Link Status	STP Mode
	Trunk-1	Enable	Enable		Enable

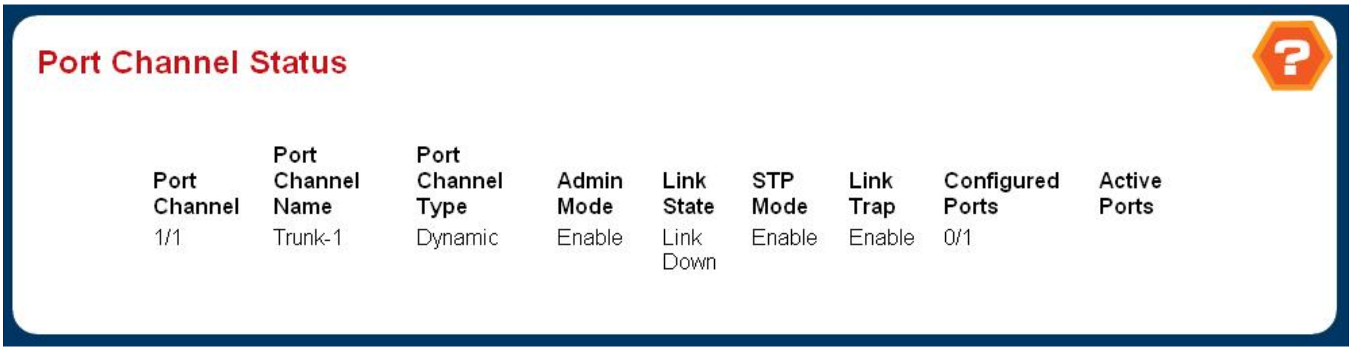
Slot/Port	Participation	Membership Conflicts
0/1	Include	
0/2	Exclude	
0/3	Include Exclude	
0/4	Exclude	
0/5	Exclude	
0/6	Exclude	

Figure 4-3-28 Port Channel Configuration

4.3.6.3 Port Channel Status

- **Port Channel -** The slot.port identification of the Port Channel.
- **Port Channel Name -** The name of the Port Channel.
- **Port Channel Type -** The type of this Port Channel.
- **Admin Mode -** The Administrative Mode of the Port Channel, enable or disable.
- **Link Status -** Indicates whether the Link is up or down.
- **STP Mode -** The Spanning Tree Protocol Administrative Mode associated with the Port Channel. The possible values are:
- **Disable -** spanning tree is disabled for this Port Channel.
- **Enable -** spanning tree is enabled for this Port Channel.

- **Link Trap -** Whether or not a trap will be sent when link status changes. The factory default is enabled.
- **Configured Ports -** A list of the ports that are members of the Port Channel, in slot.port notation. There can be a maximum of 8 ports assigned to a Port Channel.
- **Active Ports -** A listing of the ports that are actively participating members of this Port Channel, in slot.port notation. There can be a maximum of 8 ports assigned to a Port Channel.



Port Channel Status

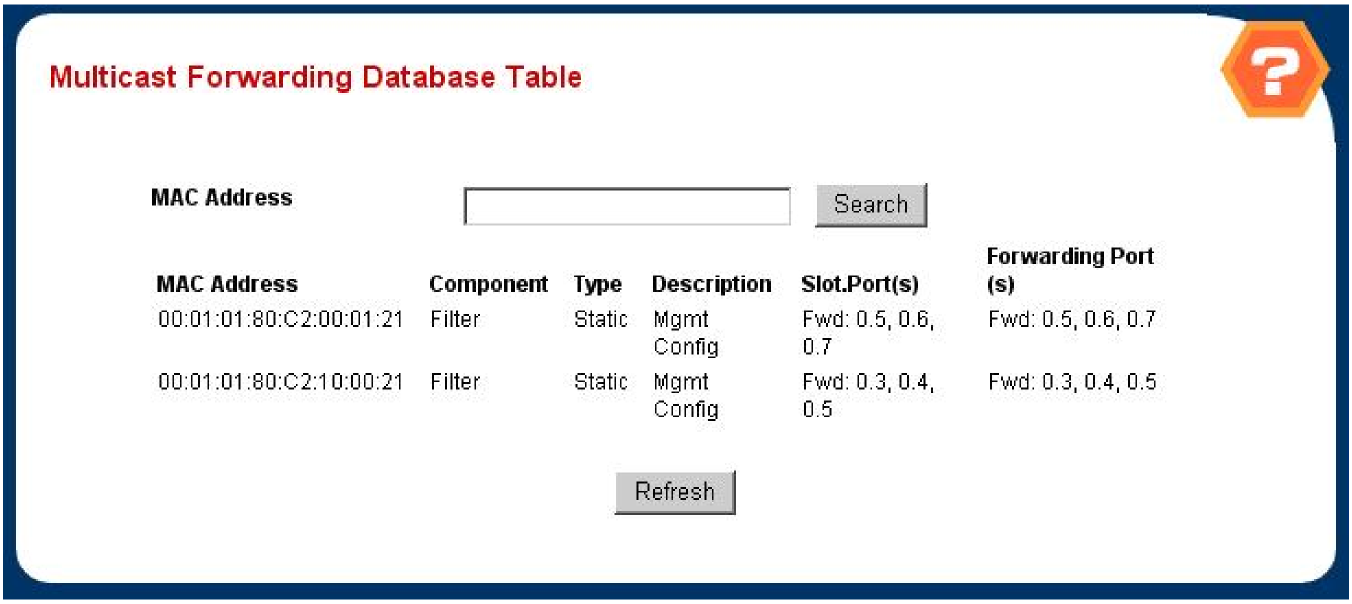
Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Link State	STP Mode	Link Trap	Configured Ports	Active Ports
1/1	Trunk-1	Dynamic	Enable	Link Down	Enable	Enable	0/1	

Figure 4-3-29 Port Channel Status

4.3.7 Multicast Forwarding Database

4.3.7.1 MFDB Table

The Multicast Forwarding Database holds the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries may contain data for more than one protocol.



Multicast Forwarding Database Table

MAC Address [ ] Search

MAC Address	Component	Type	Description	Slot.Port(s)	Forwarding Port (s)
00:01:01:80:C2:00:01:21	Filter	Static	Mgmt Config	Fwd: 0.5, 0.6, 0.7	Fwd: 0.5, 0.6, 0.7
00:01:01:80:C2:10:00:21	Filter	Static	Mgmt Config	Fwd: 0.3, 0.4, 0.5	Fwd: 0.3, 0.4, 0.5

Figure 4-3-30 Multicast Forwarding Database Table

Use this screen to display the MFDB information for a specific entry. To display all of the entries for a particular protocol use one of the following menus:

◦ **MAC Filter Summary -** Static MAC address filtering entries

◦ **MFDB GMRP Table - G**ARP Multicast Registration Protocol entries

◦ **MFDB IGMP Snooping Table -** IGMP Snooping entries

Selection Criteria

◦ **MAC Address - Enter the VLAN ID -** MAC Address pair whose MFDB table entry you want displayed. Enter eight two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67:89:AB. The first two two-digit hexadecimal numbers are the VLAN ID and the remaining numbers are the MAC address. Then click on the **"Search"** button. If the address exists, that entry will be displayed. An exact match is required.

Non-Configurable Data

◦ **MAC Address -** The multicast MAC address for which you requested data.

◦ **Type -** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

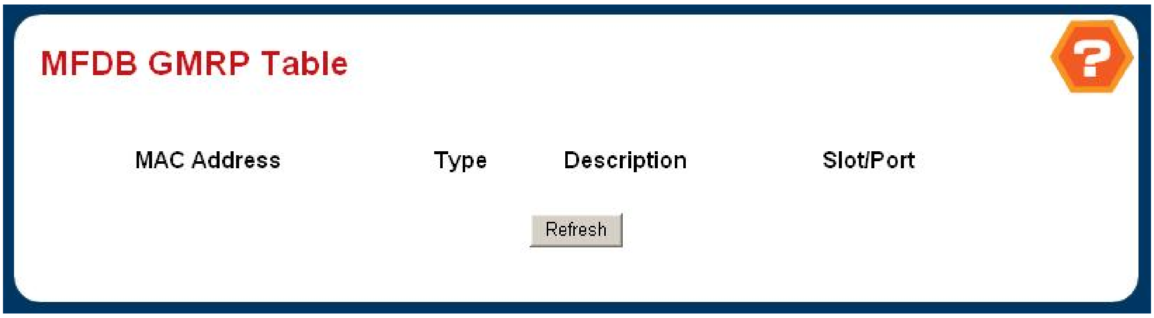
◦ **Component -** This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.

◦ **Description -** The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.

- **Slot.Port(s) -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:) for the selected address.
- **Forwarding Port(s) -** The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

4.3.7.2 GMRP Table

This screen will display all of the entries in the Multicast Forwarding Database that were created for the GARP Multicast Registration Protocol.



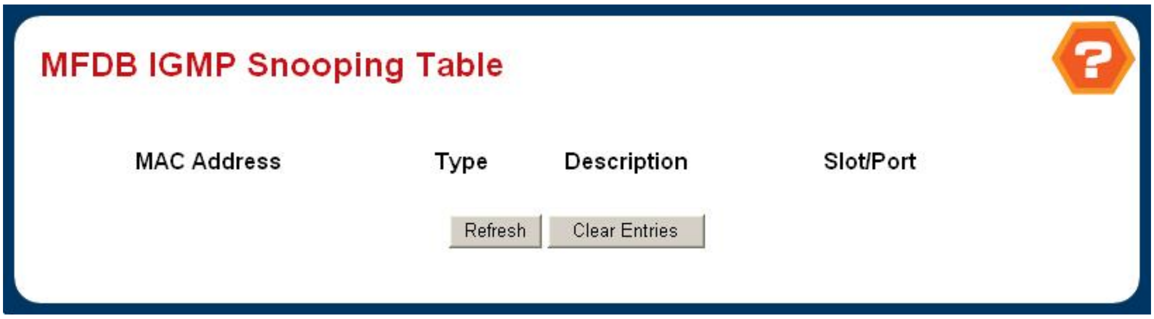
MFDB GMRP Table

MAC Address	Type	Description	Slot/Port

Figure 4-3-31 MFDB GMRP Table

- **AC Address -** A VLAN ID - multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example 00:01:23:45:67:89:AB:CD.
- **Type -** This displays the type of the entry. Static entries are those that are configured by the user. Dynamic entries are added to the table as a result of a learning process or protocol.
- **Description -** The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
- **Slot.Port(s) -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.3.7.3 IGPM Snooping Table



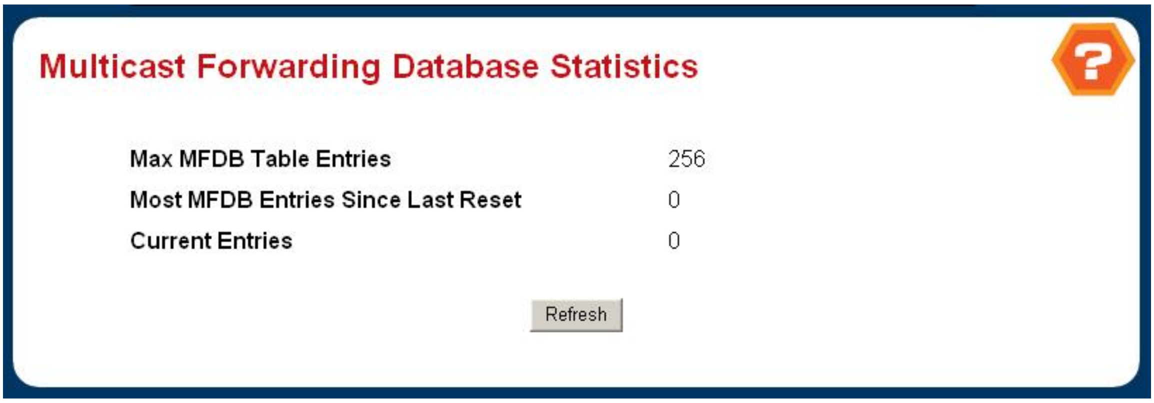
MFDB IGMP Snooping Table

MAC Address	Type	Description	Slot/Port

Figure 4-3-32 MFDB IGMP Snooping Table

- **MAC Address -** A VLAN ID - multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example 00:01:23:45:67:89:AB:CD.
- **Type -** This displays the type of the entry. Static entries are those that are configured by the user. Dynamic entries are added to the table as a result of a learning process or protocol.
- **Description -** The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
- **Slot.Port(s) -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.3.7.4 Multicast Forwarding Database Statistics



Multicast Forwarding Database Statistics

Max MFDB Table Entries	256
Most MFDB Entries Since Last Reset	0
Current Entries	0

Figure 4-3-32 Multicast Forwarding Database Statistics

Non-Configurable Data

- **Max MFDB Entries** - The maximum number of entries that the Multicast Forwarding Database table can hold.
- **Most MFDB Entries Since Last Reset** - The largest number of entries that have been present in the Multicast Forwarding Database table since last reset. This value is also known as the MFDB high-water mark.
- **Current Entries** - The current number of entries in the Multicast Forwarding Database table.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.3.8 Spanning Tree

1. Spanning Tree Protocol

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1W Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The por tidentifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

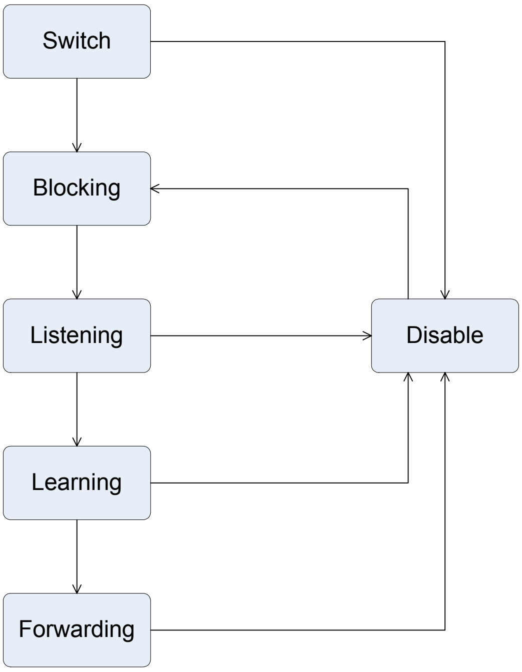
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking



STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

2. STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Notice:

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	**Description**	**Default Value**
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as	32768

	the root bridge	
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch’s factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be 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. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

Notice:	The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your 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.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Notice:

Observe the following formulas when setting the above parameters:

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

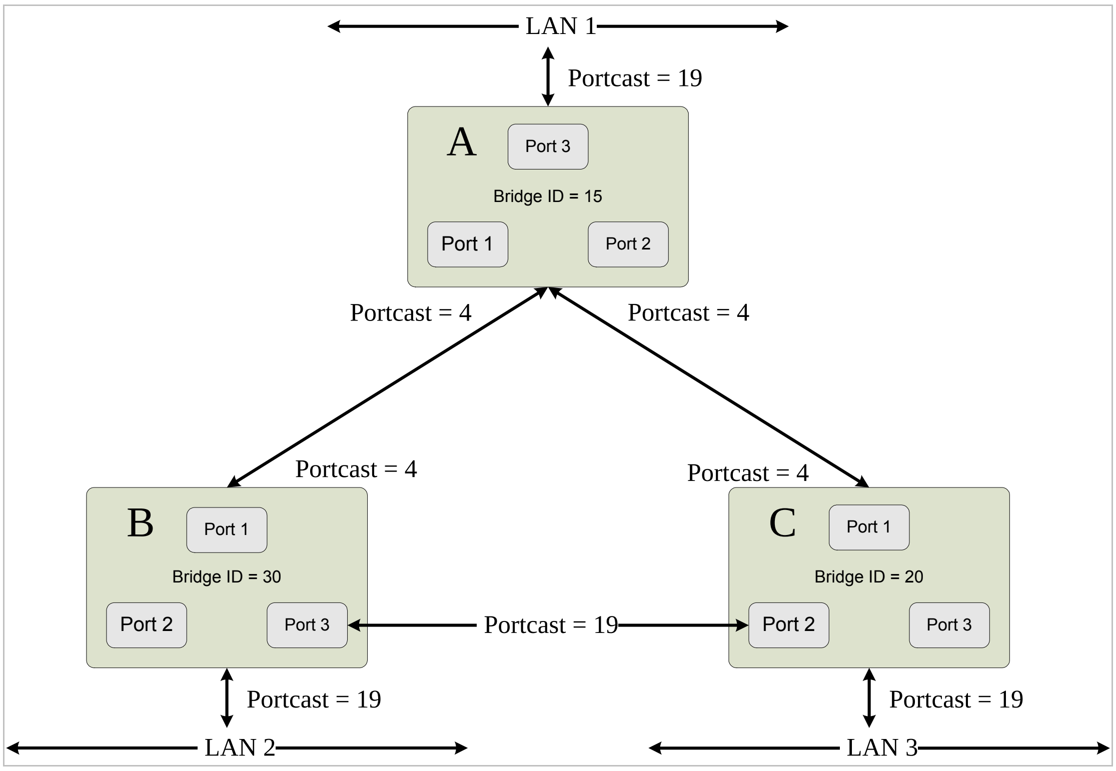
Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

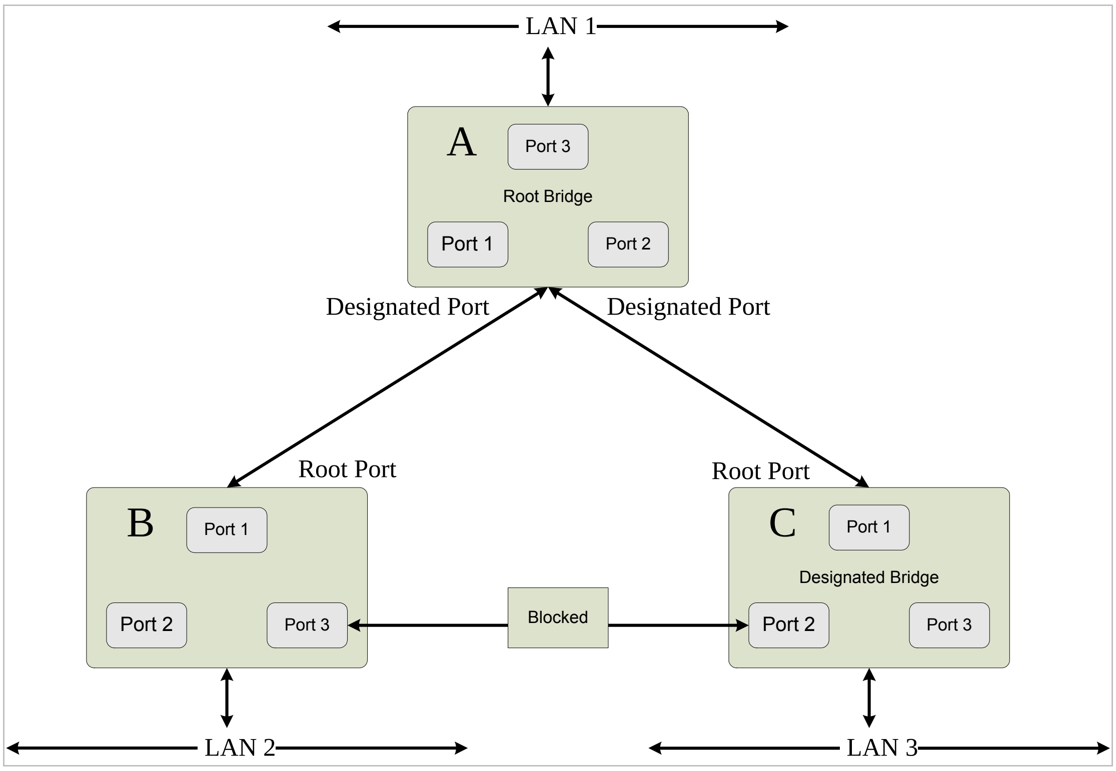
3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in Figure 5-7. In this example, you can anticipate some major network problems if the STP assistance is not applied. If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A ... and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings. Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.



Before Applying the STA Rules

In this example, only the default STP values are used.

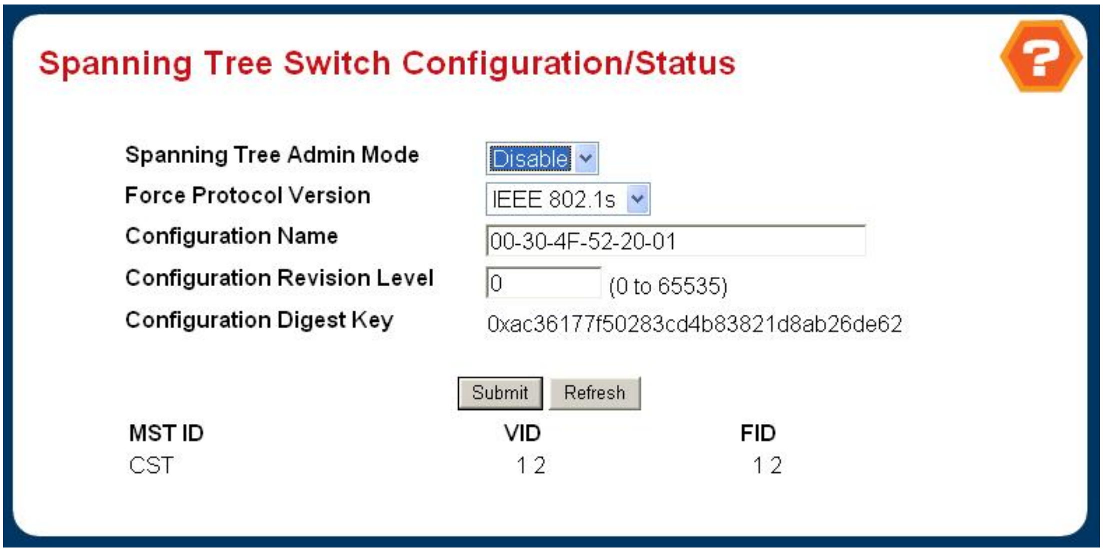


After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 4) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 19). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

4.3.8.1 Spanning Tree Switch Configuration/Status

This page is to enable/disable the Spanning Tree protocol. The switch support IEEE 802.1d Spanning Tree (STP), IEEE 802.1w Rapid Spanning Tree (RSTP) and IEEE 802.1S Multiple Spanning Tree (MSTP).



Spanning Tree Switch Configuration/Status

Spanning Tree Admin Mode	Disable
Force Protocol Version	IEEE 802.1s
Configuration Name	00-30-4F-52-20-01
Configuration Revision Level	0 (0 to 65535)
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62

MST ID	VID	FID
CST	1 2	1 2

Figure 4-3-33 Spanning Tree Switch Configuration/Status

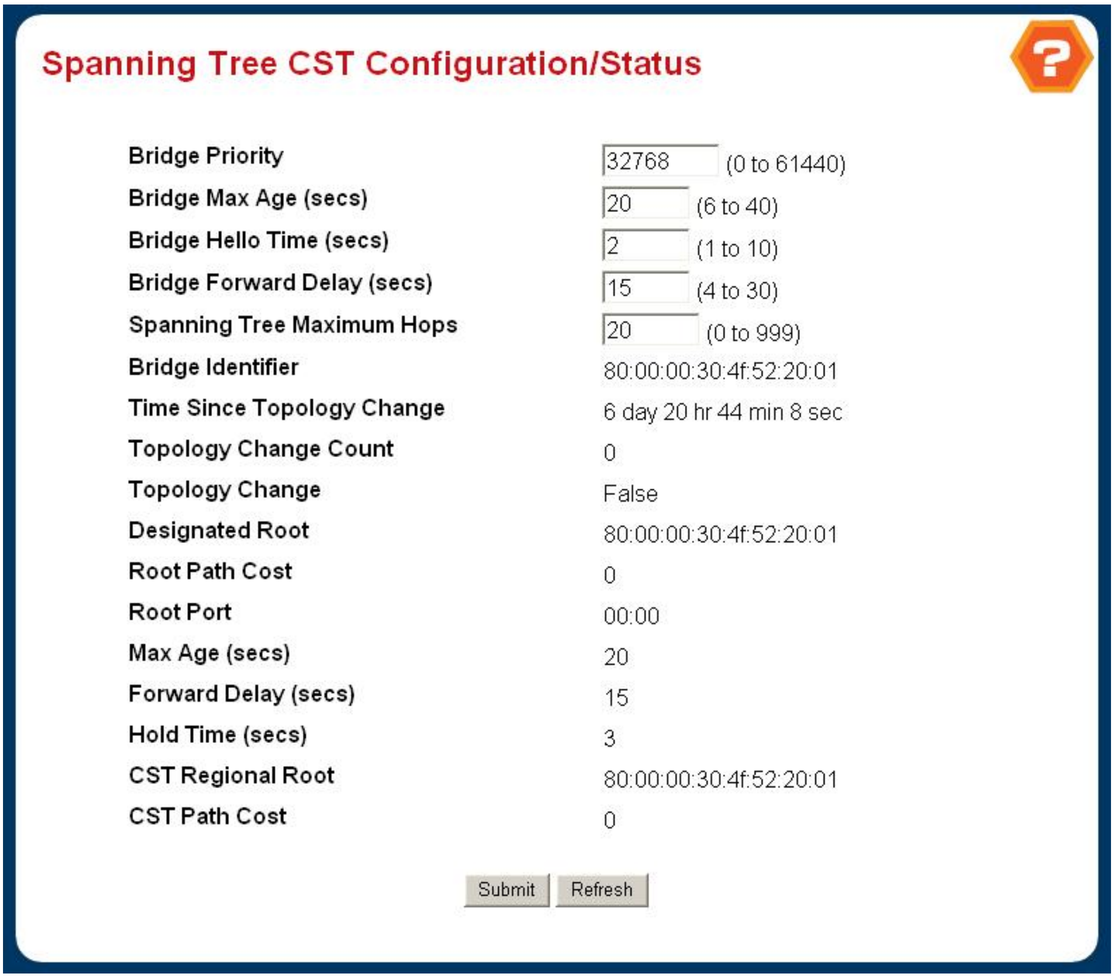
Configurable Data

- **Spanning Tree Mode -** Specifies whether spanning tree operation is enabled on the switch.
  Value is enabled or disabled
- F**orce Protocol Version -** Specifies the Force Protocol Version parameter for the switch.
  The options are **IEEE 802.1d**, **IEEE 802.1w** and **IEEE 802.1s**
- **Configuration Name-** Identifier used to identify the configuration currently being used. It may be up to 32 alphanumeric characters
- **Configuration Revision Level -** Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535.
  The default value is **0**.

Non-Configurable Data

- **Configuration digest key -** Identifier used to identify the configuration currently being used.
- **MST Table -** Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
- **VID Table -** Table consisting of the VLAN IDs and the corresponding FID associated with each of them.
- **FID Table -** Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

4.3.8.2 Spanning Tree CST Configuration/Status



Spanning Tree CST Configuration/Status

Bridge Priority	32768 (0 to 61440)
Bridge Max Age (secs)	20 (6 to 40)
Bridge Hello Time (secs)	2 (1 to 10)
Bridge Forward Delay (secs)	15 (4 to 30)
Spanning Tree Maximum Hops	20 (0 to 999)
Bridge Identifier	80:00:00:30:4f:52:20:01
Time Since Topology Change	6 day 20 hr 44 min 8 sec
Topology Change Count	0
Topology Change	False
Designated Root	80:00:00:30:4f:52:20:01
Root Path Cost	0
Root Port	00:00
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	3
CST Regional Root	80:00:00:30:4f:52:20:01
CST Path Cost	0

Figure 4-3-34 Spanning Tree CST Configuration/Status

Configurable Data

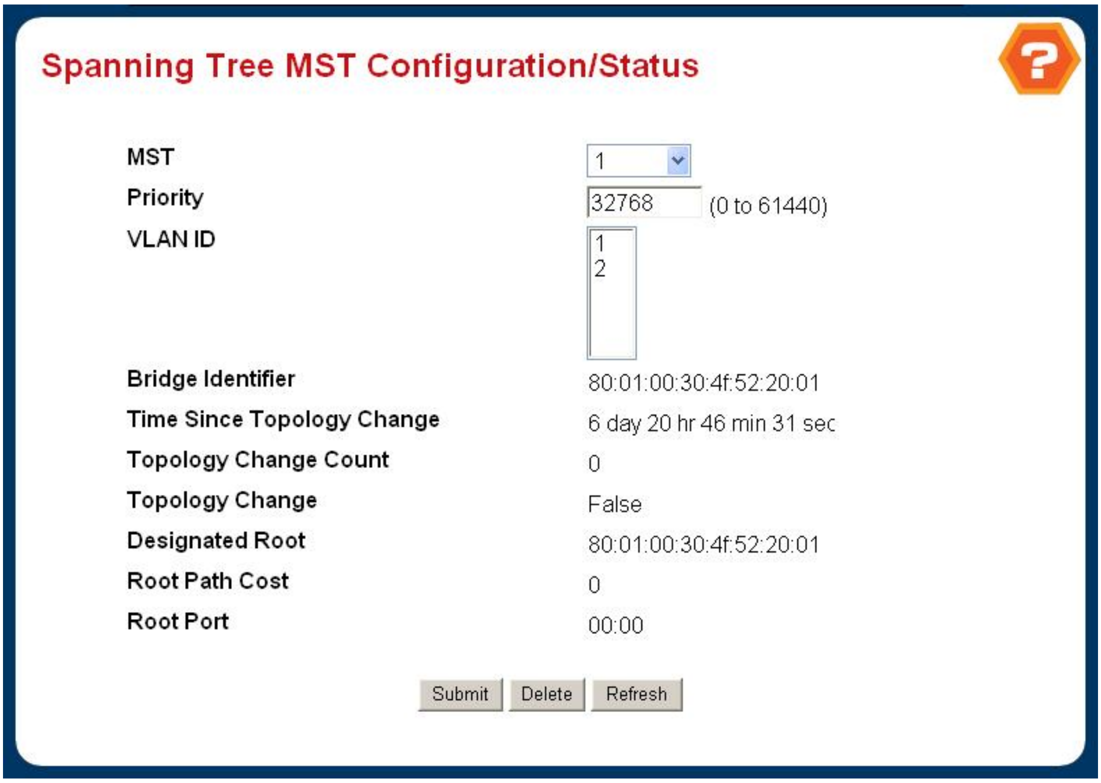
- **Bridge Priority -** Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is set in multiples of 4096. For example if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. If it is tried to be set to any value between 4096 and (2*4096-1) it will be set to 4096 and so on. The default priority is 32768.
- **Bridge Max Age -** Specifies the bridge max age for the Common and Internal Spanning tree (CST). The value lies between 6 and 40, with the value being less than or equal to "(2 * Bridge Forward Delay) - 1" and greater than or equal to "2 * (Bridge Hello Time +1)". The default value is 20.
- **Bridge Hello Time -** Specifies the bridge hello time for the Common and Internal Spanning tree (CST), with the value being less than or equal to "(Bridge Max Age / 2) - 1". The default hello time value is 2.
- **Bridge Forward Delay-** Specifies the time spent in "Listening and Learning" mode before forwarding packets. Bridge Forward Delay must be greater or equal to "(Bridge Max Age / 2) + 1". The time range is from 4 seconds to 30 seconds. The default value is 15.

Non-Configurable Data

- **Bridge identifier -** The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.

- **Time since topology change -** The time in seconds since the topology of the CST last changed.
- **Topology change count -** Number of times topology has changed for the CST.
- **Time since topology change -** The time in seconds since the topology of the
- **Topology change -** The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the selected MST instance. It takes a value of True or False.
- **Designated root -** The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
- **Root Path Cost -** Path Cost to the Designated Root for the CST.
- **Root Port -** Port to access the Designated Root for the CST.
- **Max Age -** Path Cost to the Designated Root for the CST.
- **Forward Delay -** Derived value of the Root Port Bridge Forward Delay parameter.
- **Hold Time -** Minimum time between transmission of Configuration BPDUs.
- **CST Regional Root -** Priority and base MAC address of the CST Regional Root.
- **CST Path Cost -** Path Cost to the CST tree Regional Root.

4.3.8.3 Spanning Tree MST Configuration/Status



Spanning Tree MST Configuration/Status

MST	1
Priority	32768 (0 to 61440)
VLAN ID	1 2
Bridge Identifier	80:01:00:30:4f:52:20:01
Time Since Topology Change	6 day 20 hr 46 min 31 sec
Topology Change Count	0
Topology Change	False
Designated Root	80:01:00:30:4f:52:20:01
Root Path Cost	0
Root Port	00:00

Figure 4-3-35 Spanning Tree MST Configuration/Status

Selection Criteria

- **MST ID -** Create a new MST which you wish to configure or configure already existing MSTs.

Configurable Data

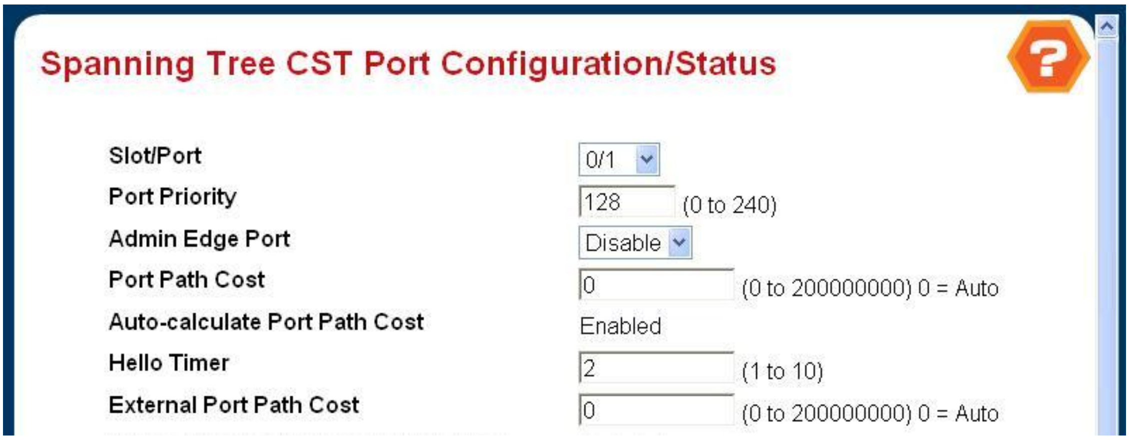
- **MST ID -** This is only visible when the select option of the MST ID select box is selected. The ID of the MST being created. Valid values for this are between 1 and 4094.

- **Priority -** The bridge priority for the MST instance selected. The bridge priority is set in multiples of 4096. For example if the priority is attempted to be set to any value between **0 and 4095**, it will be set to 0. If it is tried to be set to any value between 4096 and (2*4096-1) it will be set to 4096 and so on.
- **VLAN ID -** This gives a list box of all VLANs on the switch. The VLANs associated with the MST instance which is selected are highlighted on the list. These can be selected or unselected for re-configuring the association of VLANs to MST instances.

Non-Configurable Data

- **Bridge identifier -** The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
- **Time since topology change -** The time in seconds since the topology of the selected MST instance last changed.
- **Topology change count -** Number of times topology has changed for the selected MST instance.
- **Topology change -** The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the selected MST instance. It takes a value of True or False.
- **Designated root -** The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge
- **Root Path Cost -** Path Cost to the Designated Root for this MST instance.
- **Root port -** Port to access the Designated Root for this MST instance.

4.3.8.4 Spanning Tree CST Port Configuration/Status



Spanning Tree CST Port Configuration/Status

Slot/Port	0/1	
Port Priority	128	(0 to 240)
Admin Edge Port	Disable	
Port Path Cost	0	(0 to 200000000) 0 = Auto
Auto-calculate Port Path Cost	Enabled	
Hello Timer	2	(1 to 10)
External Port Path Cost	0	(0 to 200000000) 0 = Auto

Figure 4-3-36 Spanning Tree CST Port Configuration/Status

Selection Criteria

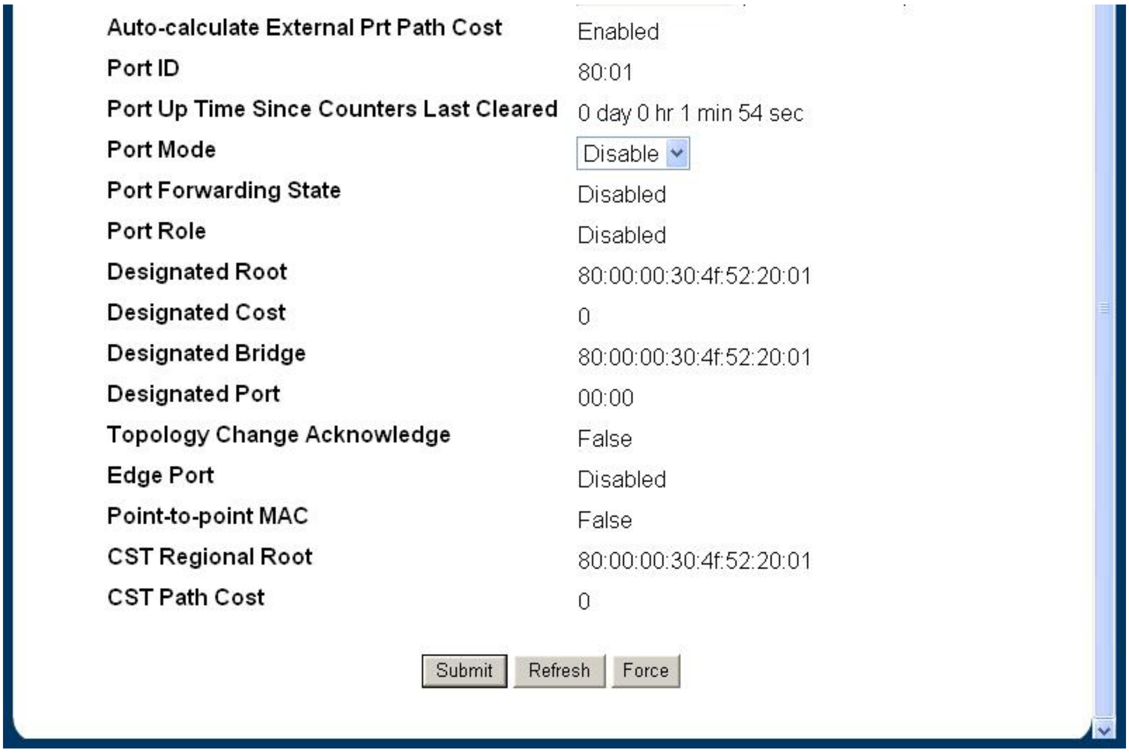
- **Slot/Port** - Selects one of the physical or port channel interfaces associated with VLANs associated with the CST.

Configurable Data

- **Port Priority** - The priority for a particular port within the CST. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and (2*16-1) it will be set to 16 and so on.

- **Admin Edge Port** - Specifies if the specified port is an Edge Port within the CIST. It takes a value of TRUE or FALSE, where the default value is FALSE.
- **Port Path Cost** - Set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of **1 to 200000000**.
- **Hello Timer** - Configure the value of the parameter for the CST.
- **External Port Path Cost** - Set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of **1 to 200000000**.
- **Port Mode** - Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable.

Non-Configurable Data



Auto-calculate External Prt Path Cost	Enabled
Port ID	80:01
Port Up Time Since Counters Last Cleared	0 day 0 hr 1 min 54 sec
Port Mode	Disable
Port Forwarding State	Disabled
Port Role	Disabled
Designated Root	80:00:00:30:4f:52:20:01
Designated Cost	0
Designated Bridge	80:00:00:30:4f:52:20:01
Designated Port	00:00
Topology Change Acknowledge	False
Edge Port	Disabled
Point-to-point MAC	False
CST Regional Root	80:00:00:30:4f:52:20:01
CST Path Cost	0

Figure 4-3-37 Spanning Tree CST Port Configuration/Status

- **Auto-calculate Port Path Cost** - Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost will be calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
- **Auto-calculate External Port Path Cost** - Displays whether the external path cost is automatically calculated (Enabled) or not (Disabled). External Path cost will be calculated based on the link speed of the port if the configured value for External Port Path Cost is zero.
- **Port ID** - The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
- **Port Up Time Since Counters Last Cleared** - Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.

- **Port Forwarding State** - The Forwarding State of this port.
- **Port Role** - Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
- **Designated Root** - Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
- **Designated Cost** - Path Cost offered to the LAN by the Designated Port.
- **Designated Bridge** - Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
- **Designated Port** - Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
- **Topology Change Acknowledge** - Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either "True" or "False".
- **Edge port** - indicates whether the port is enabled as an edge port. It takes the value "Enabled" or "Disabled".
- **Point-to-point MAC** - Derived value of the point-to-point status.
- **CST Regional Root** - Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
- **CST Path Cost** - Path Cost to the CST Regional Root.

Command Buttons

- **Submit** - Applies the new configuration and causes the changes to take effect. These changes will not be retained across a power cycle unless a save configuration is performed.
- **Force** - Clicking this button will force the port to send out 802.1w or 802.1d BPDUs.
- **Refresh** - Refreshes the screen with most recent data.

4.3.8.5 Spanning Tree MST Port Configuration/Status

Selection Criteria

- **MST ID -** Selects one MST instance from existing MST instances.
- **Slot.Port -** Selects one of the physical or lag interfaces associated with VLANs associated with the selected MST instance.

Configurable Data

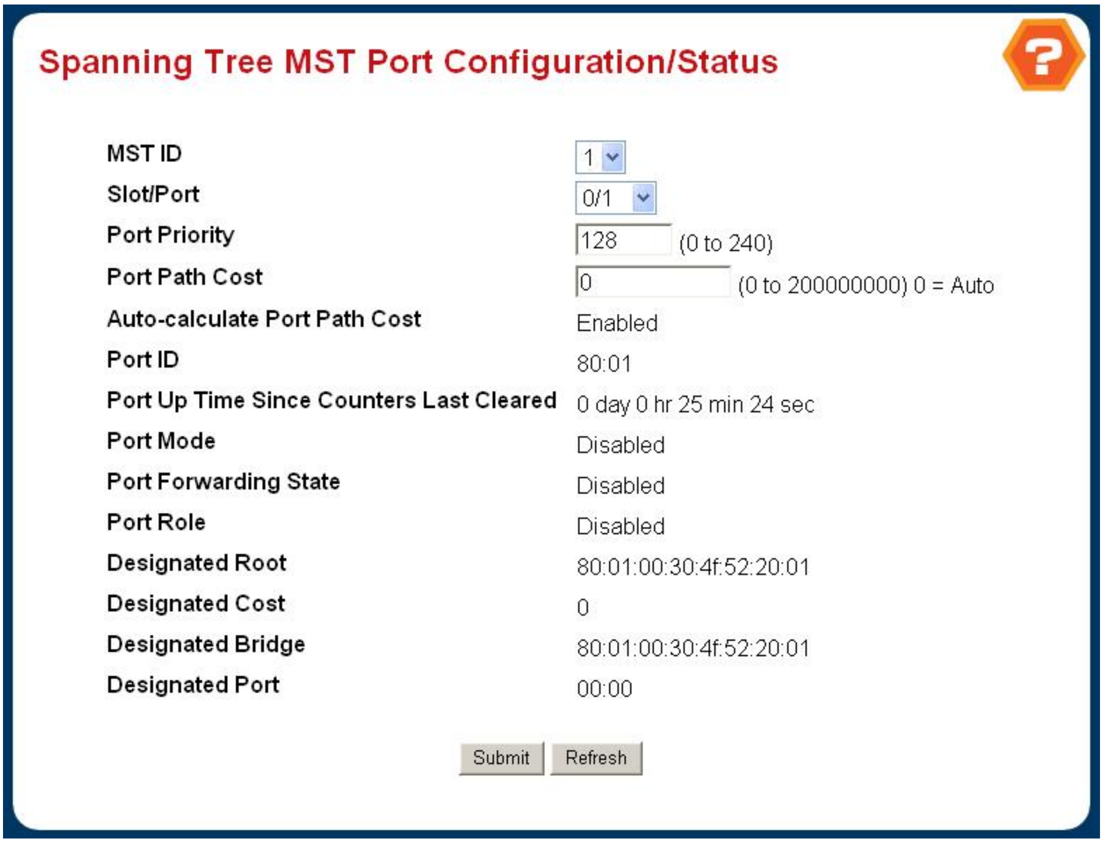
- **Port Priority -** The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and (2*16-1) it will be set to 16 and so on.
- **Port Path Cost -** Set the Path Cost to a new value for the specified port in the selected MST instance. It takes a value in the range of 1 to 200000000.

Non-Configurable Data

- **Auto-calculate Port Path Cost -** Displays whether the path cost is automatically calculated (Enabled) or not

(Disabled). Path cost will be calculated based on the link speed of the port if the configured value for Port Path Cost is zero.

- **Port ID -** The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
- **Port Up Time Since Counters Last Cleared -** Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
- **Port Mode -** Spanning Tree Protocol Administrative Mode associated with the port or lag. The possible values are Enable or Disable.
- **Port Forwarding State -** The Forwarding State of this port.
- **Port Role -** Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
- **Designated Root -** Root Bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
- **Designated Cost -** Path Cost offered to the LAN by the Designated Port.
- **Designated Bridge -** Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
- **Designated Port -** Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

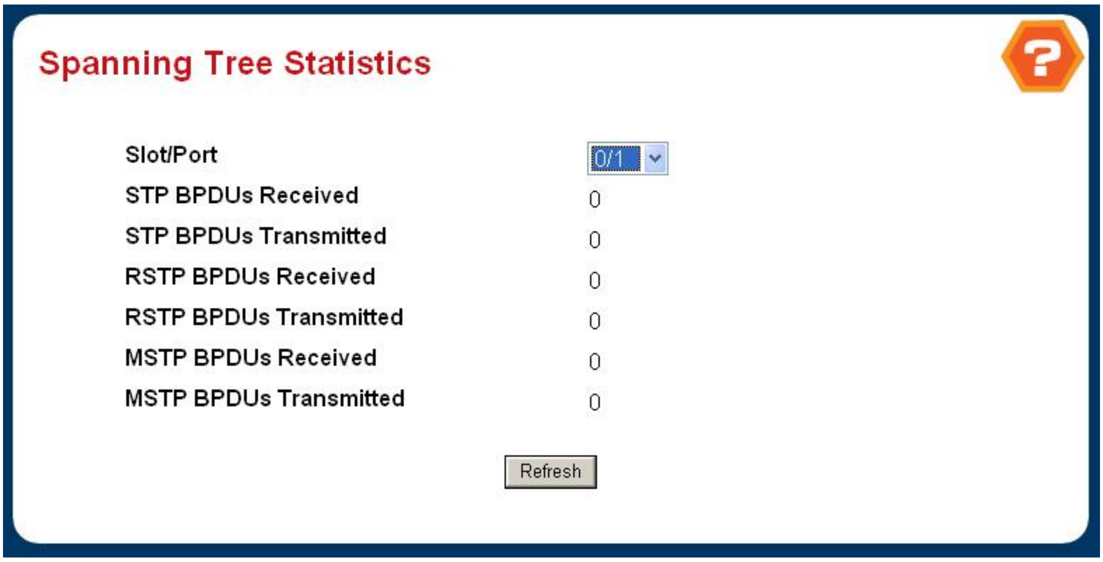


Spanning Tree MST Port Configuration/Status

MST ID	1
Slot/Port	0/1
Port Priority	128 (0 to 240)
Port Path Cost	0 (0 to 200000000) 0 = Auto
Auto-calculate Port Path Cost	Enabled
Port ID	80:01
Port Up Time Since Counters Last Cleared	0 day 0 hr 25 min 24 sec
Port Mode	Disabled
Port Forwarding State	Disabled
Port Role	Disabled
Designated Root	80:01:00:30:4f:52:20:01
Designated Cost	0
Designated Bridge	80:01:00:30:4f:52:20:01
Designated Port	00:00

Figure 4-3-38 Spanning Tree MST Port Configuration/Status

4.3.8.6 Spanning Tree Statistics



Spanning Tree Statistics

Slot/Port	0/1
STP BPDUs Received	0
STP BPDUs Transmitted	0
RSTP BPDUs Received	0
RSTP BPDUs Transmitted	0
MSTP BPDUs Received	0
MSTP BPDUs Transmitted	0

Figure 4-3-39 Spanning Tree Statistics

Selection Criteria

◦ **Slot.Port -** Selects one of the physical or lag interfaces of the switch.

Non-Configurable Data

◦ **STP BPDUs Received -** Number of STP BPDUs received at the selected port.

◦ **STP BPDUs Transmitted -** Number of STP BPDUs transmitted from the selected port.

◦ **RSTP BPDUs Received -** Number of RSTP BPDUs received at the selected port.

◦ **RSTP BPDUs Transmitted -** Number of RSTP BPDUs transmitted from the selected port.

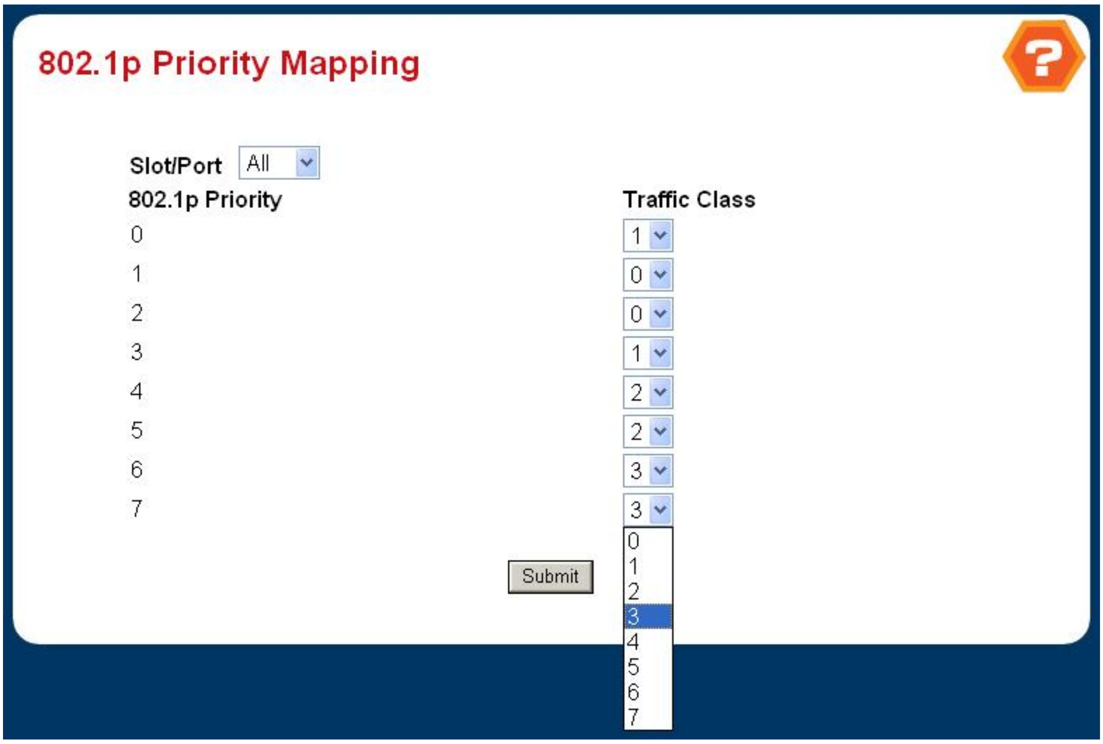
◦ **MSTP BPDUs Received -** Number of MSTP BPDUs received at the selected port.

◦ **MSTP BPDUs Transmitted -** Number of MSTP BPDUs transmitted from the selected port.

4.3.9 Class of Service

4.3.9.1 802.1p Priority Mapping

This page is to configure the IEEE 802.1p priority mapping on the port.



802.1p Priority Mapping

Slot/Port All

802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Figure 4-3-40 802.1p Priority Mapping

- **Slot.Port -** Select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to the same values.
- **Traffic Class -** Specify which internal traffic class to map the corresponding 802.1p priority.
- **802.1p Priority -** Displays the 802.1p priority to be mapped.

4.4 Security

This section is to control the access of the switch, includes the user access and management control.

The Security page contains links to the following topics:

- **Port Access Control**
- **RADIUS**
- **TACACS+**
- **Secure HTTP**
- **Secure Shell**

Understanding IEEE 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

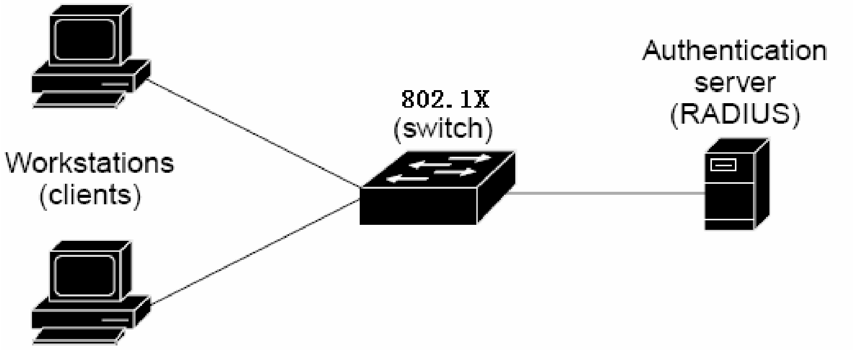
Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.



- ***Client***—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- ***Switch* (802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

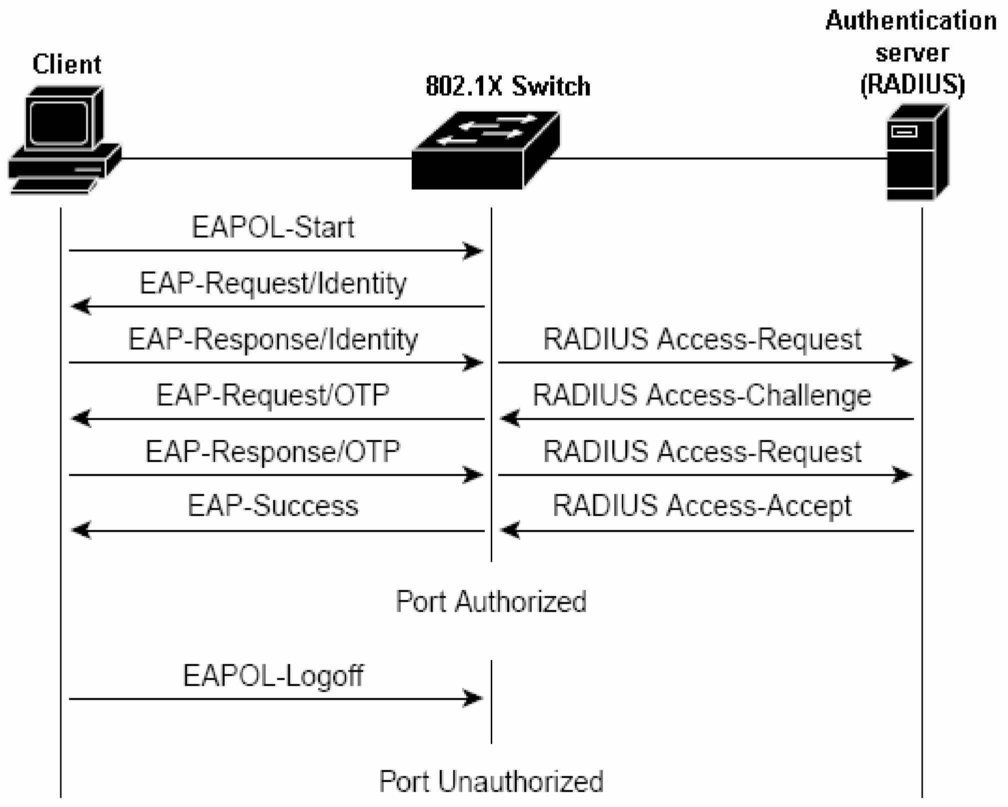
However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity

Notice:

> If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. “Figure 2-43” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.



- **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

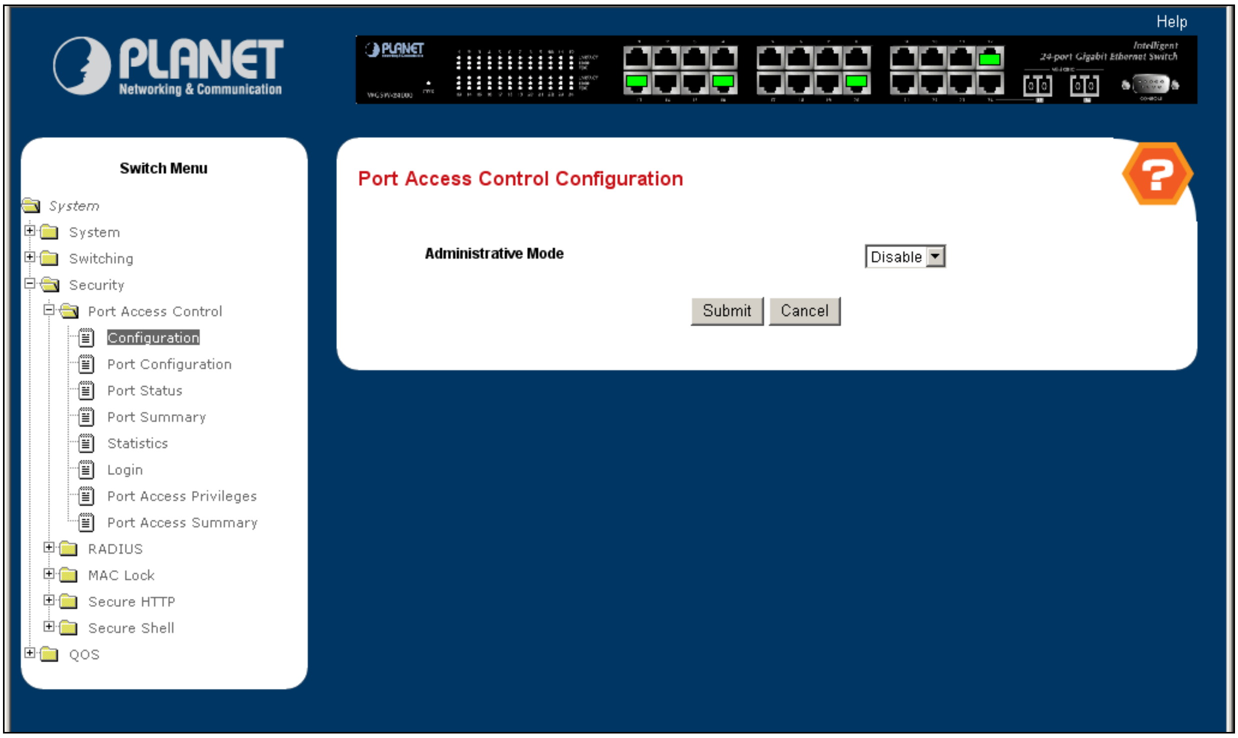
If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.4.1 Port Access Control

4.4.1.1 Port Access Control Configuration

This page is to Enable/Disable the port access control administrative mode.

- **Administrative Mode -** This selector lists the two options for administrative mode: enable and disable. The default value is disabled.



Port Access Control Configuration

Administrative Mode: Disable

Submit Cancel

Figure 4-4-1 Port Access Control Configuration

4.4.1.2 Port Access Control Port Configuration

- **Port -** Selects the port to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.
- **Control Mode -** This selector lists the options for control mode. The control mode is only set if the link status of the port is link up. The options are:
  - **force unauthorized:** The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized
  - **force authorized:** The authenticator PAE unconditionally sets the controlled port to authorized.

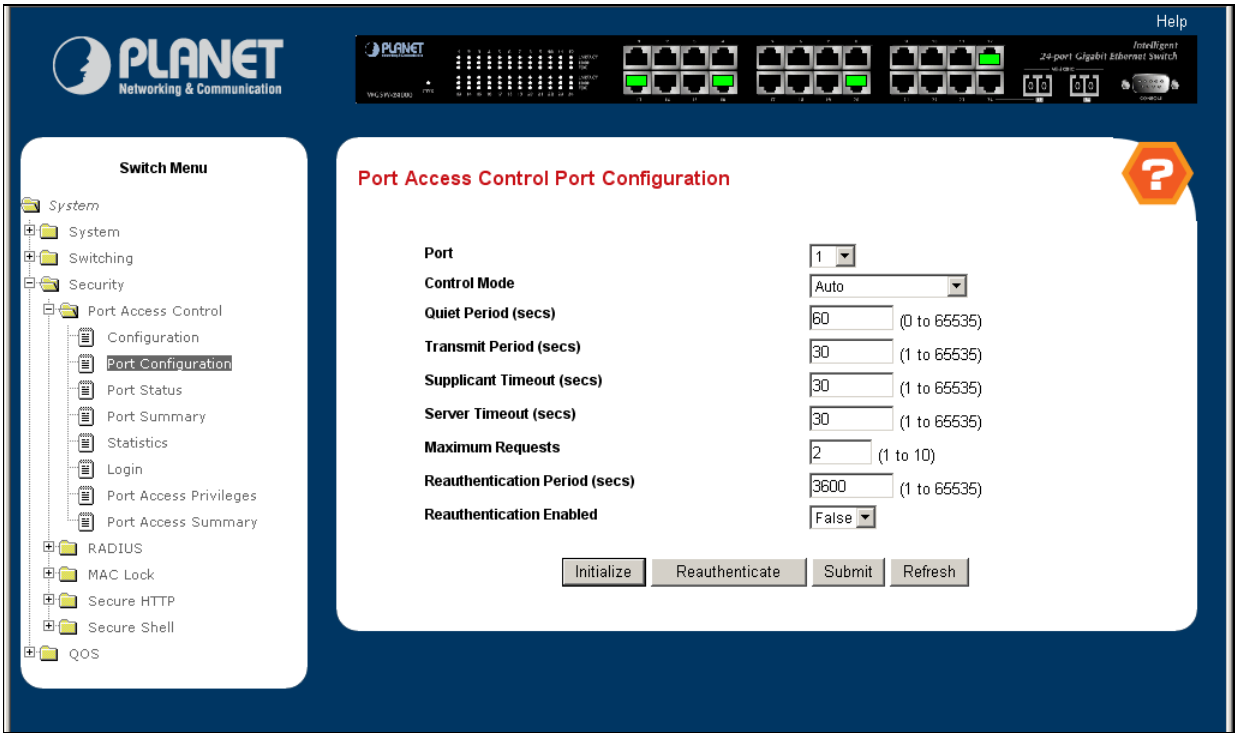
- **auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

- **Quiet Period -** This input field allows the user to configure the quiet period for the selected port. This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period must be a number in the range of 0 and 65535. A quiet period value of 0 means that the authenticator state machine will never acquire a supplicant. The default value is 60. Changing the value will not change the configuration until the Submit button is pressed.
- **Transmit Period -** This input field allows the user to configure the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The transmit period must be a number in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.
- **Supplicant Timeout -** This input field allows the user to enter the supplicant timeout for the selected port. The supplicant timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supplicant timeout must be a value in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.
- **Server Timeout -** This input field allows the user to enter the server timeout for the selected port. The server timeout is the value, in seconds, of the timer used by the authenticator on this port to timeout the authentication server. The server timeout must be a value in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.
- **Maximum Requests -** This input field allows the user to enter the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value must be in the range of 1 and 10. The default value is 2. Changing the value will not change the configuration until the Submit button is pressed.
- **Reauthentication Period -** This input field allows the user to enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1 and 65535. The default value is 3600. Changing the value will not change the configuration until the Submit button is pressed.
- **Reauthentication Enabled -** This select field allows the user to enable or disable reauthentication of the supplicant for the specified port. The selectable values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed. The default value is false. Changing the selection will not change the configuration until the Submit button is pressed.

Command Buttons

- **Initialize -** This button begins the initialization sequence on the selected port. This button is only selectable if the control mode is is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.

- **Reauthenticate -** This button begins the reauthentication sequence on the selected port. This button is only selectable if the control mode is is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.
- **Submit -** Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Update the information on the page.
- Initialize - This button begins the initialization sequence on the selected port. This button is only selectable if the control mode is is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.
- **Reauthenticate -** This button begins the reauthentication sequence on the selected port. This button is only selectable if the control mode is is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.
- **Submit -** Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Update the information on the page.



Port Access Control Port Configuration

Port	1	
Control Mode	Auto	
Quiet Period (secs)	60	(0 to 65535)
Transmit Period (secs)	30	(1 to 65535)
Supplicant Timeout (secs)	30	(1 to 65535)
Server Timeout (secs)	30	(1 to 65535)
Maximum Requests	2	(1 to 10)
Reauthentication Period (secs)	3600	(1 to 65535)
Reauthentication Enabled	False	

Figure 4-4-2 Port Access Control Port Configuration

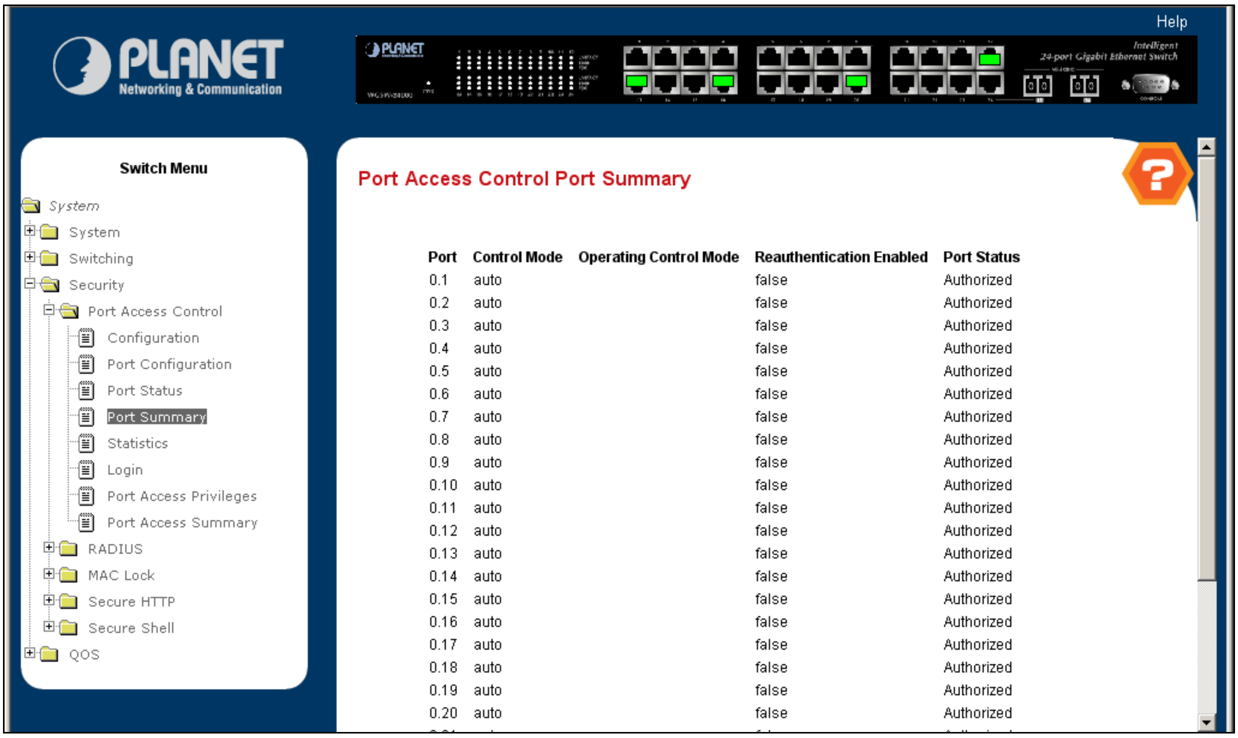
4.4.1.3 Port Access Control Port Summary

This page shows the summary of the port access control configuration parameters.

- **Port -** Specifies the port whose settings are displayed in the current table row.
- **Control Mode -** This field indicates the configured control mode for the port. Possible values are:
  - ➢ **Force Unauthorized:** The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized

- **Force Authorized:** The authenticator PAE unconditionally sets the controlled port to authorize.
- **Auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

- **Operating Control Mode -** This field indicates the control mode under which the port is actually operating. Possible values are:
  - **ForceUnauthorized**
  - **ForceAuthorized**
  - **Auto**
- **Reauthentication Enabled -** This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.
- **Port Status -** This field shows the authorization status of the specified port. The possible values are 'Authorized' and 'Unauthorized'.



Port Access Control Port Summary

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
0.1	auto		false	Authorized
0.2	auto		false	Authorized
0.3	auto		false	Authorized
0.4	auto		false	Authorized
0.5	auto		false	Authorized
0.6	auto		false	Authorized
0.7	auto		false	Authorized
0.8	auto		false	Authorized
0.9	auto		false	Authorized
0.10	auto		false	Authorized
0.11	auto		false	Authorized
0.12	auto		false	Authorized
0.13	auto		false	Authorized
0.14	auto		false	Authorized
0.15	auto		false	Authorized
0.16	auto		false	Authorized
0.17	auto		false	Authorized
0.18	auto		false	Authorized
0.19	auto		false	Authorized
0.20	auto		false	Authorized

Figure 4-4-3 Port Access Control Port Summary

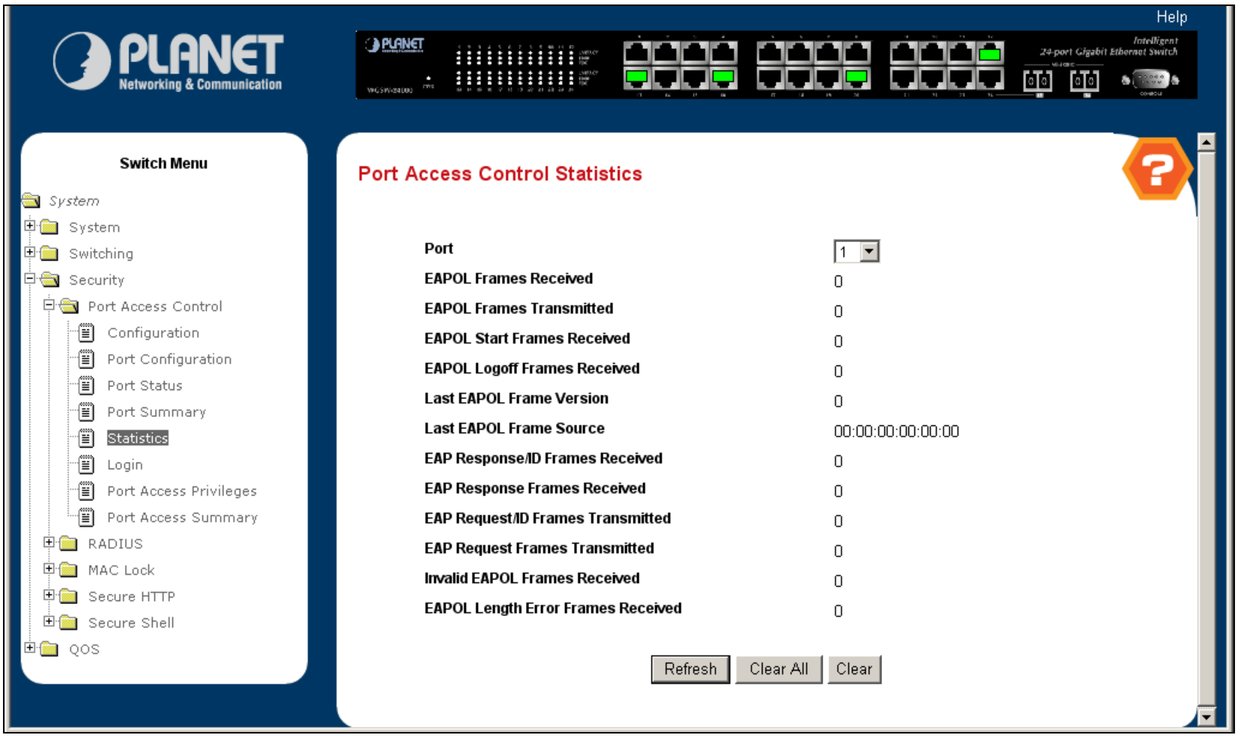
4.4.1.4 Port Access Control Statistics

This page shows the statistics of access control on each port.

- **Port -** Selects the port to be displayed. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.
- **EAPOL Frames Received -** This displays the number of valid EAPOL frames of any type that have been received by this authenticator.
- **EAPOL Frames Transmitted -** This displays the number of EAPOL frames of any type that have been transmitted by this authenticator.
- **EAPOL Start Frames Received -** This displays the number of EAPOL start frames that have been received by

this authenticator.

- **EAPOL Logoff Frames Received -** This displays the number of EAPOL logoff frames that have been received by this authenticator.
- **Last EAPOL Frame Version -** This displays the protocol version number carried in the most recently received EAPOL frame.
- **Last EAPOL Frame Source -** This displays the source MAC address carried in the most recently received EAPOL frame.
- **EAP Response/Id Frames Received -** This displays the number of EAP response/identity frames that have been received by this authenticator.
- **EAP Response Frames Received -** This displays the number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
- **EAP Request/Id Frames Transmitted -** This displays the number of EAP request/identity frames that have been transmitted by this authenticator.
- **EAP Request Frames Transmitted -** This displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
- **Invalid EAPOL Frames Transmitted -** This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
- **EAP Length Error Frames Received -** This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.



Port Access Control Statistics

Port	1
EAPOL Frames Received	0
EAPOL Frames Transmitted	0
EAPOL Start Frames Received	0
EAPOL Logoff Frames Received	0
Last EAPOL Frame Version	0
Last EAPOL Frame Source	00:00:00:00:00:00
EAP Response/ID Frames Received	0
EAP Response Frames Received	0
EAP Request/ID Frames Transmitted	0
EAP Request Frames Transmitted	0
Invalid EAPOL Frames Received	0
EAPOL Length Error Frames Received	0

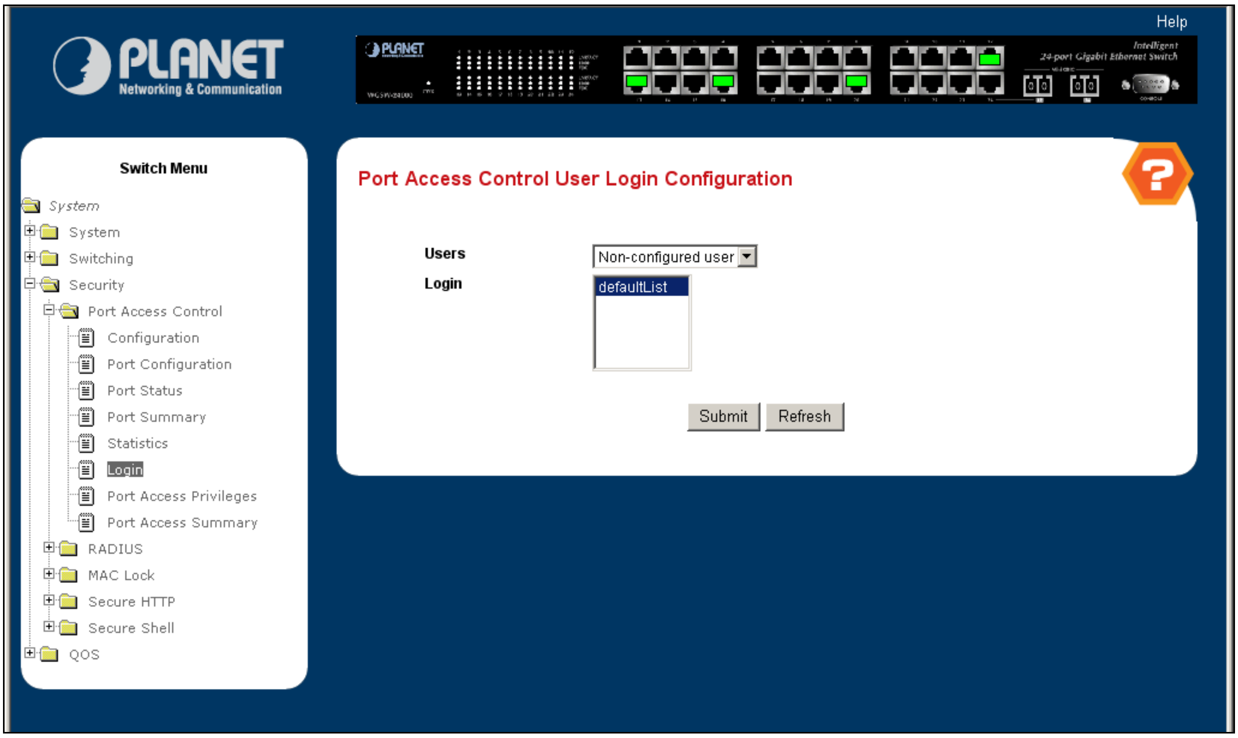
Figure 4-4-4 Port Access Control Statistics

4.4.1.5 Port Access Control User Login Configuration

This page is to configure the login control list of the user.

- **Users -** Selects the user name that will use the selected login list for 802.1x port security.
- **Login -** Selects the login to apply to the specified user. All configured logins are displayed.

- **Submit -** Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Update the information on the page.



Port Access Control User Login Configuration

Users: Non-configured user

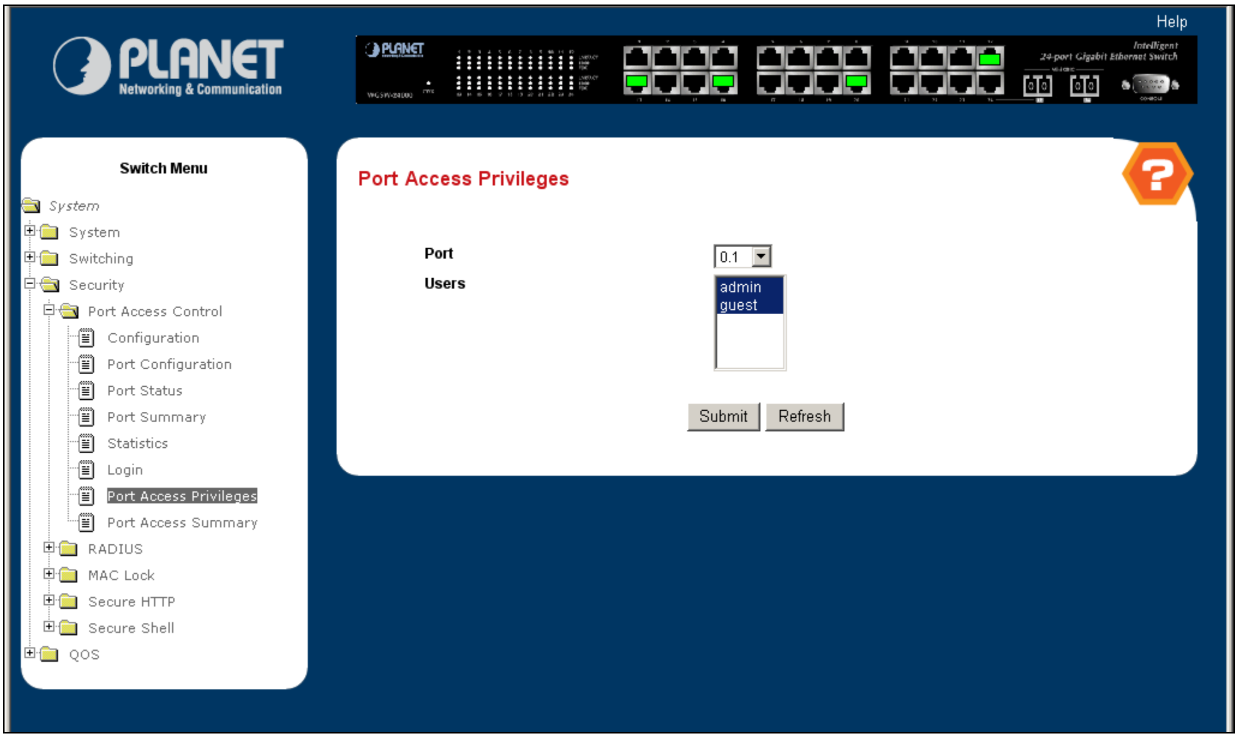
Login: defaultList

Figure 4-4-5 Port Access Control User Login Configuration

4.4.1.6 Port Access Privileges

Use this page to define the user access privilege on the port.

- **Port -** Selects the port to configure.
- **Users -** Selects the users that have access to the specified port or ports.
- **Submit -** Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Update the information on the page.



Port Access Privileges

Port 0.1

Users admin guest

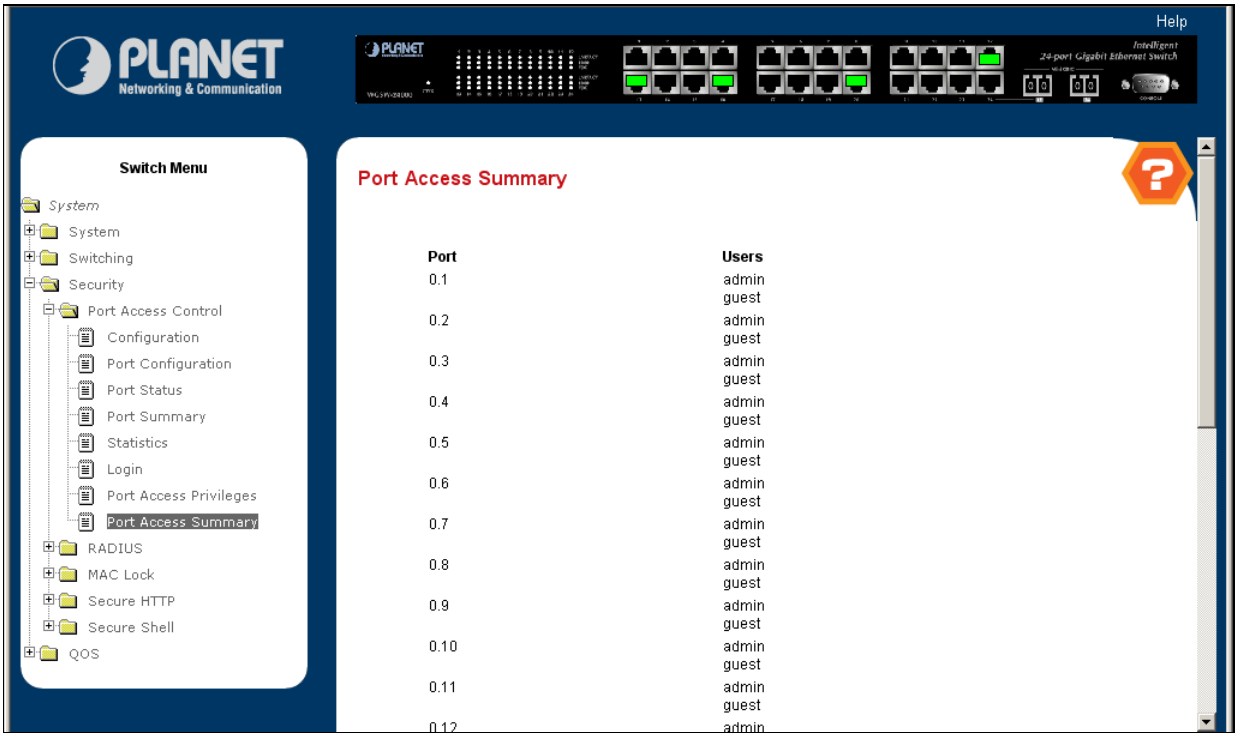
Submit Refresh

Figure 4-4-6 Port Access Privileges

4.4.1.7 Port Access Summary

This page is to show the configured access control on each port.

- **Port -** Displays the port in slot.port format.
- **Users -** Displays the users that have access to the port.



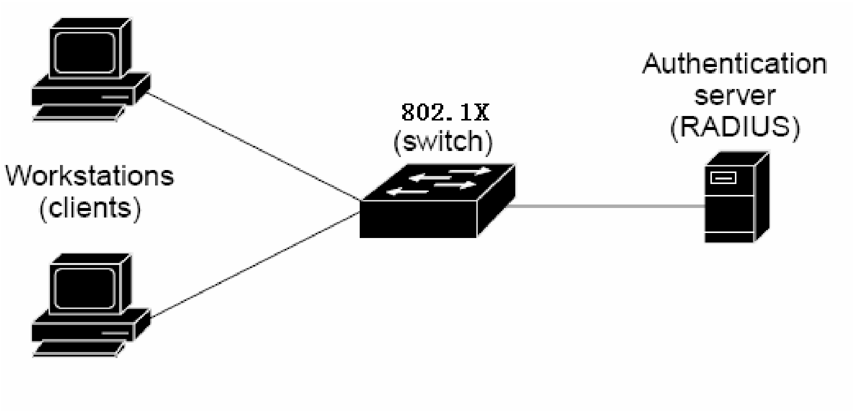
Port Access Summary

Port	Users
0.1	admin guest
0.2	admin guest
0.3	admin guest
0.4	admin guest
0.5	admin guest
0.6	admin guest
0.7	admin guest
0.8	admin guest
0.9	admin guest
0.10	admin guest
0.11	admin guest
0.12	admin

Figure 4-4-7 Port Access Summary

4.4.2 RADIUS

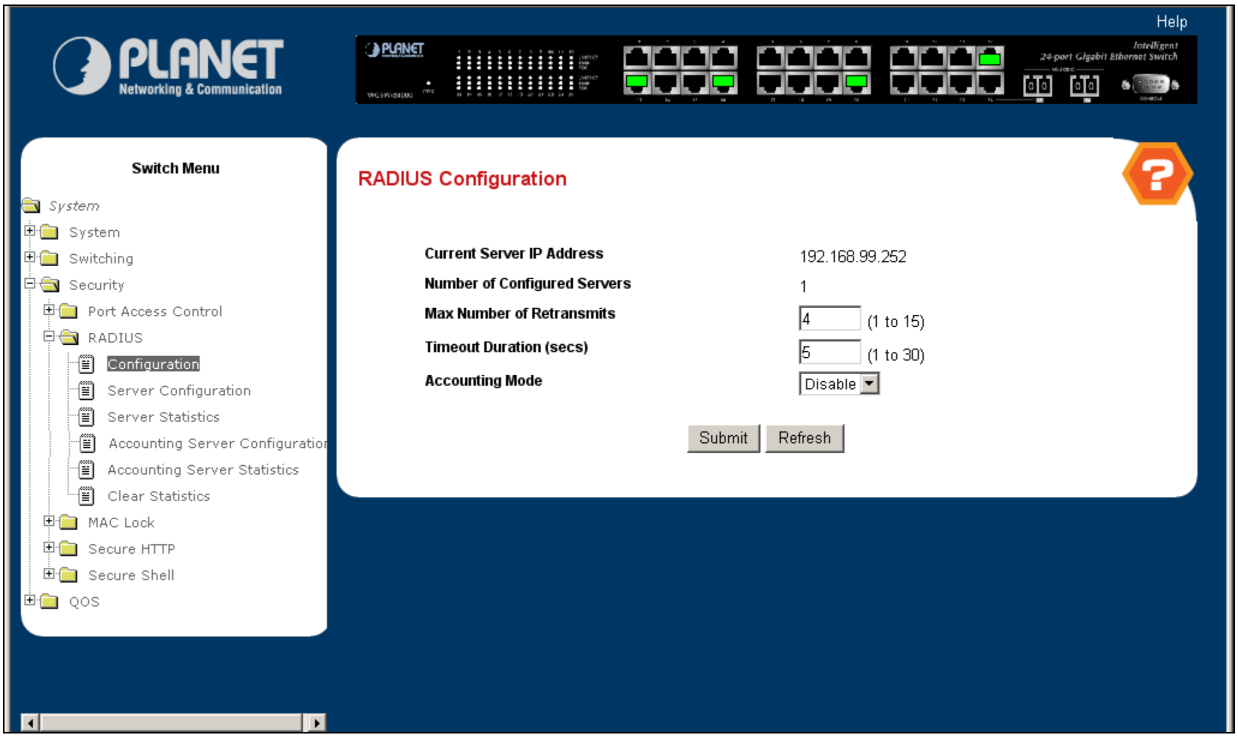
Radius Server — In this situation, need a Radius server in the network, the normal topologies as below



4.4.2.1 RADIUS Configuration

This page is to configure the RADIUS server connection session parameters.

- **Max Number of Retransmits -** The value of the maximum number of times a request packet is retransmitted. The valid range is 1 - 15. Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
- **Timeout Duration (secs) -** The timeout value, in seconds, for request retransmissions. The valid range is 1 - 30. Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
- **Accounting Mode -** Selects if the RADIUS accounting mode is enabled or disabled.
- Non-Configurable Data
- **Current Server IP Address -** The IP address of the current server. This field is blank if no servers are configured.
- **Number of Configured Servers -** The number of RADIUS servers that have been configured. This value will be in the range of 0 and 3.



RADIUS Configuration

Current Server IP Address	192.168.99.252
Number of Configured Servers	1
Max Number of Retransmits	4 (1 to 15)
Timeout Duration (secs)	5 (1 to 30)
Accounting Mode	Disable

Figure 4-4-8 RADIUS Configuration

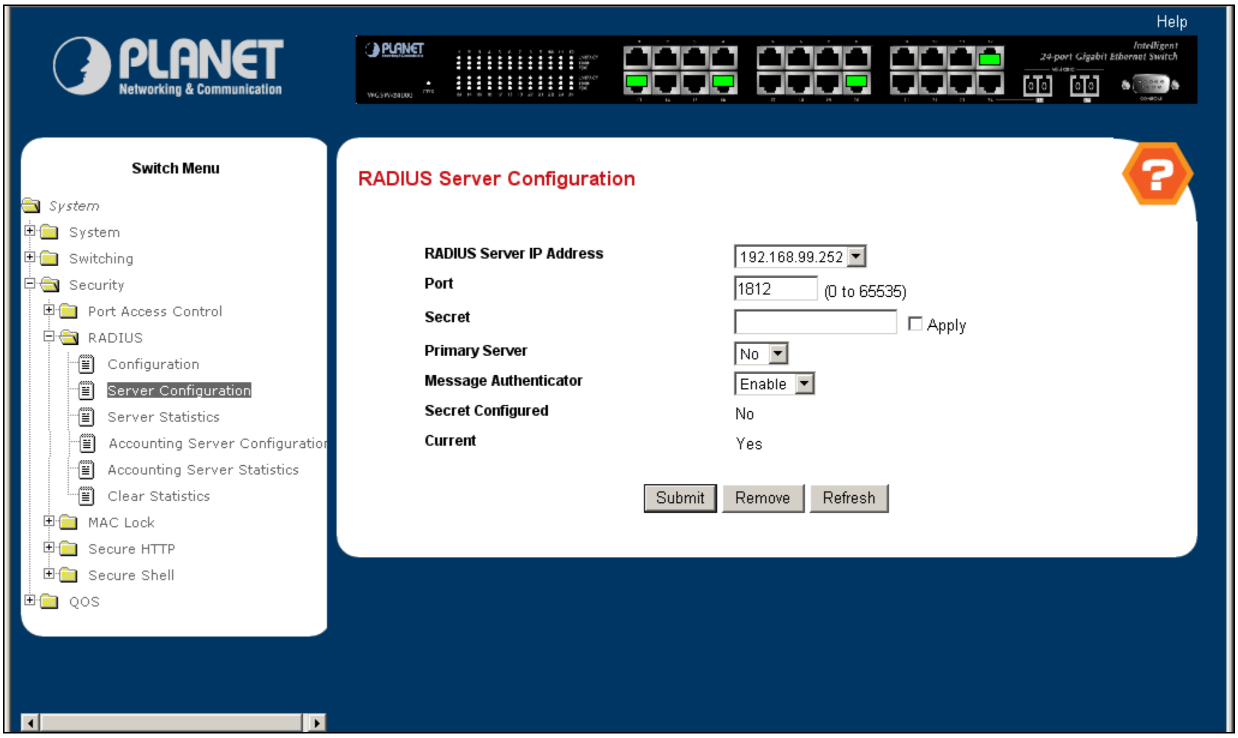
4.4.2.2 RADIUS Server Configuration

This page is to configure the RADIUS server connection features.

- **RADIUS Server IP Address -** Selects the RADIUS server to be configured. Select add to add a server.
- **IP Address -** The IP address of the server being added.
- **Port -** The UDP port used by this server. The valid range is 0 - 65535.
- **Secret -** The shared secret for this server. This is an input field only.
- **Apply -** The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.
- **Primary Server -** Sets the selected server to thePrimary or Secondary server.
- **Message Authenticator -** Enable or disable the message authenticator attribute for the selected server.
- **Current -** Indicates if this server is currently in use as the authentication server.
- **Secret Configured -** Indicates if the shared secret for this server has been configured.

Command Buttons

- **Submit -** Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Remove -** Remove the selected server from the configuration. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Update the information on the page.



RADIUS Server Configuration

RADIUS Server IP Address: 192.168.99.252

Port: 1812 (0 to 65535)

Secret: □ Apply

Primary Server: No

Message Authenticator: Enable

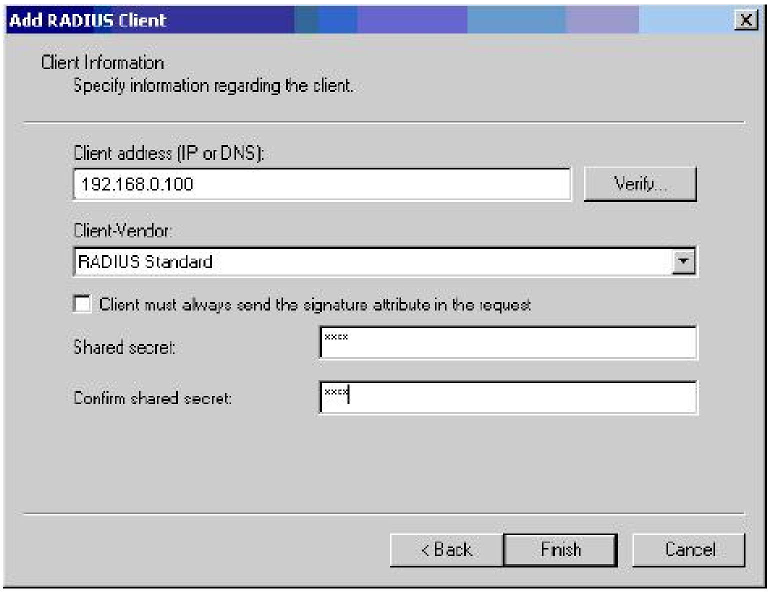
Secret Configured: No

Current: Yes

Figure 4-4-9 RADIUS Server Configuration

■ Windows Platform RADIUS Server Configuration

1. Setup the RADIUS server and assign the client IP address to the Web-Smart switch. In this case, field in the default IP Address of the Web-Smart switch with 192.168.0.100. And also make sure the shared secret key is as same as the one you had set at the switch RADIUS server – 12345678 at this case.



Client Information
Specify information regarding the client.

Client address (IP or DNS): 192.168.0.100

Client-Vendor: RADIUS Standard

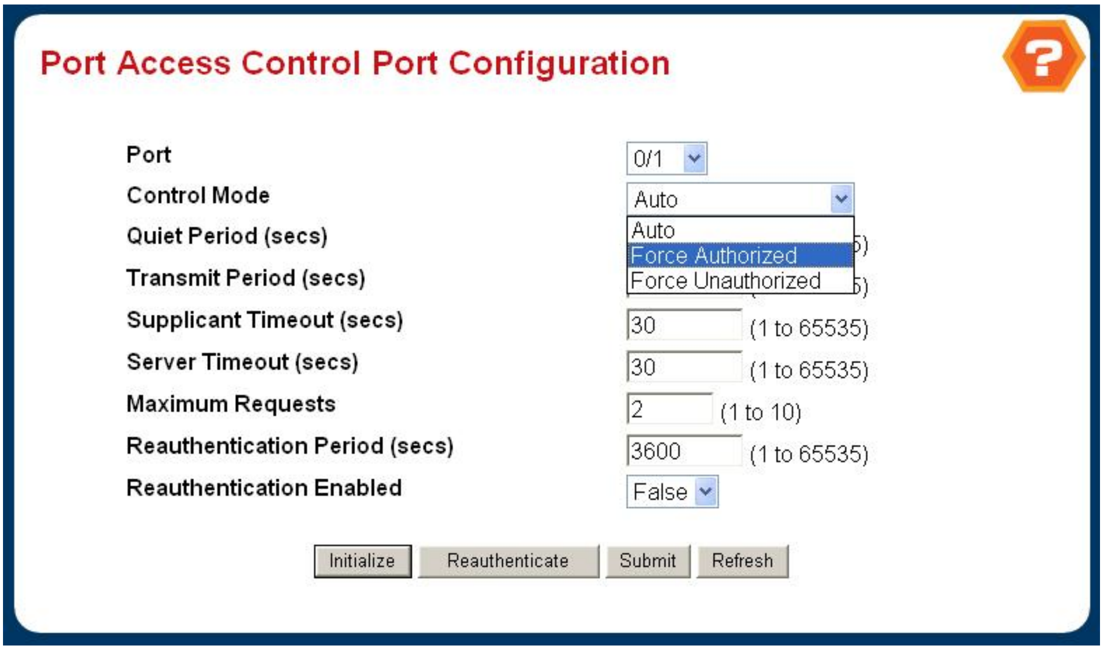
□ Client must always send the signature attribute in the request

Shared secret: xxxx

Confirm shared secret: xxxx

Figure 4-4-10 Windows Server RADIUS Server setting

2. Configure ports attribute of 802.1X, the same as “802.1X Port Status Configuration”.



Port Access Control Port Configuration

Port	0/1	
Control Mode	Auto Auto Force Authorized Force Unauthorized	
Quiet Period (secs)		5)
Transmit Period (secs)		5)
Supplicant Timeout (secs)	30	(1 to 65535)
Server Timeout (secs)	30	(1 to 65535)
Maximum Requests	2	(1 to 10)
Reauthentication Period (secs)	3600	(1 to 65535)
Reauthentication Enabled	False	

Notice: Set the Ports Authenticate Status to “Force Authorized” if the port is connected to the RADIUS server or the port is a uplink port that is connected to another switch. Or once the 802.1X stat to work, the switch might not be able to access the RADIUS server.

3. Create user data. That step are different of “Local Authenticate”, the establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2000 Server, and then:

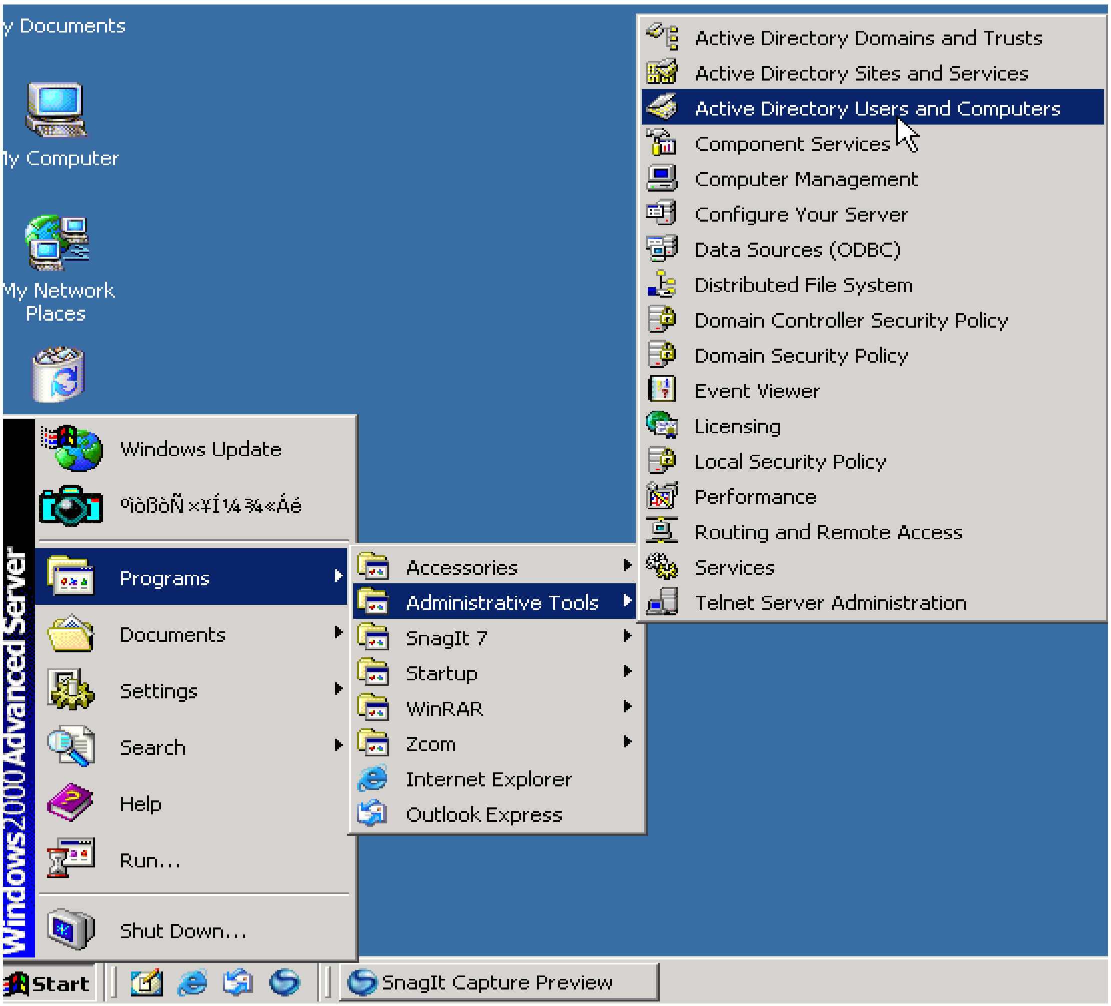
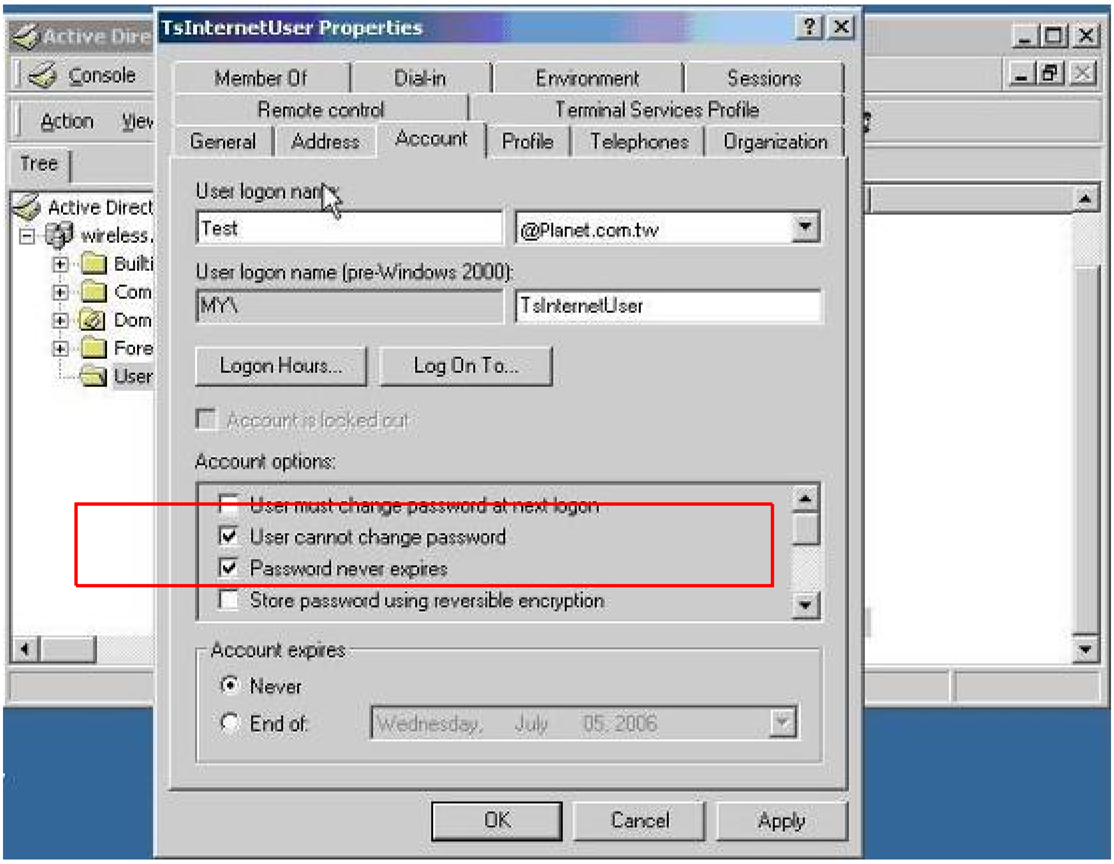


Figure 4-4-11 Windows Server RADIUS Server setting path

Enter " **Active Directory Users and Computers**", create legal user data, the next, right-click a user what you created to enter properties, and what to be noticed:



User logon name: Test @Planet.com.tw

User logon name (pre-Windows 2000): MY\ TsInternetUser

□ Account is locked out

Account options:

□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Wednesday, July 05, 2006

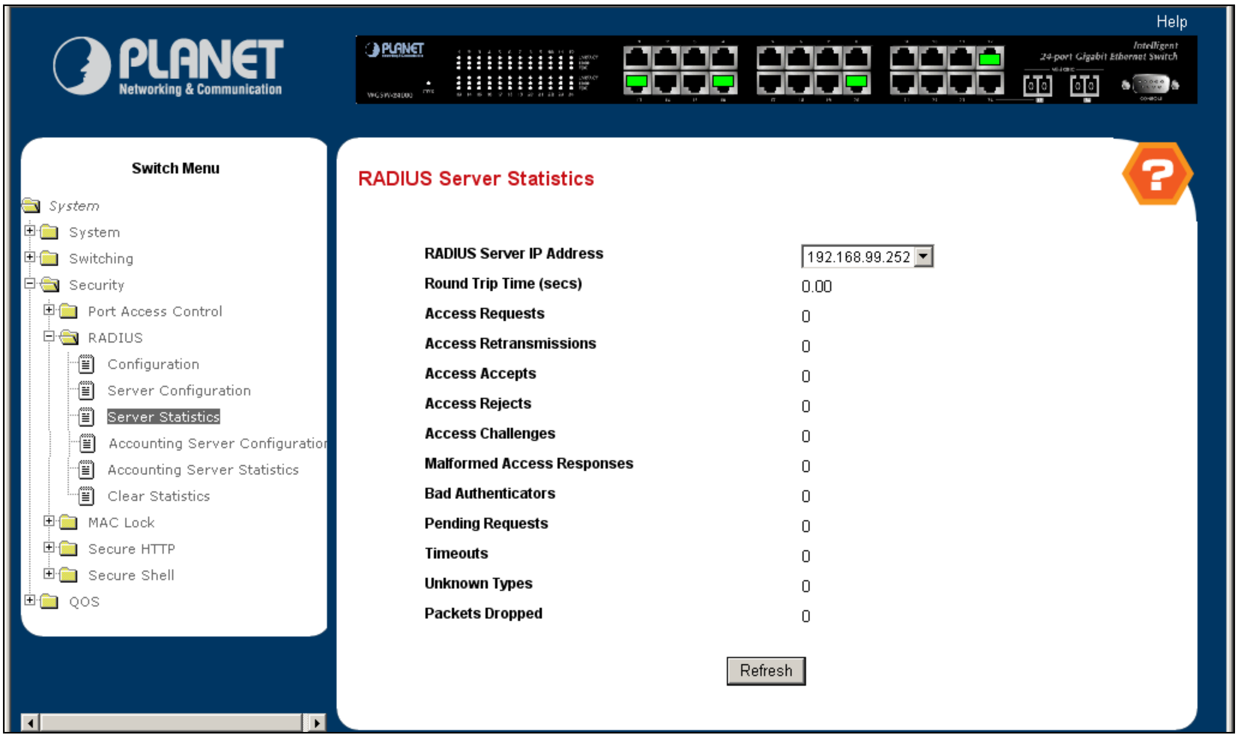
Figure 4-4-12 TsInternetUser Properties screen

4.4.2.3 RADIUS Server Statistics

This page shows the statistics of RADIUS Server usage.

- **RADIUS Server IP Address -** Selects the IP address of the RADIUS server for which to display statistics.
- **Round Trip Time (secs) -** 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.
- **Access Requests -** The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
- **Access Retransmissions -** The number of RADIUS Access-Request packets retransmitted to this server.
- **Access Accepts -** The number of RADIUS Access-Accept packets, including both valid and invalid packets that were received from this server.
- **Access Rejects -** The number of RADIUS Access-Reject packets, including both valid and invalid packets that were received from this server.
- **Access Challenges -** The number of RADIUS Access-Challenge packets, including both valid and invalid packets that were received from this server.
- **Malformed Access Responses -** 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 unknown types are not included as malformed access-responses.
- **Bad Authenticators -** The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

- **Pending Requests -** The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
- **Timeouts -** The number of authentication timeouts to this server.
- **Unknown Types -** The number of RADIUS packets of unknown type which were received from this server on the authentication port.
- **Packets Dropped -** The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.



RADIUS Server Statistics

RADIUS Server IP Address	192.168.99.252
Round Trip Time (secs)	0.00
Access Requests	0
Access Retransmissions	0
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Access Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Figure 4-4-13 RADIUS Server Statistics

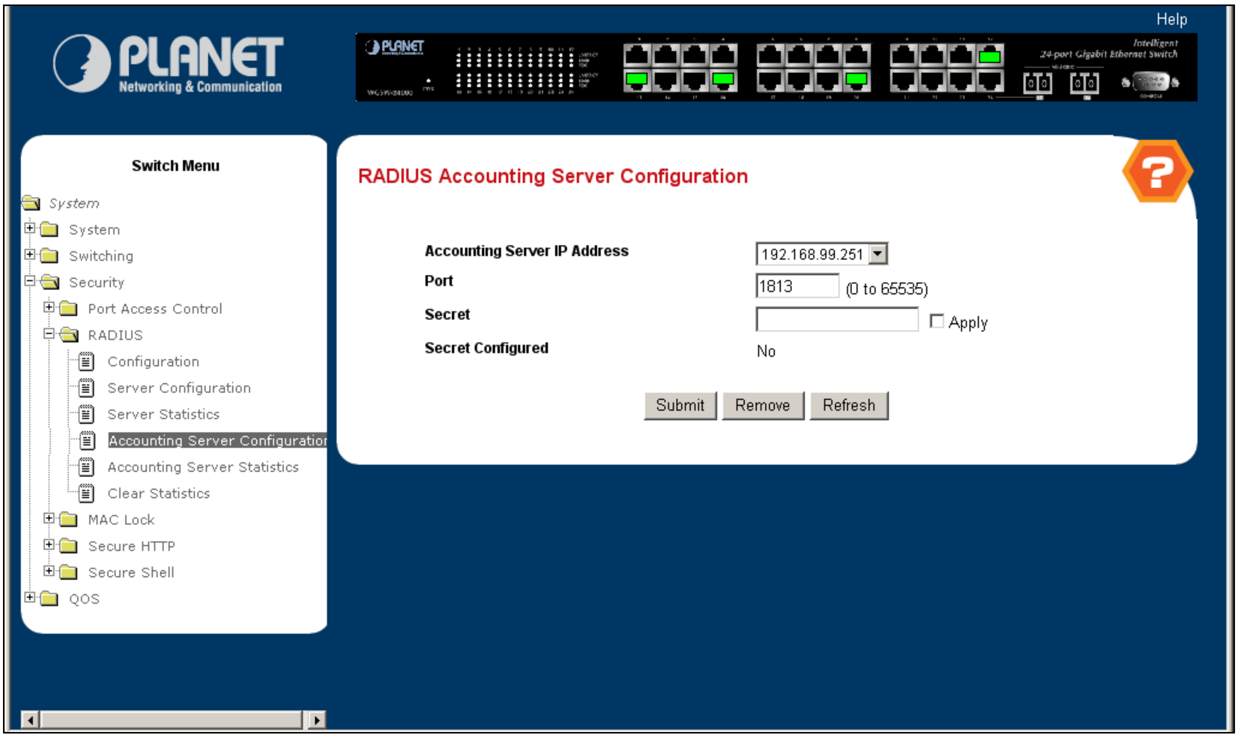
4.4.2.4 RADIUS Accounting Server Configuration

This page is to configure the RADIUS Accounting Server

- **Accounting Server IP Address -** Selects the accounting server for which data is to be displayed or configured. If the add item is selected, a new accounting server can be configured.
- **IP Address -** The IP address of the accounting server to add. This field is only configurable if the add item is selected.
- **Port - S**pecifies the UDP Port to be used by the accounting server. The valid range is 0 - 65535. If the user has READONLY access, the value is displayed but cannot be changed.
- **Secret -** Specifies the shared secret to use with the specfied accounting server. This field is only displayed if the user has READWRITE access.
- **Apply -** The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.
- **Secret Configured -** Indicates if the secret has been configured for this accounting server.

Command Buttons

- **Submit -** Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Remove -** Remove the selected accounting server from the configuration. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Update the information on the page.



RADIUS Accounting Server Configuration

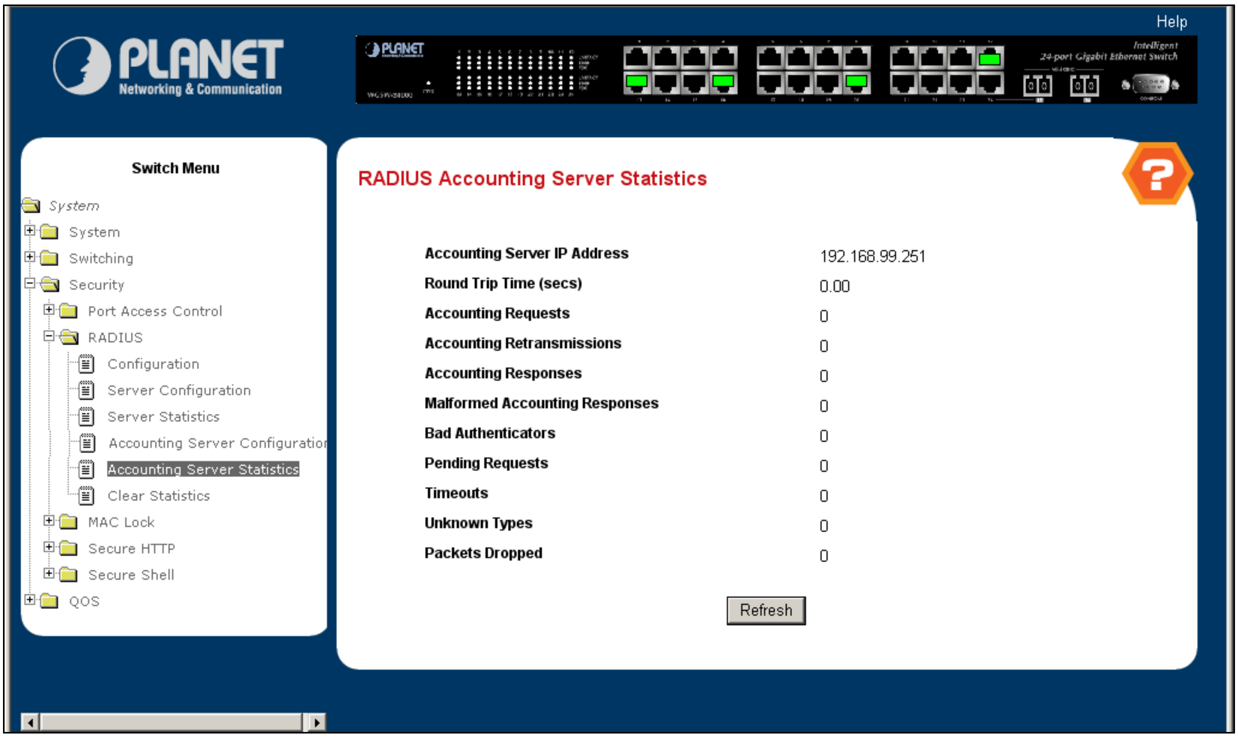
Accounting Server IP Address	192.168.99.251
Port	1813 (0 to 65535)
Secret	□ Apply
Secret Configured	No

Figure 4-4-14 RADIUS Accounting Server Configuration

4.4.2.5 RADIUS Accounting Server Statistics

This page shows the statistics of RADIUS Accounting Server.

- **Accounting Server IP Address -** Identifies the accounting server associated with the statistics.
- **Round Trip Time (secs) -** Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
- **Accounting Requests -** Displays the number of RADIUS Accounting-Request packets sent not including retransmissions.
- **Accounting Retransmissions -** Displays the number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
- **Accounting Responses -** Displays the number of RADIUS packets received on the accounting port from this server.
- **Malformed Accounting Responses -** Displays 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.
- **Bad Authenticators -** Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.
- **Pending Requests -** Displays the number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
- **Timeouts -** Displays the number of accounting timeouts to this server.
- **Unknown Types -** Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.
- **Packets Dropped -** Displays the number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.



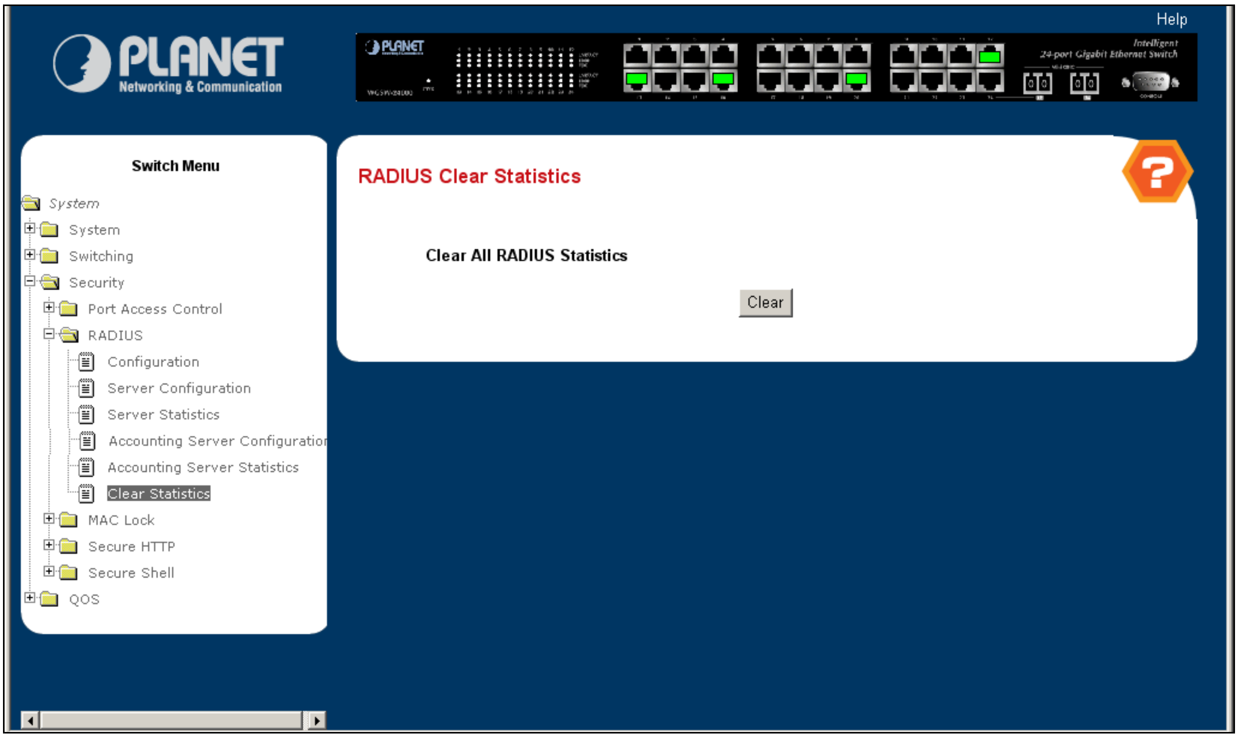
RADIUS Accounting Server Statistics

Accounting Server IP Address	192.168.99.251
Round Trip Time (secs)	0.00
Accounting Requests	0
Accounting Retransmissions	0
Accounting Responses	0
Malformed Accounting Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Figure 4-4-15 RADIUS Accounting Server Statistics

4.4.2.6 RADIUS Clear Statistics

This will clear the accounting server, authentication server and RADIUS statistics.



RADIUS Clear Statistics

Clear All RADIUS Statistics

Clear

Figure 4-4-16 RADIUS Clear Statistics

Command Buttons

- **Clear All RADIUS Statistics** - This button will clear the accounting server, authentication server and RADIUS statistics.

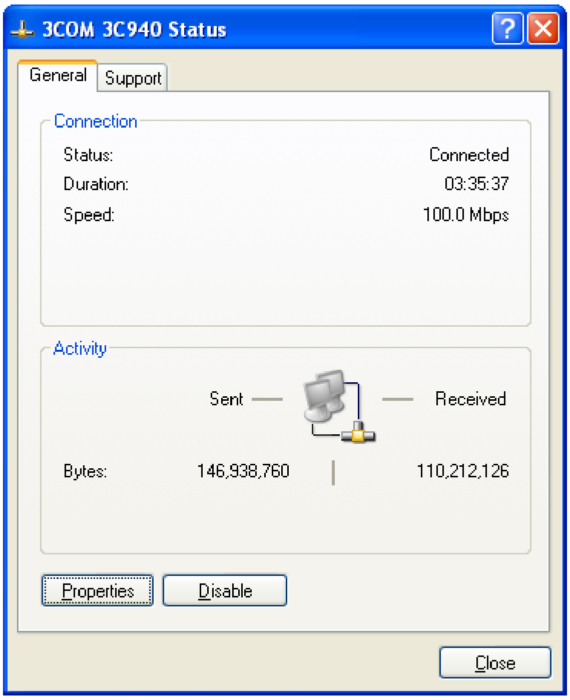
4.4.2.7 802.1X Client Configuration

Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.

Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

- **Configure Sample: EAP-MD5 Authentication**

1. Go to **Start** > **Control Panel,** double-click on “**Network Connections**”.
2. Right-click on the Local Network Connection.
3. Click “**Properties**” to open up the Properties setting window.


3COM 3C940 Status

Connection

Status: Connected
Duration: 03:35:37
Speed: 100.0 Mbps

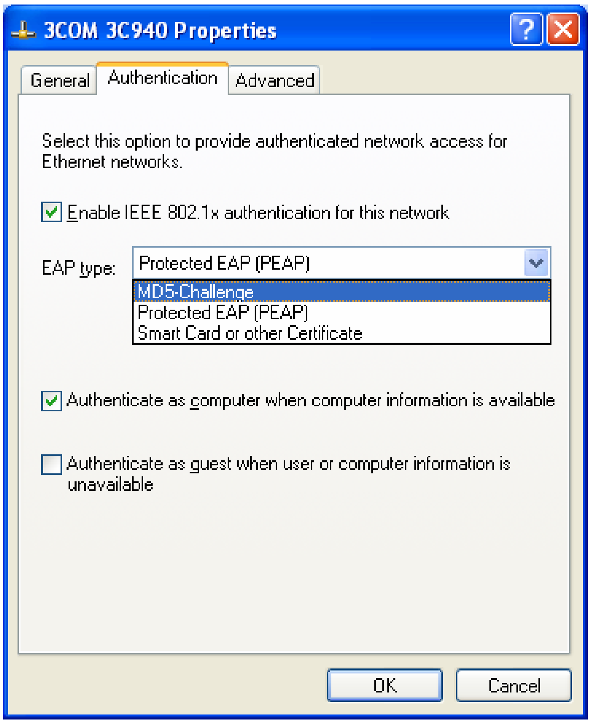
Activity

Sent — Received

Bytes: 146,938,760 | 110,212,126

4. Select “**Authentication**” tab.

5. Select “**Enable network access control using IEEE 802.1X**” to enable 802.1x authentication.


3COM 3C940 Properties

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

MD5-Challenge
Protected EAP (PEAP)
Smart Card or other Certificate

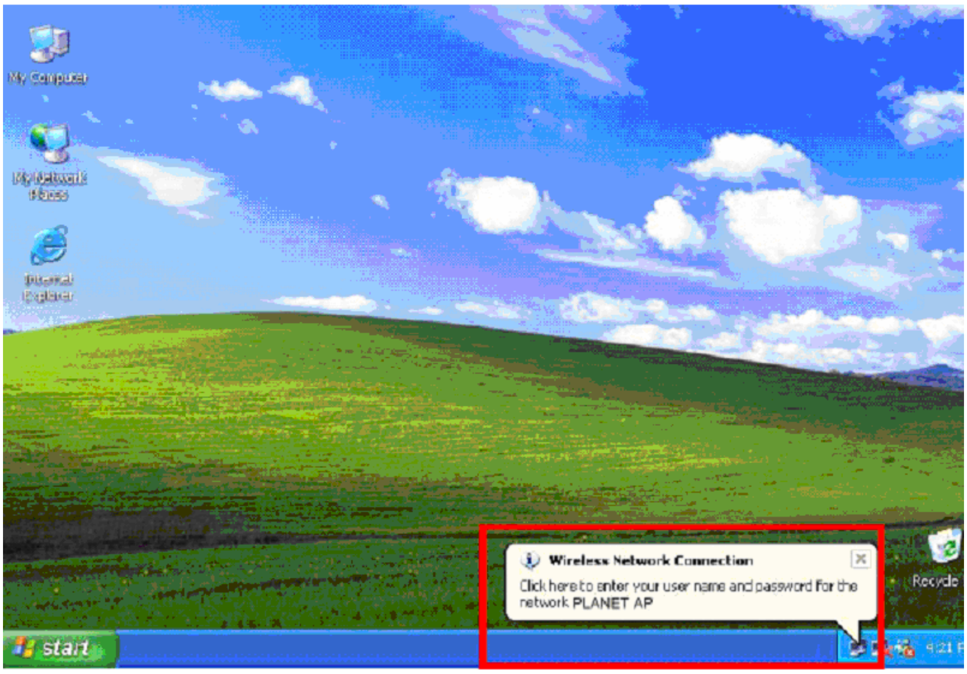
☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

6. Select “**MD-5 Challenge**” from the drop-down list box for EAP type.

7. Click “**OK**”.

8. When client has associated with WGSW-2840/5240, a user authentication notice appears in system tray. Click on the notice to continue.

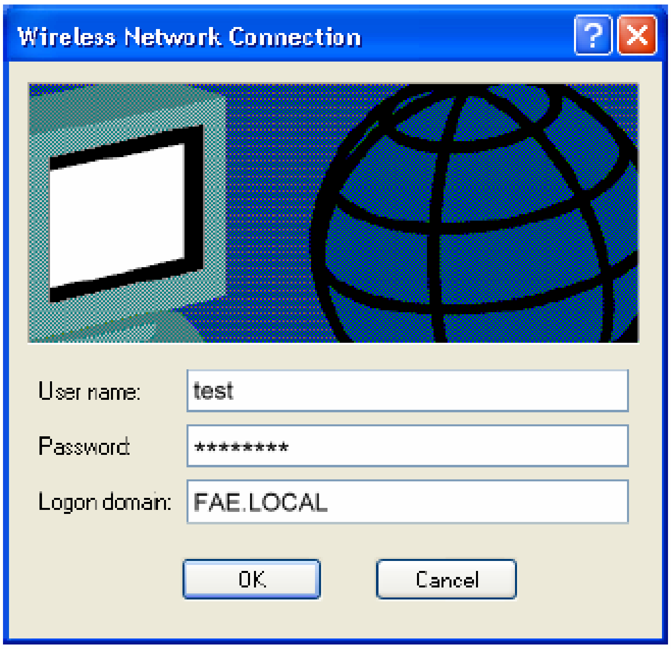


Wireless Network Connection

Click here to enter your user name and password for the network PLANET AP

9. Enter the user name, password and the logon domain that your account belongs.

10. Click “**OK**” to complete the validation process.


Wireless Network Connection

User name: test

Password: ********

Logon domain: FAE.LOCAL

4.4.3 TACACS+

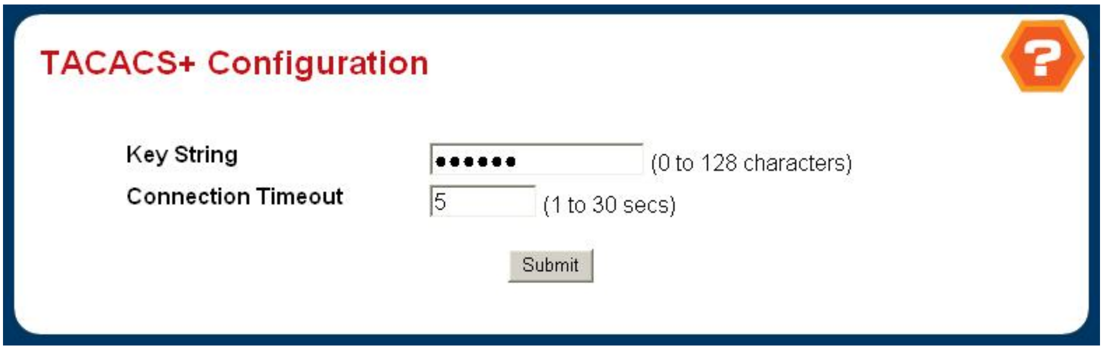
TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TACACS+ is based on TACACS, but, in spite of its name, it is an entirely new protocol which is incompatible with any previous version of TACACS. TACACS+ and RADIUS have generally replaced the earlier protocols in more recently built or updated networks, although TACACS and XTACACS are still running on many older systems.

Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates the two operations. Another difference is that TACACS+ uses the TCP while RADIUS uses the UDP. Most administrators recommend using TACACS+ because TCP is seen as a more reliable protocol.

The extensions to the TACACS+ protocol provide for more types of authentication requests and more types of response codes than were in the original specification.

4.4.3.1 TACACS+ Configuration



TACACS+ Configuration

Key String ●●●●●● (0 to 128 characters)

Connection Timeout 5 (1 to 30 secs)

Figure 4-4-17 TACACS+ Configuration

Configurable Data

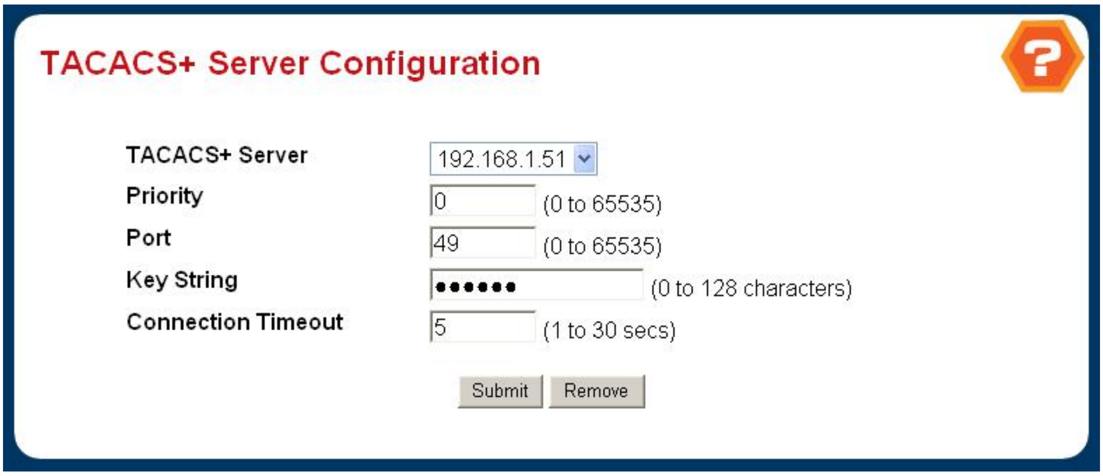
- **Key String** - Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. **The key must match the key configured on the TACACS+ server**.
- **Connection Timeout** - The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

Command Buttons

- **Submit** - Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.

4.4.3.2 Server Configuration

This page is to configure the TACACS+ Serve, include IP Address, port and and Key String.



TACACS+ Server Configuration

TACACS+ Server	192.168.1.51
Priority	0 (0 to 65535)
Port	49 (0 to 65535)
Key String	•••••• (0 to 128 characters)
Connection Timeout	5 (1 to 30 secs)

Figure 4-4-18 TACACS+ Server Configuration

Selection Criteria

- **TACACS+ Server** Selects the TACACS+ server for which data is to be displayed or configured. If the add item is selected, a new TACACS server can be configured.

Configurable Data

- **IP Address** - Specifies the TACACS+ Server IP address.
- **Priority** - Specifies the order in which the TACACS+ servers are used. It should be within the range 0-65535.
- **Port** - Specifies the authentication port. It should be within the range 0-65535.
- **Key String** - Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. **The key must match the encryption used on the TACACS+ server.**
- **Connection Timeout** - The amount of time that passes before the connection between the device and the TACACS+ server time out. The range is between 1-30.

Command Buttons

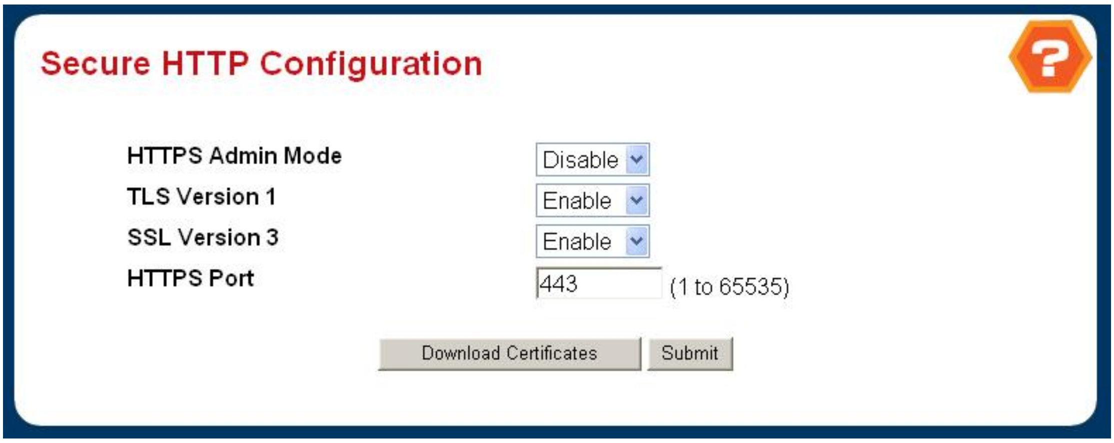
- **Submit** - Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Remove** - Remove the selected server from the configuration.

4.4.4 Secure HTTP

Https is a URI scheme used to indicate a secure HTTP connection. It is syntactically identical to the http:// scheme normally used for accessing resources using HTTP. Using an https: URL indicates that HTTP is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP. This system was designed by Netscape Communications Corporation to provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

4.4.4.1 Secure HTTP Configuration

This page is to configuration the secure HTTP connection parameters.



Secure HTTP Configuration

HTTPS Admin Mode	Disable
TLS Version 1	Enable
SSL Version 3	Enable
HTTPS Port	443 (1 to 65535)

Figure 4-4-19 Secure HTTP Configuration

Selection Criteria

- **Admin Mode -** This select field is used to Enable or Disable the Administrative Mode of Secure HTTP. The currently configured value is shown when the web page is displayed. The default value is **Disable**.
- **TLS Version 1 -** This select field is used to Enable or Disable Transport Layer Security Version 1.0. The currently configured value is shown when the web page is displayed. The default value is **Enable**.
- **SSL Version 3 -** This select field is used to Enable or Disable Secure Sockets Layer Version 3.0. The currently configured value is shown when the web page is displayed. The default value is **Enable.**
- **HTTPS Port Number -** This select field is used to set the HTTPS Port Number. The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the web page is displayed.

Command Buttons

- **Submit -** Send the updated screen to the switch. Changes take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Download Certificates -** Link to the File Transfer page for the SSL Certificate download. Note that to download SSL Certificate files SSL must be administratively disabled.

Note:	You may load the certificates keys from the WGS3-Series User’s Manual CD-ROM. And once the switch is load to factory default, the default certificaties keys will be removed.

4.4.5 Secure Shell

Secure Shell or SSH is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and (optionally) to allow the remote computer to authenticate the user. SSH provides confidentiality and integrity of data exchanged between the two computers using encryption and message authentication codes (MACs). SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports connections; it can transfer files using the associated SFTP or SCP protocols. An SSH server, by default, listens on the standard TCP port 22.

4.4.5.1 Secure Shell Configuration

- **Admin Mode -** This select field is used to Enable or Disable the Aministrative Mode of SSH. The currently configured value is shown when the web page is displayed.

  The default value is Disable.

- **SSH Version 1 -** This select field is used to Enable or Disable Protocol Level 1 for SSH. The currently configured value is shown when the web page is displayed.

  The default value is Enable.

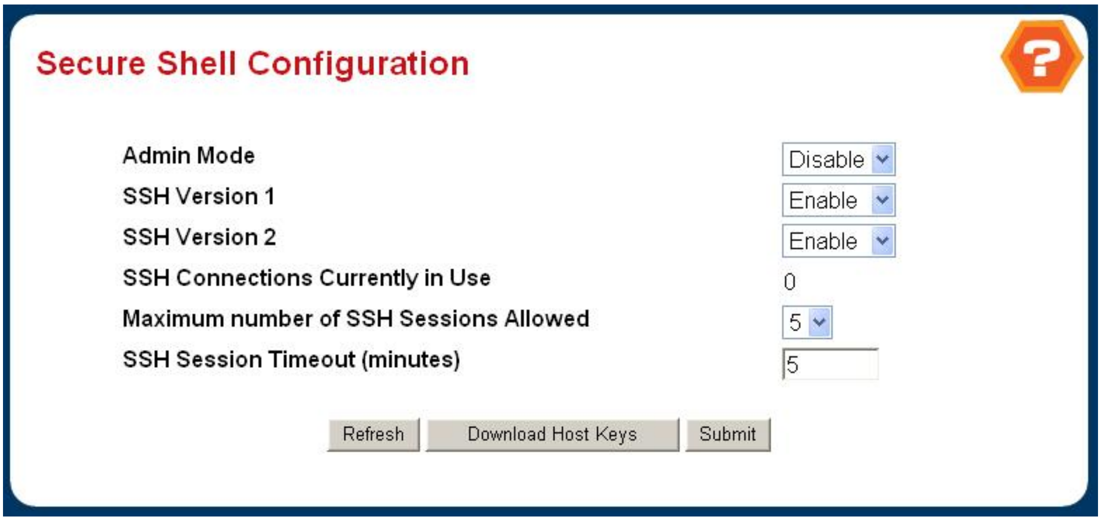
- **SSH Version 2 -** This select field is used to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page is displayed.

  The default value is Enable.

- **SSH Connections in Use -** Displays the number of SSH connections currently in use in the system.

Command Buttons

- **Submit -** Send the updated screen to the switch. Changes take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- **Refresh -** Refresh the current page with the latest settings and status.
- **Download Host Keys -** Link to the File Transfer page for the Host Key download. Note that to download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.



Secure Shell Configuration

Admin Mode	Disable
SSH Version 1	Enable
SSH Version 2	Enable
SSH Connections Currently in Use	0
Maximum number of SSH Sessions Allowed	5
SSH Session Timeout (minutes)	5

Figure 4-4-20 Secure Shell Configuration

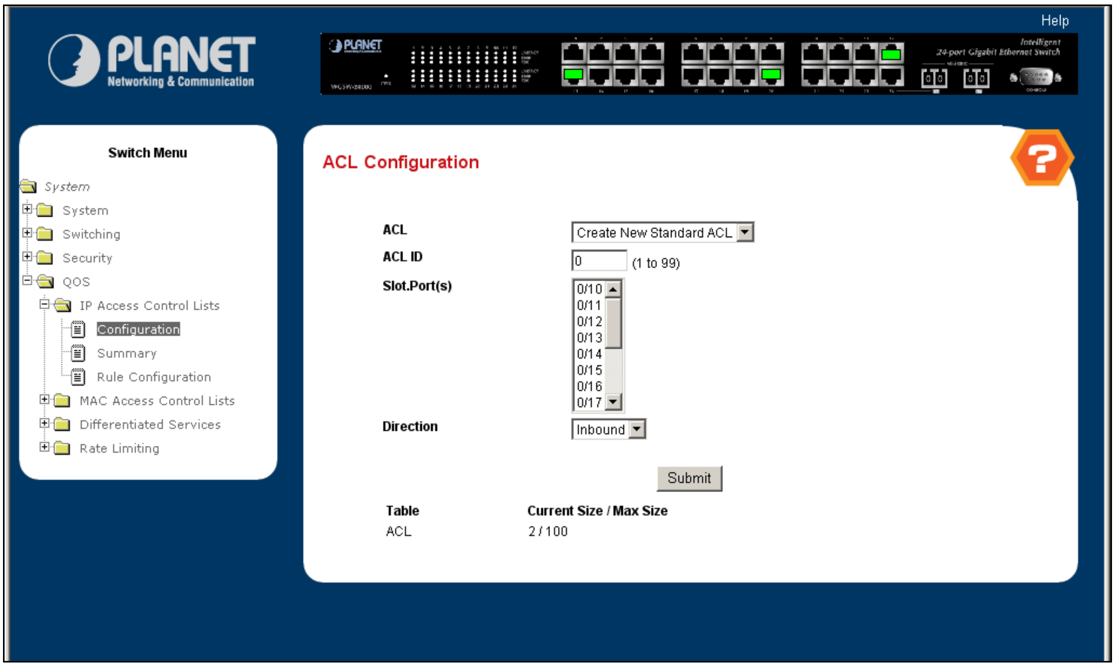
4.5 QoS

4.5.1 IP Access Control List

An ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match. On this menu the interfaces to which an ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the ACL are specified/created using the ACL Rule Configuration menu.

4.5.1.1 IP ACL Configuration

This page is to configure the access control list on ports.



ACL Configuration

ACL	Create New Standard ACL
ACL ID	0 (1 to 99)
Slot.Port(s)	0/10 0/11 0/12 0/13 0/14 0/15 0/16 0/17
Direction	Inbound

Table	Current Size / Max Size
ACL	2 / 100

Figure 4-5-1 IP ACL Configuration

Configurable Data

- **ACL -** Make a selection from the pull-down menu. A new Access Control List may be created or the configuration of an existing ACL can be updated.
- **ACL ID -** ACL ID must be a whole number in the range of 1 to 99 for IP Standard Access Lists and 100-199 for IP Extended Access Lists.
- **Slot.Port(s) -** This dynamic multi-selector lists all available valid interfaces for ACL mapping. All non-routing physical interfaces and interfaces participating in LAGs that are not already assigned to an ACL are listed. An interface can be mapped to one and only one ACL, but multiple interfaces can be assigned to one ACL.
- **Direction -** Select the packet filtering direction for the ACL from the pulldown menu.

Choices:

➢ Inbound

The packet direction for a given ACL is the same for all affected interfaces.

Non-Configurable Data

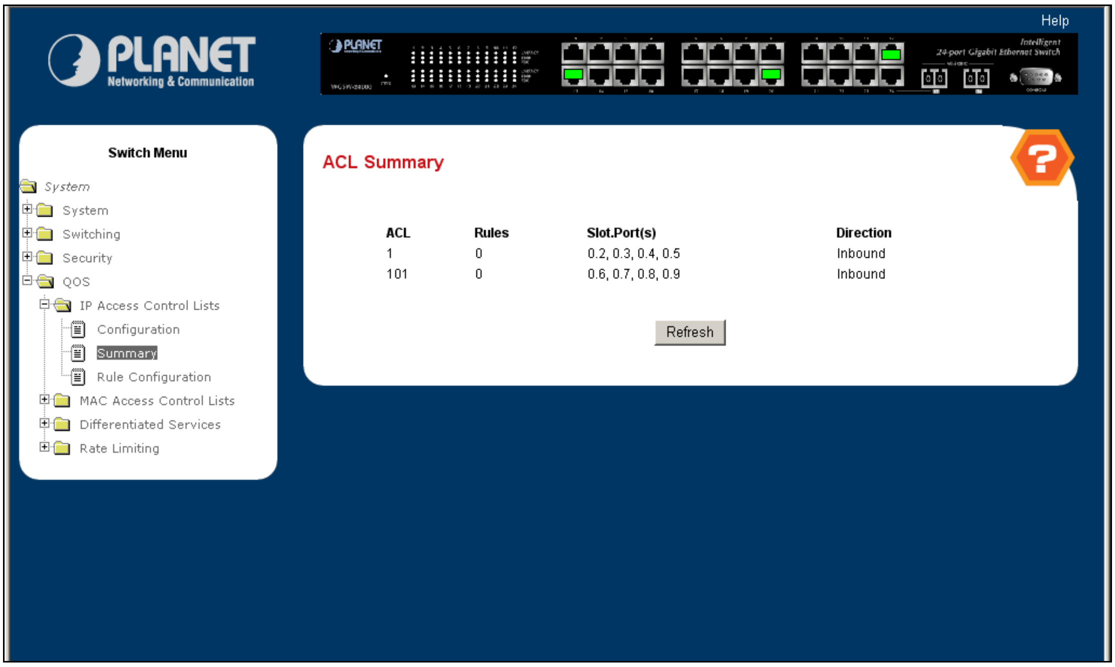
- **Table -** Displays the current and maximum number of ACLs.

Command Buttons

- **Submit -** Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Delete ACL -** Removes the currently selected ACL from the switch configuration.

4.5.1.2 IP ACL Summary

This page shows the configuration summary of access control list.



ACL Summary

ACL	Rules	Slot.Port(s)	Direction
1	0	0.2, 0.3, 0.4, 0.5	Inbound
101	0	0.6, 0.7, 0.8, 0.9	Inbound

Figure 4-5-2 ACL Summary

Non-Configurable Data

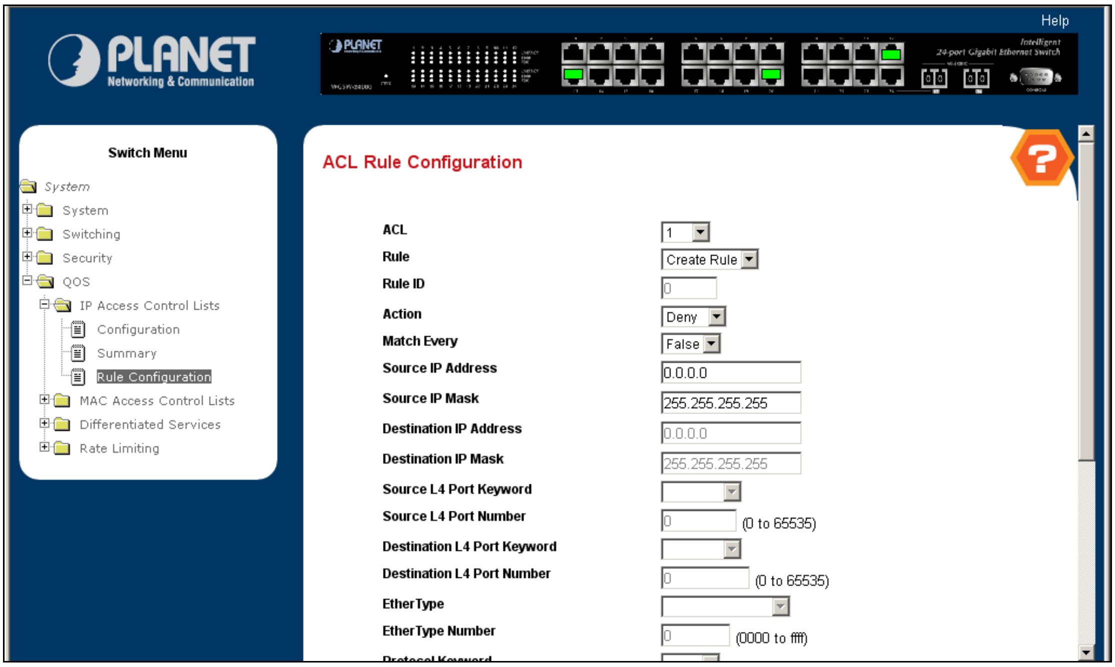
- **ACL ID -** The ACL identifier.
- **Rules -** The number of rules currently configured for the ACL.
- **Slot.Port(s) -** The interfaces to which the ACL applies.
- **Direction -** The direction of packet traffic affected by the ACL.

Direction can only be one of the following:

- Inbound

4.5.1.3 IP ACL Rule Configuration

Use these screens to configure the rules for the Access Control Lists created using the Access Control List Configuration screen. What is shown on this screen varies depending on the current step in the rule configuration process. An ACL must first be selected to configure rules for. The rule identification, and the 'Action' and 'Match Every' parameters must be specified next. If 'Match Every' is set to false a new screen will then be presented from which the match criteria can be configured.



ACL Rule Configuration

ACL	1
Rule	Create Rule
Rule ID	0
Action	Deny
Match Every	False
Source IP Address	0.0.0.0
Source IP Mask	255.255.255.255
Destination IP Address	0.0.0.0
Destination IP Mask	255.255.255.255
Source L4 Port Keyword	
Source L4 Port Number	0 (0 to 65535)
Destination L4 Port Keyword	
Destination L4 Port Number	0 (0 to 65535)
EtherType	
EtherType Number	0 (0000 to ffff)

Figure 4-5-3 ACL Rule Configuration

Selection Criteria

- **IP ACL ID** - Use the pulldown menu to select the IP ACL for which to create or update a rule.
- **Rule** - Select an existing rule from the pulldown menu, or select 'Create New Rule.' ACL as well as an option to add a new Rule. New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.

Configurable Data

- **Rule ID** - Enter a whole number in the range of 1 to 9 that will be used to identify the rule. An IP ACL may have up to 9 rules.
- **Action** - Specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
- **Assign Queue ID** - Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. Valid range of Queue Ids is (0 to 7). This field is visible when 'Permit' is chosen as 'Action'.
- **Redirect Interface** - Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field is visible when 'Permit' is chosen as 'Action'.
- **Match Every** - Select true or false from the pulldown menu. True signifies that all packets will match the selected IP ACL and Rule and will be either permitted or denied. In this case, since all packets match the rule, the option of

configuring other match criteria will not be offered. To configure specific match criteria for the rule, remove the rule and re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.

- **Protocol Keyword** - Specify that a packet's IP protocol is a match condition for the selected IP ACL rule. The possible values are ICMP, IGMP, IP, TCP, and UDP. Either the 'Protocol Keyword' field or the 'Protocol Number' field can be used to specify an IP protocol value as a match criterion.
- **Protocol Number** - Specify that a packet's IP protocol is a match condition for the selected IP ACL rule and identify the protocol by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. Either the 'Protocol Number' field or the 'Protocol Keyword' field can be used to specify an IP protocol value as a match criterion.
- **Source IP Address** - Enter an IP address using dotted-decimal notation to be compared to a packet's source IP Address as a match criteria for the selected IP ACL rule.
- **Source IP Mask** - Specify the IP Mask in dotted-decimal notation to be used with the Source IP Address value.
- **Source L4 Port Keyword** - Specify a packet's source layer 4 port as a match condition for the selected extended IP ACL rule. This is an optional configuration. The possible values are DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
- **Source L4 Port Number** - Specify a packet's source layer 4 port as a match condition for the selected extended IP ACL rule. This is an optional configuration.
- **Destination IP Address** - Enter an IP address using dotted-decimal notation to be compared to a packet's destination IP Address as a match criteria for the selected extended IP ACL rule.
- **Destination IP Mask** - Specify the IP Mask in dotted-decimal notation to be used with the Destination IP Address value.
- **Destination L4 Port Keyword** - Specify the destination layer 4 port match conditions for the selected extended IP ACL rule. The possible values are DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. This is an optional configuration.
- **Destination L4 Port Number** - Specify a packet's destination layer 4 port number match condition for the selected extended IP ACL rule. This is an optional configuration.
- **Service Type** - Select a Service Type match condition for the extended IP ACL rule from the pulldown menu. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header, however each uses a different user notation. After a selection is made the appropriate value can be specified.
    - ***IP DSCP Configuration***
      Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 63. The IP DSCP is selected by possibly selection one of the DSCP keyword from a dropdown box. If a value is to be selected by

specifying its numeric value, then select the 'Other' option in the dropdown box and a text box will appear where the numeric value of the DSCP can be entered.

- ***IP Precedence Configuration***
  The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 7.
- ***IP TOS Configuration***
  The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The TOS Bits value is a hexadecimal number from 00 to FF. The TOS Mask value is a hexadecimal number from 00 to FF. The TOS Mask denotes the bit positions in the TOS Bits value that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0xA0 and a TOS Mask of 0xFF. This is an optional configuration.

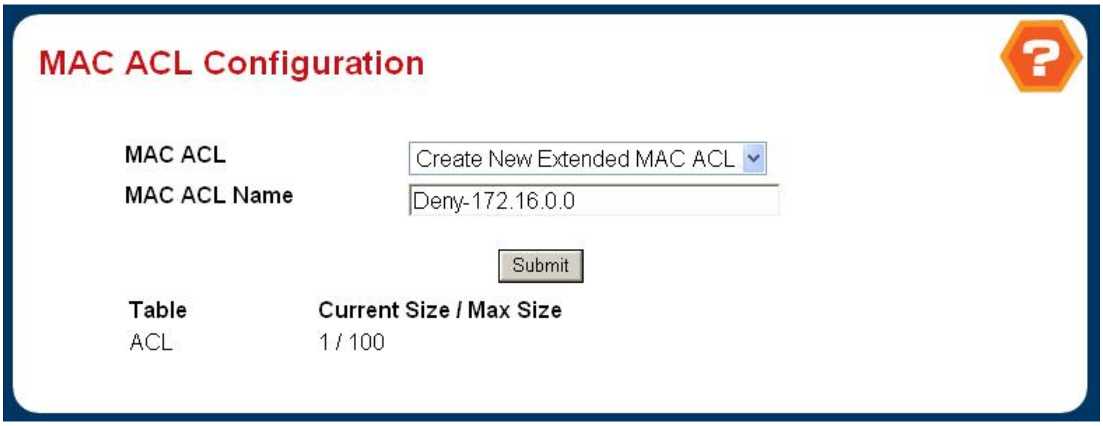
Command Buttons

- **Configure** - Configure the corresponding match criteria for the selected rule.
- **Delete** - Remove the currently selected Rule from the selected ACL. These changes will not be retained across a power cycle unless a save configuration is performed.

4.5.2 MAC Access Control List

A MAC ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match. On this menu the interfaces to which an MAC ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the MAC ACL are specified/created using the MAC ACL Rule Configuration menu.

4.5.2.1 MAC ACL Configuration



MAC ACL Configuration

MAC ACL: Create New Extended MAC ACL

MAC ACL Name: Deny-172.16.0.0

Table	Current Size / Max Size
ACL	1 / 100

Figure 4-5-4 MAC ACL Configuration

Selection Criteria

- **MAC ACL** - A new MAC Access Control List may be created or the configuration of an existing MAC ACL can be updated based on selection.

Configurable Data

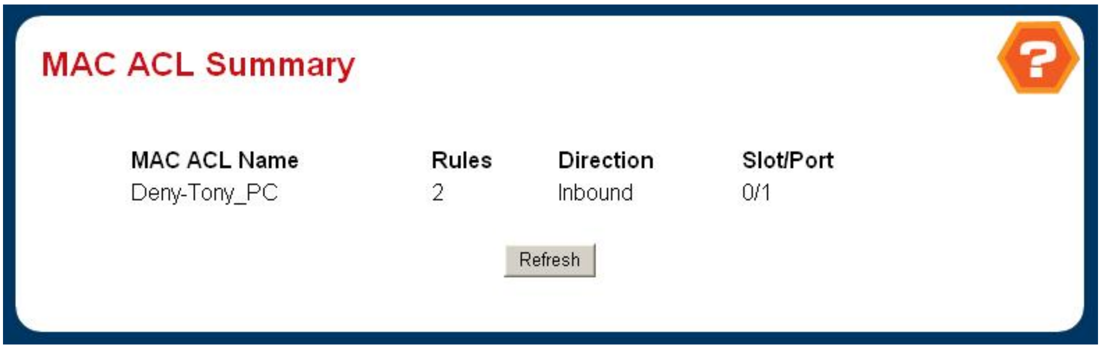
- **MAC ACL Name** - Specifies MAC ACL Name string which may include alphabetic, numeric, dash, underscore or space characters only. The name must start with an alphabetic character. This field displays the name of the currently selected MAC ACL if the ACL has already been created.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Rename** - Renames the currently selected MAC ACL.
- **Delete** - Removes the currently selected MAC ACL from the switch configuration.

4.5.2.2 MAC ACL Summary

This page shows the configuration summary of MAC access control list.



MAC ACL Summary

MAC ACL Name	Rules	Direction	Slot/Port
Deny-Tony_PC	2	Inbound	0/1

Figure 4-5-5 MAC ACL Summary

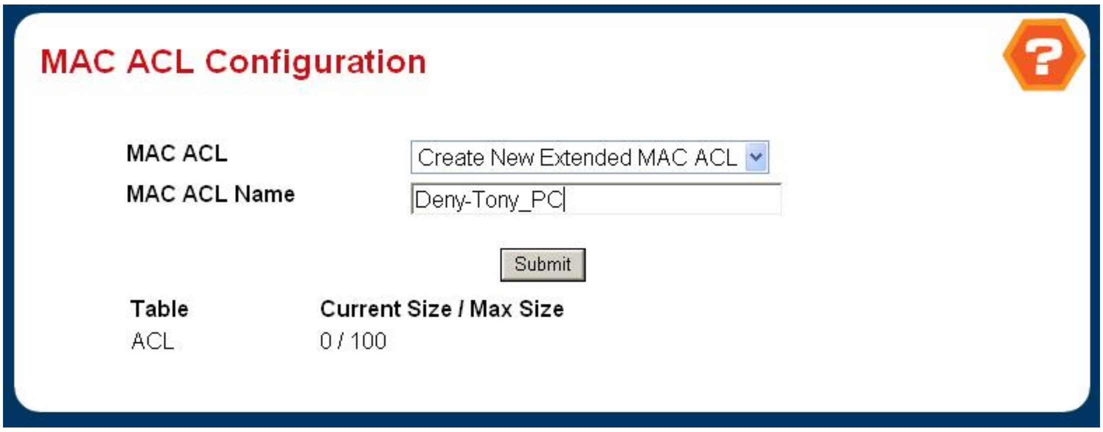
Non-Configurable Data

- **MAC ACL Name** - MAC ACL identifier.
- **Rules** - The number of rules currently configured for the MAC ACL.
- **Direction** - The direction of packet traffic affected by the MAC ACL.
  Valid Directions
  - ***Inbound***
- **Slot/Port(s)** - The interfaces to which the MAC ACL applies.

Command Buttons

- **Refresh** - Refresh the data on the screen to the latest state.

4.5.2.3 MAC ACL Rule Configuration



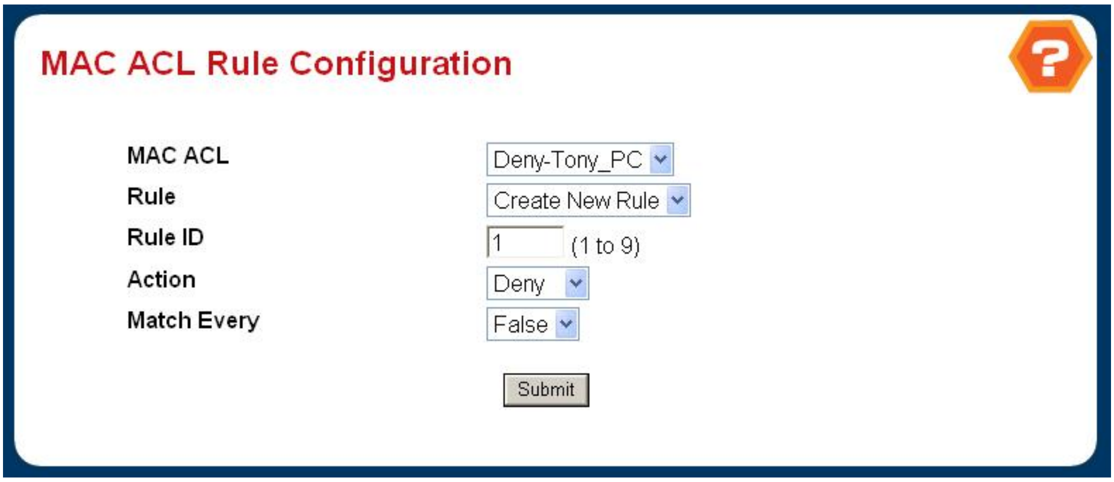
MAC ACL Configuration

MAC ACL: Create New Extended MAC ACL

MAC ACL Name: Deny-Tony_PC

Table	Current Size / Max Size
ACL	0 / 100

Figure 4-5-6 MAC ACL Rule Configuration – Create New Extended MAC ACL



MAC ACL Rule Configuration

MAC ACL: Deny-Tony_PC

Rule: Create New Rule

Rule ID: 1 (1 to 9)

Action: Deny

Match Every: False

Figure 4-5-7 MAC ACL Rule Configuration – Configure MAC ACL Rule

Selection Criteria

- **MAC ACL** - Select the MAC ACL for which to create or update a rule.
- **Rule** - Select an existing rule or select 'Create New Rule' to add a new Rule. New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.

Configurable Data

- **Rule** - Enter a whole number in the range of (1 to 9) that will be used to identify the rule.
- **Action** - Specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
- **Assign Queue ID** - Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Valid range of Queue Ids is (0 to 7).
- **Redirect Interface** - Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.
- **CoS** - Specifies the 802.1p user priority to compare against an Ethernet frame. Valid range of values is (0 to 7).

- **Destination MAC** - Specifies the destination MAC address to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx). The BPDU keyword may be specified using a Destination MAC address of 01:80:C2:xx:xx:xx.
- **Ethertype Key** - Specifies the Ethertype value to compare against an Ethernet frame.
  Valid values are

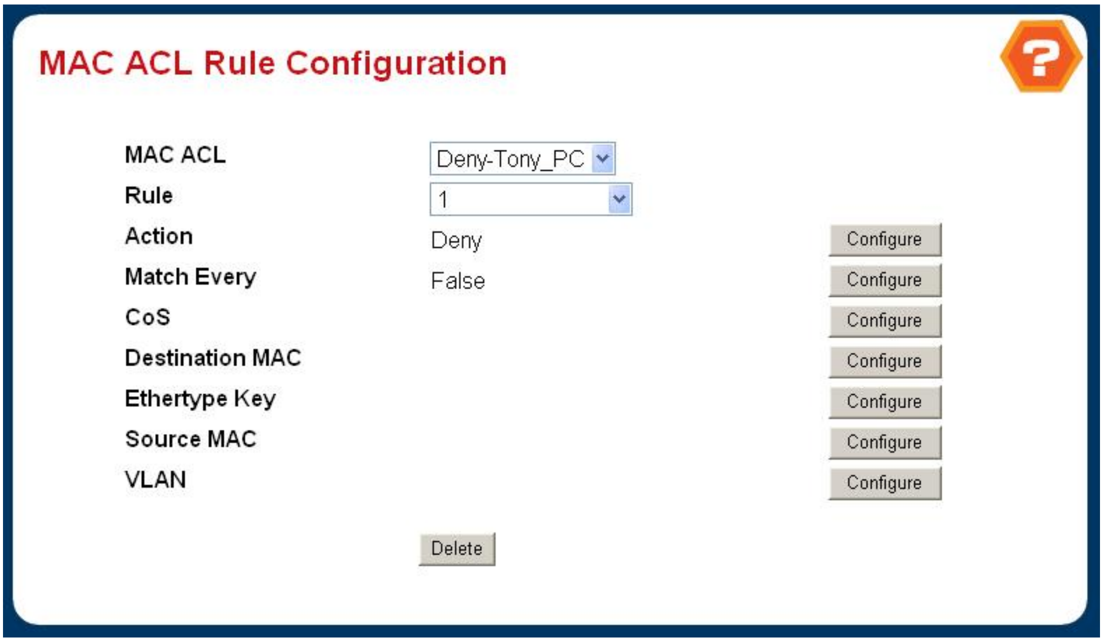
  - ***Appletalk***
  - ***ARP***
  - ***IBM SNA***
  - ***IPv4***
  - ***IPv6***
  - ***IPX***
  - ***MPLS multicast***
  - ***MPLS unicast***
  - ***NetBIOS***
  - ***Novell***
  - ***PPPoE***
  - ***Reverse ARP***
  - ***User Value***

- **Ethertype User Value** - Specifies the user defined customised Ethertype value to be used when the user has selected "User Value" as Ethertype Key, to compare against an Ethernet frame. Valid range of values is (0x0600 to 0xFFFF).
- **Source MAC** - Specifies the Source MAC address to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx).
- **VLAN** - Specifies the VLAN ID to compare against an Ethernet frame. Valid range of values is (0 to 4095). Either VLAN Range or VLAN can be configured.
- **Match Every** - Specifies an indication to match every Layer 2 MAC packet.
  Valid values are

  - ***True*** - Signifies that every packet is considered to match the selected ACL Rule.
  - ***False*** - Signifies that it is not mandatory for every packet to match the selected ACL Rule.

Command Buttons

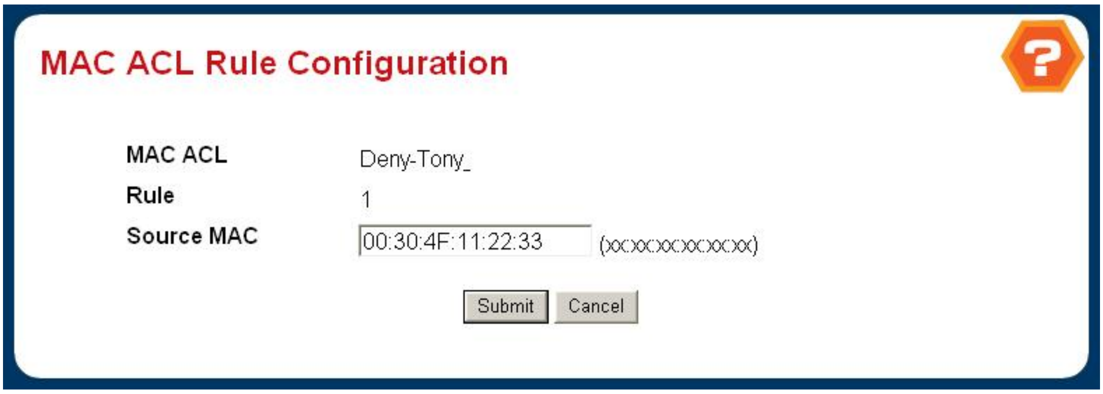
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Delete** - Remove the currently selected Rule from the selected ACL. These changes will not be retained across a power cycle unless a save configuration is performed.



MAC ACL Rule Configuration

MAC ACL	Deny-Tony_PC
Rule	1
Action	Deny
Match Every	False
CoS	
Destination MAC	
Ethertype Key	
Source MAC	
VLAN	

Figure 4-5-8 MAC ACL Rule Configuration – Setting items



MAC ACL Rule Configuration

MAC ACL	Deny-Tony_
Rule	1
Source MAC	00:30:4F:11:22:33 (xx:xx:xx:xx:xx:xx)

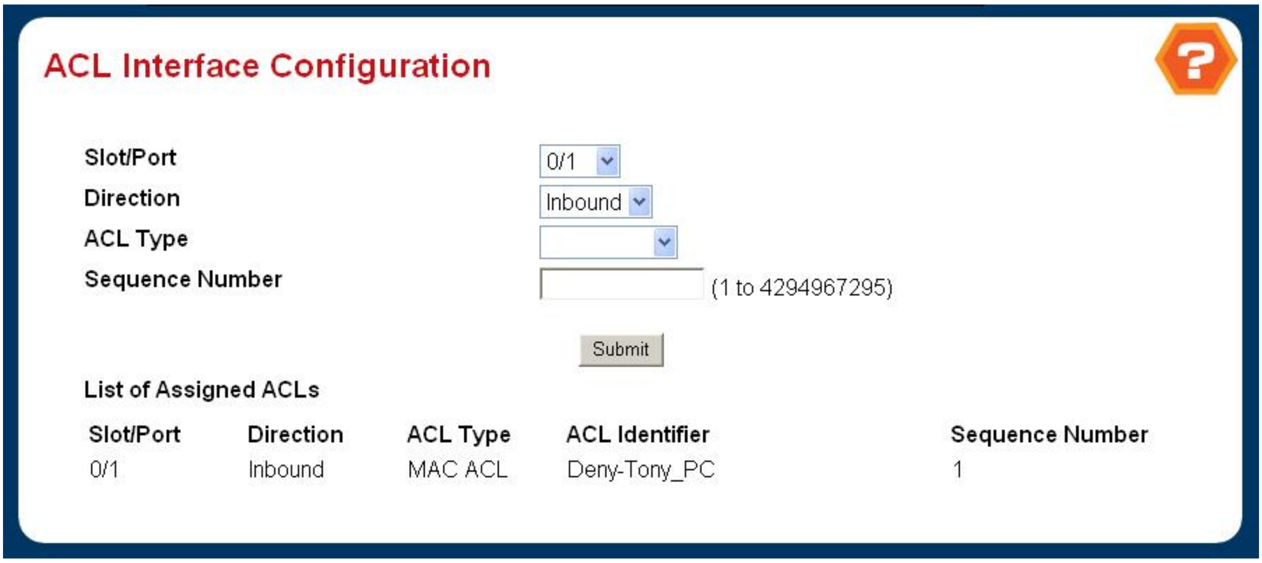
Figure 4-5-9 MAC ACL Rule Configuration – Source MAC configuration

Note:

If only one or two MAC addresses are going to be blocked, rember to add a "Permit All" rule at the end of the ACL. Or other packets would be blocked/droped too.

4.5.3 ACL Interface Configuration

Use these pages to apply the IP Based ACL or MAC Based ACL to specify interface.



ACL Interface Configuration

Slot/Port	0/1
Direction	Inbound
ACL Type	
Sequence Number	(1 to 4294967295)

List of Assigned ACLs

Slot/Port	Direction	ACL Type	ACL Identifier	Sequence Number
0/1	Inbound	MAC ACL	Deny-Tony_PC	1

Figure 4-5-10 ACL Interface Configuration

Configurable Data

- **Slot/Port** - Specifies list of all available valid interfaces for ACL mapping. All non-routing physical interfaces and interfaces participating in LAGs are listed.

- **Direction** - Specifies the packet filtering direction for ACL.

  Valid Directions

  - ***Inbound***

- **ACL Type** - Specifies the type of ACL.

  Valid ACL Types

  - ***IP ACL***

  - ***MAC ACL***

- **IP ACL** - Specifies list of all IP ACLs. This field is visible only if the user has selected "IP ACL" as "ACL Type".

- **MAC ACL** - Specifies list of all MAC ACLs. This field is visible only if the user has selected "MAC ACL" as "ACL Type".

- **Sequence Number** - An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used. Valid range is (1 to 4294967295).

Non-Configurable Data

- **Slot/Port** - Displays selected interface.

- **Direction** - Displays selected packet filtering direction for ACL.
- **ACL Type** - Displays the type of ACL assigned to selected interface and direction.
- **ACL Identifier** - Displays the ACL Number(in case of IP ACL) or ACL Name(in case of MAC ACL) identifying the ACL assigned to selected interface and direction.
- **Sequence Number** - Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Remove** - Removes the currently selected ACL Interface Direction Mapping from the switch configuration.

Note: One ACL can ba applied to an interface a time, no matter MAC ACL or IP ACL.

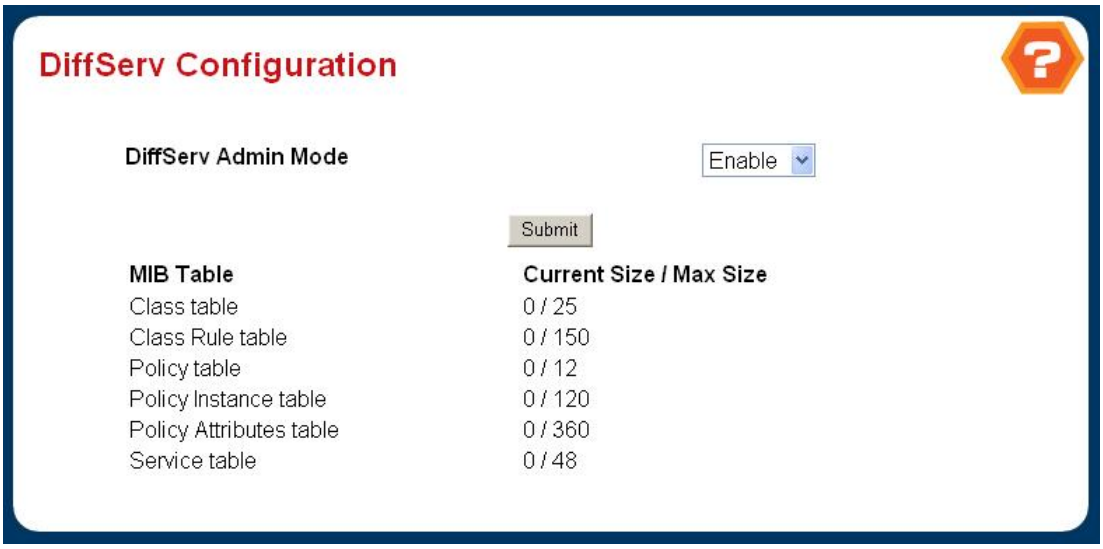
4.5.4 Differentiated Services

Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The 'all' class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The 'any' class type option defines that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

4.5.4.1 Diffserv Configuration



DiffServ Configuration

DiffServ Admin Mode: Enable

MIB Table	Current Size / Max Size
Class table	0 / 25
Class Rule table	0 / 150
Policy table	0 / 12
Policy Instance table	0 / 120
Policy Attributes table	0 / 360
Service table	0 / 48

Figure 4-5-11 Diffserv Configuration

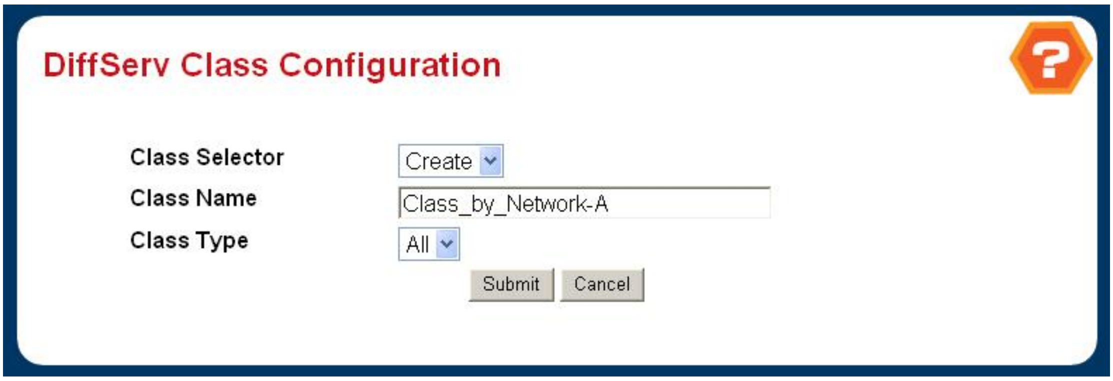
Selection Criteria

- **DiffServ Admin Mode -** This lists the options for the mode, from which one can be selected. The default value is 'enable'. While disabled, the DiffServ configuration is retained when saved and can be changed, but it is not activated. When enabled, Diffserv services are activated.

Non-Configurable Data

- **Class table -** Displays the number of configured DiffServ classes out of the total allowed on the switch.
- **Class Rule table -** Displays the number of configured class rules out of the total allowed on the switch.
- **Policy table -** Displays the number of configured policies out of the total allowed on the switch.
- **Policy Instance table -** Displays the number of configured policy class instances out of the total allowed on the switch.
- **Policy Attributes table -** Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
- **Service table -** Displays the number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

4.5.4.2 Diffserv Class Configuration



DiffServ Class Configuration

Class Selector: Create

Class Name: Class_by_Network-A

Class Type: All

Figure 4-5-12 Diffserv Class Configuration

Selection Criteria

- **Class Selector -** Along with an option to create a new class, this lists all the existing DiffServ class names, from which one can be selected. The content of this screen varies based on the selection of this field. If an existing class is selected then the screen will display the configured class. If '--create--' is selected, another screen appears to facilitate creation of a new class. The default is the first class created. If no classes exist, the default is '--create--'.
- **Class Type -** This lists all the platform supported DiffServ class types from which one can be selected. Possible options are 'all', 'any', or 'acl'. If 'acl' is (supported and) selected, then an access list (ACL) number is required which is an integer specifying an existing ACL. Only when a new class is created, this field is a selector field. After class creation this becomes a non-configurable field displaying the configured class type.
- **Class Match Selector -** This lists all match criteria from which one can be selected to be added to a specified class. The match criterion 'Every' denotes that every packet is considered to match the specified class and no additional input information is needed. The content of this drop down list varies for a specified class based on the selection of the match criterion 'Reference Class':
  - If the specified class does not reference any other class, the 'Reference Class' match criterion is included in the drop down match criteria list. A class reference can be established by selecting 'Reference Class' and invoking the 'Add Match Criteria' button.
  - If the specified class references another class, the 'Reference Class' match criterion is not included in the drop down match criteria list. This prevents the user from trying to add yet another class reference, since a specified class can reference at most one other class of the same type. Moreover, a 'Remove Class Reference' button appears on the screen that can be invoked to remove the current class reference.

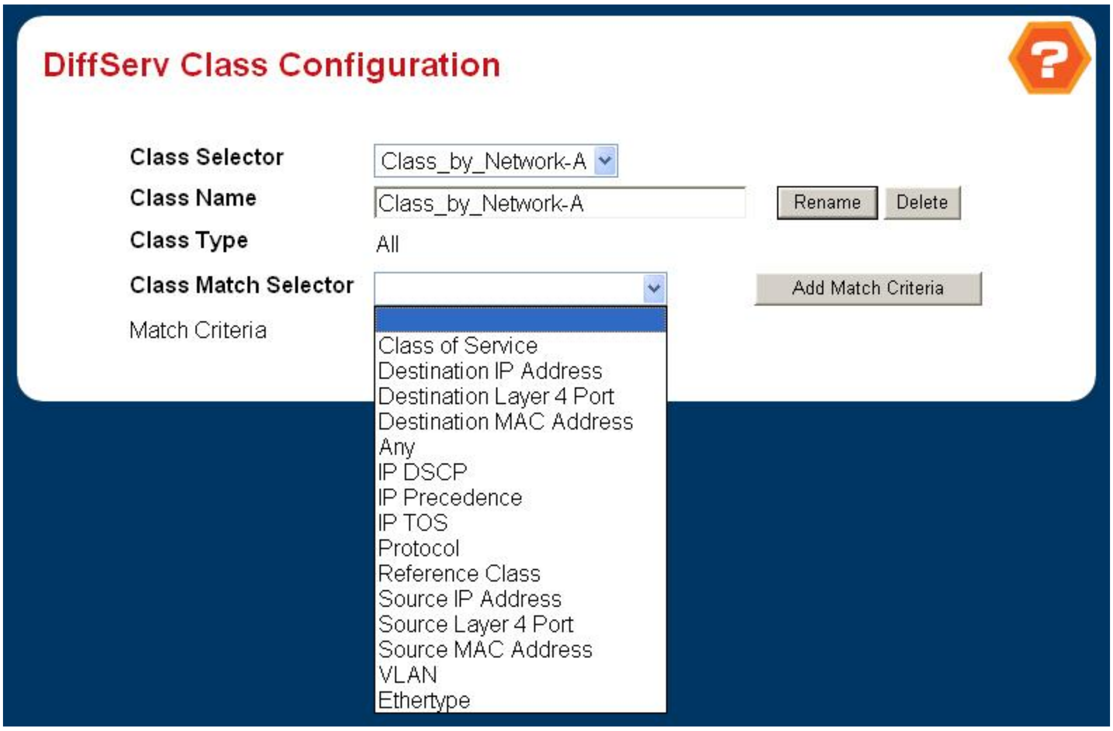
Configurable Data

- **Class Name -** This is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying a class. Class name 'default' is reserved and must not be used.

Non-Configurable Data

- **Class Type -** Displays type of the configured class as 'all', 'any', or 'acl'. Only when a new class is created, this field is a selector field. After class creation this becomes a non-configurable field.
- **Match Criteria -** Displays the configured match criteria for the specified class.
- **Values -** Displays the values of the configured match criteria.
- **Excluded -** Displays the inclusion or exclusion of the configured match criteria. When a match criterion is

configured to be excluded, 'Yes' is displayed. Conversely, when a match criterion is configured to be included, 'No' is displayed.


DiffServ Class Configuration

Class Selector: Class_by_Network-A

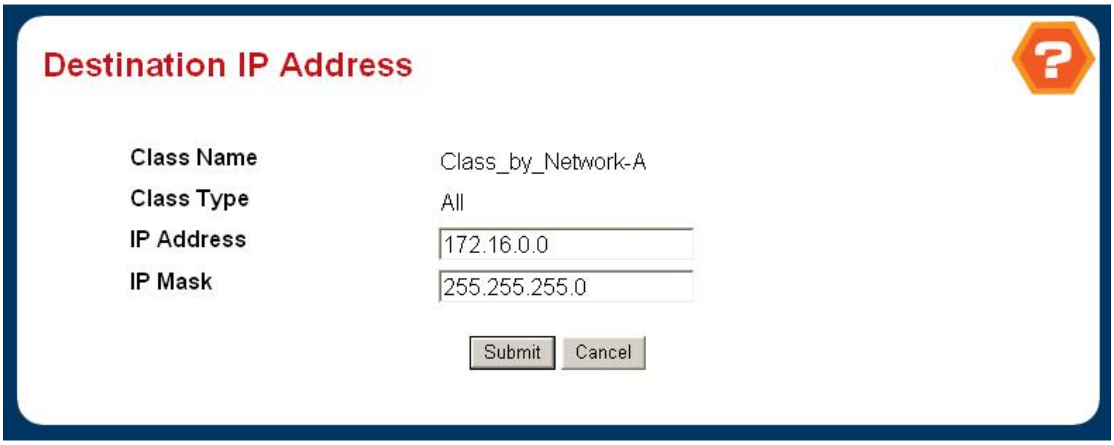
Class Name: Class_by_Network-A

Class Type: All

Class Match Selector:

Match Criteria

Figure 4-5-13 DiffServ Class Configuration – Class Match selector


Destination IP Address

Class Name: Class_by_Network-A

Class Type: All

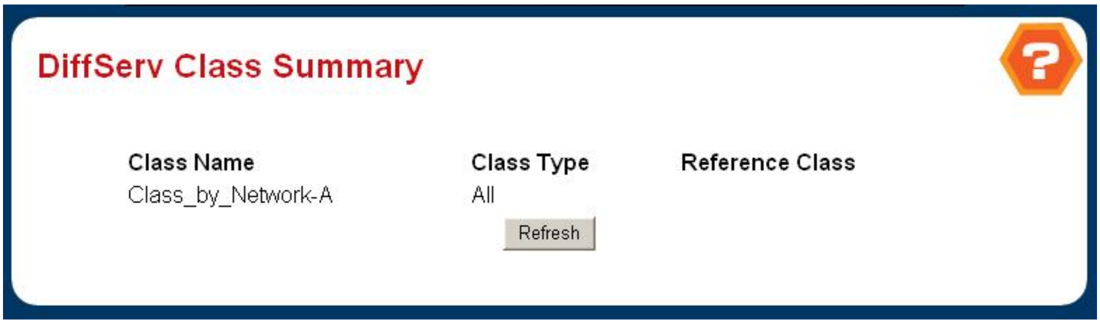
IP Address: 172.16.0.0

IP Mask: 255.255.255.0

Figure 4-5-14 DiffServ Class Configuration – Destination IP Address

4.5.4.3 Diffserv Class Summary

This page shows the configuration summary of the Diffserv.



DiffServ Class Summary

Class Name	Class Type	Reference Class
Class_by_Network-A	All	

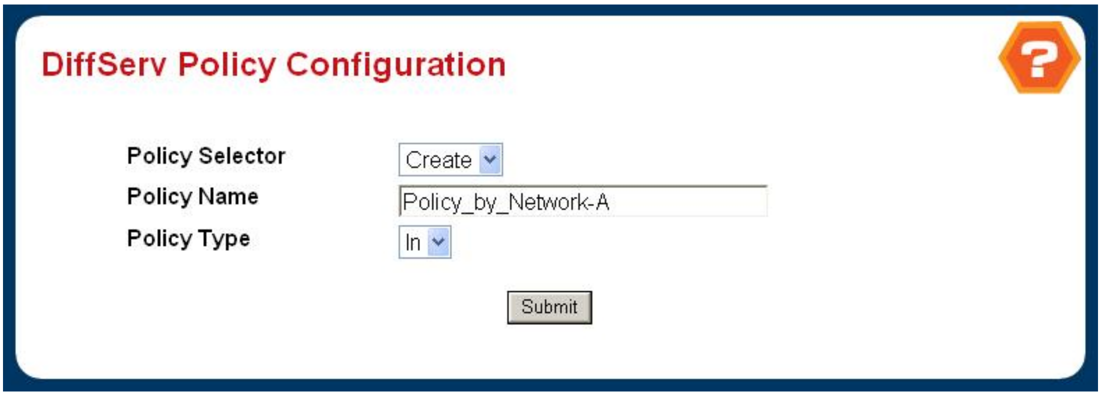
Figure 4-5-15 Diffserv Class Summary

Non-Configurable Data

- **Class Name -** Displays names of the configured DiffServ classes.
- **Class Type -** Displays types of the configured classes as 'all', 'any', or 'acl'. Class types are platform dependent.
- **Reference Class/ACL Number -** Displays name of the configured class of type 'all' or 'any' referenced by the specified class of the same type. For the specified class type of 'acl', the ACL number attached to the specified class is displayed.

4.5.4.4 Diff Policy Configuration

This page is to configure the member class of the Diffserv policy.



DiffServ Policy Configuration

Policy Selector	Create
Policy Name	Policy_by_Network-A
Policy Type	In

Figure 4-5-16 DiffServ Policy Configuration

Selection Criteria

- **Policy Selector -** Along with an option to create a new policy, this lists all the existing DiffServ policy names, from which one can be selected. The content of this screen varies based on the selection of this field. If an existing policy is selected then the screen will display Member Classes for that DiffServ policy. If 'create' is selected, another screen appears to facilitate creation of a new policy. The default is 'create'.
- **Policy Type -** This lists the DiffServ policy types from which one can be selected. Possible options are 'In' or 'Out'. Policy type 'In' indicates the type is specific to inbound traffic direction and 'Out' indicates the type is specific to outbound traffic direction. Only when a new policy is created, this field is a selector field. After policy creation this

becomes a non-configurable field displaying the configured policy type.

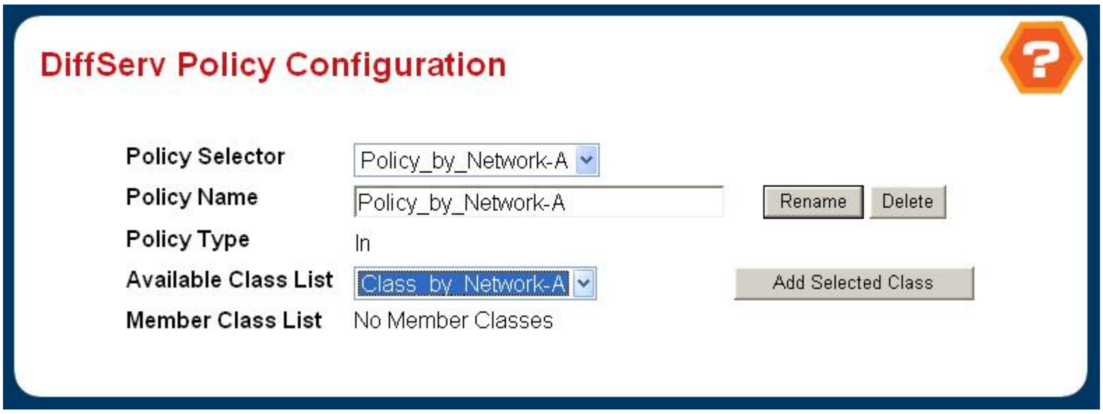
- **Available Class List -** This lists all existing DiffServ class names, from which one can be selected. This field is a selector field only when a new policy class instance is to be created. After creation of the policy class instance this becomes a non-configurable field.
- **Member Class List -** This lists all existing DiffServ classes currently defined as members of the specified Policy, from which one can be selected. This list is automatically updated as a new class is added to or removed from the policy. This field is a selector field only when an existing policy class instance is to be removed. After removal of the policy class instance this becomes a non-configurable field.

Configurable Data

- **Policy Name -** This is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying a policy.

Non-Configurable Data

- **Policy Type -** Displays type of the configured policy as 'In' or 'Out'. Only when a new policy is created, this field is a selector field. After policy creation this becomes a non-configurable field.
- **Member Class List -** Displays all the member classes for the selected DiffServ policy. It is automatically updated as a new class is added to or removed from the policy. Only when an existing policy class instance is to be removed, this field is a selector field. After removal of the policy class instance this becomes a non-configurable field.
- **Available Class List -** Displays all the member classes for the specified policy. It is automatically updated as a new class is added to or removed from the policy. Only when a new policy class instance is to be created this field is a selector field. After creation of the policy class instance this becomes a non-configurable field.



DiffServ Policy Configuration

Policy Selector: Policy_by_Network-A

Policy Name: Policy_by_Network-A

Policy Type: In

Available Class List: Class_by_Network-A

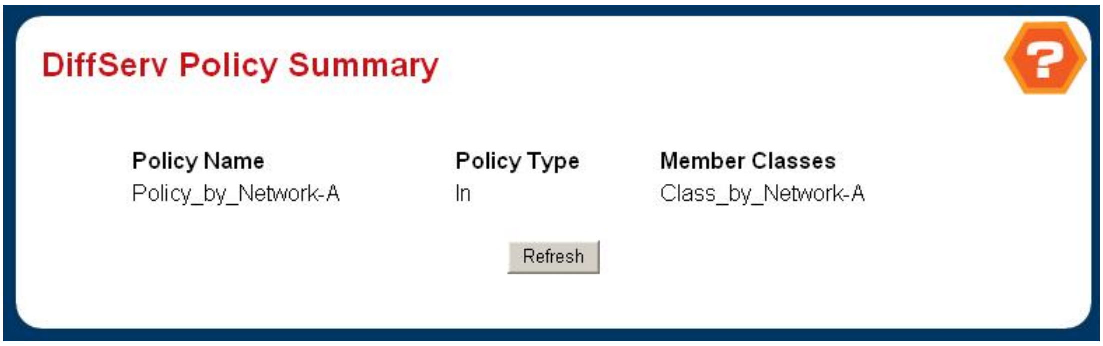
Member Class List: No Member Classes

Figure 4-5-17 DiffServ Policy Configuration – Add Selected Class

4.5.4.5 DiffServ Policy Summary

This page shows the summary configuration of the DiffServ Policy.

- **Policy Name -** Displays name of the DiffServ policy.
- **Policy Type -** Displays type of the policy as 'In' or 'Out'.
- **Member Classes -** Displays name of each class instance within the policy.



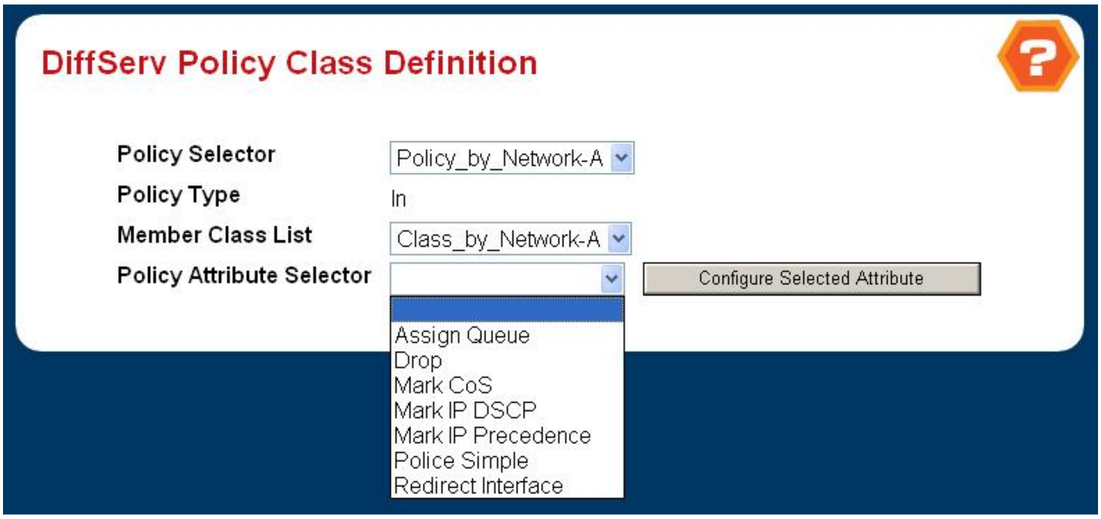
DiffServ Policy Summary

Policy Name	Policy Type	Member Classes
Policy_by_Network-A	In	Class_by_Network-A

Figure 4-5-18 DiffServ Policy Summary

4.5.4.6 DiffServ Policy Class Definition

- **Policy Selector -** This lists all the existing DiffServ policy names, from which one can be selected.
- **Member Class List -** This lists all existing DiffServ classes currently defined as members of the specified Policy, from which one can be selected. This list is automatically updated as a new class is added to or removed from the policy.
- **Policy Attribute Selector -** This lists all attributes supported for this type of policy, from which one can be selected.
- **Policy Type -** Displays type of the configured policy as 'In' or 'Out'.



DiffServ Policy Class Definition

Policy Selector: Policy_by_Network-A

Policy Type: In

Member Class List: Class_by_Network-A

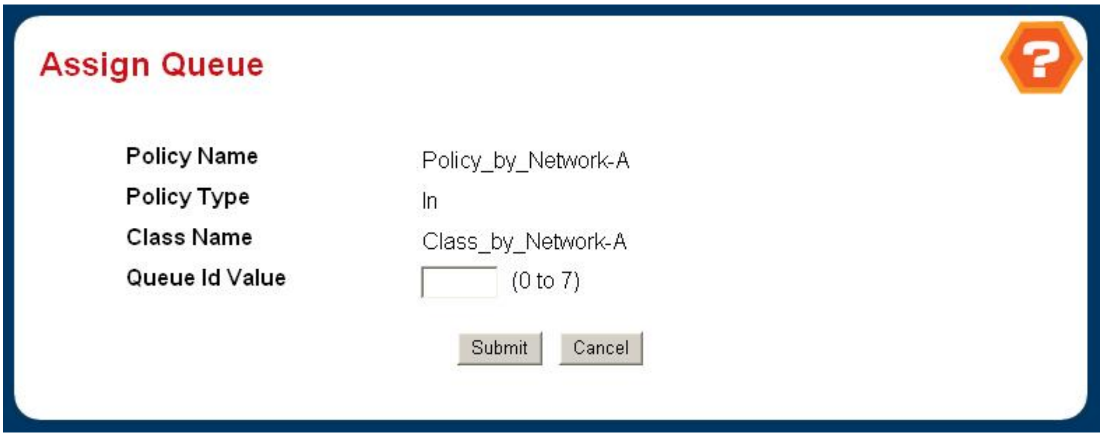
Policy Attribute Selector:

Figure 4-5-19 DiffServ Policy Class Definition

4.5.4.7 DiffServ Policy Attribute Summary

This page shows the configuration summary of DiffServ Policy Attribute.

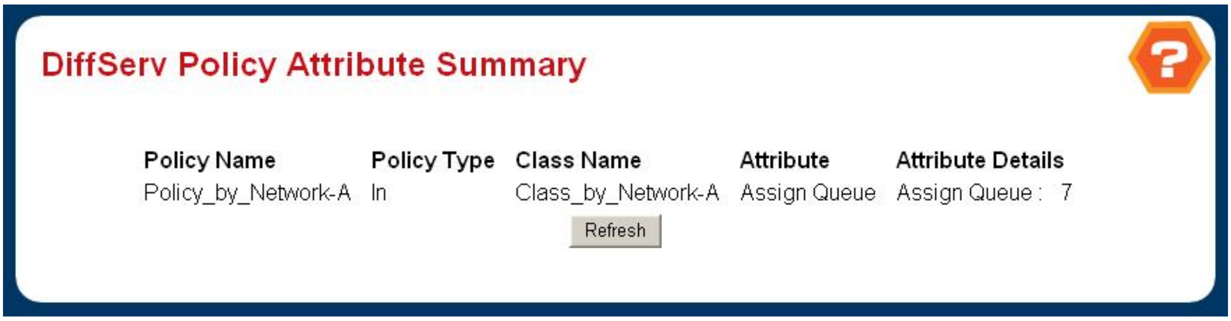
- **Policy Name -** Displays name of the specified DiffServ policy.
- **Policy Type -** Displays type of the specified policy as 'In' or 'Out'.
- **Class Name -** Displays name of the DiffServ class to which this policy is attached.
- **Attribute -** Displays the attributes attached to the policy class instances.
- **Attribute Details -** Displays the configured values of the attached attributes.



Assign Queue

Policy Name	Policy_by_Network-A
Policy Type	In
Class Name	Class_by_Network-A
Queue Id Value	(0 to 7)

Figure 4-5-20 DiffServ Policy Class Definition – Assign Queue



DiffServ Policy Attribute Summary

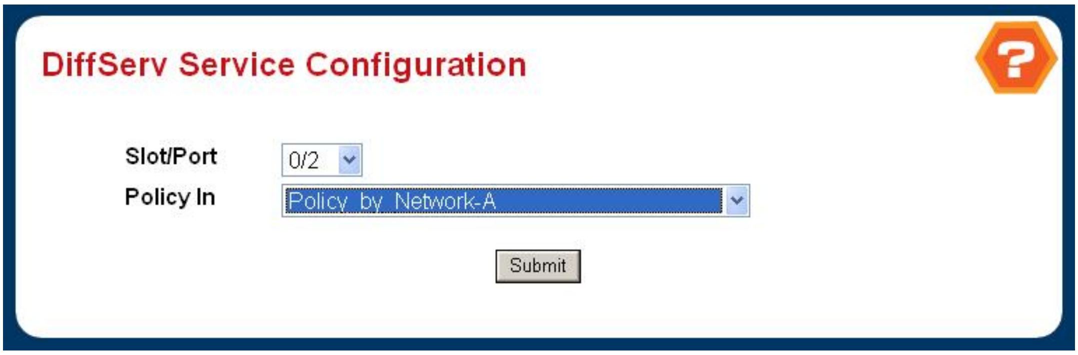
Policy Name	Policy Type	Class Name	Attribute	Attribute Details
Policy_by_Network-A	In	Class_by_Network-A	Assign Queue	Assign Queue : 7

Figure 4-5-21 DiffServ Policy Attribute Summary

4.5.4.8 DiffServ Service Configuration

Use this page to define the DiffServ policy on each port.

- **Slot.Port -** Select the Slot.Port that uniquely specifies an interface. This is a list of all valid slot number and port number combinations in the system. For Read/Write users where 'All' appears in the list, select it to specify all interfaces.
- **Policy In -** This lists all the policy names of type 'In' from which one can be selected. If 'none' is selected, this will detach the policy from the interface in this direction. This field is not shown for Read/Write users where inbound service policy attachment is not supported by the platform.
- **Policy Out -** This lists all the policy names of type 'Out' from which one can be selected. If 'none' is selected, this will detach the policy from the interface in this direction. This field is not shown for Read/Write users where outbound service policy attachment is not supported by the platform.



DiffServ Service Configuration

Slot/Port 0/2

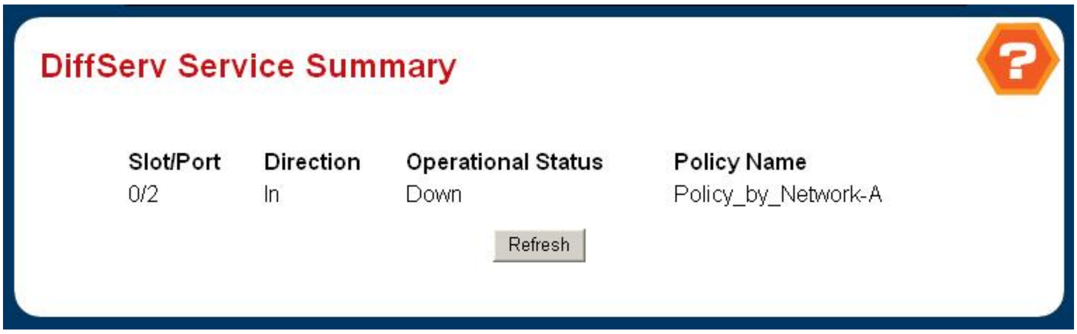
Policy In Policy_by_Network-A

Figure 4-5-22 DiffServ Service Configuration

4.5.4.9 DiffServ Service Summary

This page shows the configuration summary of DiffServ service.

- **Slot.Port -** Shows the Slot.Port that uniquely specifies an interface.
- **Direction -** Shows the traffic direction of this service interface, either In or Out.
- **Operational Status** - Shows the operational status of this service interface, either Up or Down.
- **Policy Name -** Shows the name of the attached policy.



DiffServ Service Summary

Slot/Port	Direction	Operational Status	Policy Name
0/2	In	Down	Policy_by_Network-A

Figure 4-5-23 DiffServ Service Summary

4.5.4.10 DiffServ Service Statistics

This screen displays service-level statistical information in tabular form for all interfaces in the system to which a DiffServ policy has been attached in the inbound and/or outbound traffic directions. Use the 'Counter Mode Selector' to specify the counter display mode as either octets or packets (the default).

Selection Criteria

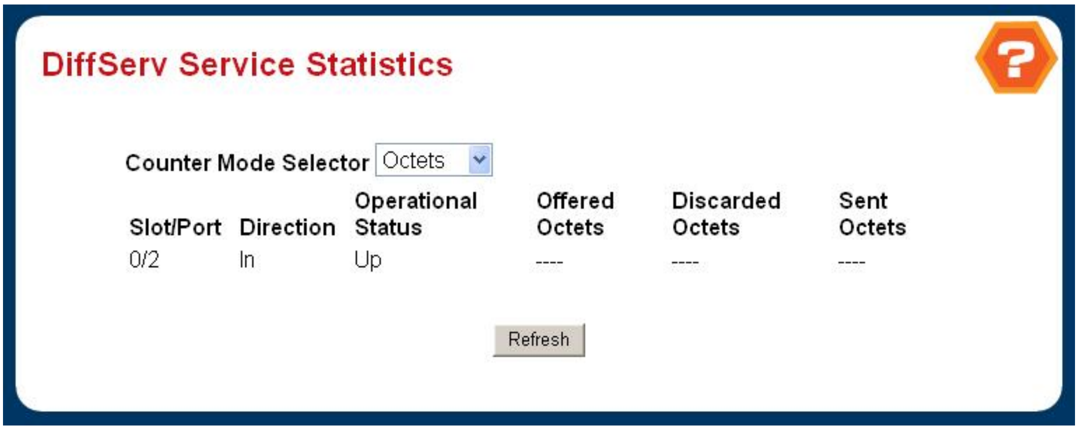
- **Counter Mode Selector -** Specifies the format of the displayed counter values, which must be either Octets or Packets. The default is 'Packets'.

Non-Configurable Data

- **Slot.Port -** Shows the Slot.Port that uniquely specifies an interface.
- **Direction -** Shows the traffic direction of this service interface, either In or Out.
- **Operational Status -** Shows the operational status of this service interface, either Up or Down.
- **Offered Packets/Octets -** A count of the total number of packets/octets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
- **Discarded Packets/Octets -** A count of the total number of packets/octets discarded for all class instances in this

service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.

- **Sent Packets/Octets -** A count of the total number of packets/octets forwarded for all class instances in this service policy after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function of an outbound link transmission element. This is the overall count per-interface, per-direction.



DiffServ Service Statistics

Counter Mode Selector: Octets

Slot/Port	Direction	Operational Status	Offered Octets	Discarded Octets	Sent Octets
0/2	In	Up	----	----	----

Figure 4-5-24 DiffServ Service Statistics

4.5.4.11 DiffServ Service Detailed Statistics

This screen displays class-oriented statistical information for the policy, which is specified by the interface and direction. The 'Member Classes' drop down list is populated on the basis of the specified interface and direction and hence the attached policy (if any). Highlighting a member class name displays the statistical information for the policy-class instance for the specified interface and direction.

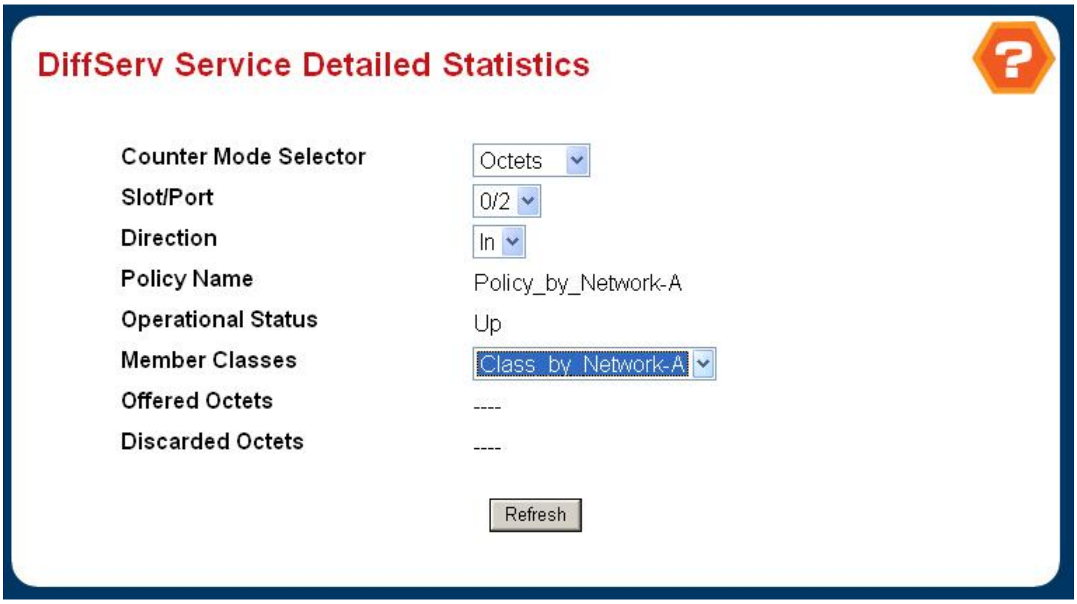
Selection Criteria

- **Counter Mode Selector -** Specifies the format of the displayed counter values, which must be either Octets or Packets. The default is 'Packets'.
- **Slot.Port -** List of all valid slot number and port number combinations in the system that have a DiffServ policy currently attached (in either direction), from which one can be chosen.
- **Direction -** List of the traffic direction of interface as either In or Out, from which one can be chosen. Only shows the direction(s) for which a DiffServ policy is currently attached.
- **Member Classes -** List of all DiffServ classes currently defined as members of the selected Policy Name. Choose one member class name at a time to display its statistics.If no class is associated with the chosen policy then nothing will be populated in the list.

Non-Configurable Data

- **Policy Name -** Name of the policy currently attached to the specified interface and direction.
- **Operational Status -** Operational status of the policy currently attached to the specified interface and direction. The value is either Up or Down.
- **Offered Packets/Octets (In) -** Displays the count of the packets/octets offered to this class instance before the defined DiffServ treatment is applied.
- **Discarded Packets/Octets (In) -** Displays the count of the packets/octets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

- **Sent Packets/Octets (Out) -** Displays the count of the packets/octets forwarded for this class instance after the defined DiffServ treatment was applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element
- **Tail Dropped Packets/Octets (Out) -** Displays the count of the packets/octets discarded due to tail dropping from a transmission queue, typically due to the effects of traffic shaping.
- **Random Dropped Packets/Octets (Out) -** Displays the count of the packets/octets discarded due to WRED active queue depth management, typically due to the effects of traffic shaping. This count is only applicable for a class instance whose policy attributes includes random dropping.
- **Shape Delayed Packets/Octets (Out) -** Displays the count of the packets/octets that were delayed due to traffic shaping. This count is only applicable for a class instance whose policy attributes includes shaping.



DiffServ Service Detailed Statistics

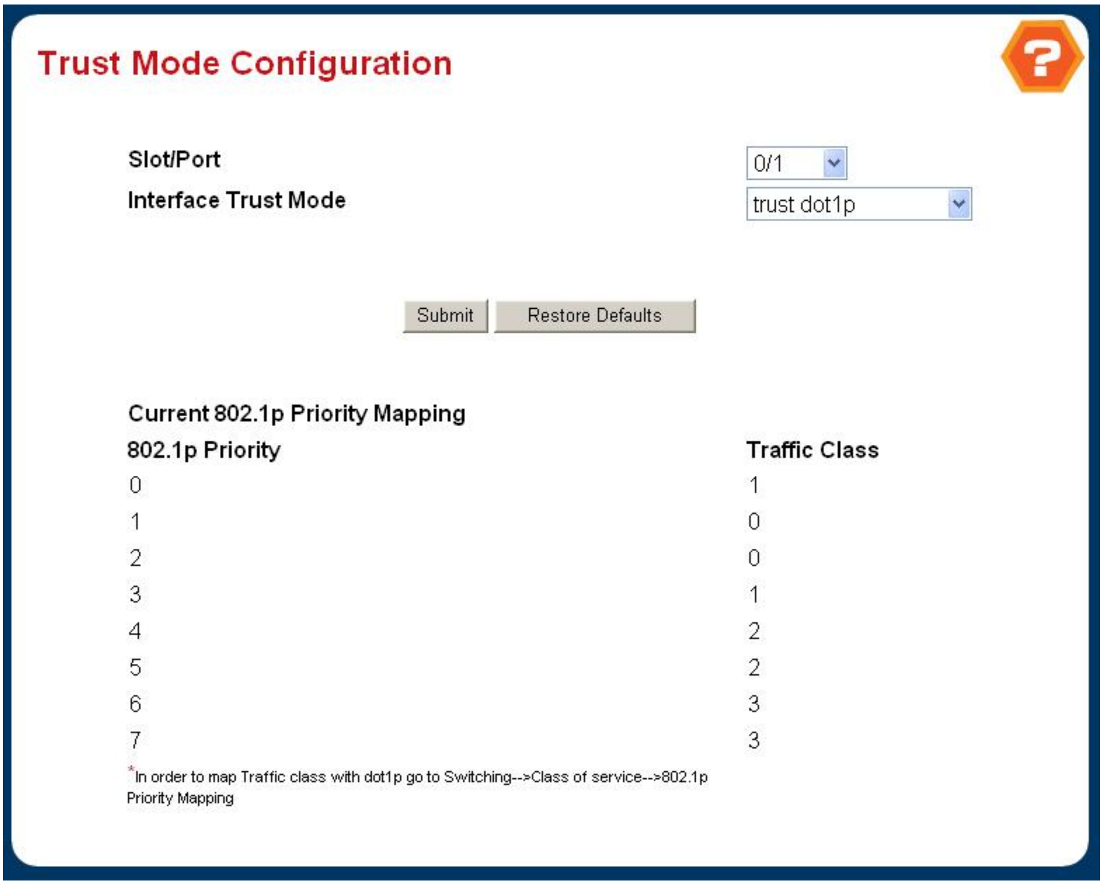
Counter Mode Selector	Octets
Slot/Port	0/2
Direction	In
Policy Name	Policy_by_Network-A
Operational Status	Up
Member Classes	Class_by_Network-A
Offered Octets	----
Discarded Octets	----

Figure 4-5-25 DiffServ Service Detailed Statistics

4.5.5 Class of Service

4.5.5.1 Trust Mode Configuration

Use this page to access Class of Service (CoS) Mapping Table Configuration



Trust Mode Configuration

Slot/Port	0/1
Interface Trust Mode	trust dot1p

Current 802.1p Priority Mapping

802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

*In order to map Traffic class with dot1p go to Switching-->Class of service-->802.1p Priority Mapping

Figure 4-5-26 Trust Mode Configuration

Selection Criteria

- **Slot/Port** - Specifies all CoS configurable interfaces. The option "Global" represents the most recent global configuration settings.

Configurable Data

- **Interface Trust Mode** - Specifies whether or not to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following:
    - ***untrusted***
    - ***trust dot1p***
    - ***trust ip-precedence***
    - ***trust ip-dscp***

  Default value is **trust dot1p.**

- **IP Precedence Traffic Class** - Specify which internal traffic class to map the corresponding IP Precedence value. Valid Range is (0 to 7) .

- **IP DSCP Traffic Class** - Specify which internal traffic class to map the corresponding IP DSCP value. Valid Range is (0 to 7) .

Non-Configurable Data

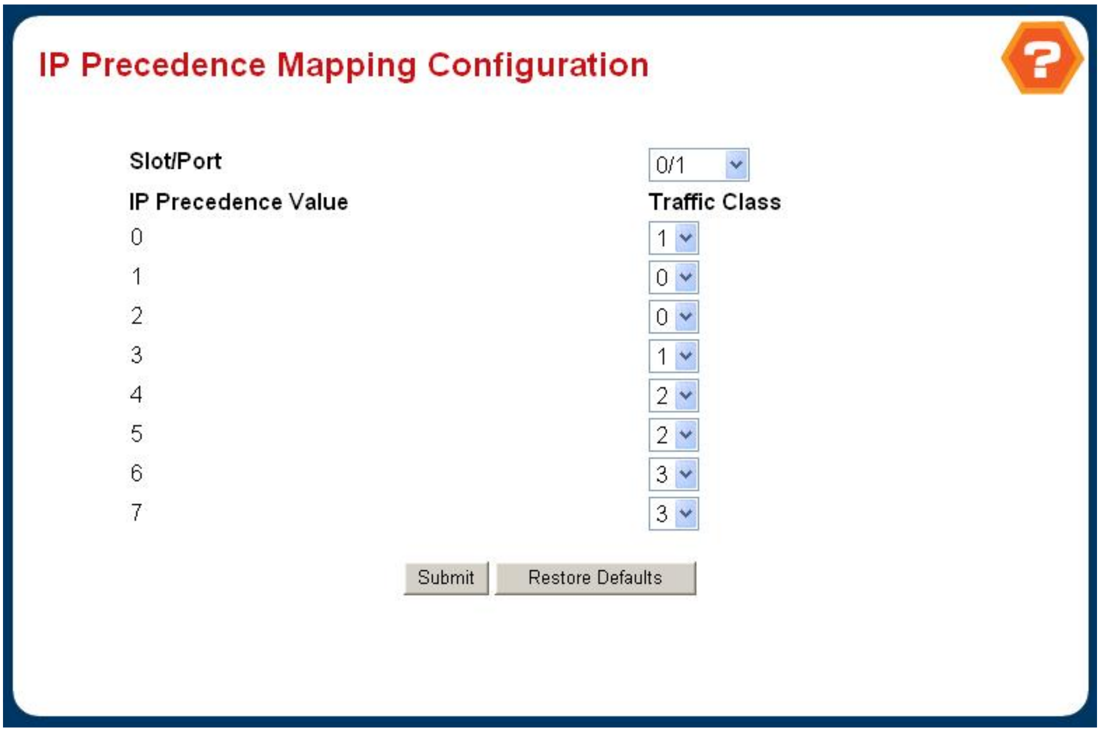
- **Untrusted Traffic Class** - Displays traffic class (i.e. queue) to which all traffic is directed when in 'untrusted' mode. Valid Range is (0 to 7).
- **Non-IP Traffic Class** - Displays traffic class (i.e. queue) to which all non-IP traffic is directed when in 'trust ip-precedence' or 'trust ip-dscp' mode. Valid Range is (0 to 7).
- **802.1p Priority** - Displays the 802.1p priority to be mapped.
- **IP Precedence Value** - Displays IP Precedence value. Valid Range is (0 to 7).
- **IP DSCP Value** - Displays IP DSCP value. Valid Range is (0 to 63).

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Restore Defaults** - Restores default settings.

4.5.5.2 IP Precedence Mapping Configuration

This page is to configure the IP Precedence mapping on the port.



IP Precedence Mapping Configuration

Slot/Port: 0/1

IP Precedence Value	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

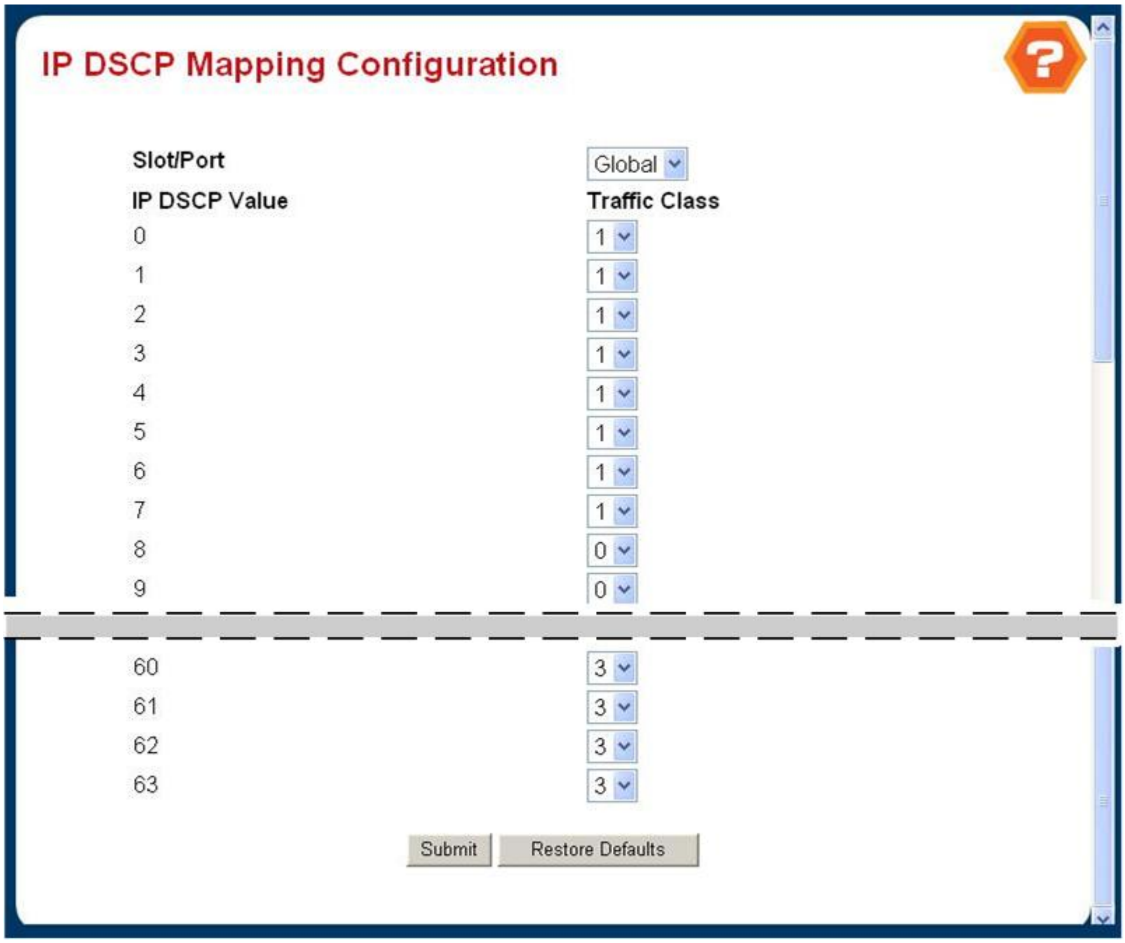
Figure 4-5-27 IP Precedence Mapping Configuation

- **Slot.Port -** Select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to the same values.

- **Traffic Class -** Specify which internal traffic class to map the corresponding IP Precedence.
- **IP Precedence -** Displays the IP Precedence to be mapped.

4.5.5.3 IP DSCP Mapping Configuration

This page is to configure the IP DSCP mapping on the port.



IP DSCP Mapping Configuration

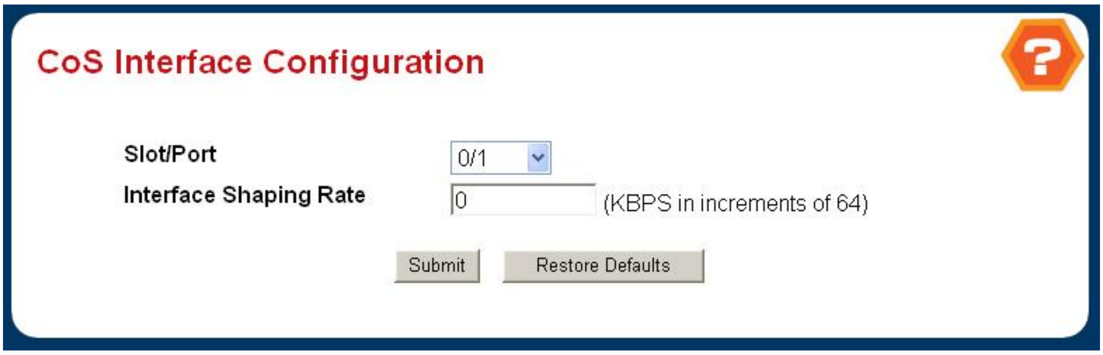
Slot/Port: Global

IP DSCP Value	Traffic Class
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	0
9	0
60	3
61	3
62	3
63	3

Figure 4-5-28 IP DSCP Mapping Configuation

- **Slot.Port -** Select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to the same values.
- **Traffic Class -** Specify which internal traffic class to map the corresponding IP DSCP.
- **IP DSCP -** Displays the IP Precedence to be mapped.

4.5.5.4 Interface Configuration



CoS Interface Configuration

Slot/Port 0/1

Interface Shaping Rate 0 (KBPS in increments of 64)

Figure 4-5-29 CoS Interface Configuation

Class of Service (CoS) Interface Configuration

Selection Criteria

- **Slot/Port** - Specifies all CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.

Configurable Data

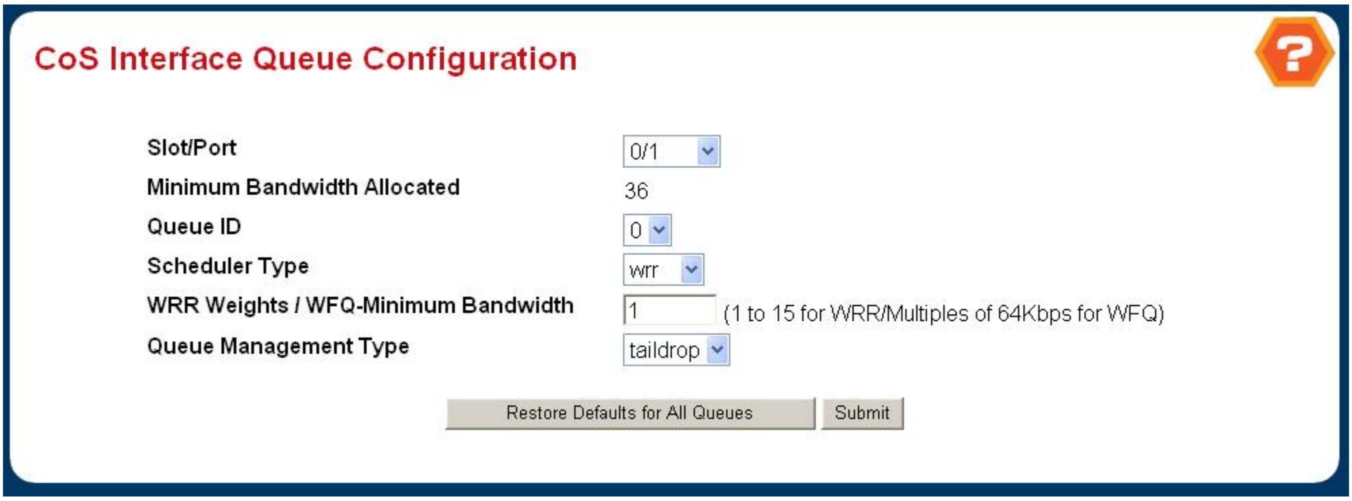
- **Interface Shaping Rate** - Specifies the maximum bandwidth allowed, typically used to shape the outbound transmission rate. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. Default value is 0. Valid Range is (0 to 10000000) KBPS with a step size of 64 .The value 0 means maximum is unlimited.

Command Buttons

- **Restore Defaults** - Restores default settings.
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.5.5.5 Interface Queue Configuration

Class of Service (CoS) Interface Queue Configuration



CoS Interface Queue Configuration

Slot/Port	0/1
Minimum Bandwidth Allocated	36
Queue ID	0
Scheduler Type	wrr
WRR Weights / WFQ-Minimum Bandwidth	1 (1 to 15 for WRR/Multiples of 64Kbps for WFQ)
Queue Management Type	taildrop

Figure 4-5-30 CoS Interface Queue Configuration

Selection Criteria

◦ **Slot/Port** - Specifies all CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.

◦ **Queue ID** - Specifies all the available queues per interface(platform based).

Configurable Data

◦ **WRR weights / Minimum Bandwidth** - Specifies the minimum guaranteed bandwidth allotted to this queue when scheduling is WFQ. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. WRR weights are the corresponding weights when scheduling is WRR Valid Range is (1 to 15)

◦ **Scheduler Type** - Specifies the type of scheduling used for this queue. the scheduling on a interface can be one the following

- ***strict***
- ***wfq***
  - ***wrr***
  - ***strict + wrr***
  - ***strict + wfq***

Default value is **weighted**.

◦ **Queue Management Type** - Queue depth management technique used for queues on this interface. This is only used if device supports independent settings per-queue.
Queue Management Type can only be one of the following:

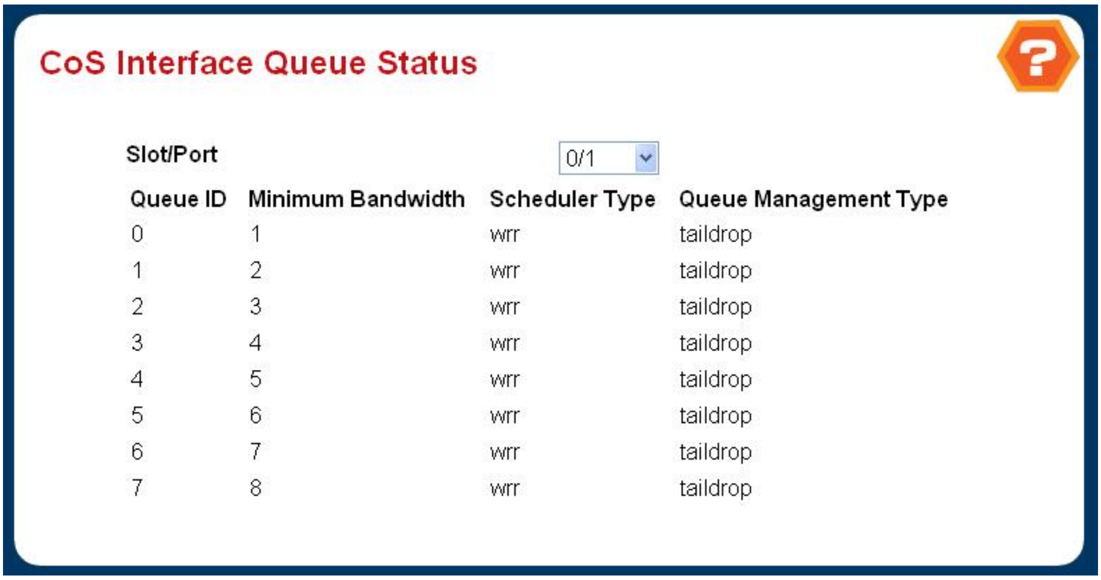
- ***taildrop***

Default value is **taildrop**.

Command Buttons

- **Restore Defaults for All Queues** - Restores default settings for all queues on the selected interface.
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.5.5.6 Interface Queue Status



CoS Interface Queue Status

Slot/Port 0/1

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	1	wrr	taildrop
1	2	wrr	taildrop
2	3	wrr	taildrop
3	4	wrr	taildrop
4	5	wrr	taildrop
5	6	wrr	taildrop
6	7	wrr	taildrop
7	8	wrr	taildrop

Figure 4-5-31 CoS Interface Queue Status

Selection Criteria

- **Slot/Port** - Specifies all CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.

Non-Configurable Data

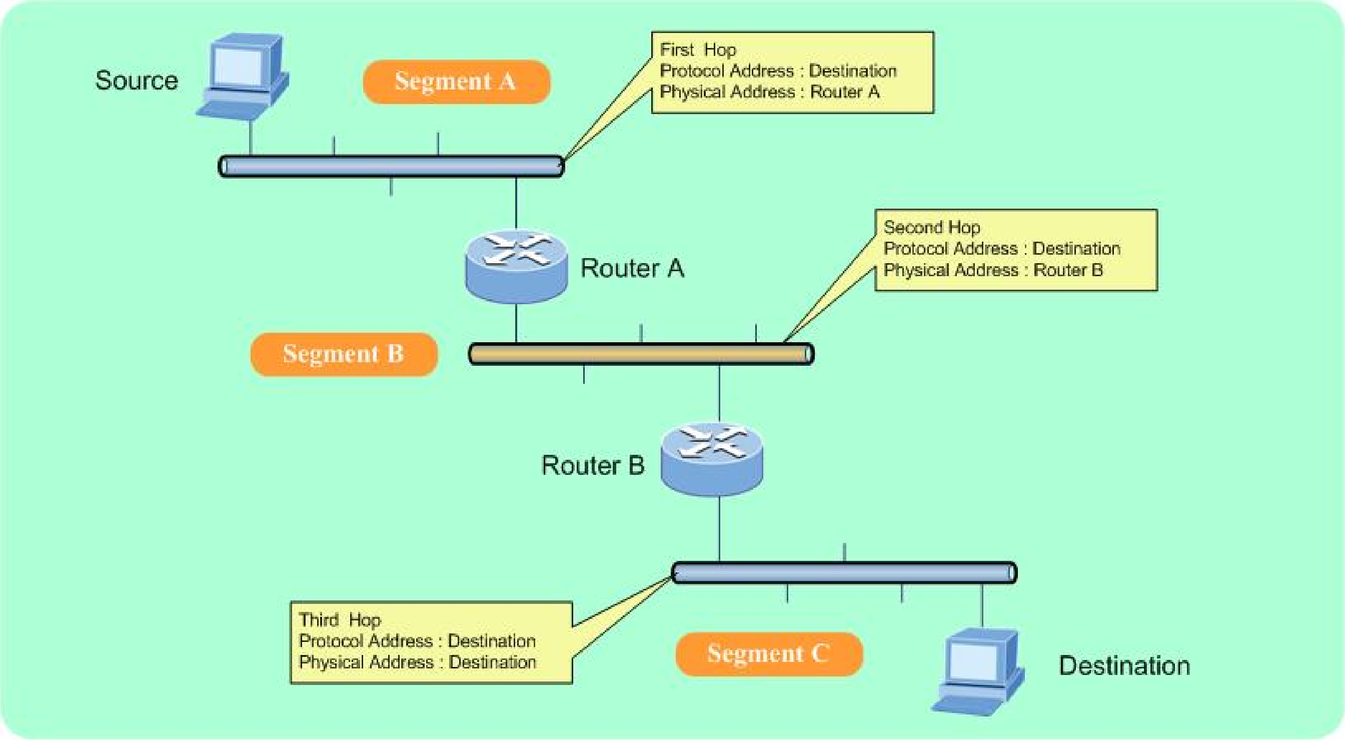
- **Queue ID** - Specifies the queueID.
- **WRR weights / Minimum Bandwidth** - Specifies the WRR weights or Minimum Bandwidth the valid range for WRR weights is 1 to 15. minimum guaranteed bandwidth allotted to this queue when scheduling is WFQ.
- **Scheduler Type** - Specifies thei type of scheduling used for this queue. the scheduling on a interface can be one the following
    - ***strict***
    - ***wfq***
        - ***wrr***
        - ***strict + wrr***
        - ***strict + wfq***
- **Queue Management Type** - Queue depth management technique used for queues on this interface. This is only used if device supports independent settings per-queue.

  Queue Management Type can only be one of the following:
    - ***taildrop***

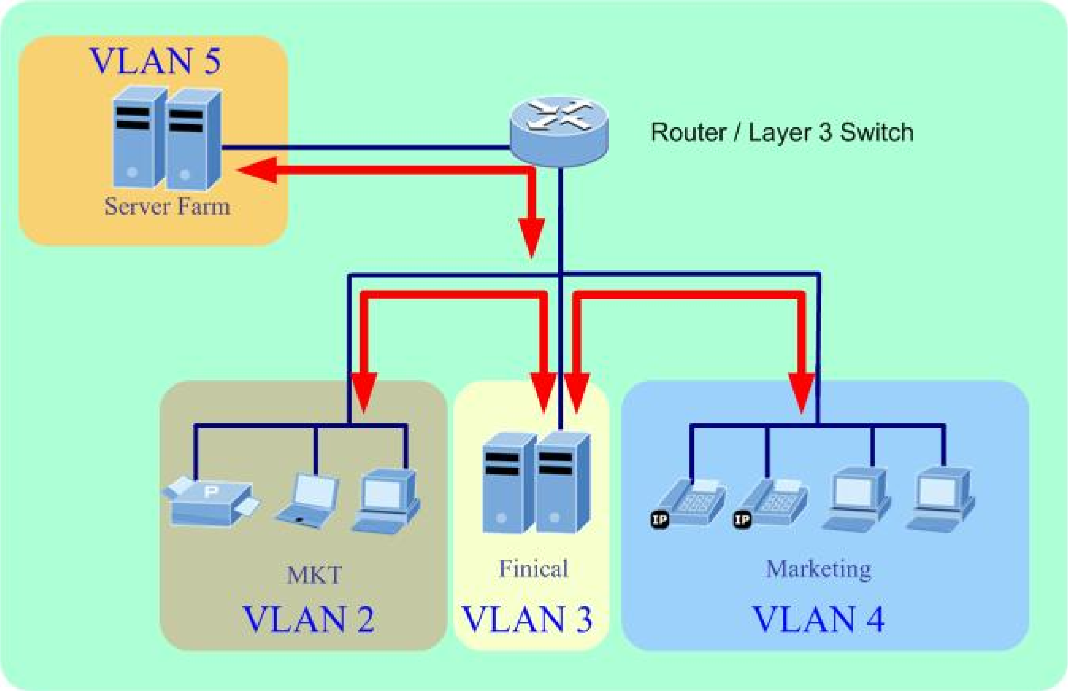
4.6 Routing

The PLANET new WGS3 Layer 3 seriew switches provide powerful IP routing, Multicast routing and Layer 3 redundancy capabilities. They support high density multilayer Gigabit Ethernet solutions to the enterprise and ISP.

The WGS3 forwards IP packets between IP networks. When it receives an IP packet through one of its interfaces, it forwards the packet through one of its interfaces.


Source
Segment A
First Hop
Protocol Address : Destination
Physical Address : Router A
Router A
Second Hop
Protocol Address : Destination
Physical Address : Router B
Segment B
Router B
Third Hop
Protocol Address : Destination
Physical Address : Destination
Segment C
Destination

The WGS3 supports multinetting, enabling it to forward packets between IP subnets on the same VLAN as well as between different VLANs.



The Routing folder provides access to the following windows:

4.6.1 IP

4.6.2 VLAN Routing

4.6.3 RIP

4.6.4 OSPF

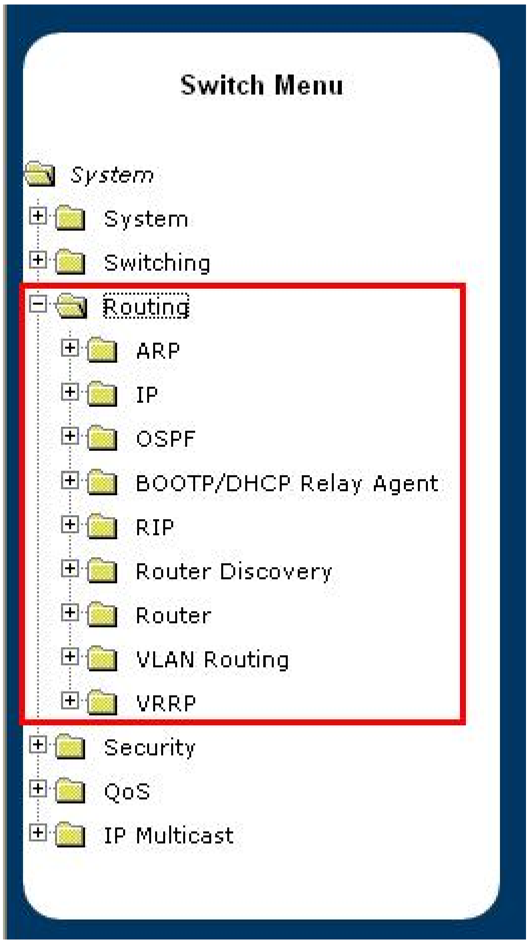
4.6.5 Router

4.6.6 ARP

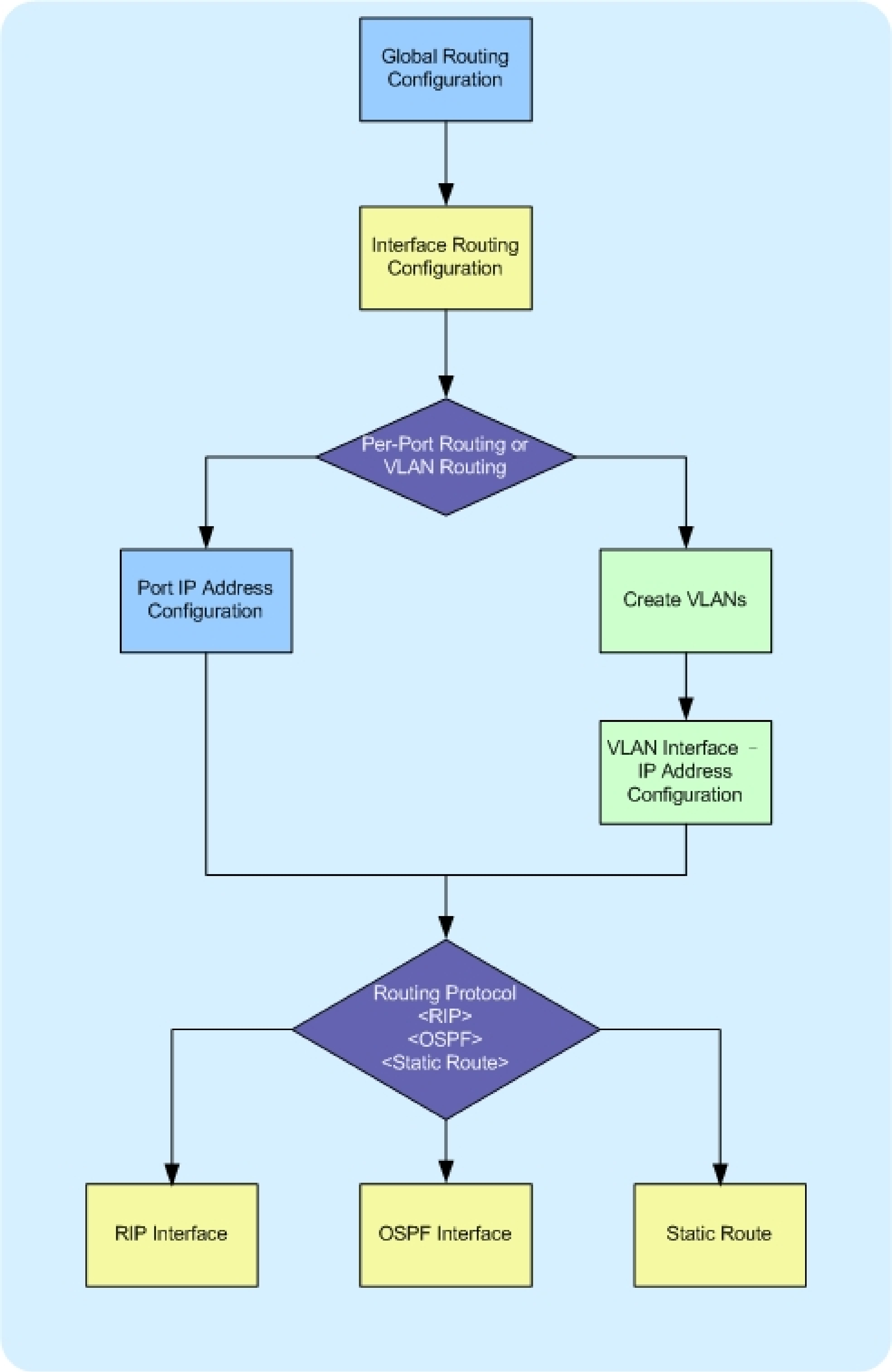
4.6.7 BOOTP/DHCP Realy Agent

4.6.8 Router Discovery

4.6.9 VRRP



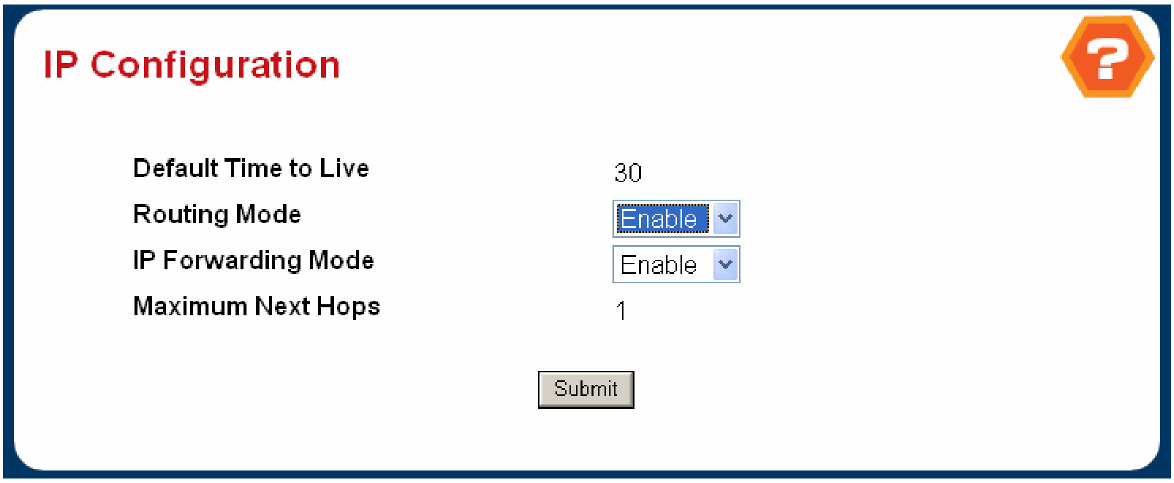
To configure the Layer 3 routing of the WGS3, the set up flow as following flow chart:


Global Routing Configuration
Interface Routing Configuration
Per-Port Routing or VLAN Routing
Port IP Address Configuration
Create VLANs
VLAN Interface – IP Address Configuration
Routing Protocol <RIP> <OSPF> <Static Route>
RIP Interface
OSPF Interface
Static Route

4.6.1 IP

4.6.1.1 IP Configuration

Use this menu to configure routing parameters for the switch as opposed to an interface.



IP Configuration

Default Time to Live 30

Routing Mode Enable

IP Forwarding Mode Enable

Maximum Next Hops 1

Figure 4-6-1 IP Configuation

Configurable Data

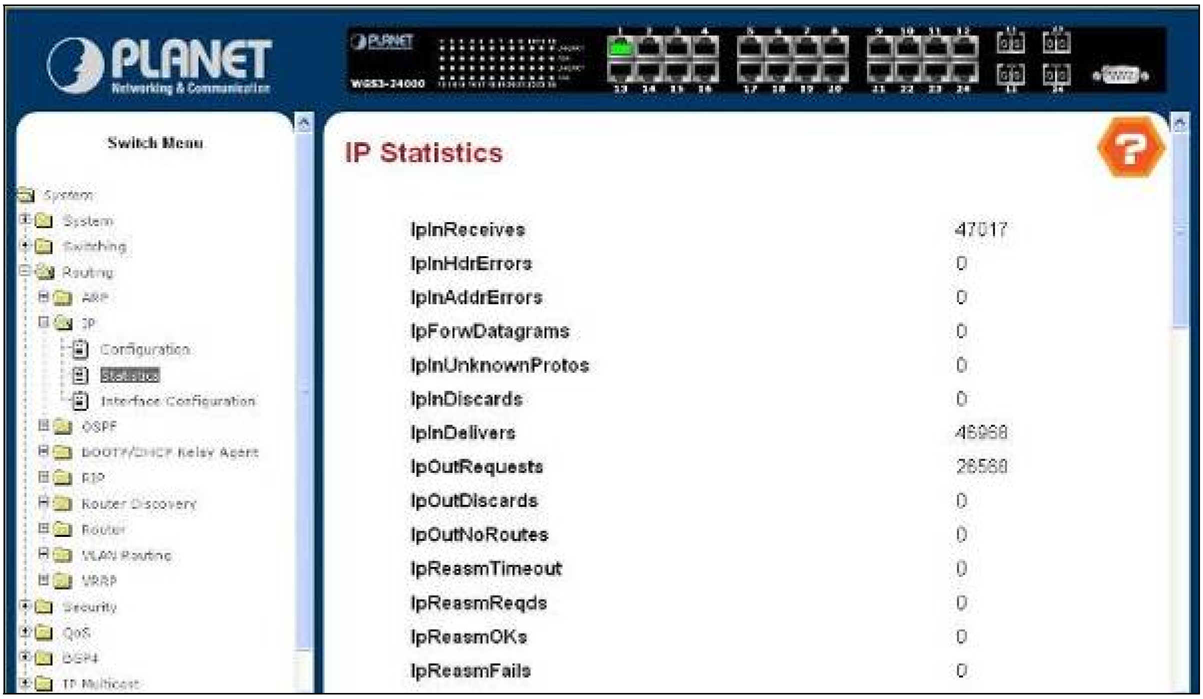
- **Routing Mode** - Select enable or disable from the pulldown menu. You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.
- **IP Forwarding Mode** - Select enable or disable from the pulldown menu. This enables or disables the forwarding of IP frames. The default value is enable.

Non-Configurable Data

- **Default Time to Live** - The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
- **Maximum Next Hops** - The maximum number of hops supported by the switch. This is a compile-time constant.

4.6.1.2 IP Statistics

The statistics reported on this screen are as specified in RFC 1213.



IP Statistics

```
IpInReceives          47017
IpInHdrErrors         0
IpInAddrErrors        0
IpForwDatagrams       0
IpInUnknownProtos     0
IpInDiscards          0
IpInDelivers          46968
IpOutRequests         26588
IpOutDiscards         0
IpOutNoRoutes         0
IpReasmTimeout        0
IpReasmReqds          0
IpReasmOKs            0
IpReasmFails          0
```

Figure 4-6-2 IP Statistics

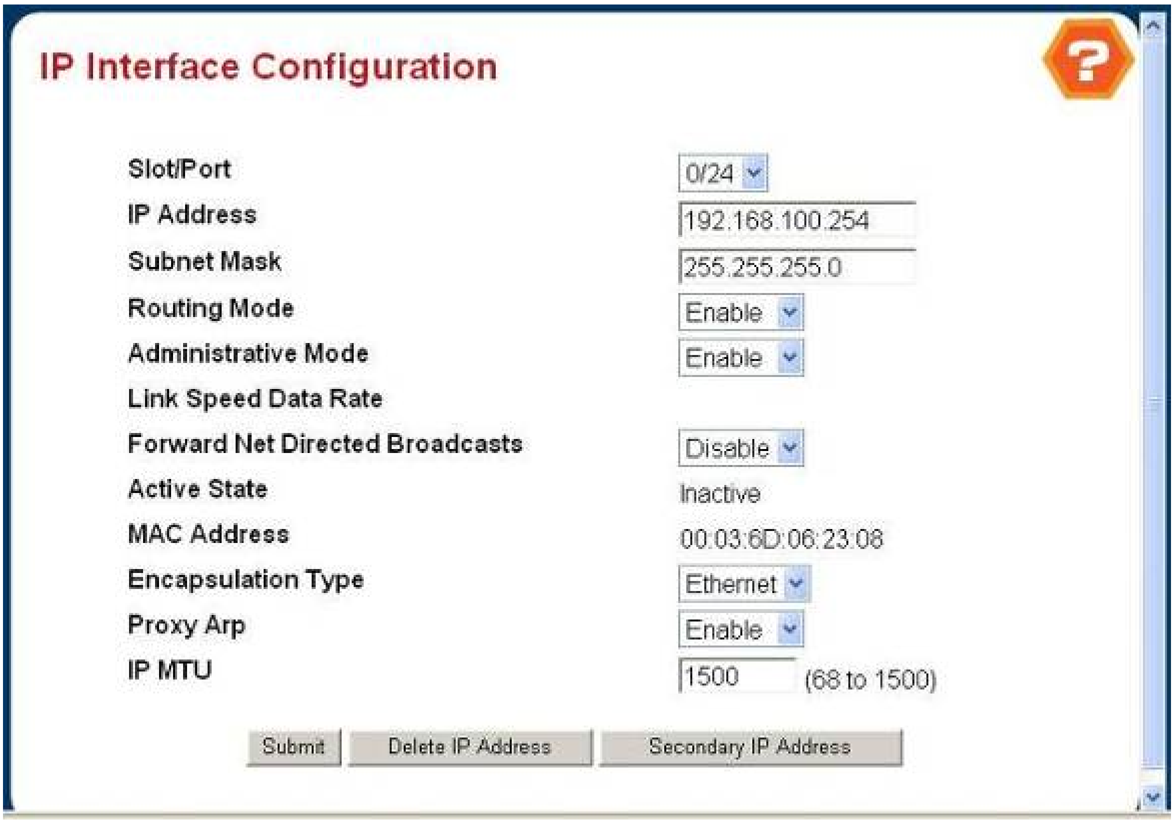
Non-Configurable Data

- **IpInReceives** - The total number of input datagrams received from interfaces, including those received in error.
- **IpInHdrErrors** - The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
- **IpInAddrErrors** - The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
- **IpForwDatagrams** - The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
- **IpInUnknownProtos** - The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
- **IpInDiscards** - The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

- **IpInDelivers** - The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
- **IpOutRequests** - The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
- **IpOutDiscards** - The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
- **IpNoRoutes** - The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
- **IpReasmTimeout** - The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
- **IpReasmReqds** - The number of IP fragments received which needed to be reassembled at this entity.
- **IpReasmOKs** - The number of IP datagrams successfully re-assembled.
- **IpReasmFails** - The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
- **IpFragOKs** - The number of IP datagrams that have been successfully fragmented at this entity.
- **IpFragFails** - The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
- **IpFragCreates** - The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
- **IpRoutingDiscards** - The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
- **IcmpInMsgs** - The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
- **IcmpInErrors** - The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
- **IcmpInDestUnreachs** - The number of ICMP Destination Unreachable messages received.
- **IcmpInTimeExcds** - The number of ICMP Time Exceeded messages received.
- **IcmpInParmProbs** - The number of ICMP Parameter Problem messages received.
- **IcmpInSrcQuenchs** - The number of ICMP Source Quench messages received.
- **IcmpInRedirects** - The number of ICMP Redirect messages received.
- **IcmpInEchos** - The number of ICMP Echo (request) messages received.
- **IcmpInEchoReps** - The number of ICMP Echo Reply messages received.
- **IcmpInTimestamps** - The number of ICMP Timestamp (request) messages received.
- **IcmpInTimestampReps** - The number of ICMP Timestamp Reply messages received.
- **IcmpInAddrMasks** - The number of ICMP Address Mask Request messages received.
- **IcmpInAddrMaskReps** - The number of ICMP Address Mask Reply messages received.

- **IcmpOutMsgs** - The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
- **IcmpOutErrors** - The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
- **IcmpOutDestUnreachs** - The number of ICMP Destination Unreachable messages sent.
- **IcmpOutTimeExcds** - The number of ICMP Time Exceeded messages sent.
- **IcmpOutParmProbs** - The number of ICMP Parameter Problem messages sent.
- **IcmpOutSrcQuenchs** - The number of ICMP Source Quench messages sent.
- **IcmpOutRedirects** - The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
- **IcmpOutEchos** - The number of ICMP Echo (request) messages sent.
- **IcmpOutEchoReps** - The number of ICMP Echo Reply messages sent.
- **IcmpOutTimestamps** - The number of ICMP Timestamp (request) messages.
- **IcmpOutTimestampReps** - The number of ICMP Timestamp Reply messages sent.
- **IcmpOutAddrMasks** - The number of ICMP Address Mask Request messages sent.
- **IcmpOutAddrMaskReps** - The number of ICMP Address Mask Reply messages sent.

4.6.1.3 IP Interface Configuration



IP Interface Configuration

Slot/Port	0/24
IP Address	192.168.100.254
Subnet Mask	255.255.255.0
Routing Mode	Enable
Administrative Mode	Enable
Link Speed Data Rate	
Forward Net Directed Broadcasts	Disable
Active State	Inactive
MAC Address	00:03:6D:06:23:08
Encapsulation Type	Ethernet
Proxy Arp	Enable
IP MTU	1500 (68 to 1500)

Figure 4-6-3 IP Interface Configuation

Selection Criteria

- **Slot/Port** - Select the interface for which data is to be displayed or configured.

Configurable Data

- **IP Address** - Enter the IP address for the interface.
- **Subnet Mask** - Enter the subnet mask for the interface. This is also referred to as the subnet/network mask, and defines the portion of the interface's IP address that is used to identify the attached network.
- **Routing Mode** - Setting this enables or disables routing for an interface. The default value is enable.
- **Forward Net Directed Broadcasts** - Select how network directed broadcast packets should be handled. If you select enable from the pulldown menu network directed broadcasts will be forwarded. If you select disable they will be dropped. The default value is disable.
- **Encapsulation Type** - Select the link layer encapsulation type for packets transmitted from the specified interface from the pulldown menu. The possible values are Ethernet and SNAP. The default is Ethernet.
- **Proxy Arp** - Select to disable or enable proxy Arp for the specified interface from the pulldown menu.
- **IP MTU** - Specifies the maximum transmission unit (MTU) size of IP packets sent on an interface. Valid range is (68 to 1500). Default value is 1500.

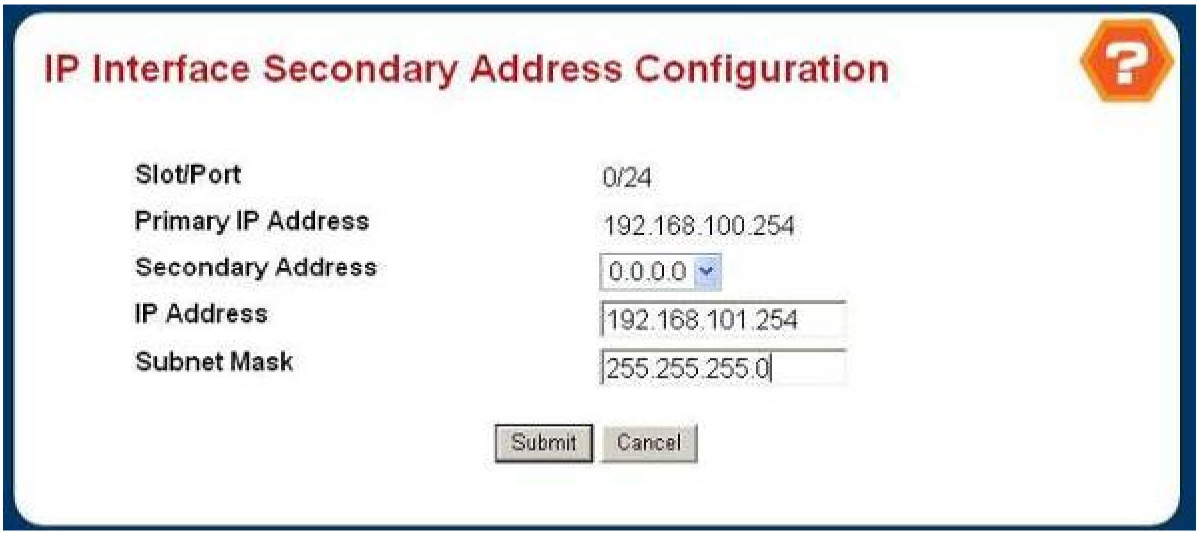
Non-Configurable Data

- **Administrative Mode** - The Administrative Mode of the interface. The default value is enable.
- **Active State** - The state of the specified interface is either Active or Inactive. An interface is considered active if it the link is up and it is in forwarding state.
- **MAC Address** - The burned-in physical address of the specified interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

Command Buttons

- **Submit** - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.
- **Delete IP Address** - Delete the IP Address from the interface. Note that the address can not be deleted if there are secondary addresses configured.
- **Secondary IP Address** - Proceed to the Secondary IP Address configuration screen.

4.6.1.4 IP Interface Secondary Address Configuration



IP Interface Secondary Address Configuration

Slot/Port	0/24
Primary IP Address	192.168.100.254
Secondary Address	0.0.0.0
IP Address	192.168.101.254
Subnet Mask	255.255.255.0

Figure 4-6-4 IP Interface Secondary Address Configuration

Selection Criteria

- **Secondary Address** - The IP Address for which data is to be displayed. Create must be selected to add a secondary address to the interface.

Configurable Data

- **IP Address** - Enter the IP Address for the interface. This value is readonly once configured.
- **Subnet Mask** - Enter the subnet mask for the interface. This is also referred to as the subnet/network mask, and defines the portion of the interface's IP Address that is used to identify the attached network. This value is readonly once configured.

Non-Configurable Data

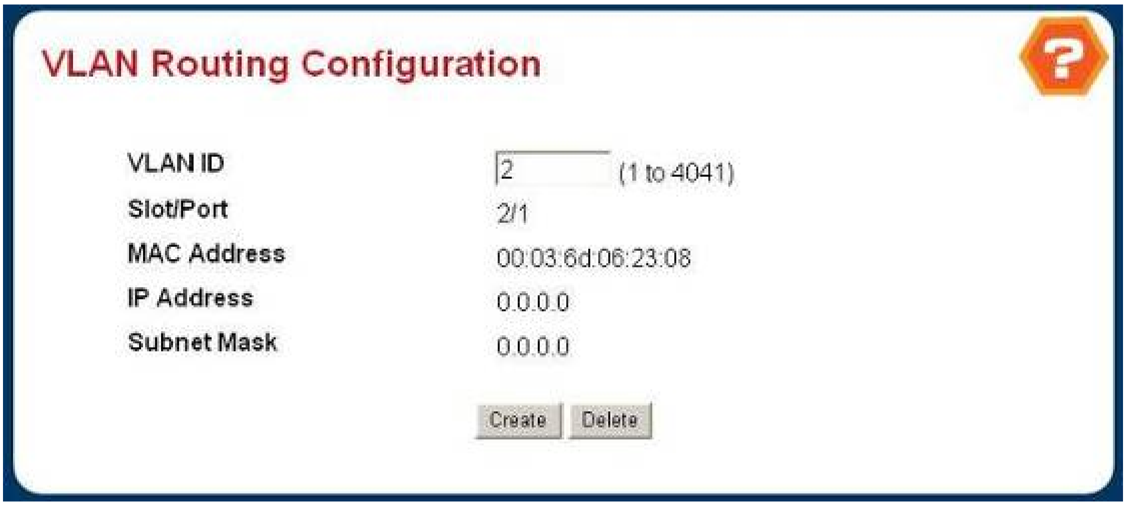
- **Slot/Port** - The interface for which data is to be displayed or configured.
- **Primary IP Address** - The Primary IP Address for the Interface.

Command Buttons

- **Submit** - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.
- **Delete** - Delete the IP Address from the interface.
- **Cancel** - Return to the IP Interface Configuration screen

4.6.2 VLAN Routing

4.6.2.1 VLAN Routing Configuration



VLAN Routing Configuration

VLAN ID 2 (1 to 4041)

Slot/Port 2/1

MAC Address 00:03:6d:06:23:08

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

Figure 4-6-5 VLAN Routing Configuraiton

Selection Criteria

- **VLAN ID** - Enter the ID of a VLAN you want to configure for VLAN Routing. Initially, the field will display the ID of the first VLAN. After you enter a new VLAN ID and click on the Create button the non-configurable data will be displayed. See below for detailed instructions on how to use that data to complete the configuration of the VLAN.

Non-Configurable Data

- **Slot/Port** - The interface assigned to the VLAN for routing.
- **MAC Address** - The MAC Address assigned to the VLAN Routing Interface
- **IP Address** - The configured IP Address of the VLAN Routing Interface. This will be 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the IP Interface Configuration page.
- **Subnet Mask** - The configured Subnet Mask of the VLAN Routing Interface. This will be 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the IP Interface Configuration page.

Command Buttons

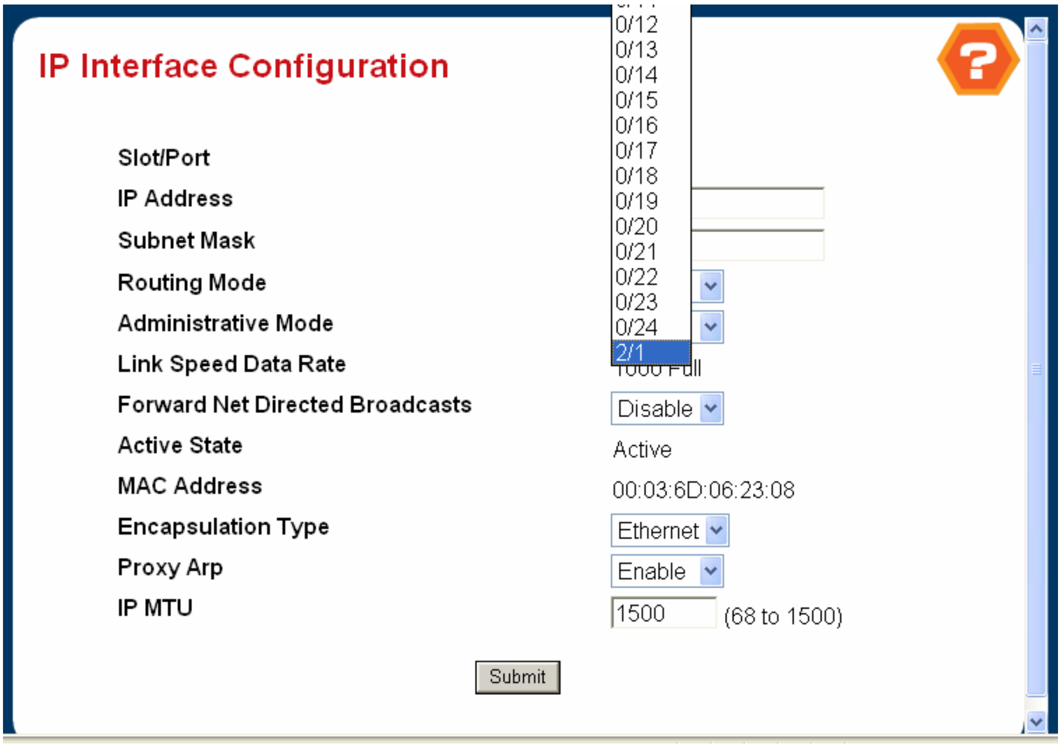
- **Create** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Delete** - Remove the VLAN Routing Interface SPECIFIED in the *VLAN ID input field* from the router configuration.

Instructions for creating a VLAN

- Enter a new VLAN ID in the field labeled VLAN ID.

- ◦ Click on the Create button. The page will be updated to display the interface and MAC address assigned to this new VLAN. The IP address and Subnet Mask fields will be 0.0.0.0.
- ◦ Note the interface assigned to the VLAN.
- ◦ Use the index pane to change to the IP Interface Configuration page.
- ◦ Select the interface assigned to the VLAN. The IP address and Subnet Mask fields will be 0.0.0.0.
- ◦ Enter the IP address and subnet mask for the VLAN.
- ◦ Select the Submit button.

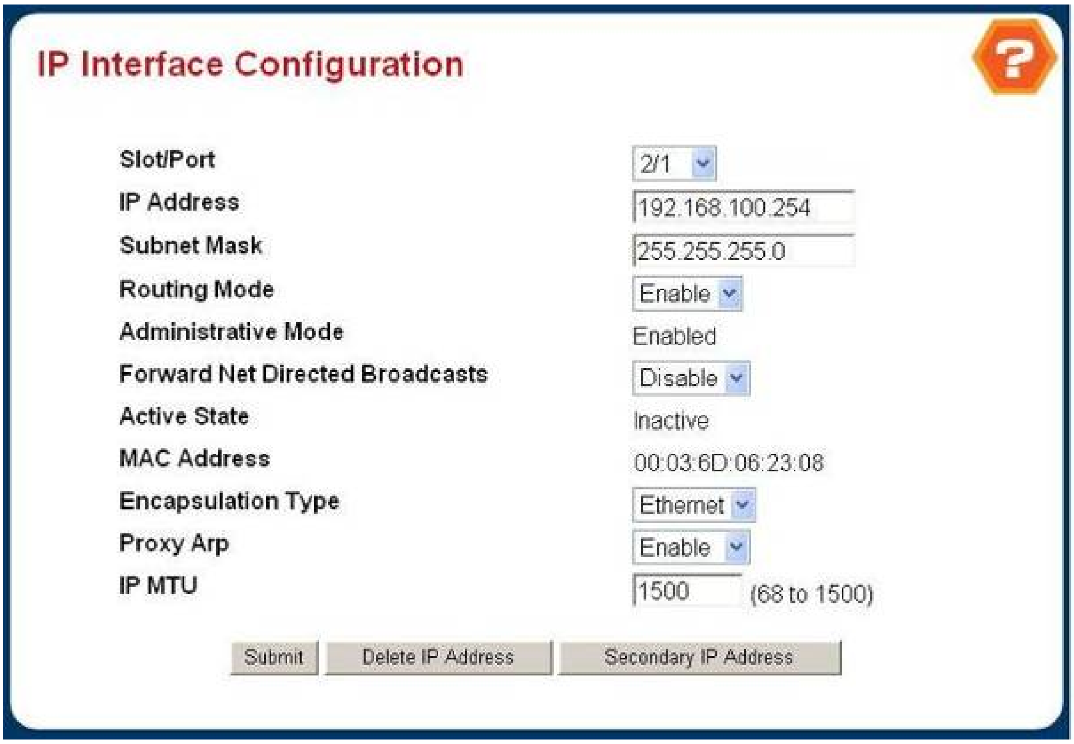
Change back to the VLAN Routing Summary page. The new VLAN should appear in the table with the correct IP address and subnet mask assigned.



IP Interface Configuration

Slot/Port	2/1
IP Address	
Subnet Mask	
Routing Mode	
Administrative Mode	
Link Speed Data Rate	1000 Full
Forward Net Directed Broadcasts	Disable
Active State	Active
MAC Address	00:03:6D:06:23:08
Encapsulation Type	Ethernet
Proxy Arp	Enable
IP MTU	1500 (68 to 1500)

Figure 4-6-6 IP Interface Configuation

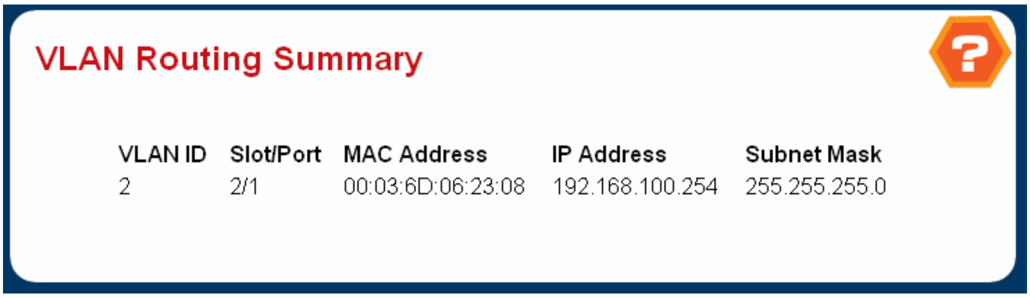


IP Interface Configuration

Slot/Port	2/1
IP Address	192.168.100.254
Subnet Mask	255.255.255.0
Routing Mode	Enable
Administrative Mode	Enabled
Forward Net Directed Broadcasts	Disable
Active State	Inactive
MAC Address	00:03:6D:06:23:08
Encapsulation Type	Ethernet
Proxy Arp	Enable
IP MTU	1500 (68 to 1500)

Figure 4-6-7 IP Interface Configuration

4.6.2.2 VLAN Routing Summary



VLAN Routing Summary

VLAN ID	Slot/Port	MAC Address	IP Address	Subnet Mask
2	2/1	00:03:6D:06:23:08	192.168.100.254	255.255.255.0

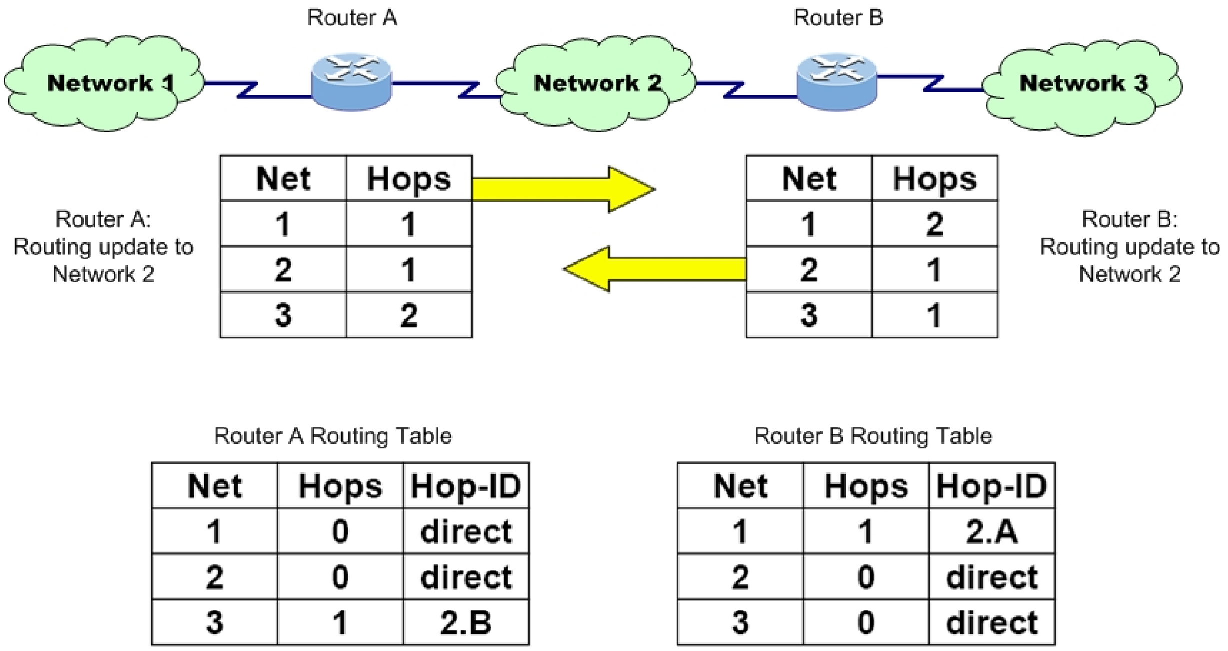
Figure 4-6-8 VLAN Routing Summary

Non-Configurable Data

- **VLAN ID** - The ID of the VLAN whose data is displayed in the current table row
- **Slot/Port** - The Slot/Port assigned to the VLAN Routing Interface
- **MAC Address** - The MAC Address assigned to the VLAN Routing Interface
- **IP Address** - The configured IP Address of the VLAN Routing Interface. This will be 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the IP Interface Configuration page.
- **Subnet Mask** - The configured Subnet Mask of the VLAN Routing Interface. This will be 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the IP Interface Configuration page.

4.6.3 RIP

The Routing Information Protocol is used to specify how routers exchange routing table information. (See “RIP and RIP-2 Dynamic Routing Protocols” on Chapter “Advanced Topics”.) When RIP is enabled on this routing switch, it broadcasts RIP messages to all devices in the network every 30 seconds, and updates its own routing table when RIP messages are received from other routers. RIP messages contain both the IP address and a metric for each destination network it knows about, where the metric indicates the number of hops from this device to the destination network.



Net	Hops
1	1
2	1
3	2

Net	Hops
1	2
2	1
3	1

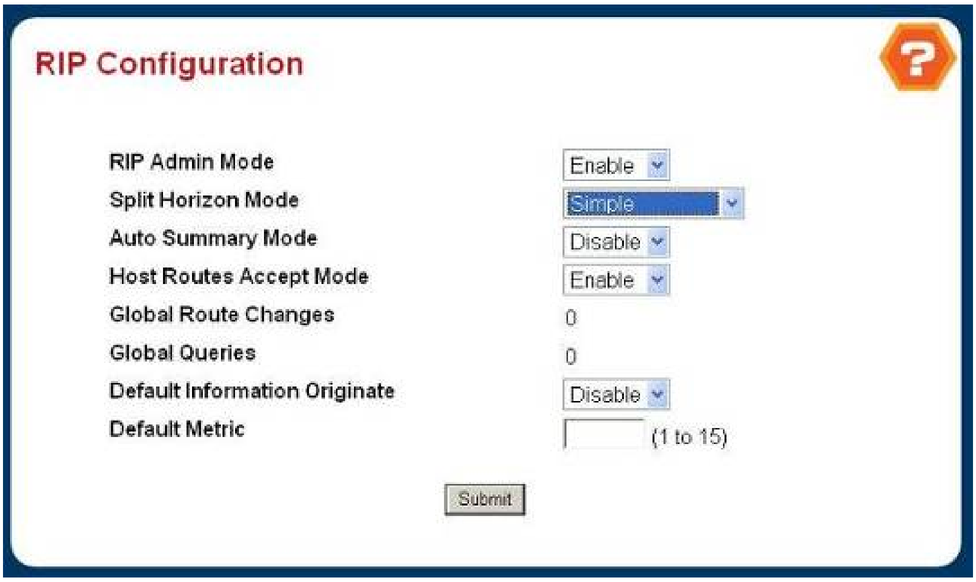
Router A Routing Table

Net	Hops	Hop-ID
1	0	direct
2	0	direct
3	1	2.B

Router B Routing Table

Net	Hops	Hop-ID
1	1	2.A
2	0	direct
3	0	direct

4.6.3.1 RIP Configuration



RIP Configuration

RIP Admin Mode	Enable
Split Horizon Mode	Simple
Auto Summary Mode	Disable
Host Routes Accept Mode	Enable
Global Route Changes	0
Global Queries	0
Default Information Originate	Disable
Default Metric	(1 to 15)

Figure 4-6-9 RIP Configuration

Configurable Data

- **RIP Admin Mode** - Select enable or disable from the pulldown menu. If you select enable RIP will be enabled for the switch. The default is disable.

- **Split Horizon Mode** - Select none, simple or poison reverse from the pulldown menu. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are:

  - ***None*** - no special processing for this case.
  - ***Simple*** - a route will not be included in updates sent to the router from which it was learned.
  - ***Poisoned reverse*** - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

  The default is simple.

- **Auto Summary Mode** - Select enable or disable from the pulldown menu. If you select enable groups of adjacent routes will be summarized into single entries, in order to reduce the total number of entries The default is enable.
- **Host Routes Select Mode** - Select enable or disable from the pulldown menu. If you select enable the router will be accept host routes. The default is enable.
- **Default Information Originate** - Enable or Disable Default Route Advertise.
- **Default Metric** - Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)

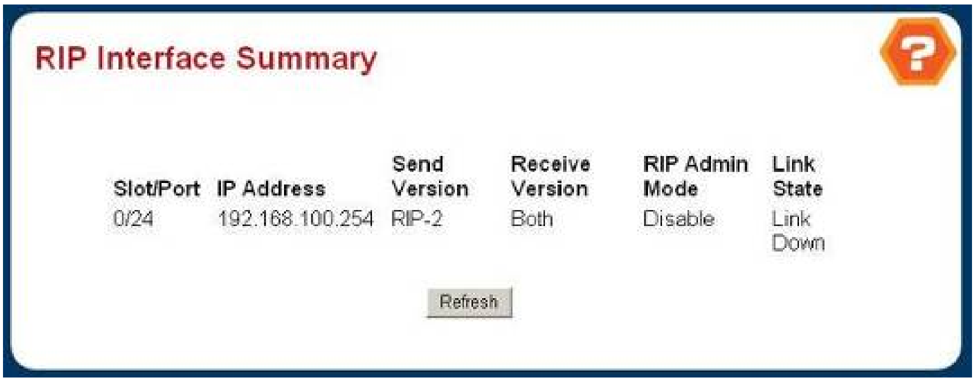
Non-Configurable Data

- **Global Route Changes** - The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
- **Global queries** - The number of responses sent to RIP queries from other systems.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.6.3.2 RIP Interface Summary



RIP Interface Summary

Slot/Port	IP Address	Send Version	Receive Version	RIP Admin Mode	Link State
0/24	192.168.100.254	RIP-2	Both	Disable	Link Down

Figure 4-6-10 RIP Interface Summary

Non-Configurable Data

- **Slot/Port** - The slot and port for which the information is being displayed.
- **IP Address** - The IP Address of the router interface.
- **Send Version** - The RIP version to which RIP control packets sent from the interface conform. The value is one of the following:

  - ***RIP-1*** - RIP version 1 packets will be sent using broadcast.
  - ***RIP-1c*** - RIP version 1 compatibility mode. RIP version 2 formatted packets will be transmitted using broadcast.
  - ***RIP-2*** - RIP version 2 packets will be sent using multicast.
  - ***None*** - RIP control packets will not be transmitted.

  The default is RIP-2.

- **Receive Version** - Which RIP version control packets will be accepted by the interface. The value is one of the following:

  - ***RIP-1*** - only RIP version 1 formatted packets will be received.
  - ***RIP-2*** - only RIP version 2 formatted packets will be received.
  - ***Both*** - packets will be received in either format.
  - ***None*** - no RIP control packets will be received.

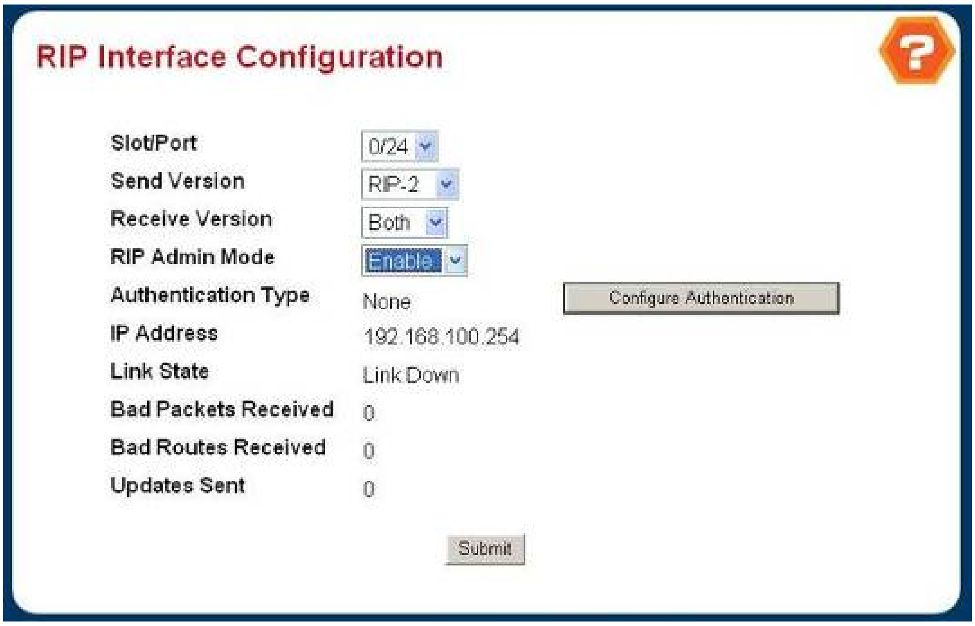
  The default is Both.

- **RIP Admin Mode** - Whether RIP is enabled or disabled on the interface.
- **Link State** - Whether the RIP interface is up or down.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.3.3 RIP Interface Configuration



RIP Interface Configuration

Slot/Port	0/24
Send Version	RIP-2
Receive Version	Both
RIP Admin Mode	Enable
Authentication Type	None
IP Address	192.168.100.254
Link State	Link Down
Bad Packets Received	0
Bad Routes Received	0
Updates Sent	0

Figure 4-6-11 RIP Interface Configuation

Selection Criteria

- **Slot/Port** - Select the interface for which data is to be configured.

Configurable Data

- **Send Version** - Select the version of RIP control packets the interface should send from the pulldown menu. The value is one of the following:
  - ***RIP-1*** - send RIP version 1 formatted packets via broadcast.
  - ***RIP-1c*** - RIP version 1 compatibility mode. Send RIP version 2 formatted packets via broadcast.
  - ***RIP-2*** - send RIP version 2 packets using multicast.
  - ***None*** - no RIP control packets will be sent.

  The default is RIP-2.

- **Receive Version** - Select what RIP control packets the interface will accept from the pulldown menu. The value is one of the following:
  - ***RIP-1*** - accept only RIP version 1 formatted packets.
  - ***RIP-2*** - accept only RIP version 2 formatted packets.
  - ***Both*** - accept packets in either format.
  - ***None*** - no RIP control packets will be accepted.

  The default is Both.

- **RIP Admin Mode** - Select enable or disable from the pulldown menu. Before you enable RIP version 1 or version 1c on an interface, you must first enable network directed broadcast mode on the corresponding interface. The default value is disable.
- **Authentication Type** - You may select an authentication type other than none by clicking on the 'Configure Authentication' button. You will then see a new screen, where you can select the authentication type from the pulldown menu. The choices are:

  - ***None*** - This is the initial interface state. If you select this option from the pulldown menu on the second screen you will be returned to the first screen and no authentication protocols will be run.
  - ***Simple*** - If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
  - ***Encrypt*** - If you select 'Encrypt' you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

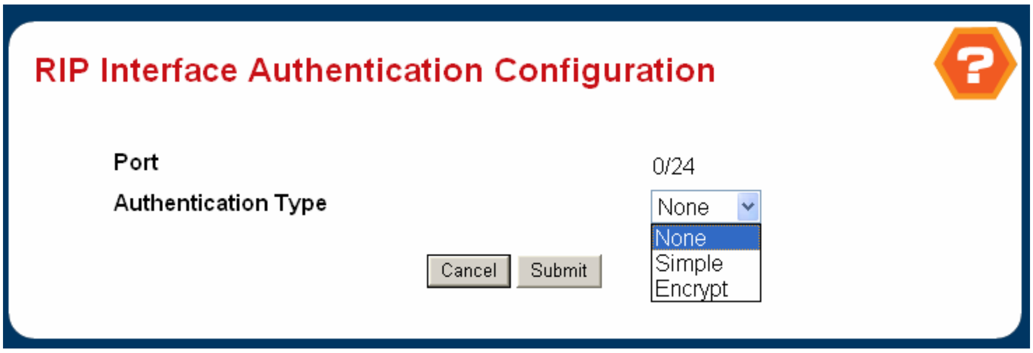
- **Authentication Key** - Enter the RIP Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' or 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.

Non-Configurable Data

- **IP Address** - The IP Address of the router interface.
- **Link State** - Indicates whether the RIP interface is up or down.
- **Bad Packets Received** - The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
- **Bad Routes Received** - The number of routes, in valid RIP packets, which were ignored for any reason (e.g. unknown address family, or invalid metric).
- **Updates Sent** - The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

Command Buttons

- **Configure Authentication** - Display a new screen where you can select the authentication method for the virtual link.
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

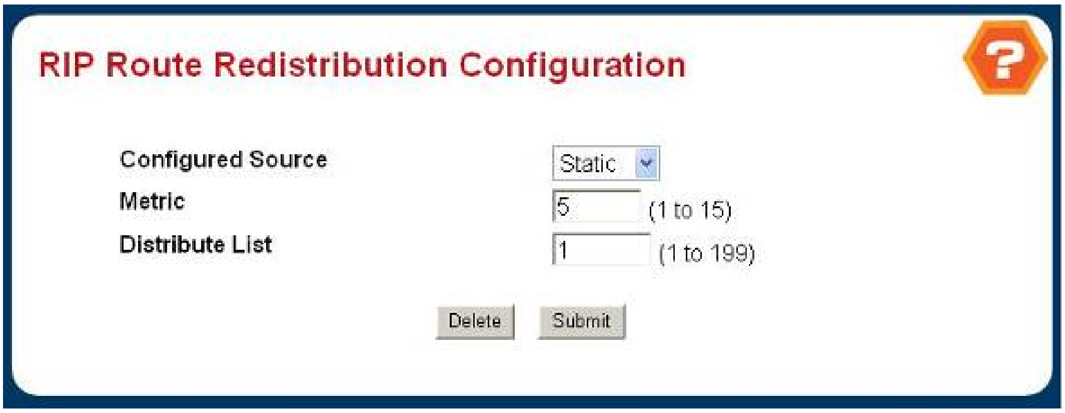


RIP Interface Authentication Configuration

Port	0/24
Authentication Type	None

Figure 4-6-12 RIP Interface Authentication Configuation

4.6.3.4 RIP Route Redistribution Configuration



RIP Route Redistribution Configuration

Configured Source	Static	
Metric	5	(1 to 15)
Distribute List	1	(1 to 199)

Figure 4-6-13 RIP Route Redistribution Configuration

Configuration

This screen can be used to configure the RIP Route Redistribution parameters. The allowable values for each fields are displayed next to the field. If any invalid values are entered, an alert message will be displayed with the list of all the valid values.

Configurable Data

- **Configured Source** - This select box is a dynamic selector and would be populated by only those Source Routes that have already been configured for redistribute by RIP. However, the topmost option in the select box would be "Create", and this allows the user to configure another, among the Available Source Routes. The valid values are

  - Create
  - Static
  - Connected
  - OSPF
  - BGP

- **Available Source** - This select box is a dynamic selector and would be populated by only those Source Routes that have not previously been configured for redistribution by RIP. This select box would appear only if the user selects "Create" option as Configured Source. The valid values are

    - Static
    - Connected
    - OSPF
    - BGP

- **Metric**- Sets the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. The valid values are (1 to 15)
- **Match** - One or more of these checkboxes must be selected to set the type of OSPF routes to be redistributed. This field would appear only if Source is "OSPF". This field displays the configured match options if "OSPF" was pre-configured and can be modified.

    - ***Internal*** - Sets Internal OSPF Routes to be redistributed
    - ***External 1*** - Sets External Type 1 OSPF Routes to be redistributed
    - ***External 2*** - Sets External Type 2 OSPF Routes to be redistributed
    - ***NSSA-External 1*** - Sets NSSA External Type 1 OSPF Routes to be redistributed
    - ***NSSA-External 2*** - Sets NSSA External Type 2 OSPF Routes to be redistributed

  The default is Internal.

- **Distribute List** - Distribute List - Sets the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to a non-existent access list, all routes are permitted. The valid values for Access List IDs are (1 to 199). When used for route filtering, the only fields in an access list that get used are

    - ***Source IP Address and netmask***
    - ***Destination IP Address and netmask***
    - ***Action (permit or deny)***

  All other fields (source and destination port, precedence, tos, etc.) are ignored.

  The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route. (Note that a 1 in the mask indicates a "don’t care" in the corresponding address bit.)

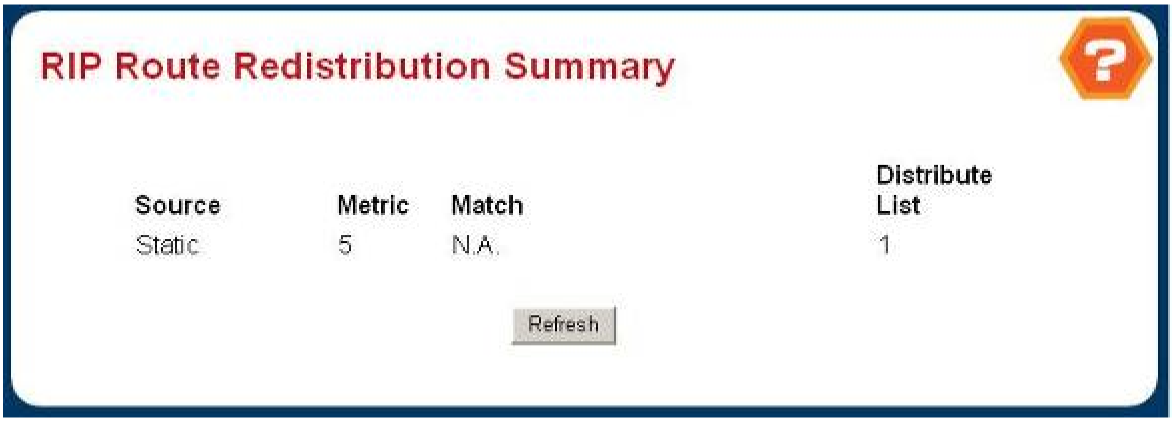
  When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route’s destination mask are significant for the filtering operation.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately.

- **Delete** - Delete the entry of the Source Route selected as Configured Source from the list of Sources configured for RIP Route Redistribution.

4.6.3.5 RIP Route Redistribution Summary



RIP Route Redistribution Summary

Source	Metric	Match	Distribute List
Static	5	N.A.	1

Figure 4-6-14 RIP Route Redistribution Summary

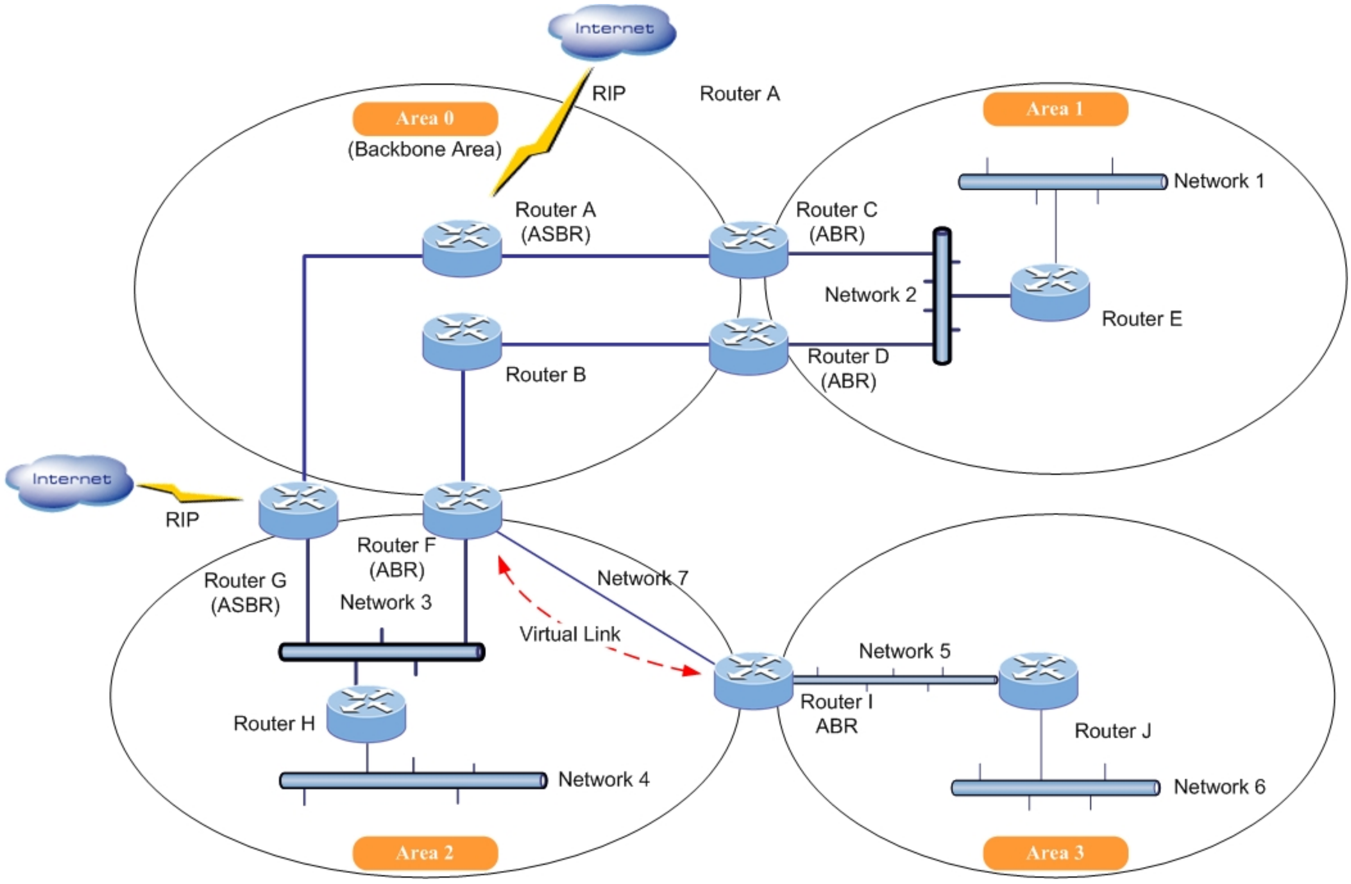
This screen displays the RIP Route Redistribution Configurations.

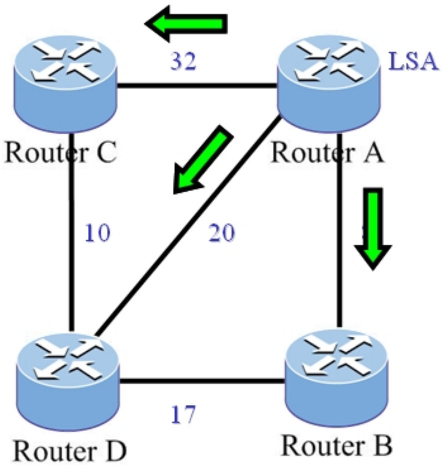
Non Configurable Data

- **Source** - The Source Route to be Redistributed by RIP.
- **Metric**- The Metric of redistributed routes for the given Source Route. Displays "Unconfigured" when not configured.
- **Match** - List of Routes redistributed when "OSPF" is selected as Source. The list may include one or more of:
    - ***Internal***
    - ***External 1***
    - ***External 2***
    - ***NSSA-External 1***
    - ***NSSA-External 2***
- **Distribute List** - The Access List that filters the routes to be redistributed by the Destination Protocol. Displays 0 when not configured.

4.6.4 OSPF

To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange **Link State Advertisements (LSAs)**. You can then define an OSPF interface by assigning an IP interface configured on this switch to one of these groups. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers. You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between **Area Border Routers (ABRs)**. And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

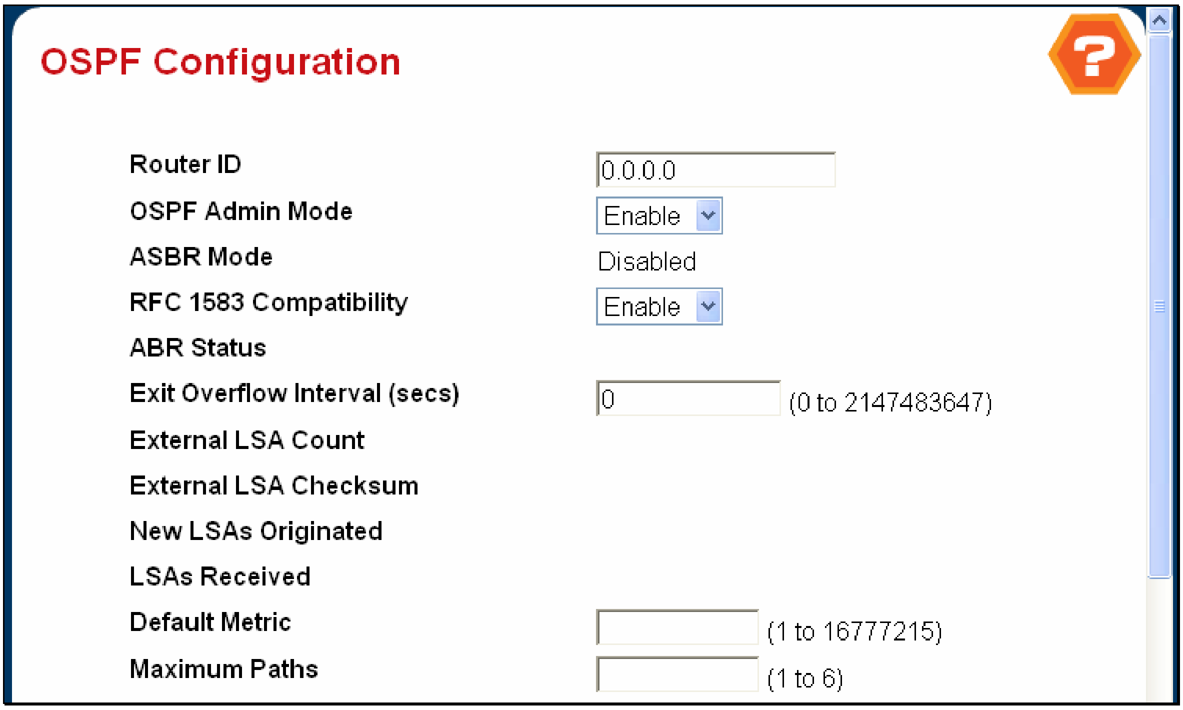




Neighbor	Metric
B	8
C	32
D	20

LSA of Router A

4.6.4.1 OSPF Configuration



OSPF Configuration

Router ID	0.0.0.0
OSPF Admin Mode	Enable
ASBR Mode	Disabled
RFC 1583 Compatibility	Enable
ABR Status	
Exit Overflow Interval (secs)	0 (0 to 2147483647)
External LSA Count	
External LSA Checksum	
New LSAs Originated	
LSAs Received	
Default Metric	(1 to 16777215)
Maximum Paths	(1 to 6)

Figure 4-6-15 OSPF Configuration

Configurable Data

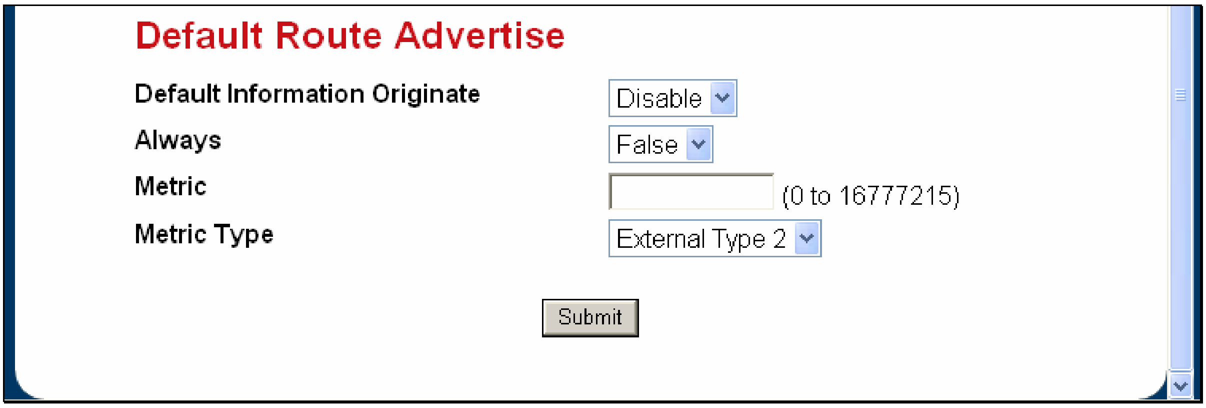
- **Router ID** - The 32 bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
- **OSPF Admin Mode*** - Select enable or disable from the pulldown menu. If you select enable OSPF will be activated for the switch. The default value is disable. You must configure a Router ID before OSPF can become operational. You do this on the IP Configuration page or by issuing the CLI command: config router id.

Note: Once OSPF is initialized on the router, it will remain initialized until the router is reset.

- **RFC 1583 Compatibility** - Select enable or disable from the pulldown menu to specify the preference rules that will be used when choosing among multiple AS-external-LSAs advertising the same destination. If you select enable, the preference rules will be those defined by RFC 1583. If you select disable, the preference rules will be those defined in Section 16.4.1 of the OSPF-2 standard (RFC 2328), which will prevent routing loops when AS-external-LSAs for the same destination have been originated from different areas. The default value is 'enable'. To prevent routing loops, you should select 'disable', but only if all OSPF routers in the routing domain are capable of operating according to RFC 2328.

- **Exit Overflow Interval** - Enter the number of seconds that, after entering overflow state, the router should wait before attempting to leave overflow state. This allows the router to again originate non-default AS-external-LSAs. If you enter 0, the router will not leave Overflow State until restarted. The range is 0 to 2147483647 seconds.
- **Default Metric** - Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 16777215)

Default Route Advertise



Default Route Advertise

Default Information Originate: Disable

Always: False

Metric: (0 to 16777215)

Metric Type: External Type 2

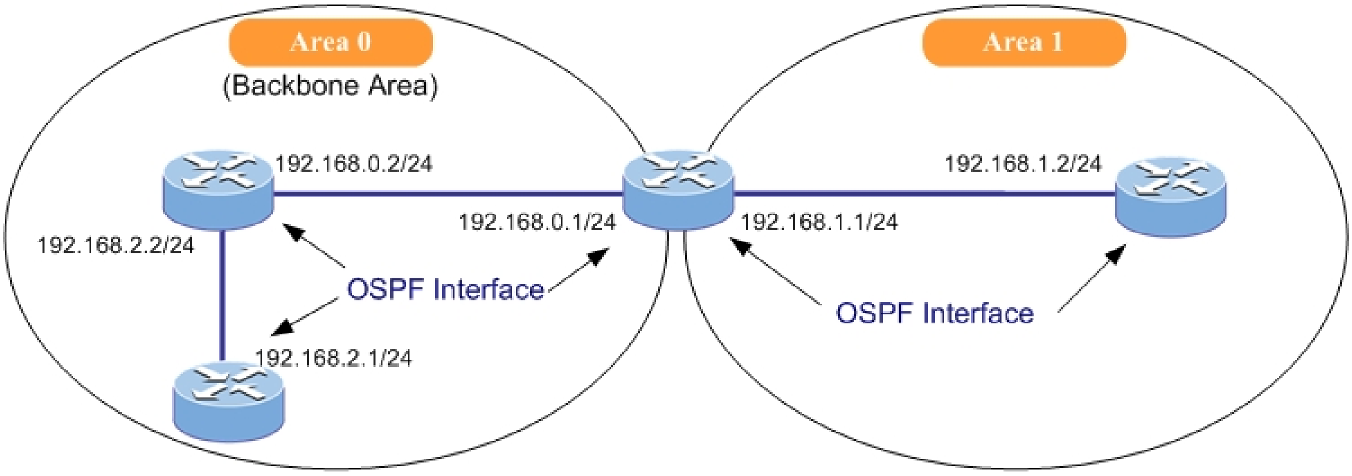
Figure 4-6-16 OSPF Configuration

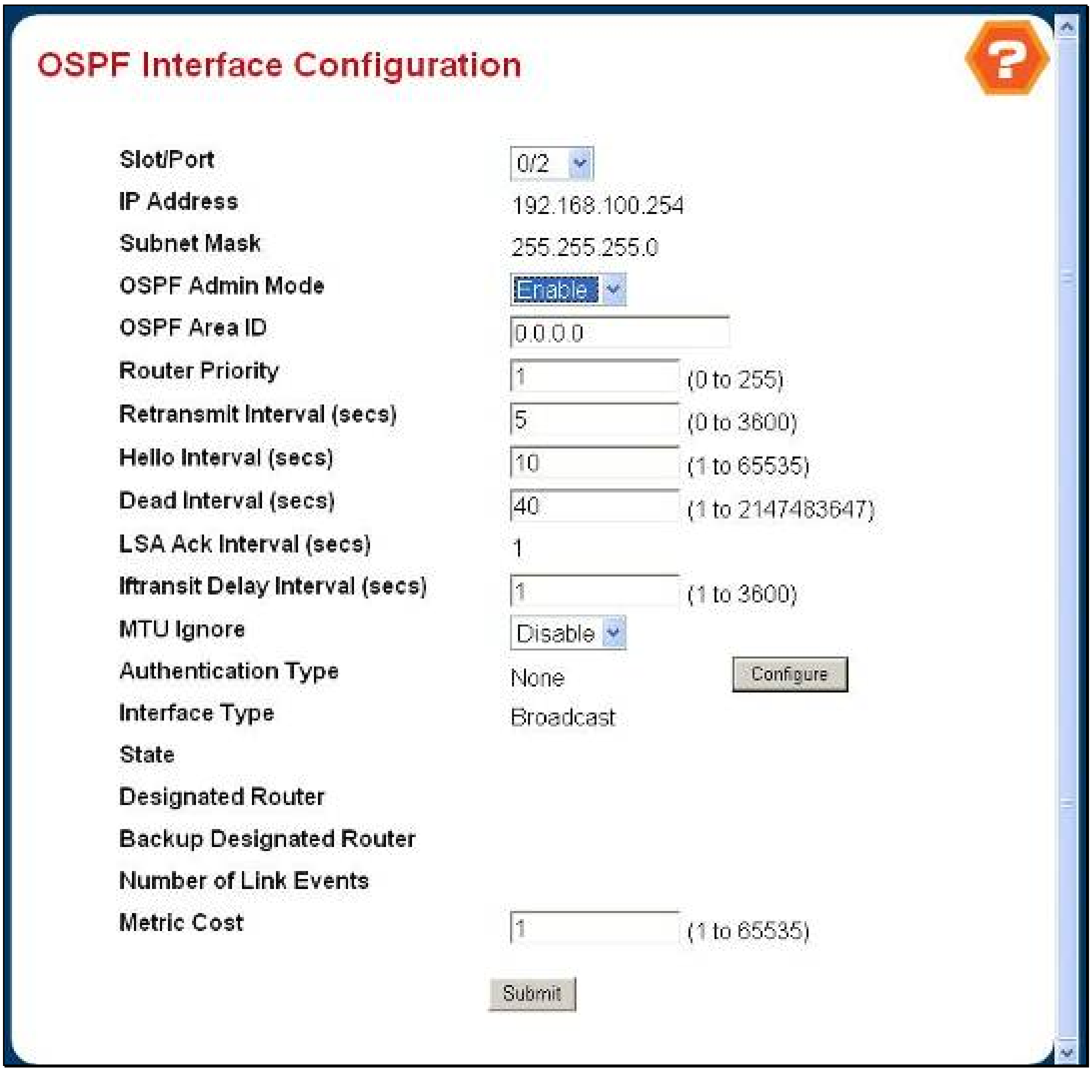
- **Default Information Originate** - Enable or Disable Default Route Advertise.
- **Always** - Sets the router advertise 0.0.0.0/0.0.0.0 when set to "True".
- **Metric** - Specifies the metric of the default route. The valid values are (0 to 16777215)
- **Metric Type** - Sets the metric type of the default route.

Non-Configurable Data

- **ASBR Mode** - Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol.
- **ABR Status** - The values of this are enabled or disabled. Enabled implies that the router is an area border router. Disabled implies that it is not an area border router.
- **External LSA Count** - The number of external (LS type 5) LSAs (link state advertisements) in the link state database.
- **External LSA Checksum** - The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers.
- **New LSAs Originated** - In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by this router.
- **LSAs Received** - The number of LSAs (link state advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

4.6.4.2 OSPF Interface Configuration





OSPF Interface Configuration

Slot/Port	0/2	
IP Address	192.168.100.254	
Subnet Mask	255.255.255.0	
OSPF Admin Mode	Enable	
OSPF Area ID	0.0.0.0	
Router Priority	1	(0 to 255)
Retransmit Interval (secs)	5	(0 to 3600)
Hello Interval (secs)	10	(1 to 65535)
Dead Interval (secs)	40	(1 to 2147483647)
LSA Ack Interval (secs)	1	
Iftransit Delay Interval (secs)	1	(1 to 3600)
MTU Ignore	Disable	
Authentication Type	None	Configure
Interface Type	Broadcast	
State		
Designated Router		
Backup Designated Router		
Number of Link Events		
Metric Cost	1	(1 to 65535)

Submit

Figure 4-6-17 OSPF Interface Configuration

Selection Criteria

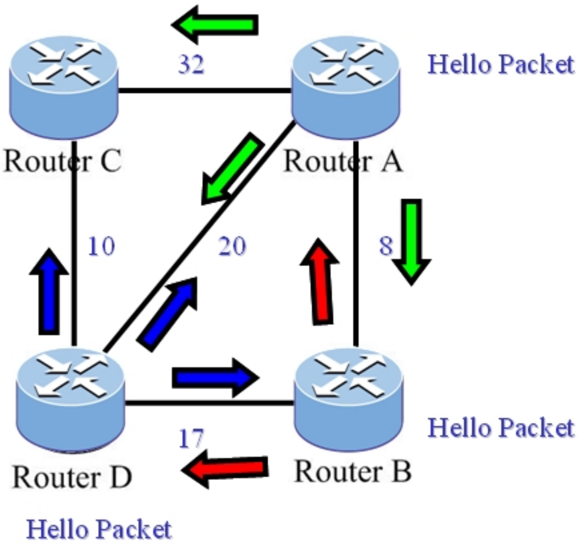
- **Slot/Port** - Select the interface for which data is to be displayed or configured.

Configurable Data

- **OSPF Admin Mode*** - You may select enable or disable from the pulldown menu. The default value is 'disable.' You can configure OSPF parameters without enabling OSPF Admin Mode, but they will have no effect until you enable Admin Mode. The following information will be displayed only if the Admin Mode is enabled: State, Designated Router, Backup Designated Router, Number of Link Events, LSA Ack Interval, and Metric Cost. For OSPF to be fully functional, you must enter a valid IP Address and Subnet Mask via the Interface IP Configuration page or through the CLI command: config ip interface network.

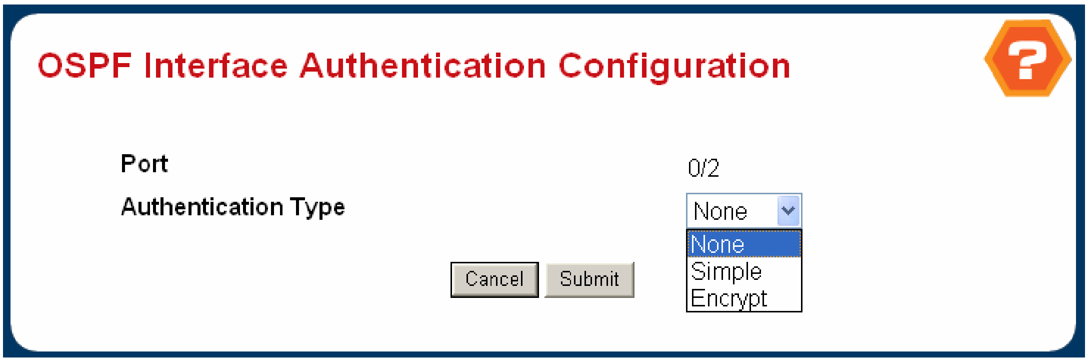
Note:	Once OSPF is initialized on the router, it will remain initialized until the router is reset.

- **OSPF Area ID** - Enter the 32 bit integer in dotted decimal format that uniquely identifies the OSPF area to which the selected router interface connects. If you assign an Area ID which does not exist, the area will be created with default values.
- **Router Priority** - Enter the OSPF priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is 1, which is the highest router priority. A value of '0' indicates that the router is not eligible to become the designated router on this network
- **Retransmit Interval** - Enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
- **Hello Interval** - Enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.



- **Dead Interval** - Enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should a multiple of the Hello Interval (e.g. 4). Valid values range from 1 to 2147483647. The default is 40.

- **Iftransit Delay Interval** - Enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
- **MTU Ignore** - Disables OSPF MTU mismatch detection on receiving packets. Default value is Disable.
- **Authentication Type** - You may select an authentication type other than none by clicking on the 'Configure' button. You will then see a new screen, where you can select the authentication type from the pulldown menu. The choices are:



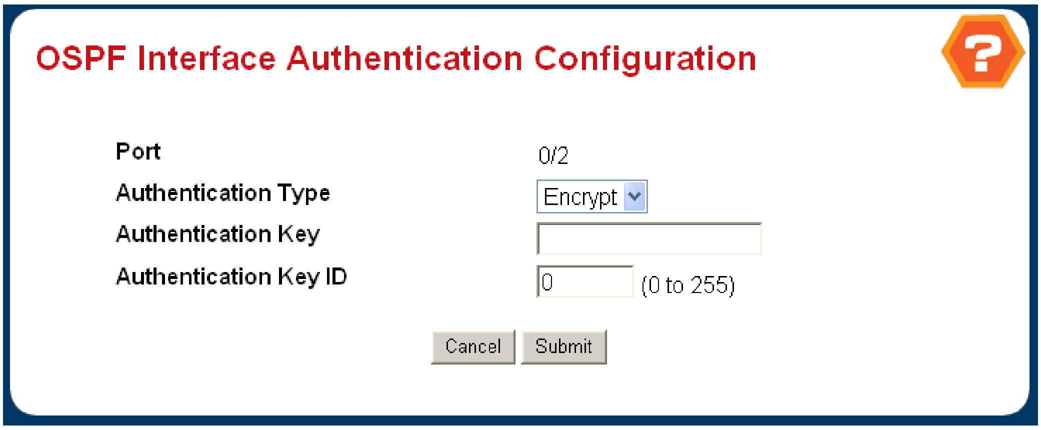
OSPF Interface Authentication Configuration

Port 0/2

Authentication Type None

Figure 4-6-18 OSPF Interfac Authentication Configuration

- ***None*** - This is the initial interface state. If you select this option from the pulldown menu on the second screen you will be returned to the first screen and no authentication protocols will be run.
- ***Simple*** - If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
- ***Encrypt*** - If you select 'Encrypt' you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.



OSPF Interface Authentication Configuration

Port 0/2

Authentication Type Encrypt

Authentication Key

Authentication Key ID 0 (0 to 255)

Figure 4-6-19 OSPF Interface Authentication Configuration

- **Authentication Key** - Enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' authentication you cannot use a key of more than 8 octets. If you choose 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.
- **Authentication ID** - Enter the ID to be used for authentication. You will only be prompted to enter an ID when you select 'Encrypt' as the authentication type. The ID is a number between 0 ad 255, inclusive.
- **Metric Cost** - Enter the value on this interface for the cost TOS (type of service). The range for the metric cost is between 1 and 65,535. Metric Cost is only configurable / displayed if OSPF is initialized on the interface.

Non-Configurable Data

- **IP Address** - The IP address of the interface.
- **Subnet Mask** - The subnet/network mask, that indicates the portion of the IP interface address that identifies the attached network.
- **LSA Ack Interval** - The number of seconds between LSA Acknowledgment packet transmissions, which must be less than the Retransmit Interval.
- **OSPF Interface Type** - The OSPF interface type, which will always be broadcast.
- **State** - The current state of the selected router interface. One of:

    - ***Down*** - This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.
    - ***Loopback*** - In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address.
    - ***Waiting*** - The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.
    - ***Designated Router*** - This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network.
    - ***Backup Designated Router*** - This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.

- ***Other Designated Router*** - The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

The State is only displayed if the OSPF admin mode is enabled.

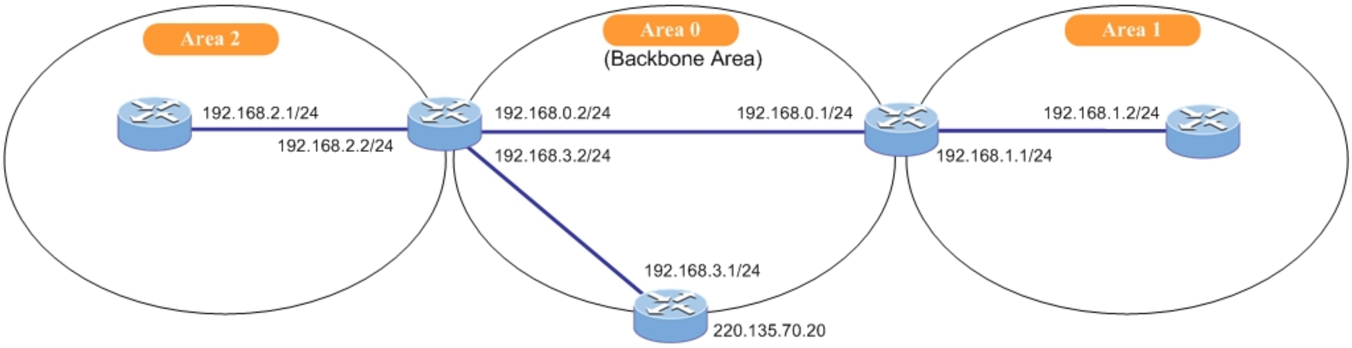
- **Designated Router** - The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router. This field is only displayed if the OSPF admin mode is enabled.
- **Backup Designated Router** - The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router. This field is only displayed if the OSPF admin mode is enabled.
- **Number of Link Events** - This is the number of times the specified OSPF interface has changed its state. This field is only displayed if the OSPF admin mode is enabled.

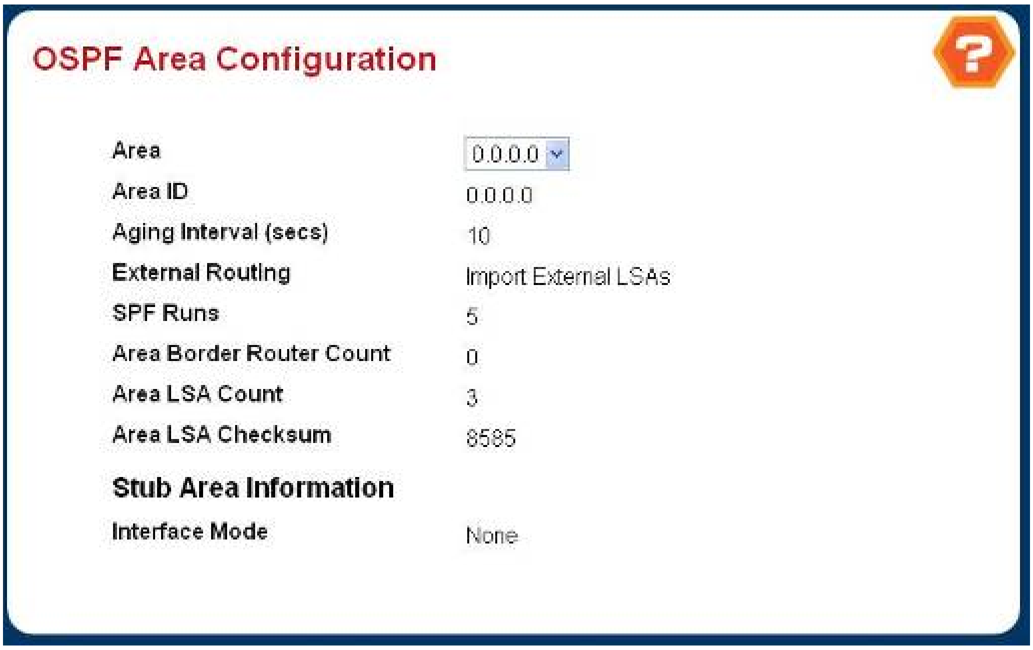
Command Buttons

- **Configure Authentication** - Display a new screen where you can select the authentication method for the virtual link.
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.6.4.3 OSPF Area Configuration

OSPF protocol broadcast messages (i.e., Link State Advertisements) are restricted by area to limit their impact on network performance. Before assigning an Area ID to a specific OSPF interface, you must first specify the Area ID in this table. Each entry in this table identifies a logical group of OSPF routers that actively exchange Link State Advertisements (LSAs) to ensure that they share an identical view of the network topology. You can configure the area as a normal one which can send and receive external Link State Advertisements (LSAs), a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area.





OSPF Area Configuration

Area	0.0.0.0
Area ID	0.0.0.0
Aging Interval (secs)	10
External Routing	Import External LSAs
SPF Runs	5
Area Border Router Count	0
Area LSA Count	3
Area LSA Checksum	8585

Stub Area Information

Interface Mode	None

Figure 4-6-20 OSPF Area Configuration

Selection Criteria

- **Area ID** - Select the area to be configured.

Configurable Data

- **Import Summary LSAs** - Select enable or disable from the pulldown menu. If you select enable summary LSAs will be imported into stub areas.

- **Metric Value** - Enter the metric value you want applied for the default route advertised into the stub area. Valid values range from 1 to 16,777,215.
- **Metric Type** - Select the type of metric specified in the Metric Value field.

    - ***OSPF Metric*** - Regular OSPF metric
    - ***Comparable Cost*** - External Type 1 metrics that are comparable to the OSPF metric
    - ***Non-comparable Cost*** - External Type 2 metrics that are assumed to be larger than the cost of the OSPF metric

Non-Configurable Data

- **Area ID** - The OSPF area. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
- **Aging Interval** - The Link State Advertisement (LSA) aging timer interval.
- **External Routing** - A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is a stub area, then these are the possible options for which you may configure the external routing capability, otherwise the only option is "Import External LSAs".

    - ***Import External LSAs*** - Import and propagate external LSAs
    - ***Import No LSAs*** - Do not import and propagate external LSAs

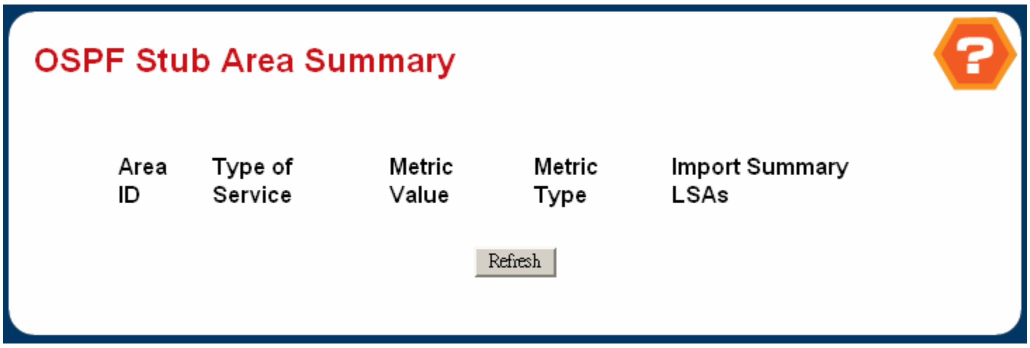
- **Authentication Type** - Currently set to 'None'.
- **SPF Runs** - The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
- **Area Border Router Count** - The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
- **Area LSA Count** - The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
- **Area LSA Checksum** - The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
- **Mode** - This field tells you whether the area is or is not a stub area. If the area may be a stub area, a 'Create Stub Area' button will be displayed. If you have configured the area as a stub area a 'Delete Stub Area' button will be displayed. Otherwise neither button will be displayed.

Command Buttons

- **Create Stub Area** - Configure the area as a stub area.
- **Delete Stub Area** - Delete the stub area designation. The area will be returned to normal state.
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Note: To add a new Area ID, use the <Add> button. (The default 0.0.0.0 indicates the OSPF backbone.) To modify or delete an existing Area ID, highlight the table entry with the cursor and select Enter.

4.6.4.4 OSPF Stub Area Summary



OSPF Stub Area Summary

Area ID	Type of Service	Metric Value	Metric Type	Import Summary LSAs

Figure 4-6-21 OSPF Stub Area Summary

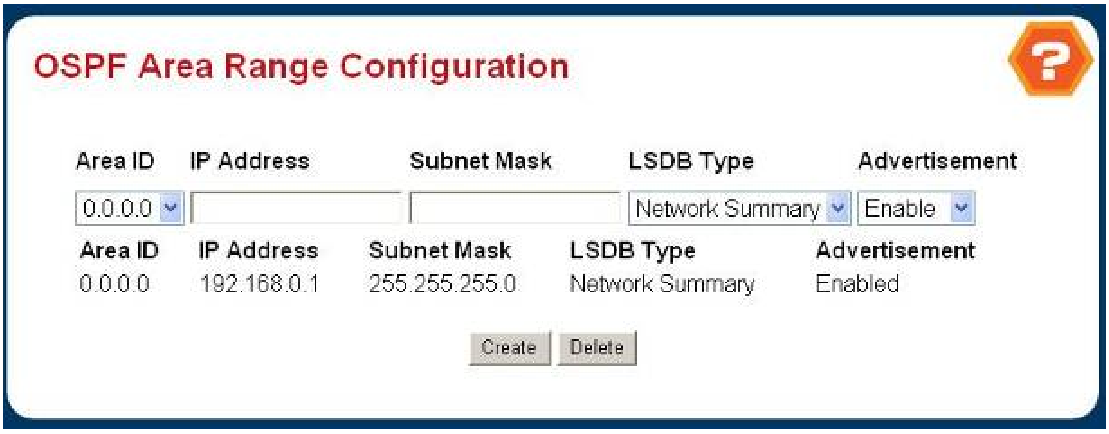
Non-Configurable Data

- **Area ID** - The Area ID of the Stub area
- **Type of Service** - The type of service associated with the stub metric. The switch supports Normal only.
- **Metric Value** - Set the metric value you want applied for the default route advertised into the area. Valid values range from 1 to 16,777,215.
- **Metric Type** - The type of metric for the stub area where valid types are:
    - OSPF Metric - Regular OSPF metric
    - Comparable Cost - External Type 1 metrics that are comparable to the OSPF metric
    - Non-comparable Cost - External Type 2 metrics that are assumed to be larger than the cost of the OSPF metric
- **Import Summary LSAs** - Whether the import of Summary LSAs is enabled or disabled.

4.6.4.5 OSPF Area Range Configuration

After you configure an area identifier, you can specify a subnetwork address range that covers all the individual networks in this area. This technique limits the amount of traffic exchanged between Area Border Routers (ABRs) by allowing them to advertise a single summary range. By summarizing routes, the routing changes within an area do not have to be updated in the backbone ABRs or in other areas.

To optimize the route summary, first configure all the OSPF routers in an area so that they fall within a contiguous address range. The route summary consists of an address and mask, where the mask can be a Variable Length Subnet Mask (VLSM). Using VLSMs allows you to configure each subnetwork within a larger network with its own subnet mask. This provides a longer subnet mask that covers fewer host IP addresses, thereby reducing the size of the routing tables that have to be exchanged. (For more information on VSLMs, see RFCs 1219 and 1878.)



OSPF Area Range Configuration

Area ID	IP Address	Subnet Mask	LSDB Type	Advertisement
0.0.0.0			Network Summary	Enable

Area ID	IP Address	Subnet Mask	LSDB Type	Advertisement
0.0.0.0	192.168.0.1	255.255.255.0	Network Summary	Enabled

Figure 4-6-22 OSPF Area Range Configuration

Selection Criteria

- **Area ID** - Selects the area for which data is to be configured.

Configurable Data

- **IP address** - Enter the IP Address for the address range for the selected area.
- **Subnet Mask** - Enter the Subnet Mask for the address range for the selected area.
- **LSDB Type** - Select the type of Link Advertisement associated with the specified area and address range. The default type is 'Network Summary'.
- **Advertisement** - Select enable or disable from the pulldown menu. If you selected enable the address range will be advertised outside the area via a Network Summary LSA. The default is enable.

Non-Configurable Data

- **Area ID** - The OSPF area.
- **IP address** - The IP Address of an address range for the area.
- **Subnet Mask** - The Subnet Mask of an address range for the area.
- **LSDB Type** - The Link Advertisement type for the address range and area.

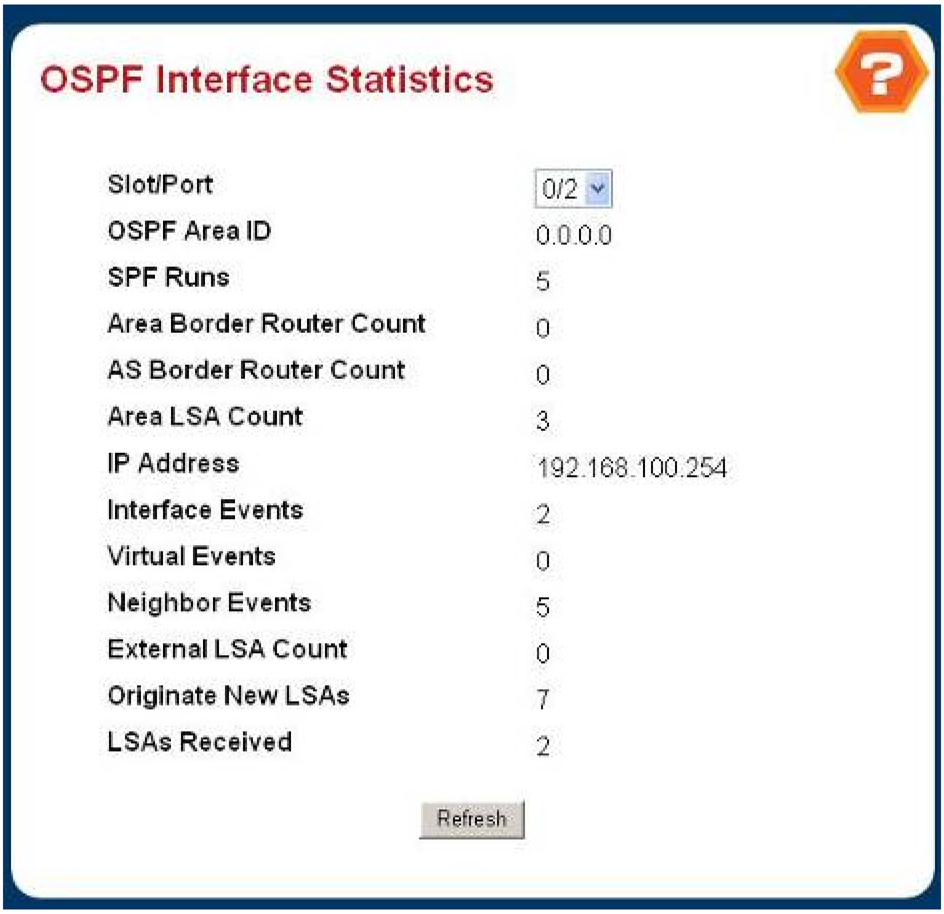
- **Advertisement** - The Advertisement mode for the address range and area.

Command Buttons

- **Create** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed. The new address range will be added to the display in the non-configurable data area.
- **Delete** - Removes the specified address range from the area configuration.

4.6.4.6 OSPF Interface Statistics

This screen displays statistics for the selected interface. The information will be displayed only if OSPF is enabled.



OSPF Interface Statistics

Slot/Port	0/2
OSPF Area ID	0.0.0.0
SPF Runs	5
Area Border Router Count	0
AS Border Router Count	0
Area LSA Count	3
IP Address	192.168.100.254
Interface Events	2
Virtual Events	0
Neighbor Events	5
External LSA Count	0
Originate New LSAs	7
LSAs Received	2

Figure 4-6-23 OSPF Interface Statistics

Selection Criteria

◦ **Slot/Port** - Select the interface for which data is to be displayed.

Non-Configurable Data

◦ **OSPF Area ID** - The OSPF area to which the selected router interface belongs. An OSPF Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.

◦ **SPF Runs** - The number of times that the intra-area route table has been calculated using this area's link-state database.

◦ **Area Border Router Count** - The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.

◦ **AS Border Router Count** - The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.

◦ **Area LSA Count** - The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

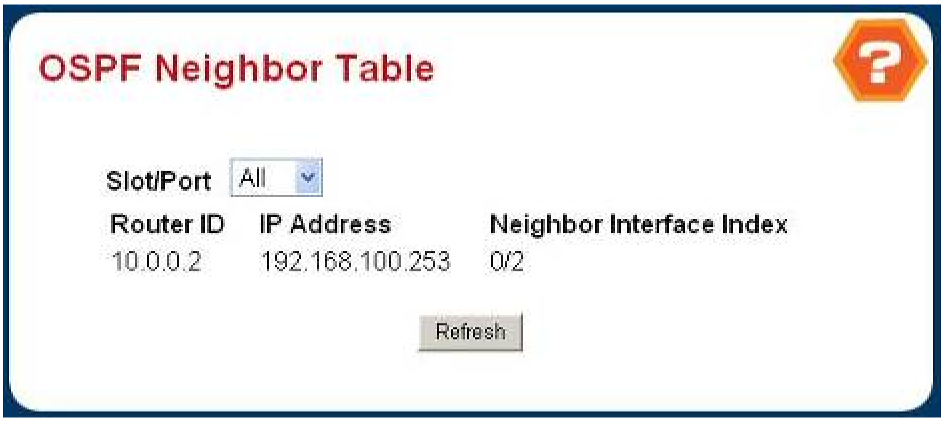
- **IP Address** - The IP address of the interface.
- **Interface Events** - The number of times the specified OSPF interface has changed its state, or an error has occurred.
- **Virtual Events** - The number of state changes or errors that have occurred on this virtual link.
- **Neighbor Events** - The number of times this neighbor relationship has changed state, or an error has occurred.
- **External LSA Count** - The number of external (LS type 5) link-state advertisements in the link-state database.
- **Originate New LSAs** - The number of new link-state advertisements that have been originated. In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks.
- **LSAs Received** - The number of link-state advertisements that have been received that have been determined to be new instantiations. This number does not include newer instantiations of self-originated link-state advertisements.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.4.7 OSPF Neighbor Table

This screen displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled.



OSPF Neighbor Table

Slot/Port: All

Router ID	IP Address	Neighbor Interface Index
10.0.0.2	192.168.100.253	0/2

Figure 4-6-24 OSPF Neighbor Table

Selection Criteria

- **Slot/Port** - Selects the interface for which data is to be displayed or configured. Slot 0 is the base unit.

Non-Configurable Data

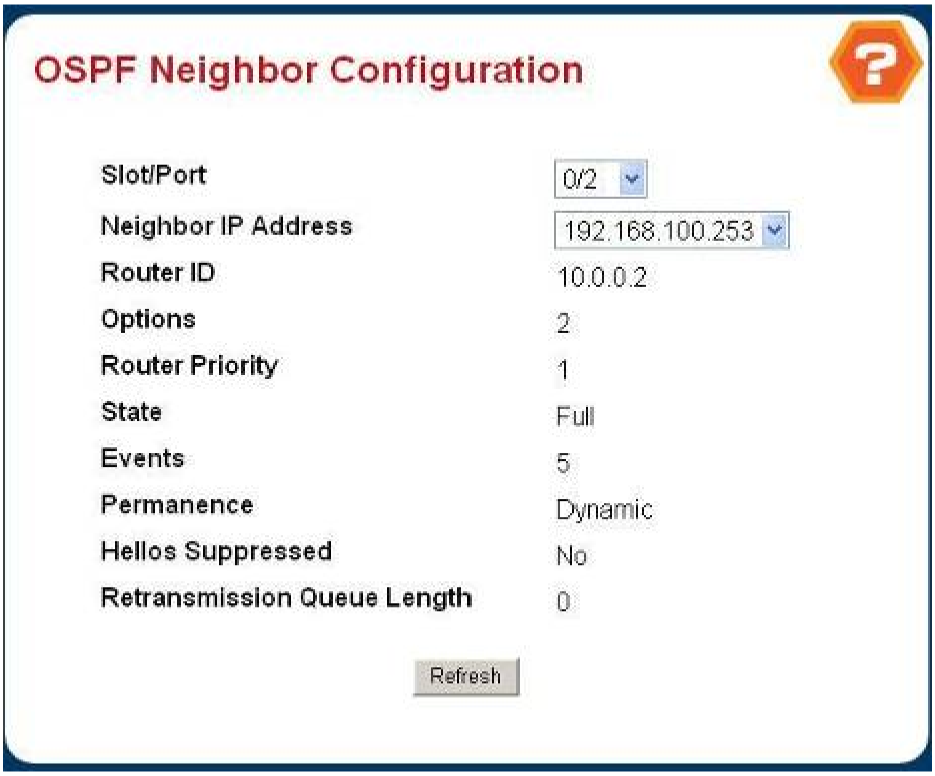
- **Router ID** - A 32 bit integer in dotted decimal format representing the neighbor interface.
- **IP Address** - The IP address of the neighboring router's interface to the attached network. It is used as the destination IP address when protocol packets are sent as unicasts along this adjacency. Also used in router-LSAs as the Link ID for the attached network if the neighboring router is selected to be designated router. The Neighbor IP address is learned when Hello packets are received from the neighbor. For virtual links, the Neighbor IP address is learned during the routing table build process.
- **Neighbor Interface Index** - A Slot/Port identifying the neighbor interface index.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.4.8 OSPF Neighbor Configuration

This screen displays the OSPF neighbor configuration for a selected neighbor ID. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled and the interface has a neighbor. The IP address is the IP address of the neighbor.



OSPF Neighbor Configuration

Slot/Port	0/2
Neighbor IP Address	192.168.100.253
Router ID	10.0.0.2
Options	2
Router Priority	1
State	Full
Events	5
Permanence	Dynamic
Hellos Suppressed	No
Retransmission Queue Length	0

Figure 4-6-25 OSPF Neighbor Configuration

Selection Criteria

- **Slot/Port** - Selects the interface for which data is to be displayed or configured. Slot 0 is the base unit.
- **Neighbor Router ID** - Selects the IP Address of the neighbor for which data is to be displayed.

Non-Configurable Data

- **Router ID** - A 32 bit integer in dotted decimal format that identifies the neighbor router.
- **Options** - The optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
- **Router Priority** - Displays the OSPF priority for the specified neighbor. The priority of a neighbor is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
- **State** - The state of a neighbor can be the following:

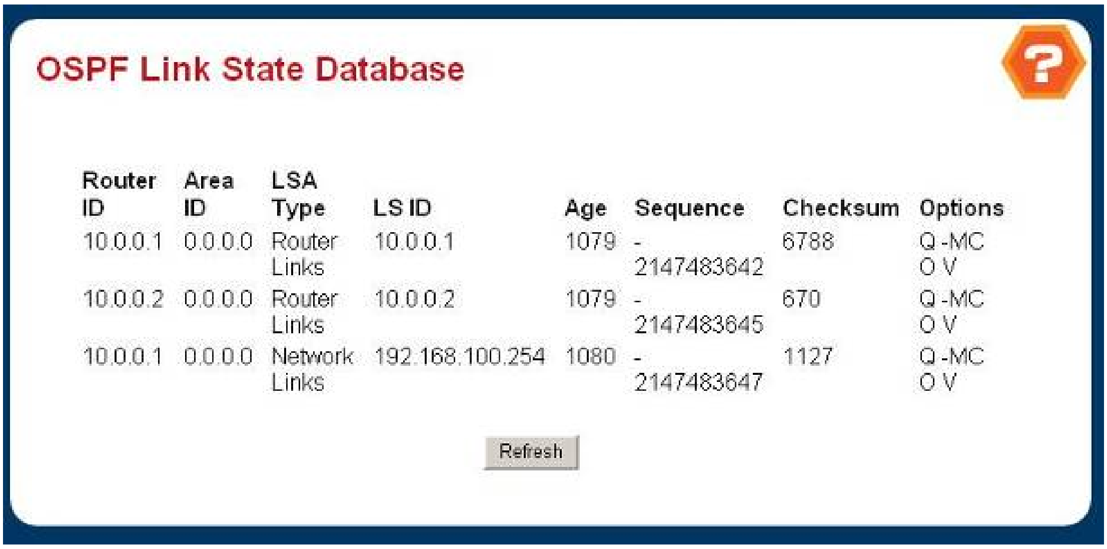
  - ***Down*** - This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor. On NBMA networks, Hello packets may still be sent to "Down" neighbors, although at a reduced frequency.
  - ***Attempt*** - This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. This is done by sending the neighbor Hello packets at intervals of Hello Interval.
  - ***Init*** - In this state, a Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or greater) are listed in the Hello packets sent from the associated interface.
  - ***2-Way*** - In this state, communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater.
  - ***Exchange Start*** - This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.
  - ***Exchange*** - In this state the router is describing its entire link state database by sending Database Description packets to the neighbor. In this state, Link State Request Packets may also be sent asking for the neighbor's more recent LSAs. All adjacencies in Exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.
  - ***Loading*** - In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.
  - ***Full*** - In this state, the neighboring routers are fully adjacent. These adjacencies will now appear in router-LSAs and network-LSAs.

- **Events** - The number of times this neighbor relationship has changed state, or an error has occurred.
- **Permanence** - This variable displays the status of the entry. 'dynamic' and 'permanent' refer to how the neighbor became known.
- **Hellos Suppressed** - This indicates whether Hellos are being suppressed to the neighbor.
- **Retransmission Queue Length** - The current length of the retransmission queue.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.4.9 OSPF Link State Database



OSPF Link State Database

Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options
10.0.0.1	0.0.0.0	Router Links	10.0.0.1	1079	-2147483642	6788	Q -MC O V
10.0.0.2	0.0.0.0	Router Links	10.0.0.2	1079	-2147483645	670	Q -MC O V
10.0.0.1	0.0.0.0	Network Links	192.168.100.254	1080	-2147483647	1127	Q -MC O V

Figure 4-6-26 OSPF Link State Database

Non-Configurable Data

- **Router ID** - The 32 bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the IP Configuration page. If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
- **Area ID** - The ID of an OSPF area to which one of the router interfaces is connected. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.
- **LSA Type** - The format and function of the link state advertisement. One of the following:
  - ***Router Links***
  - ***Network Links***
  - ***Network Summary***
  - ***ASBR Summary***
  - ***AS-external***
  - **LS ID** - The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
  - **Age** - The time since the link state advertisement was first originated, in seconds.
  - **Sequence** - The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
  - **Checksum** - The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

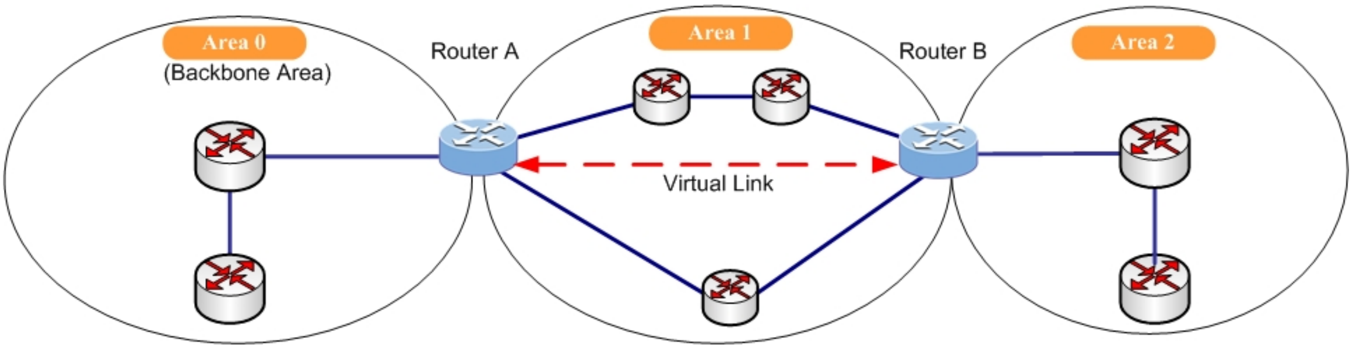
- **Options** - The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are:
  - ***Q*** - This enables support for QoS Traffic Engineering.
  - ***E*** - This describes the way AS-external-LSAs are flooded.
  - ***MC*** - This describes the way IP multicast datagrams are forwarded according to the standard specifications.
  - ***O*** - This describes whether Opaque-LSAs are supported.
  - ***V*** - This describes whether OSPF++ extensions for VPN/COS are supported

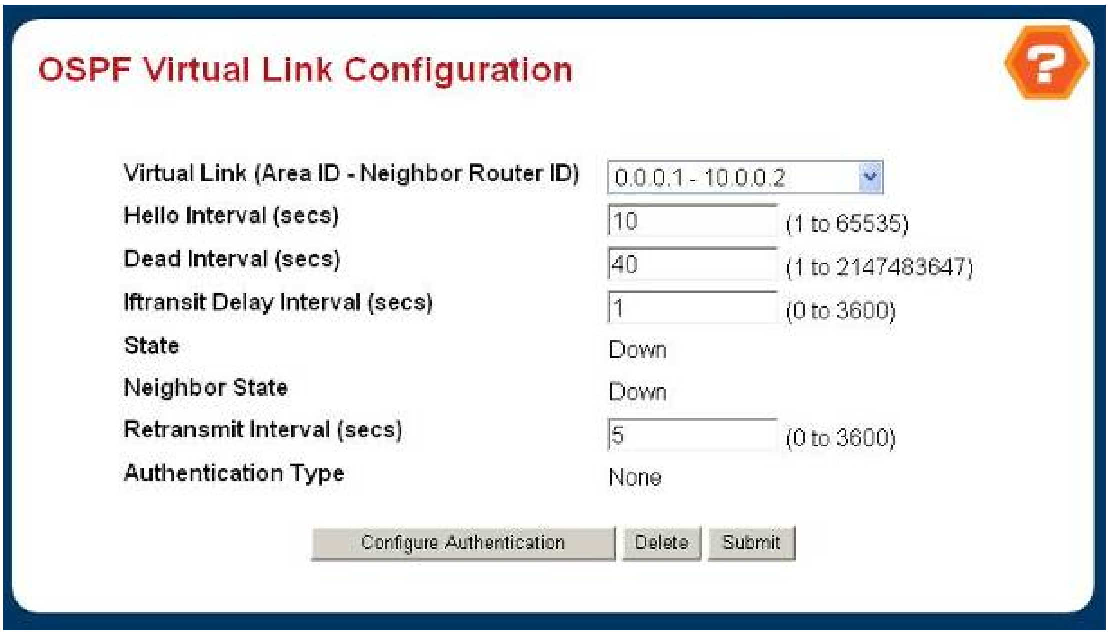
4.6.4.10 OSPF Virtual Link Configuration

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single nonbackbone area to reach the backbone. To define the path, you must specify one endpoint on the ABR that connects the isolated area to the common nonbackbone area, and the other endpoint on the ABR that connects this common nonbackbone area and the backbone itself. (However, note that you cannot configure a virtual link that runs through a stub or NSSA area.)

Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

To configure a virtual link, specify the transit area through which the endpoint routers connect, and the address of the router on this side of the link.





OSPF Virtual Link Configuration

Virtual Link (Area ID - Neighbor Router ID)	0.0.0.1 - 10.0.0.2
Hello Interval (secs)	10 (1 to 65535)
Dead Interval (secs)	40 (1 to 2147483647)
Iftransit Delay Interval (secs)	1 (0 to 3600)
State	Down
Neighbor State	Down
Retransmit Interval (secs)	5 (0 to 3600)
Authentication Type	None

Figure 4-6-27 OSPF Virtual Link Configuration

Selection Criteria

- **Create New Virtual Link** - Select this option from the dropdown menu to define a new virtual link. The area portion of the virtual link identification is fixed: you will be prompted to enter the Neighbor Router ID on a new screen.

- **Area ID and Neighbor Router ID** - Select the virtual link for which you want to display or configure data. It consists of the Area ID and Neighbor Router ID.

Configurable Data

- **Neighbor Router ID** - Enter the neighbor portion of a Virtual Link specification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area. You only enter this ID when you are creating a new virtual link.
- **Hello Interval** - Enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds. .
- **Dead Interval** - Enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should a multiple of the Hello Interval (e.g. 4). Valid values range from 1 to 2147483647. The default is 40.
- **Iftransit Delay Interval** - Enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
- **Retransmit Interval** - Enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
- **Authentication Type** - You may select an authentication type other than none by clicking on the 'Configure Authentication' button. You will then see a new screen, where you can select the authentication type from the pulldown menu. The choices are:

    - ***None*** - This is the initial interface state. If you select this option from the pulldown menu on the second screen you will be returned to the first screen.
    - ***Simple*** - If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
    - ***Encrypt*** - If you select 'Encrypt' you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

- **Authentication Key** - Enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' authentication you cannot use a key of more than 8 octets. If you choose 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.
- **Authentication ID** - Enter the ID to be used for authentication. You will only be prompted to enter an ID when you select 'Encrypt' as the authentication type. The ID is a number between 0 ad 255, inclusive.

Non-Configurable Data

    - ***Down*** - This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.
    - ***Waiting*** - The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.
    - ***Point-to-Point*** - The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.
    - ***Designated Router*** - This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network.
    - ***Backup Designated Router*** - This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.
    - ***Other Designated Router*** - The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

- **Neighbor State** - The state of the Virtual Neighbor Relationship.

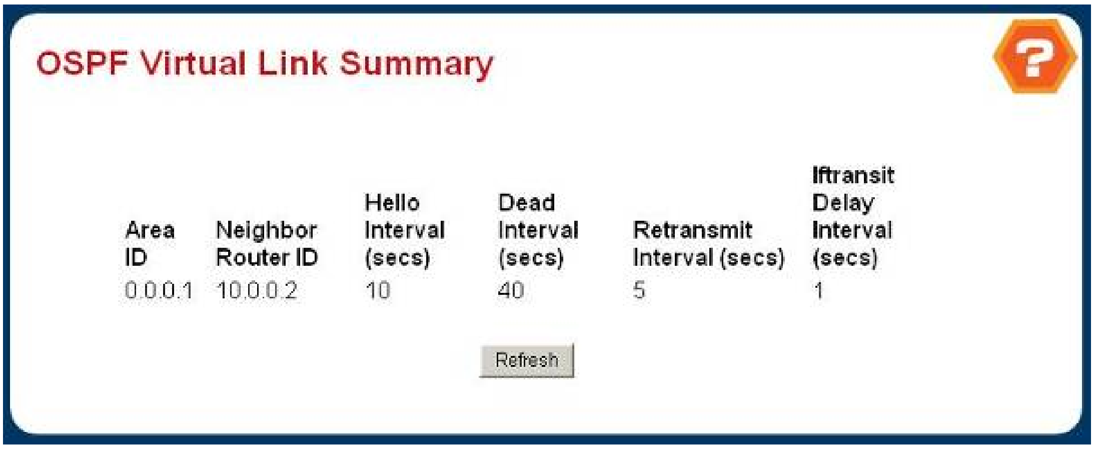
Command Buttons

- **Configure Authentication** - Display a new screen where you can select the authentication method for the virtual link.
- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Delete** - Removes the specified virtual link from the router configuration.

Note: For the first time to create the OSPF Virtual Link, please via Console or telnet – the CLI interface to set up.

```
(config)# router ospf
(config-router)# area 0.0.0.1 virtual-link 10.0.0.2
```

4.6.4.11 OSPF Virtual Link Summary



OSPF Virtual Link Summary

Area ID	Neighbor Router ID	Hello Interval (secs)	Dead Interval (secs)	Retransmit Interval (secs)	Iftransit Delay Interval (secs)
0.0.0.1	10.0.0.2	10	40	5	1

Figure 4-6-28 OSPF Virtual Link Summary

Non-Configurable Data

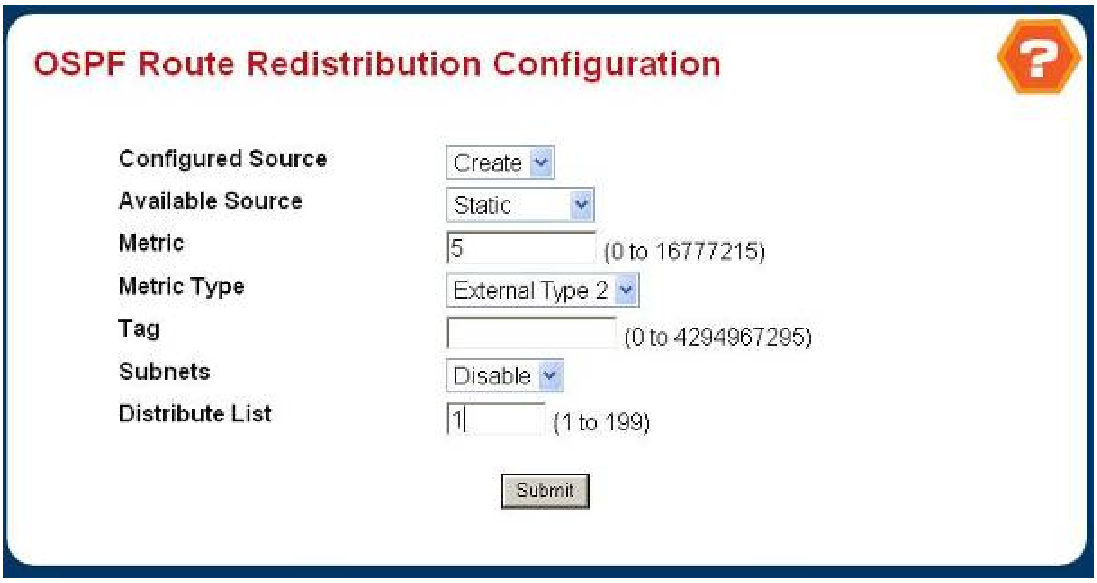
- **Area ID** - The ID of an OSPF area to which one of the router interfaces is connected. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.
- **Neighbor Router ID -** The input neighbor Router ID
- **Hello Interval -** The configured hello interval for the OSPF virtual interface.
- **Dead Interval -** The configured dead interval for the OSPF virtual interface.
- **Retransmit Interval -** The configured retransmit interval for the OSPF virtual interface.
- **Iftransit Delay Interval -** The configured transit delay for the OSPF virtual interface.

Command Buttons

Refresh - Refresh the data on the screen with the present state of the data in the switch.

4.6.4.12 OSPF Route Redistribution Configuration

This screen can be used to configure the OSPF Route Redistribution parameters. The allowable values for each fields are displayed next to the field. If any invalid values are entered, an alert message will be displayed with the list of all the valid values.



OSPF Route Redistribution Configuration

Configured Source	Create
Available Source	Static
Metric	5 (0 to 16777215)
Metric Type	External Type 2
Tag	(0 to 4294967295)
Subnets	Disable
Distribute List	1 (1 to 199)

Figure 4-6-29 OSPF Route Redistribution Configuration

Configurable Data

- **Configured Source** - This select box is a dynamic selector and would be populated by only those Source Routes that have already been configured for redistribute by OSPF. However, the topmost option in the select box would be "Create", and this allows the user to configure another, among the Available Source Routes. The valid values are 'Static', 'Connected', 'RIP' ,'BGP' and 'Create'.
- **Available Source** - This select box is a dynamic selector and would be populated by only those Source Routes that have not previously been configured for redistribution by OSPF. This select box would appear only if the user selects "Create" option as Configured Source. The valid values are 'Static', 'Connected', 'RIP' and 'BGP'.
- **Metric**- Sets the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. The valid values are (0 to 16777215)
- **Metric Type** - Sets the OSPF metric type of redistributed routes.
- **Tag** - Sets the tag field in routes redistributed. This field displays the tag if the source was pre-configured, otherwise 0 and can be modified. The valid values are (0 to 4294967295)
- **Subnets** - Sets whether the subnetted routes should be redistributed or not.
- **Distribute List** - Sets the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to a non-existent access list, all routes are permitted. The valid values for Access List IDs are (1 to 199). When used for route filtering, the only fields in an access list that get used are

  - ***Source IP Address and netmask***
  - ***Destination IP Address and netmask***
  - ***Action (permit or deny)***

All other fields (source and destination port, precedence, tos, etc.) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route. (Note that a 1 in the mask indicates a "don’t care" in the corresponding address bit.)

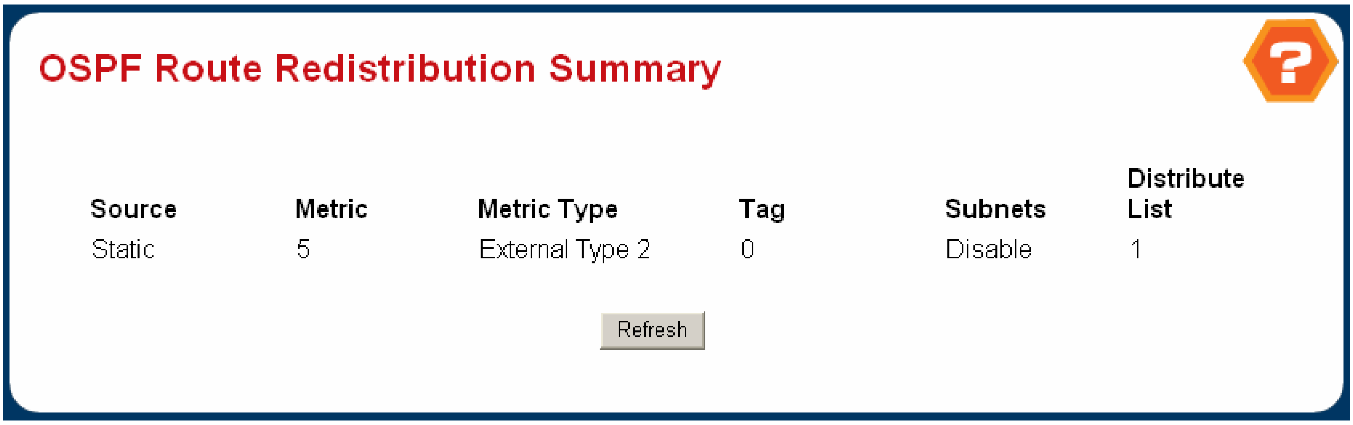
When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route’s destination mask are significant for the filtering operation.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately.
- **Delete** - Delete the entry of the Source Route selected as Configured Source from the list of Sources configured for OSPF Route Redistribution.

4.6.4.13 OSPF Route Redistribution Summary

This screen displays the OSPF Route Redistribution Configurations.



OSPF Route Redistribution Summary

Source	Metric	Metric Type	Tag	Subnets	Distribute List
Static	5	External Type 2	0	Disable	1

Figure 4-6-30 OSPF Route Redistribution Summary

Non Configurable Data

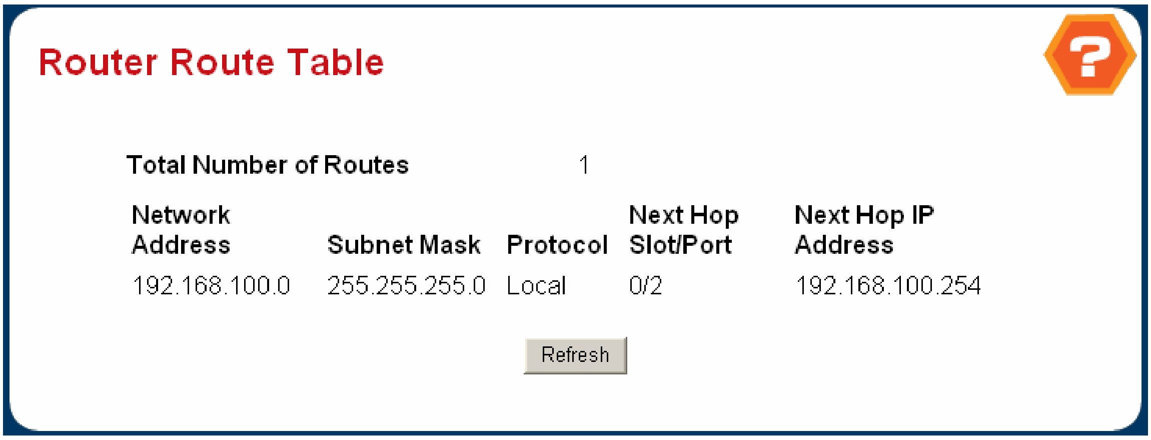
- **Source** - The Source Route to be Redistributed by OSPF.
- **Metric**- The Metric of redistributed routes for the given Source Route. Displays "Unconfigured" when not configured.
- **Metric Type** - The OSPF metric type of redistributed routes.
- **Tag** - The tag field in routes redistributed. This field displays the tag if the source was pre-configured, otherwise 0 and can be modified. The valid values are
- **Subnets** - Whether the subnetted routes should be redistributed or not.
- **Distribute List** - The Access List that filters the routes to be redistributed by the Destination Protocol. Displays 0 when not configured.

Command Buttons

- **Refresh** - Displays the latest OSPF Route Redistribution Configuration data.

4.6.5 Router

4.6.5.1 Router Table



Router Route Table

Total Number of Routes		1		
Network Address	Subnet Mask	Protocol	Next Hop Slot/Port	Next Hop IP Address
192.168.100.0	255.255.255.0	Local	0/2	192.168.100.254

Figure 4-6-31 Router Route Table

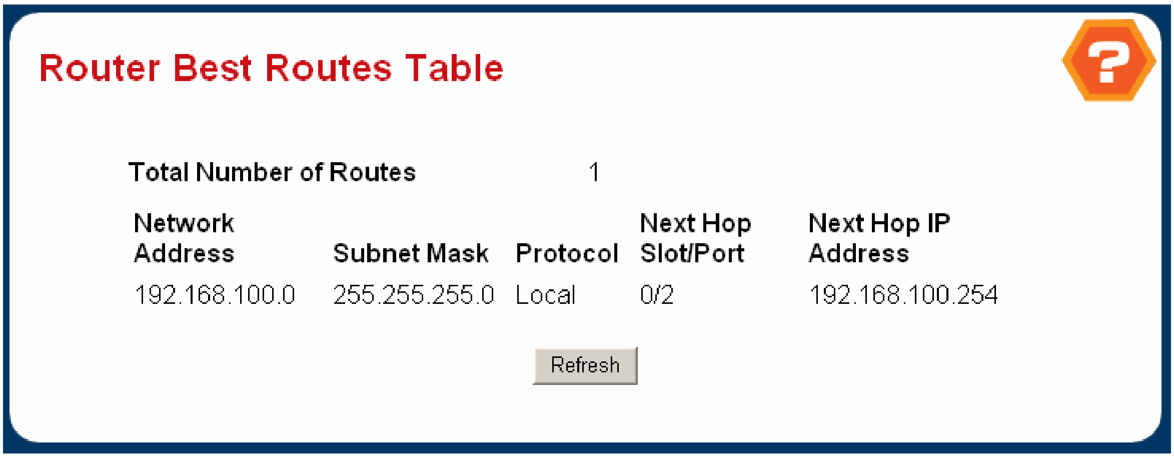
Non-Configurable Data

- **Network Address** - The IP route prefix for the destination.
- **Subnet Mask** - Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Protocol** - This field tells which protocol created the specified route. The possibilities are one of the following:
    - ***Local***
    - ***Static***
    - ***Default***
    - ***OSPF Intra***
    - ***OSPF Inter***
    - ***OSPF Type-1***
    - ***OSPF Type-2***
    - ***RIP***
    - ***BGP4***
- **Next Hop Slot/Port** - The outgoing router interface to use when forwarding traffic to the destination.
- **Next Hop IP Address** - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
- **Total Number of Routes** - The total number of routes in the route table.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.5.2 Router Best Routes Table



Router Best Routes Table

Total Number of Routes 1

Network Address	Subnet Mask	Protocol	Next Hop Slot/Port	Next Hop IP Address
192.168.100.0	255.255.255.0	Local	0/2	192.168.100.254

Figure 4-6-32 Router Best Routes Table

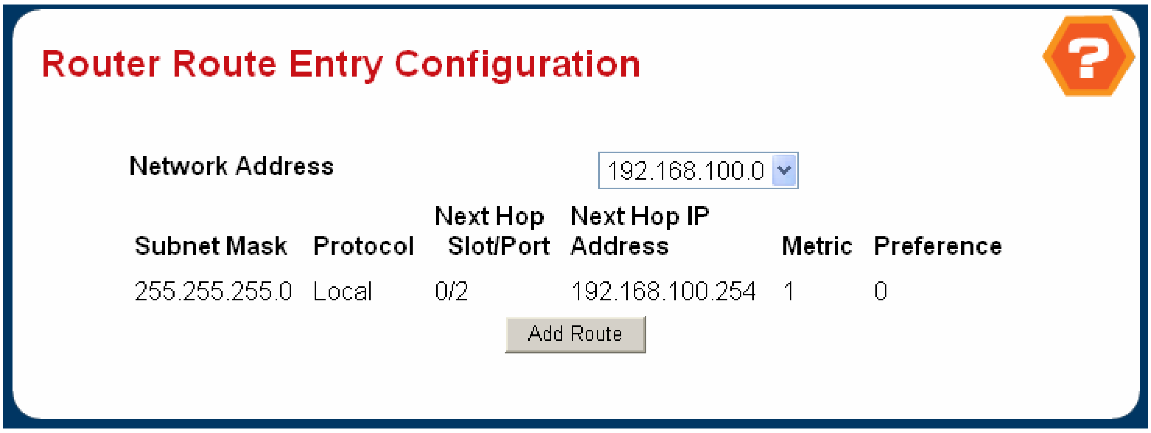
Non-Configurable Data

- **Network Address** - The IP route prefix for the destination.
- **Subnet Mask** - Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Protocol** - This field tells which protocol created the specified route. The possibilities are one of the following:
  - ***Local***
  - ***Static***
  - ***Default***
  - ***OSPF Intra***
  - ***OSPF Inter***
  - ***OSPF Type-1***
  - ***OSPF Type-2***
  - ***RIP***
  - ***BGP4***
- **Next Hop Slot/Port** - The outgoing router interface to use when forwarding traffic to the destination.
- **Next Hop IP Address** - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
- **Total Number of Routes** - The total number of routes in the route table.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.5.3 Route Entry Configuration



Router Route Entry Configuration

Network Address 192.168.100.0

Subnet Mask	Protocol	Next Hop Slot/Port	Next Hop IP Address	Metric	Preference
255.255.255.0	Local	0/2	192.168.100.254	1	0

Figure 4-6-33 Route Route Entry Configuration

Selection Criteria

- **Network Address** - Specifies the IP route prefix for the destination. In order to create a route a valid routing interface must exist and the next hop IP Address must be on the same network as the routing interface. Routing interfaces are created on the IP Interface Configuration page. Valid next hop IP Addresses can be viewed on the 'Route Table' screen.
- **Route Type** - This field can be either default or static. If creating a default route, all that needs to be specified is the next hop IP address, otherwise each field needs to be specified.

Configurable Data

Non-Configurable Data

- **Subnet Mask** - Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
- **Protocol** - This field tells which protocol created the specified route. The possibilities are one of the following:
  - ***Local***
  - ***Static***
  - ***Default***
  - ***OSPF Intra***
  - ***OSPF Inter***
  - ***OSPF Type-1***
  - ***OSPF Type-2***
  - ***RIP***
  - ***BGP4***
- **Next Hop Slot/Port** - The outgoing router interface to use when forwarding traffic to the destination.

- **Next Hop IP Address** - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen on the 'Route Table' page.
- **Metric** - Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255.

Command Buttons

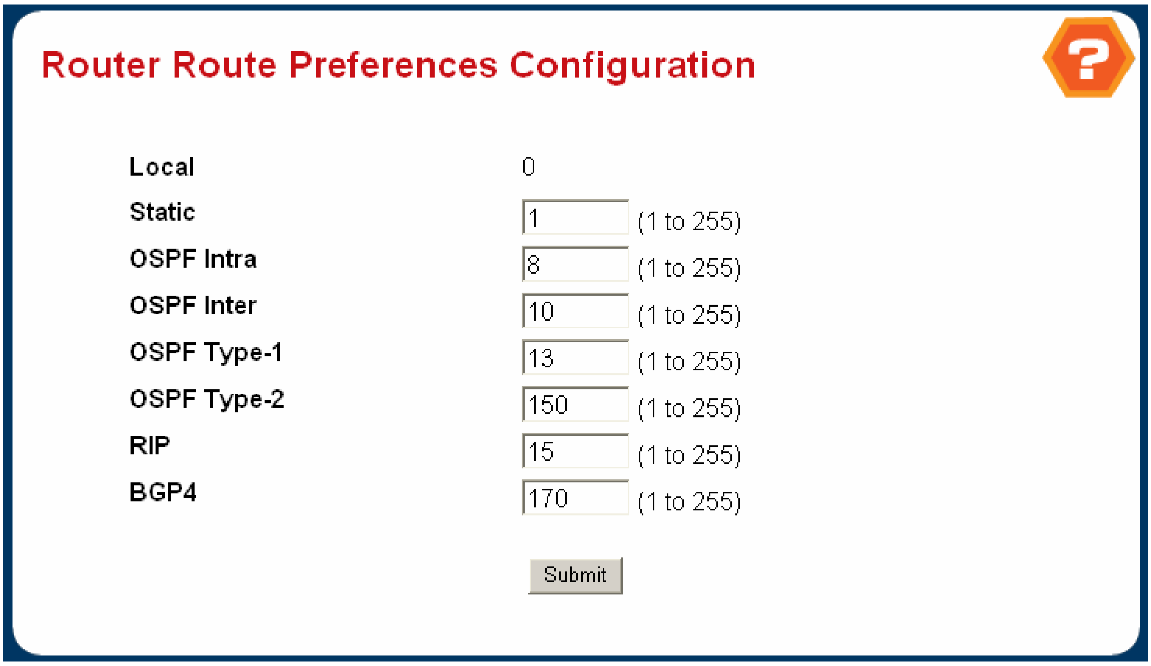
- **Create Route** - Go to a separate page where a route can be created.

4.6.5.4 Route Preferences Configuration

Use this panel to configure the default preference for each protocol (e.g. 60 for static routes, 170 for BGP). These values are arbitrary values in the range of 1 to 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol.

The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric will be chosen. To avoid problems with mismatched metrics (i.e. RIP and OSPF metrics are not directly comparable) you must configure different preference values for each of the protocols.

Configurable Data



Router Route Preferences Configuration

Local	0	
Static	1	(1 to 255)
OSPF Intra	8	(1 to 255)
OSPF Inter	10	(1 to 255)
OSPF Type-1	13	(1 to 255)
OSPF Type-2	150	(1 to 255)
RIP	15	(1 to 255)
BGP4	170	(1 to 255)

Figure 4-6-34 Router Route Preference Configuration

- **Static** - The static route preference value in the router. The default value is 1. The range is 1 to 255.

- **OSPF Intra** - The OSPF intra route preference value in the router. The default value is 8. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.
- **OSPF Inter** - The OSPF inter route preference value in the router. The default value is 10. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.
- **OSPF Type-1** - The OSPF type-1 route preference value in the router. The default value is 13. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.
- **OSPF Type-2** - The OSPF type-2 route preference value in the router. The default value is 150. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.
- **RIP** - The RIP route preference value in the router. The default value is 15. The range is 1 to 255.
- **BGP4** - The BGP4 route preference value in the router. The default value is 170. The range is 1 to 255.

Non-Configurable Data

- **Local** - This field displays the local route preference value.

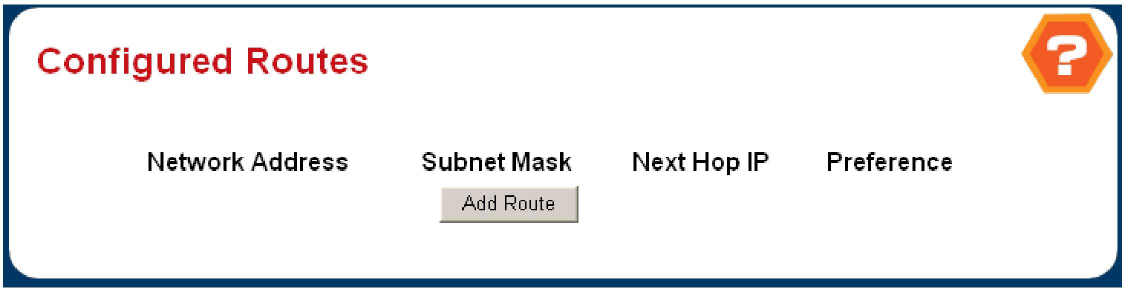
Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.6.5.5 Configured Routes

This switch can be configured to dynamically learn the routes to other IP networks, subnets or hosts using unicast or multicast routing protocols. If the route to a specific destination cannot be learned via these protocols or you wish to restrict the path used for transmitting traffic to a destination, then it can be statically configured using the Static Route Table.

Before defining a static route, remember that you must first configure at least one IP interface on this switch. Static routes take precedence over dynamically learned routes, and remain in the table until you remove them or the corresponding IP interface from this switch.



Configured Routes

Network Address	Subnet Mask	Next Hop IP	Preference

Figure 4-6-35 Configured Routes

- **Network Address** - Specifies the IP route prefix for the destination. This field will be present only when creating a static route.
- **Subnet Mask** - Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network. This field will be present only when creating a static route.
- **Next Hop IP Address** - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen on the 'Route Table' page.
- **Metric** - Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255. This field will be present only when creating a static route.
- **Preference** - Specifies a preference value for the configured next hop.

Command Buttons

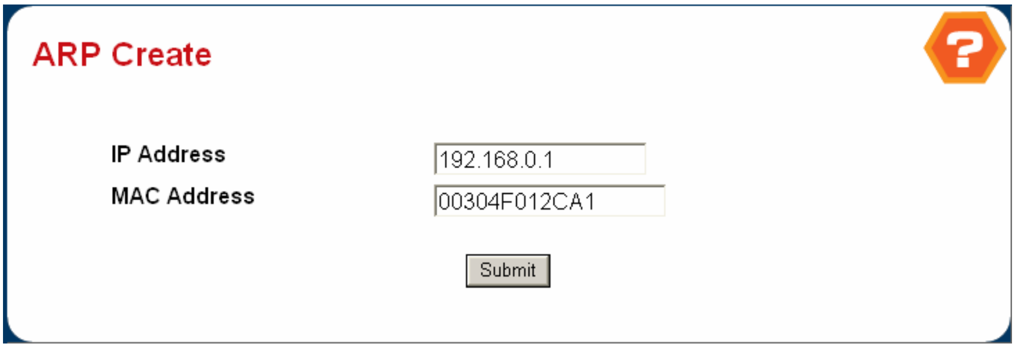
- **Cancel** - Disregard changes made to input fields and return to the Route Entry Configuration page.
- **Submit** - Create the route, sending the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.6.6 ARP

Use the following screen to display or edit entries in the Static ARP Table. Entries added to this table are retained until the associated IP interface is deleted or the switch is reset to the factory defaults.

4.6.6.1 ARP Create

Use this screen to add an entry to the Address Resolution Protocol table.



ARP Create

IP Address 192.168.0.1

MAC Address 00304F012CA1

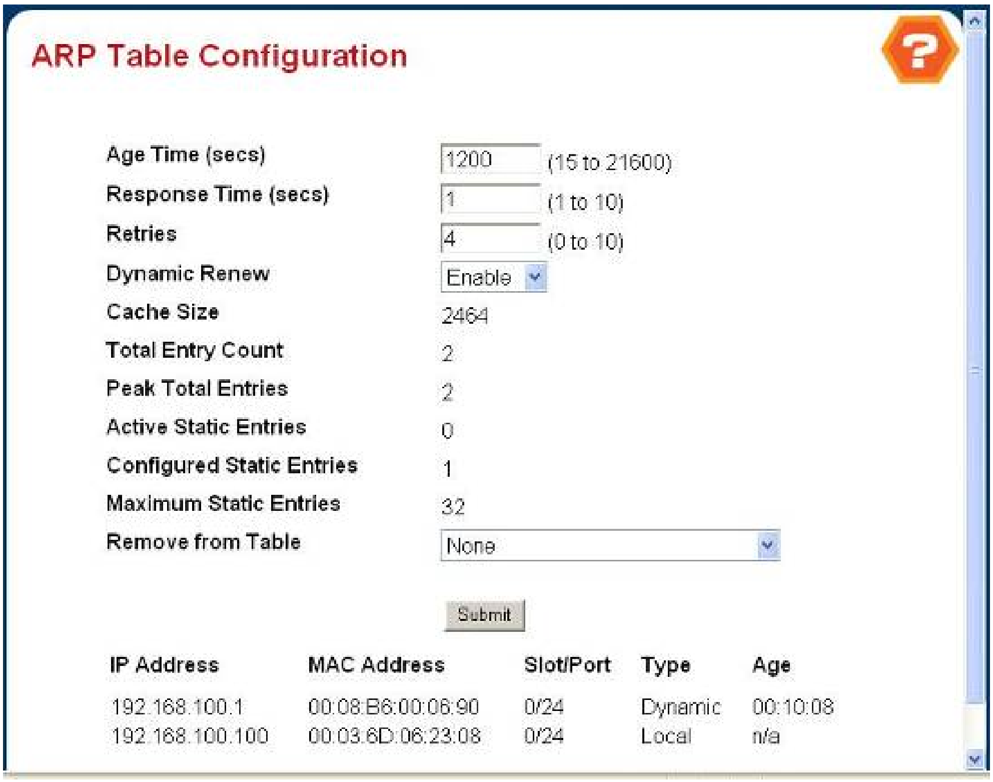
Figure 4-6-36 ARP Create

Configurable Data

- **IP Address** - Enter the IP address you want to add. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
- **MAC Address** - The unicast MAC address of the device. Enter the address as six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

4.6.6.2 ARP Table Configuration

You can use this screen to change the configuration parameters for the Address Resolution Protocol Table. You can also use this screen to display the contents of the table.



ARP Table Configuration

Age Time (secs)	1200	(15 to 21600)
Response Time (secs)	1	(1 to 10)
Retries	4	(0 to 10)
Dynamic Renew	Enable	
Cache Size	2464	
Total Entry Count	2	
Peak Total Entries	2	
Active Static Entries	0	
Configured Static Entries	1	
Maximum Static Entries	32	
Remove from Table	None	

IP Address	MAC Address	Slot/Port	Type	Age
192.168.100.1	00:08:B6:00:06:90	0/24	Dynamic	00:10:08
192.168.100.100	00:03:6D:06:23:08	0/24	Local	n/a

Figure 4-6-37 ARP Table Configuation

Configurable Data

- **Age Time** - Enter the value you want the switch to use for the ARP entry ageout time. You must enter a valid integer, which represents the number of seconds it will take for an ARP entry to age out. The range for this field is 15 to 21600 seconds. The default value for Age Time is 1200 seconds.
- **Response Time** - Enter the value you want the switch to use for the ARP response timeout. You must enter a valid integer, which represents the number of seconds the switch will wait for a response to an ARP request. The range for this field is 1 to 10 seconds. The default value for Response Time is 1 second.
- **Retries** - Enter an integer which specifies the maximum number of times an ARP request will be retried. The range for this field is 0 to 10. The default value for Retries is 4.
- **Dynamic Renew** - This controls whether the ARP component automatically attempts to renew ARP Entries of type Dynamic when they age out. The default setting is Enable.
- **Remove from Table** - Allows the user to remove certain entries from the ARP Table. The choices listed specify the type of ARP Entry to be deleted:

  - ***All Dynamic Entries***
  - ***All Dynamic and Gateway Entries***
  - ***Specific Dynamic/Gateway Entry*** - Selecting this allows the user to specify the required IP Address
  - ***Specific Static Entry*** - Selecting this allows the user to specify the required IP Address
  - ***None*** - Selected if the user does not want to delete any entry from the ARP Table

- **Remove IP Address** - This appears only if the user selects Specific Dynamic/Gateway Entry or Specific Static Entry in the Remove from Table Drop Down List. Allows the user to enter the IP Address against the entry that is to be removed from the ARP Table.

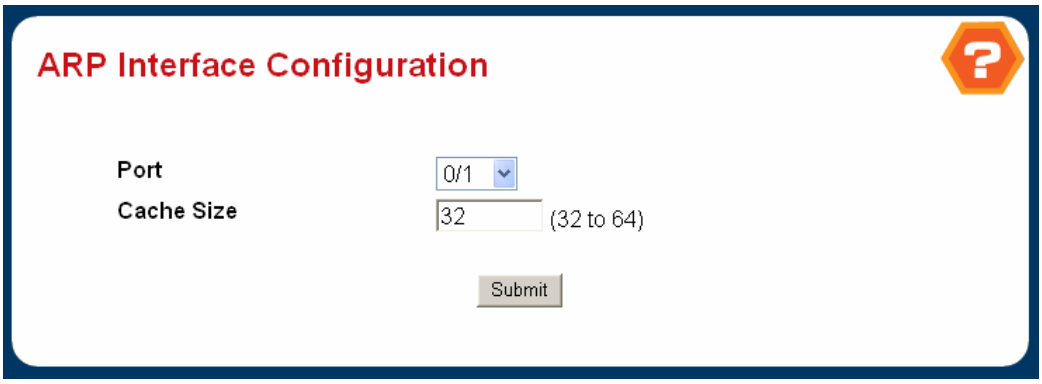
Non-Configurable Data

- **Cache Size** - Maximum number of ARP cache entries allowed. This is the cumulative number we get after adding the Maximum ARP entries for each interface
- **Total Entry Count** - Total number of Entries in the ARP table.
- **Peak Total Entries** - Highest value reached by Total Entry Count. This counter value is restarted whenever the ARP table Cache Size value is changed.
- **Active Static Entries** - Total number of Active Static Entries in the ARP table.
- **Configured Static Entries** - Total number of Configured Static Entries in the ARP table.
- **Maximum Static Entries** - Maximum number of Static Entries that can be defined.
- **IP Address** - The IP address of a device on a subnet attached to one of the switch's routing interfaces.
- **MAC Address** - The unicast MAC address for the device. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
- **Slot/Port** - The routing interface associated with the ARP entry.
- **Type** - The type of the ARP entry:

    - **Local** - An ARP entry associated with one of the switch's routing interface's MAC addresses
    - **Gateway** - A dynamic ARP entry whose IP address is that of a router
    - **Static** - An ARP entry configured by the user
    - **Dynamic** - An ARP entry which has been learned by the router

- **Age** - Age since the entry was last refreshed in the ARP Table. The format is hh:mm:ss.

4.6.6.3 ARP Interface Configuration



ARP Interface Configuration

Port: 0/1

Cache Size: 32 (32 to 64)

Figure 4-6-38 ARP Interface Configuration

Selection Criteria

- **Port** - Select the interface for which data is to be configured.

Configurable Data

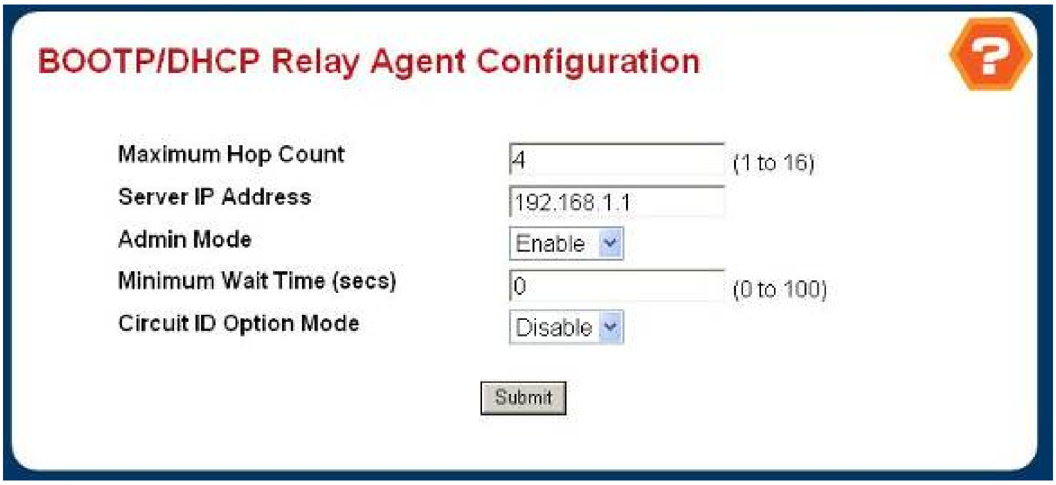
- **Cache Size** - Specifies the Cache size for the selected interface. Valid range is from 8 to 16.

4.6.7 BOOTP/DHCP Relay Agent

If a DHCP server is not located in the same subnet with a host, you can configure this switch to forward any host configuration queries to a server located on another subnet or on another network. Depending on the configuration setup, the switch either:

- Forwards the packet to a preferred server as defined in the switch configuration using unicast routing, or
- Broadcasts the DHCP Request again to another directly attached IP subnet specified in the switch configuration.

Specify the address for any DHCP server, or specify the subnet address for an outbound IP interface already configured on this switch as described in the following screens.



BOOTP/DHCP Relay Agent Configuration

Maximum Hop Count	4	(1 to 16)
Server IP Address	192.168.1.1	
Admin Mode	Enable	
Minimum Wait Time (secs)	0	(0 to 100)
Circuit ID Option Mode	Disable	

Figure 4-6-39 BOOTP/DHCP Relay Agent Configuration

4.6.7.1 BOOTP/DHCP Relay Agent Configuration

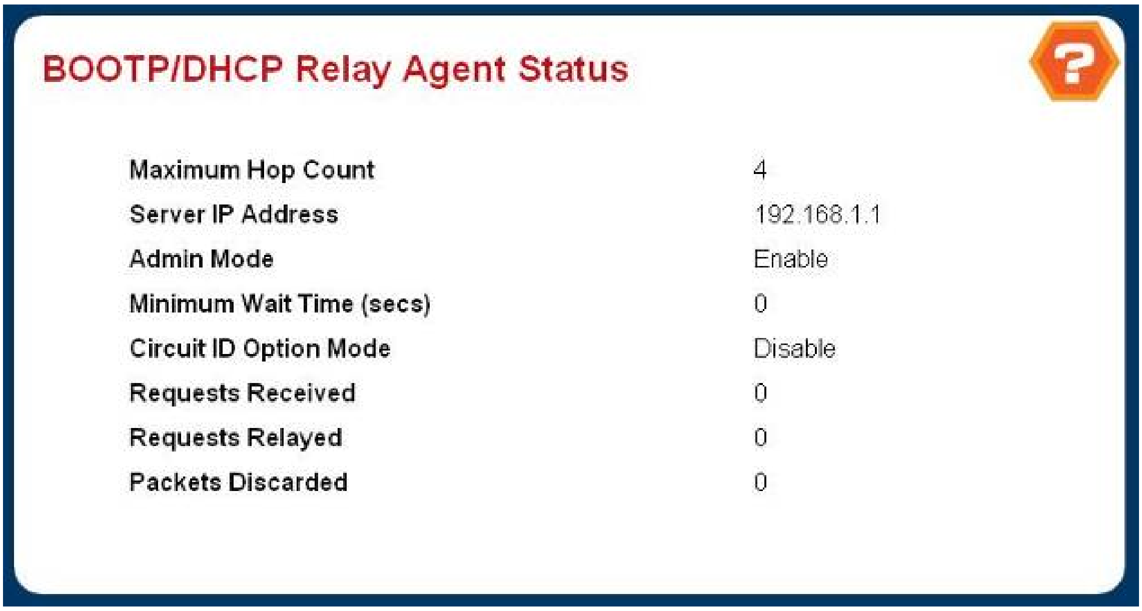
Configurable Data

- **Maximum Hop Count** - Enter the maximum number of hops a client request can take before being discarded.
- **Server IP Address** - Enter either the IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.
- **Admin Mode** - Select enable or disable from the pulldown menu. When you select 'enable' BOOTP/DHCP requests will be forwarded to the IP address you entered in the 'Server IP address' field.
- **Minimum Wait Time** - Enter a time in seconds. This value will be compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets will only be forwarded when the time stamp exceeds the minimum wait time.
- **Circuit Id Option Mode** - Select enable or disable from the pulldown menu. If you select 'enable' Relay Agent options will be added to requests before they are forwarded to the server and removed from replies before they are forwarded to clients.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.6.7.2 BOOTP/DHCP Relay Agent Status



BOOTP/DHCP Relay Agent Status

Maximum Hop Count	4
Server IP Address	192.168.1.1
Admin Mode	Enable
Minimum Wait Time (secs)	0
Circuit ID Option Mode	Disable
Requests Received	0
Requests Relayed	0
Packets Discarded	0

Figure 4-6-40 BOOTP/DHCP Relay Agent Status

Non-Configurable Data

- **Maximum Hop Count** - The maximum number of Hops a client request can go without being discarded.
- **Server IP Address** - IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.
- **Admin Mode** - Administrative mode of the relay. When you select 'enable' BOOTP/DHCP requests will be forwarded to the IP address you entered in the 'Server IP address' field.
- **Minimum Wait Time** - The Minimum time in seconds. This value will be compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets will only be forwarded when the time stamp exceeds the minimum wait time.
- **Circuit Id Option Mode** - This is the Relay agent option which can be either enabled or disabled. When enabled Relay Agent options will be added to requests before they are forwarded to the server and removed from replies before they are forwarded to clients.
- **Requests Received** - The total number of BOOTP/DHCP requests received from all clients since the last time the switch was reset.
- **Requests Relayed** - The total number of BOOTP/DHCP requests forwarded to the server since the last time the switch was reset.
- **Packets Discarded** - The total number of BOOTP/DHCP packets discarded by this Relay Agent since the last time the switch was reset.

4.6.8 Router Discovery

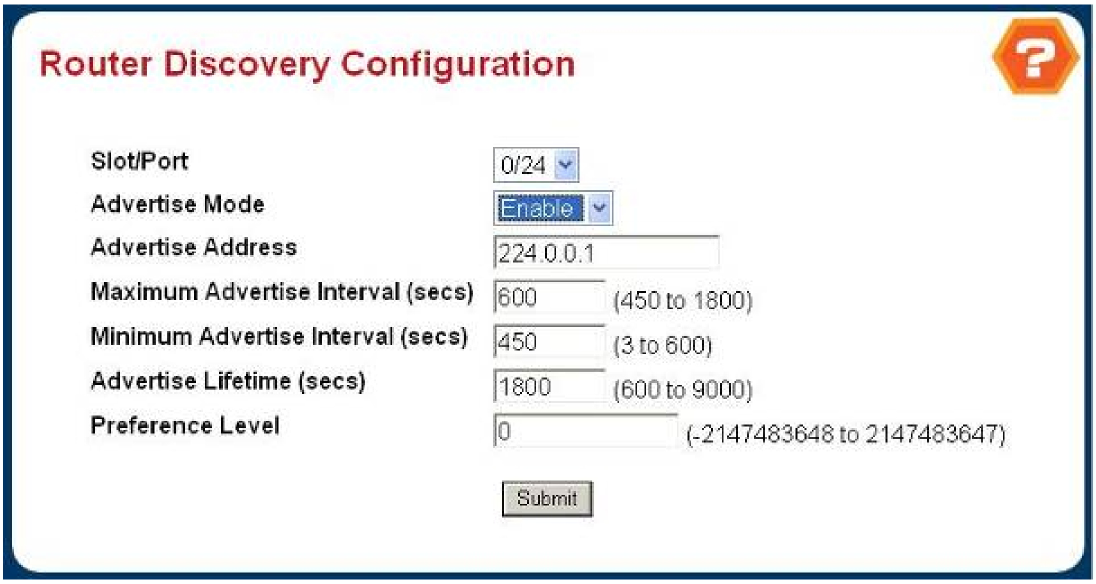
The Router Discovery is not a routing protocol but a Router Discovery Protocol. The function Router Discovery allows neighboring routers to be found from ICMP Router Advertisement messages. It also be named as IRDP (ICMP Router Discovery Protocol). – implemented as defined in RFC-1256.

The ICMP router discovery messages are called "Router Advertisements" and "Router Solicitations". Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface.

Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if (and only if) no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations.

Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements. (Links that suffer high packet loss rates or frequent partitioning are accommodated by increasing the rate of advertisements, rather than increasing the number of solicitations that hosts are permitted to send.)

4.6.8.1 Router Discovery Configuration



Router Discovery Configuration

Slot/Port	0/24	
Advertise Mode	Enable	
Advertise Address	224.0.0.1	
Maximum Advertise Interval (secs)	600	(450 to 1800)
Minimum Advertise Interval (secs)	450	(3 to 600)
Advertise Lifetime (secs)	1800	(600 to 9000)
Preference Level	0	(-2147483648 to 2147483647)

Figure 4-6-41 Router Discovery Configuration

Selection Criteria

- **Slot/Port** - Select the router interface for which data is to be configured.

Configurable Data

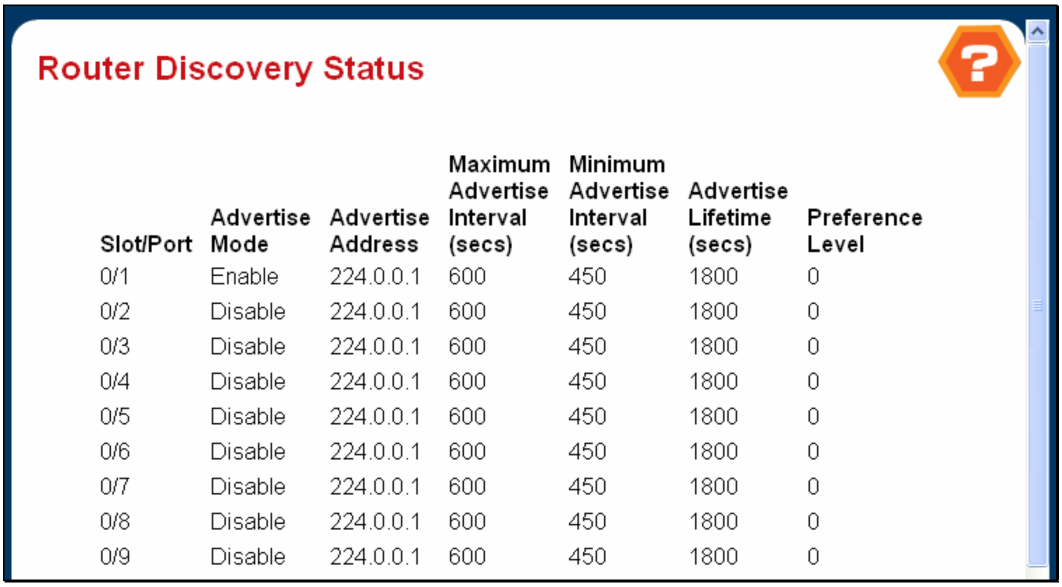
- **Advertise Mode** - Select enable or disable from the pulldown menu. If you select enable, Router Advertisements will be transmitted from the selected interface.

- **Advertise Address** - Enter the IP Address to be used to advertise the router.
- **Maximum Advertise Interval** - Enter the maximum time (in seconds) allowed between router advertisements sent from the interface.
- **Minimum Advertise Interval** - Enter the minimum time (in seconds) allowed between router advertisements sent from the interface.
- **Advertise Lifetime** - Enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.
- **Preference Level** - Specify the preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred. You must enter an integer.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. The changes will not be retained across a power cycle unless a save is performed.

4.6.8.2 Router Discovery Status



Router Discovery Status

Slot/Port	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
0/1	Enable	224.0.0.1	600	450	1800	0
0/2	Disable	224.0.0.1	600	450	1800	0
0/3	Disable	224.0.0.1	600	450	1800	0
0/4	Disable	224.0.0.1	600	450	1800	0
0/5	Disable	224.0.0.1	600	450	1800	0
0/6	Disable	224.0.0.1	600	450	1800	0
0/7	Disable	224.0.0.1	600	450	1800	0
0/8	Disable	224.0.0.1	600	450	1800	0
0/9	Disable	224.0.0.1	600	450	1800	0

Figure 4-6-42 Router Discovery Status

Non-Configurable Data

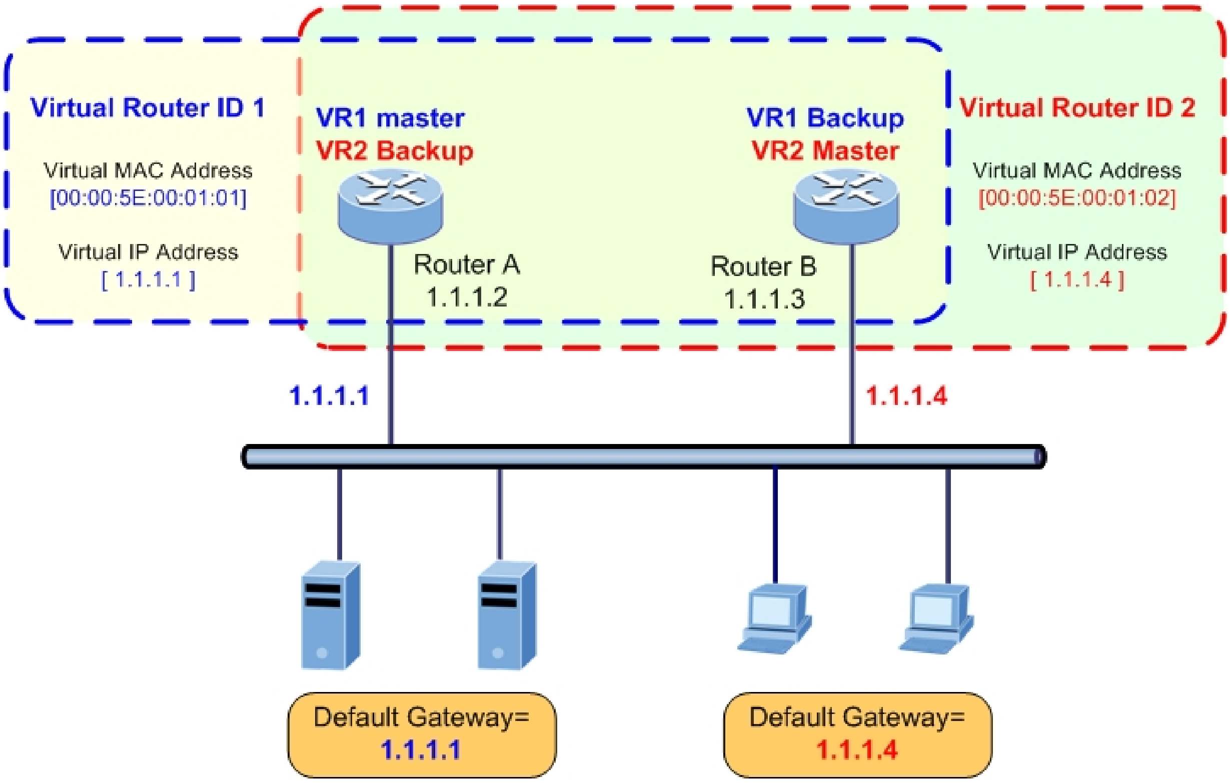
- **Slot/Port** - The router interface for which data is displayed.
- **Advertise Mode** - The values are enable or disable. Enable denotes that Router Discovery is enabled on that interface.
- **Advertise Address** - The IP Address used to advertise the router.
- **Maximum Advertise Interval** - The maximum time (in seconds) allowed between router advertisements sent from the interface.
- **Minimum Advertise Interval** - The minimum time (in seconds) allowed between router advertisements sent from the interface.
- **Advertise Lifetime** - The value (in seconds) used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.
- **Preference Level** - The preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred.

4.6.9 VRRP

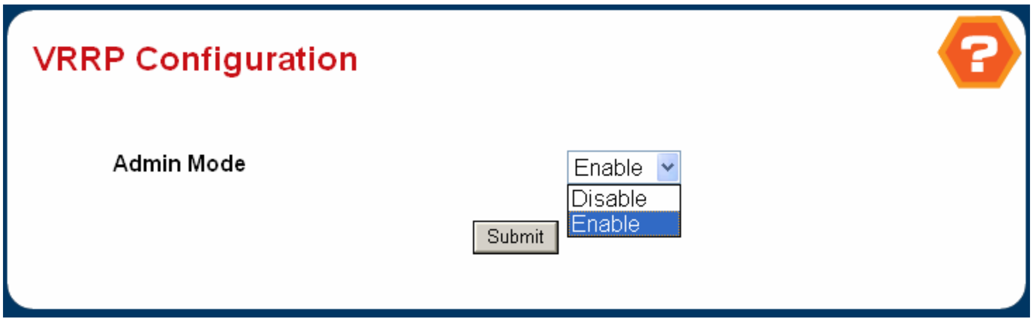
The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

The feature of VRRP protocol:

- IP Address Backup
  - Virtual IP for Default Gateway
  - Multiple Virtual Routers for Load Balancing
- Elect Best Path
  - According to Priority and IP Address
- Efficient Operation
  - No More Packet Besides ADVERTISEMENT
  - No State Transition is Triggered by Any Backup Router of Equal or Lower Priority



4.6.9.1 VRRP Configuration



VRRP Configuration

Admin Mode	Enable

Figure 4-6-43 VRRP Configuration

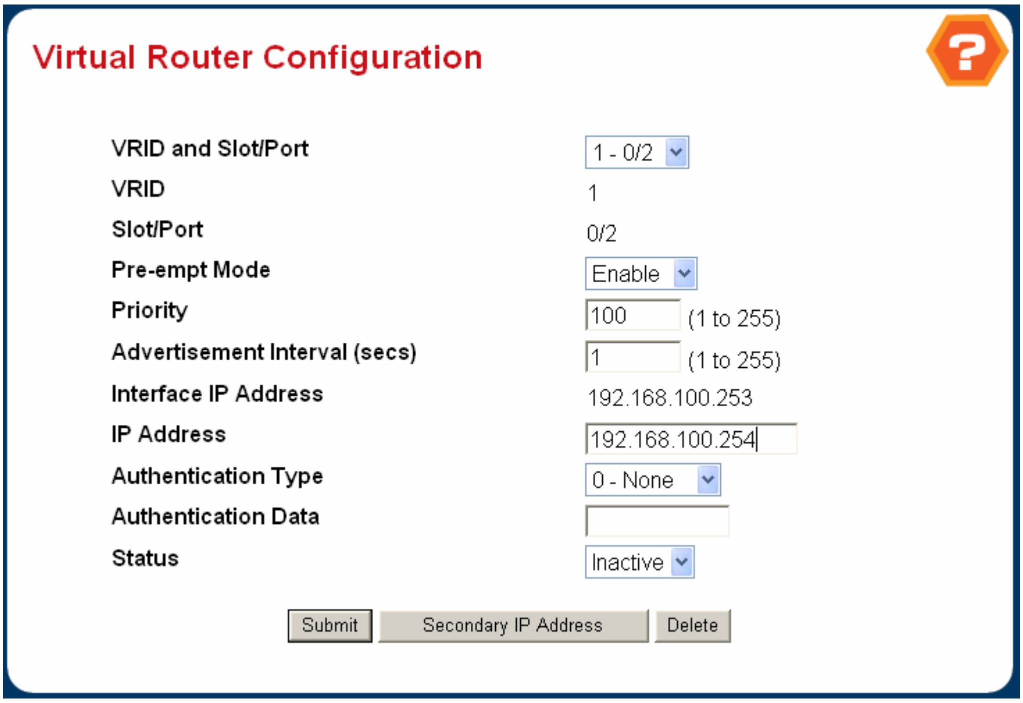
Configurable Data

- **VRRP Admin Mode** - This sets the administrative status of VRRP in the router to active or inactive. Select enable or disable from the pulldown menu. The default is disable.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.6.9.2 Virtual Router Configuration



Virtual Router Configuration

VRID and Slot/Port	1 - 0/2
VRID	1
Slot/Port	0/2
Pre-empt Mode	Enable
Priority	100 (1 to 255)
Advertisement Interval (secs)	1 (1 to 255)
Interface IP Address	192.168.100.253
IP Address	192.168.100.254
Authentication Type	0 - None
Authentication Data	
Status	Inactive

Figure 4-6-44 Virtual Router Configuration

Selection Criteria

- **VRID and Slot/Port** - Select 'Create' from the pulldown menu to configure a new Virtual Router, or select one of the existing Virtual Routers, listed by interface number and VRID.

Configurable Data

- **VRID** - This field is only configurable if you are creating new Virtual Router, in which case enter the VRID in the range 1 to 255 .
- **Slot/Port** - This field is only configurable if you are creating new Virtual Router, in which case select the Slot/Port for the new Virtual Router from the pulldown menu.
- **Pre-empt Mode** - Select enable or disable from the pulldown menu. If you select enable a backup router will preempt the master router if it has a priority greater than the master virtual router's priority provided the master is not the owner of the virtual router IP address. The default is enable.
- **Priority** - Enter the priority value to be used by the VRRP router in the election for the master virtual router. If the Virtual IP Address is the same as the interface IP Address, the priority gets set to 255 no matter what the user enters. If the user enters a priority of 255 when the Virtual and interface IP Addresses are not the same, the priority gets set to the default value of 100.
- **Advertisement Interval** - Enter the time, in seconds, between the transmission of advertisement packets by this virtual router. Enter a number between 1 and 255. The default value is 1 second.
- **IP Address** - Enter the IP Address associated with the Virtual Router. The default is 0.0.0.0.
- **Authentication Type** - Select the type of Authentication for the Virtual Router from the pulldown menu. The default is None. The choices are:

  - ***0-None*** - No authentication will be performed.
  - ***1-Simple*** - Authentication will be performed using a text password.

- **Authentication Data** - If you selected simple authentication, enter the password.
- **Status** - Select active or inactive from the pulldown menu to start or stop the operation of the Virtual Router. The default is inactive.

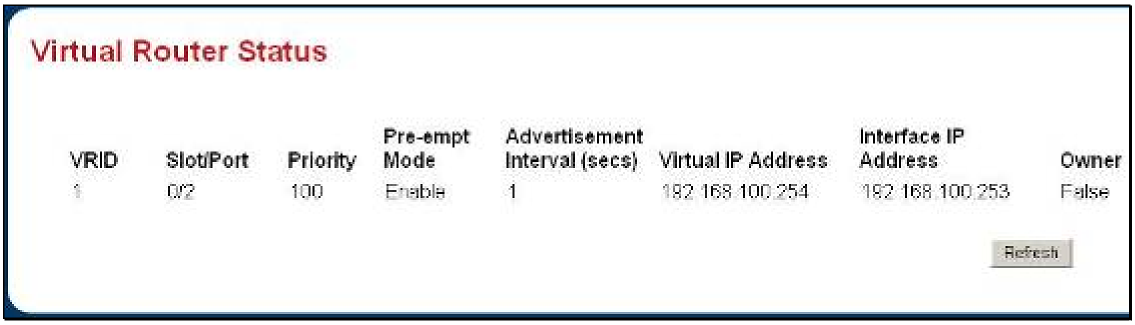
Non-Configurable Data

- **Interface IP Address** - Indicates the IP Address associated with the selected interface.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Delete** - Delete the selected Virtual Router. Note that the router can not be deleted if there are secondary addresses configured.
- **Secondary IP Address** - Proceed to the Secondary IP Address configuration screen.

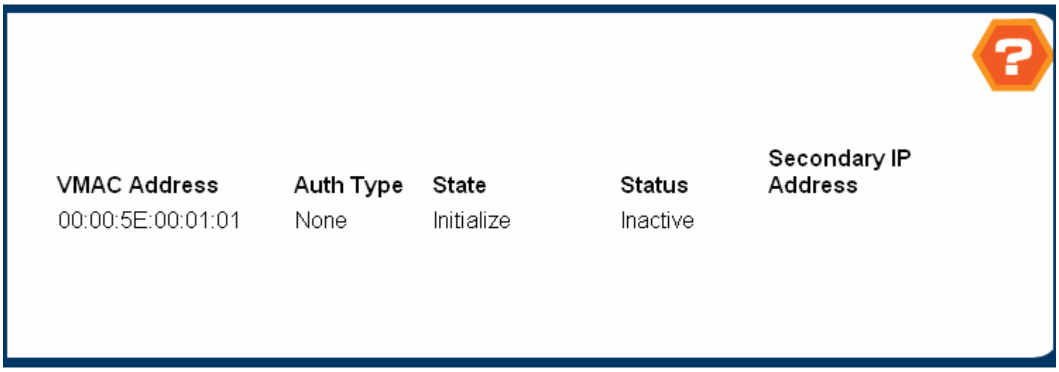
4.6.9.3 Virtual Router Status



Virtual Router Status

VRID	Slot/Port	Priority	Pre-empt Mode	Advertisement Interval (secs)	Virtual IP Address	Interface IP Address	Owner
1	0/2	100	Enable	1	192.168.100.254	192.168.100.253	False

Figure 4-6-45 Virtual Router Status



VMAC Address	Auth Type	State	Status	Secondary IP Address
00:00:5E:00:01:01	None	Initialize	Inactive	

Figure 4-6-46 Virtual Route Status

Non-Configurable Data

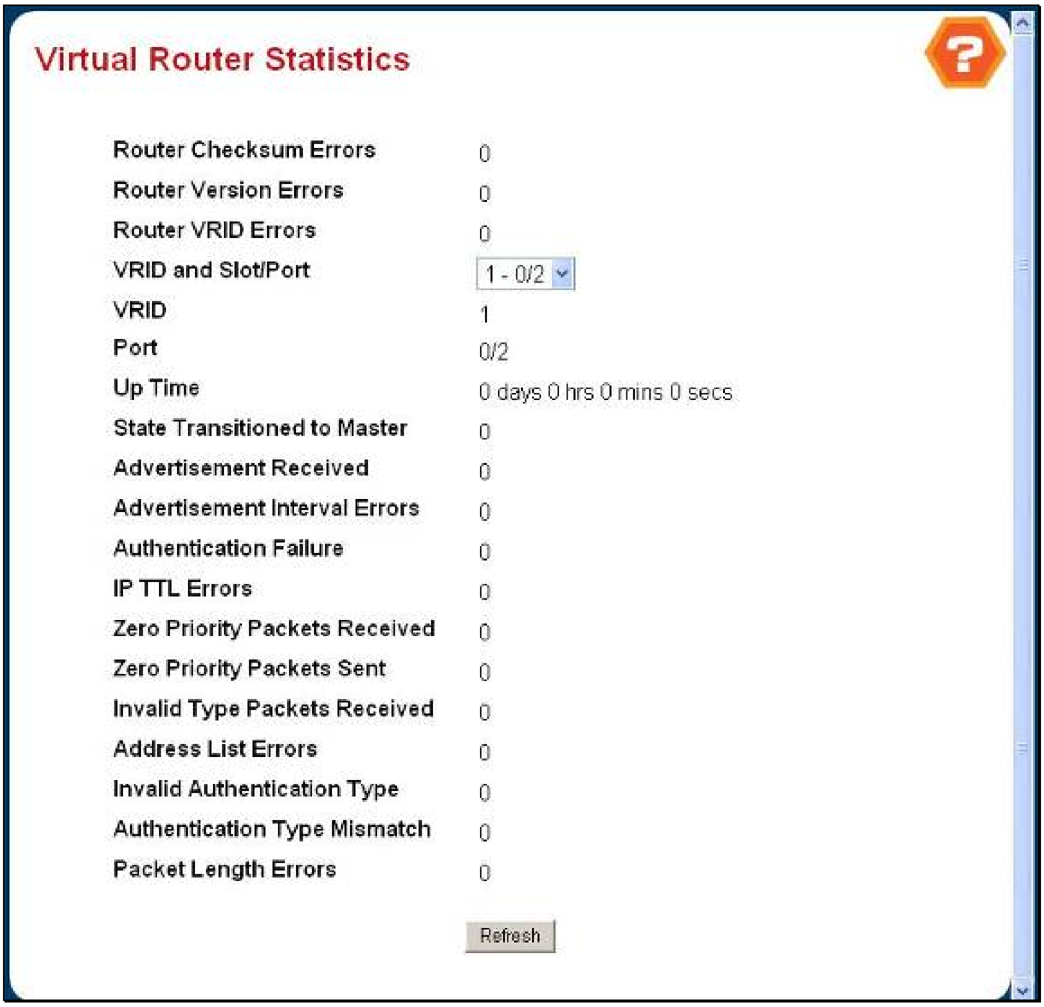
- **VRID** - Virtual Router Identifier.
- **Slot/Port** - Indicates the interface associate with the VRID.
- **Priority** - The priority value used by the VRRP router in the election for the master virtual router.
- **Pre-empt Mode** -
    - ***Enable*** - if the Virtual Router is a backup router it will preempt the master router if it has a priority greater than the master virtual router's priority provided the master is not the owner of the virtual router IP address.
    - ***Disable*** - if the Virtual Router is a backup router it will not preempt the master router even if its priority is greater.
- **Advertisement Interval** - the time, in seconds, between the transmission of advertisement packets by this virtual router.
- **Virtual IP Address** - The IP Address associated with the Virtual Router.
- **Interface IP Address** - The actual IP Address associated with the interface used by the Virtual Router.
- **Owner** - Set to 'True' if the Virtual IP Address and the Interface IP Address are the same, otherwise set to 'False'. If this parameter is set to 'True', the Virtual Router is the owner of the Virtual IP Address, and will always win an election for master router when it is active.

- **VMAC Address** - The virtual MAC Address associated with the Virtual Router, composed of a 24 bit organizationally unique identifier, the 16 bit constant identifying the VRRP address block and the 8 bit VRID.
- **Auth Type** - The type of authentication in use for the Virtual Router
  - ***None***
  - ***Simple***
- **State** - The current state of the Virtual Router:
  - ***Initialize***
  - ***Master***
  - ***Backup***
- **Status** - The current status of the Virtual Router:
  - ***Inactive***
  - ***Active***

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.9.4 Virtual Router Statistics



Virtual Router Statistics

Router Checksum Errors	0
Router Version Errors	0
Router VRID Errors	0
VRID and Slot/Port	1 - 0/2
VRID	1
Port	0/2
Up Time	0 days 0 hrs 0 mins 0 secs
State Transitioned to Master	0
Advertisement Received	0
Advertisement Interval Errors	0
Authentication Failure	0
IP TTL Errors	0
Zero Priority Packets Received	0
Zero Priority Packets Sent	0
Invalid Type Packets Received	0
Address List Errors	0
Invalid Authentication Type	0
Authentication Type Mismatch	0
Packet Length Errors	0

Figure 4-6-47 Virtual Router Statistics

Selection Criteria

- **VRID and Slot/Port** - Select the existing Virtual Router, listed by interface number and VRID, for which you want to display statistical information.

Non-Configurable Data

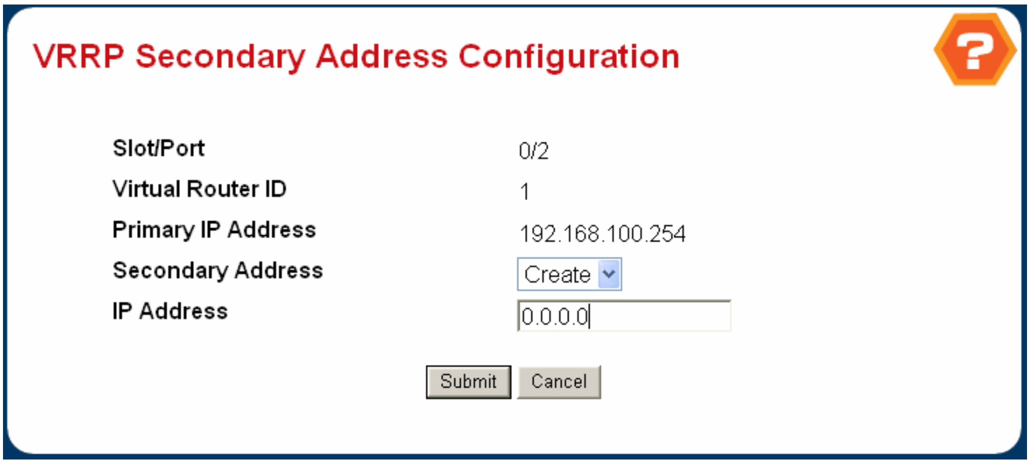
- **Router Checksum Errors** - The total number of VRRP packets received with an invalid VRRP checksum value.
- **Router Version Errors** - The total number of VRRP packets received with an unknown or unsupported version number.
- **Router VRID Errors** - The total number of VRRP packets received with an invalid VRID for this virtual router.
- **VRID** - the VRID for the selected Virtual Router.
- **Slot/Port** - The Slot/Port for the selected Virtual Router.
- **Up Time** - The time, in days, hours, minutes and seconds, that has elapsed since the virtual router transitioned to the initialized state.
- **State Transitioned to Master** - The total number of times that this virtual router's state has transitioned to Master.

- **Advertisement Received** - The total number of VRRP advertisements received by this virtual router.
- **Advertisement Interval Errors** - The total number of VRRP advertisement packets received for which the advertisement interval was different than the one configured for the local virtual router .
- **Authentication Failure** - The total number of VRRP packets received that did not pass the authentication check.
- **IP TTL Errors** - The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
- **Zero Priority Packets Received** - The total number of VRRP packets received by the virtual router with a priority of '0'.
- **Zero Priority Packets Sent** - The total number of VRRP packets sent by the virtual router with a priority of '0'.
- **Invalid Type Packets Received** - The number of VRRP packets received by the virtual router with an invalid value in the 'type' field.
- **Address List Errors** - The total number of packets received for which the address list does not match the locally configured list for the virtual router.
- **Invalid Authentication Type** - The total number of packets received with an unknown authentication type.
- **Authentication Type Mismatch** - The total number of packets received with an authentication type different to the locally configured authentication method.
- **Packet Length Errors** - The total number of packets received with a packet length less than the length of the VRRP header.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

4.6.9.5 VRRP Secondary Address Configuration



VRRP Secondary Address Configuration

Slot/Port	0/2
Virtual Router ID	1
Primary IP Address	192.168.100.254
Secondary Address	Create
IP Address	0.0.0.0

Figure 4-6-48 VRRP Secondary Address Configuration

Selection Criteria

- **Secondary Address** - The ip address for which data is to be displayed. Create must be selected to add a secondary address to the interface.

Configurable Data

- **IP Address** - Enter the IP address for the interface. This address must be a member of one of the subnets currently configured on the interface. This value is readonly once configured.

Non-Configurable Data

- **Slot/Port** - The interface for which data is to be displayed or configured.
- **Virtual Router ID** - The Virtual Router ID for which data is to be displayed or configured.
- **Primary IP Address** - The Primary IP Address of the Virtual Router.

Command Buttons

- **Submit** - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.
- **Delete** - Delete the selected secondary IP Address
- **Cancel** - Return to the Virtual Router Configuration screen.

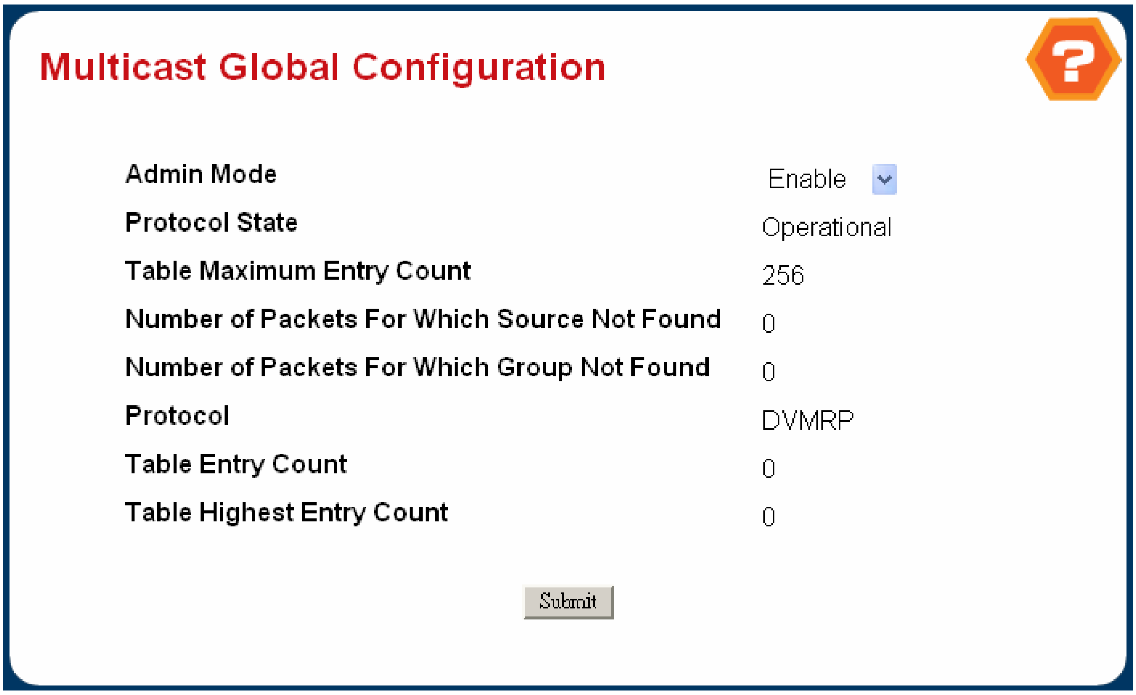
4.7 IP Multicast

The WGS3 supports the following Multicast routing protocol :

- DVMRP
- IGMP
- Multicast
- Mdebug
- PIM-DM
- PIM-SM

4.7.1 Multicast

4.7.1.1 Multicast Global Configuration



Multicast Global Configuration

Admin Mode	Enable
Protocol State	Operational
Table Maximum Entry Count	256
Number of Packets For Which Source Not Found	0
Number of Packets For Which Group Not Found	0
Protocol	DVMRP
Table Entry Count	0
Table Highest Entry Count	0

Figure 4-6-49 Multicast Global Configuation

Selection Criteria

- **Admin Mode** - Select enable or disable to set the administrative status of Multicast Forwarding in the router. The default is disable.
- **Protocol State** - The operational state of the multicast forwarding module.
- **Table Maximum Entry Count** - The maximum number of entries in the IP Multicast routing table.

- **Number Of Packets For Which Source Not Found** - The number of multicast packets that were supposed to be routed but which failed the RPF check.

- **Number Of Packets For Which Group Not Found** - The number of multicast packets that were supposed to be routed but for which no multicast route was found.

- **Protocol** - The multicast routing protocol presently activated on the router, if any.

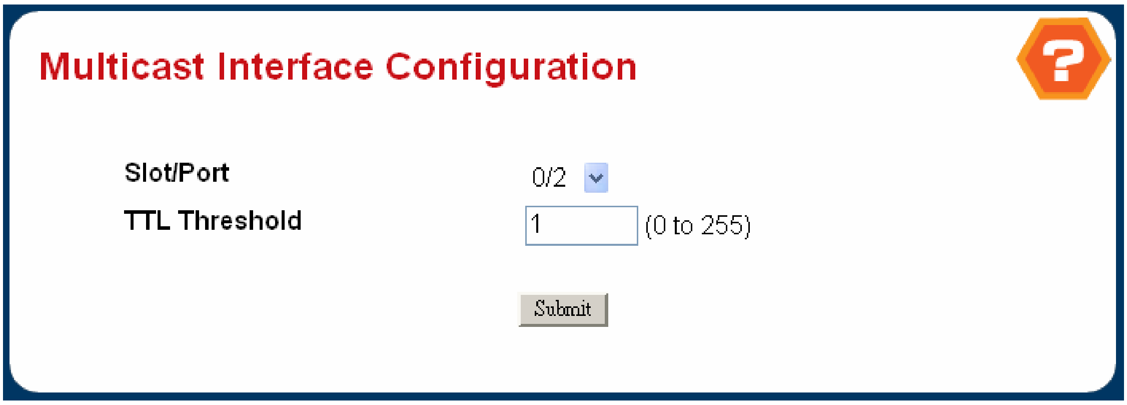
- **Table Entry Count** - The number of multicast route entries currently present in the Multicast route table.

- **Table Highest Entry Count** - The highest number of multicast route entries that have been present in the Multicast route table.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.1.2 Multicast Interface Configuration



Multicast Interface Configuration

Slot/Port	0/2
TTL Threshold	1 (0 to 255)

Figure 4-6-50 Multicast Interface Configuation

Selection Criteria

- **Slot/Port** - Select the routing interface you want to configure from the dropdown menu.

Configurable Data

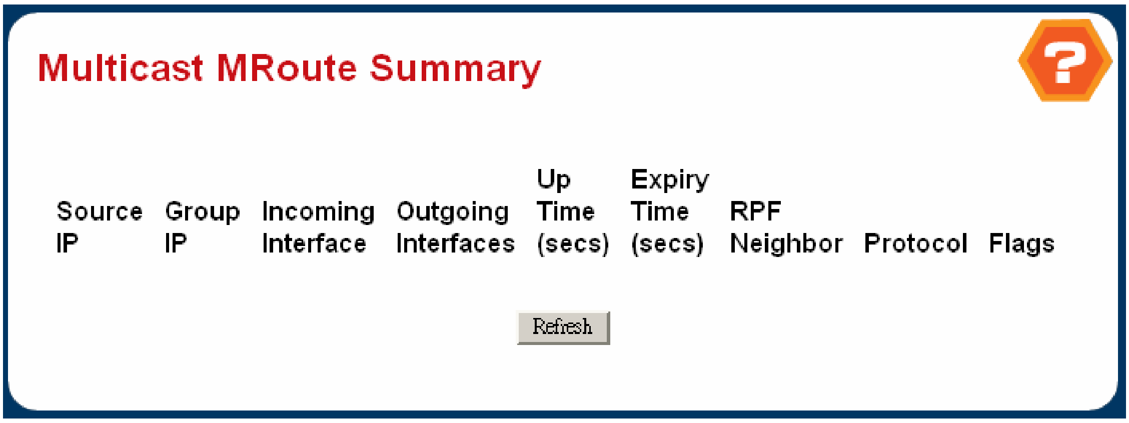
- **TTL Threshold** - Enter the TTL threshold below which a multicast data packet will not be forwarded from the selected interface. You should enter a number between 0 and 255. If you enter 0 all multicast packets for the selected interface will be forwarded. You must configure at least one router interface before you will see this field.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.1.3 Multicast Mroute Summary

This screen displays selected contents of the Mroute Table in tabular form. If there are no routes in the table you will not be presented with the Selection Criteria.



Multicast MRoute Summary

Source IP	Group IP	Incoming Interface	Outgoing Interfaces	Up Time (secs)	Expiry Time (secs)	RPF Neighbor	Protocol	Flags

Figure 4-6-51 Multicast Mroute Summary

Selection Criteria

- **Source IP** - Enter the IP address of the multicast packet source to be combined with the Group IP to fully identify a single route whose Mroute table entry you want to display or clear. You may leave this field blank.
- **Group IP** - Enter the destination group IP address whose multicast route(s) you want to display or clear.

Non-Configurable Data

- **Incoming Interface** - The incoming interface on which multicast packets for this source/group arrive.
- **Outgoing Interface(s)** - The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
- **Up Time** - The time in seconds since the entry was created.
- **Expiry Time** - The time in seconds before this entry will age out and be removed from the table.
- **RPF Neighbor** - The IP address of the Reverse Path Forwarding neighbor.
- **Protocol** - The multicast routing protocol which created this entry. The possibilities are:
    - ***PIM-DM***
    - ***PIM-SM***
    - ***DVMRP***
- **Flags** - The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The possible values are RPT or SPT. For other protocols an "------" is displayed.

Command Buttons

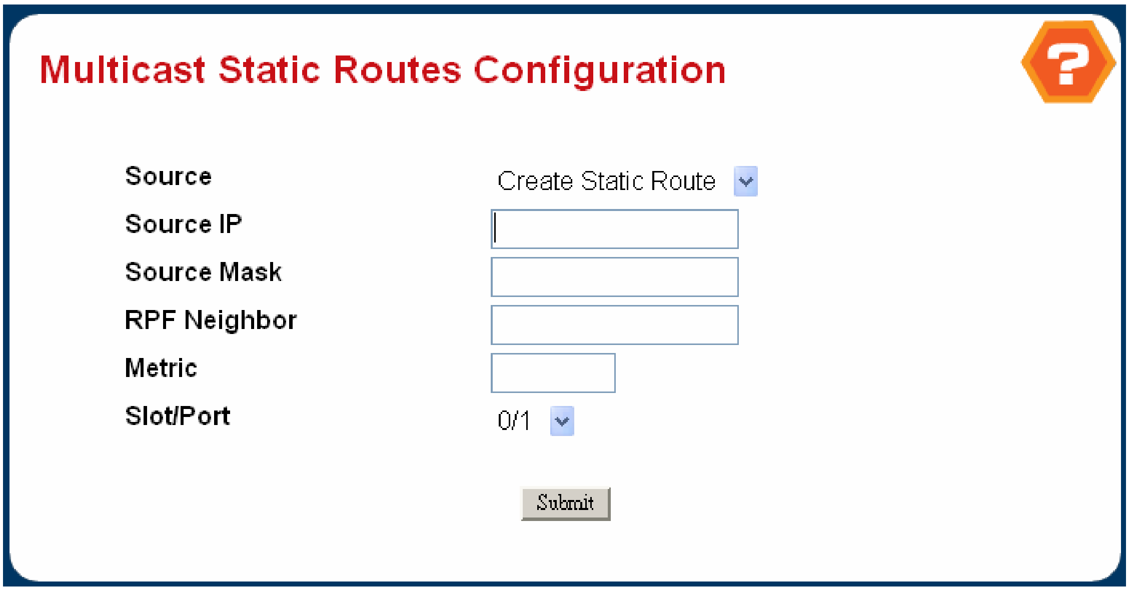
- **Search** - Search the Mroute table for an entry matching the Source IP (if entered) and Group IP address.

- **Clear Route** - Remove the data on the screen for the Source IP (if entered) and Group IP address you have specified.

- **Clear All** - Remove all the data on the screen.

- **Refresh** - Refresh the information on the screen with the present state of the data in the router.

4.7.1.4 Multicast Static Routes Configuration



Multicast Static Routes Configuration

Source	Create Static Route
Source IP	
Source Mask	
RPF Neighbor	
Metric	
Slot/Port	0/1

Figure 4-6-52 Multicast static Routes Configuration

Selection Criteria

- **Source** - Select Create Static Route to configure a new static entry in the Mroute table, or select one of the existing entries from the pulldown menu.

Configurable Data

- **Source IP** - Enter the IP Address that identifies the multicast packet source for the entry you are creating.

- **Source Mask** - Enter the subnet mask to be applied to the Source IP address.

- **RPF Neighbor** - Enter the IP address of the neighbor router on the path to the source.

- **Metric** - Enter the link state cost of the path to the multicast source. The range is 0 - 255 and the default is one. You can change the metric for a configured route by selecting the static route and editing this field.

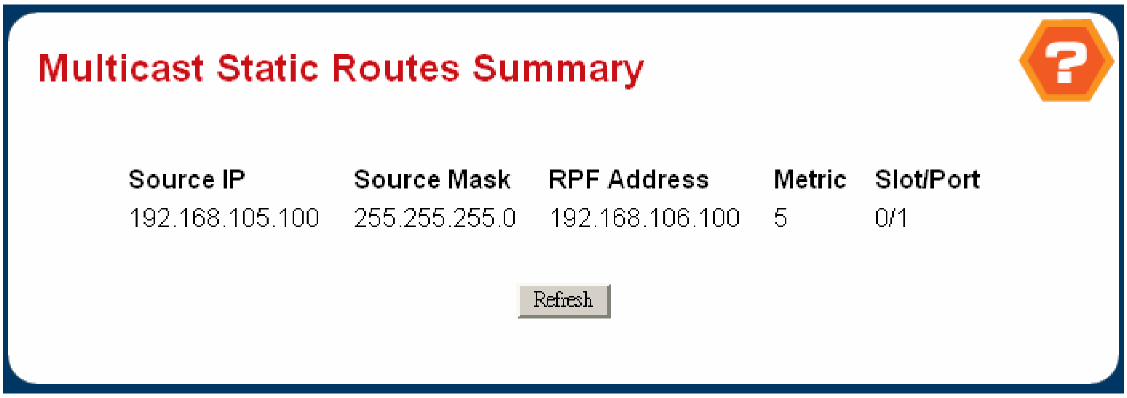
- **Slot/Port** - Select the interface number from the dropdown menu. This is the interface that connects to the neighbor router for the given source IP address.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

- **Delete** - Delete the static entry with the selected Source IP address from the Mroute table.

4.7.1.5 Multicast Static Routes Summary



Multicast Static Routes Summary

Source IP	Source Mask	RPF Address	Metric	Slot/Port
192.168.105.100	255.255.255.0	192.168.106.100	5	0/1

Figure 4-6-53 Milticast Static Routes Summary

Non-Configurable Data

- **Source IP** - The IP Address that identifies the multicast packet source for this route.

- **Source Mask** - The subnet mask applied to the Source IP address.

- **RPF Neighbor** - The IP address of the RPF neighbor.

- **Metric** - The link state cost of the path to the multicast source. The range is 0 - 255.

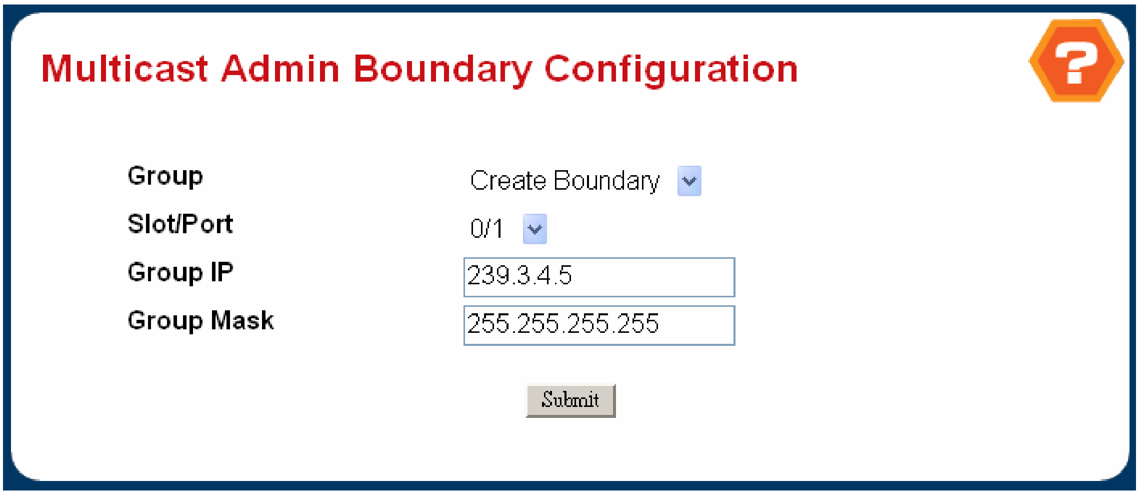
- **Slot/Port** - The number of the incoming interface whose IP address is used as RPF for the given source IP address.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.1.6 Multicast Admin Boundary Configuration

The definition of an administratively scoped boundary is a mechanism is a way to stop the ingress and egress of multicast traffic for a given range of multicast addresses on a given routing interface.



Multicast Admin Boundary Configuration

Group	Create Boundary
Slot/Port	0/1
Group IP	239.3.4.5
Group Mask	255.255.255.255

Figure 4-6-54 Multicast Admin Boundary Configuration

Selection Criteria

- **Group IP** - Select 'Create Boundary' from the pulldown menu to create a new admin scope boundary, or select one of the existing boundary specifications to display or update its configuration.

- **Slot/Port** - Select the router interface for which the administratively scoped boundary is to be configured.

Configurable Data

- **Group IP** - Enter the multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.

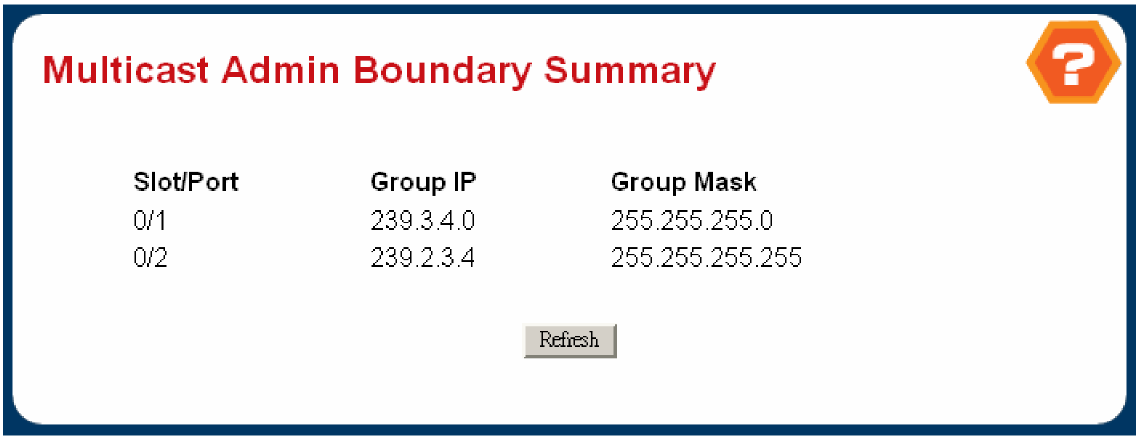
- **Mask** - Enter the mask to be applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

- **Delete** - Delete the selected administrative scoped boundary.

4.7.1.7 Multicast Admin Boundary Summary



Multicast Admin Boundary Summary

Slot/Port	Group IP	Group Mask
0/1	239.3.4.0	255.255.255.0
0/2	239.2.3.4	255.255.255.255

Figure 4-6-55 Multicast Admin Boundary Summary

Non-Configurable Data

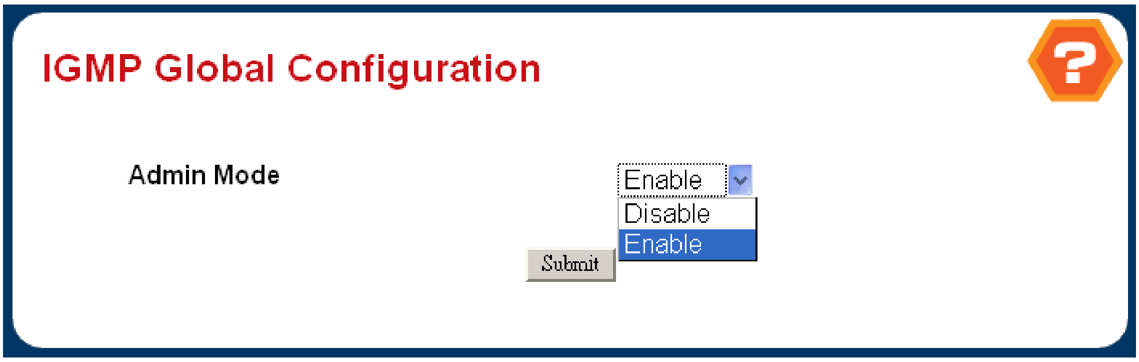
- **Slot/Port** - The router interface to which the administratively scoped address range is applied.
- **Group IP** - The multicast group address for the start of the range of addresses to be excluded.
- **Mask** - The mask that is applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.2 IGMP

4.7.2.1 IGMP Global Configuration



IGMP Global Configuration

Admin Mode Enable

Figure 4-6-56 IGMP Global Configuation

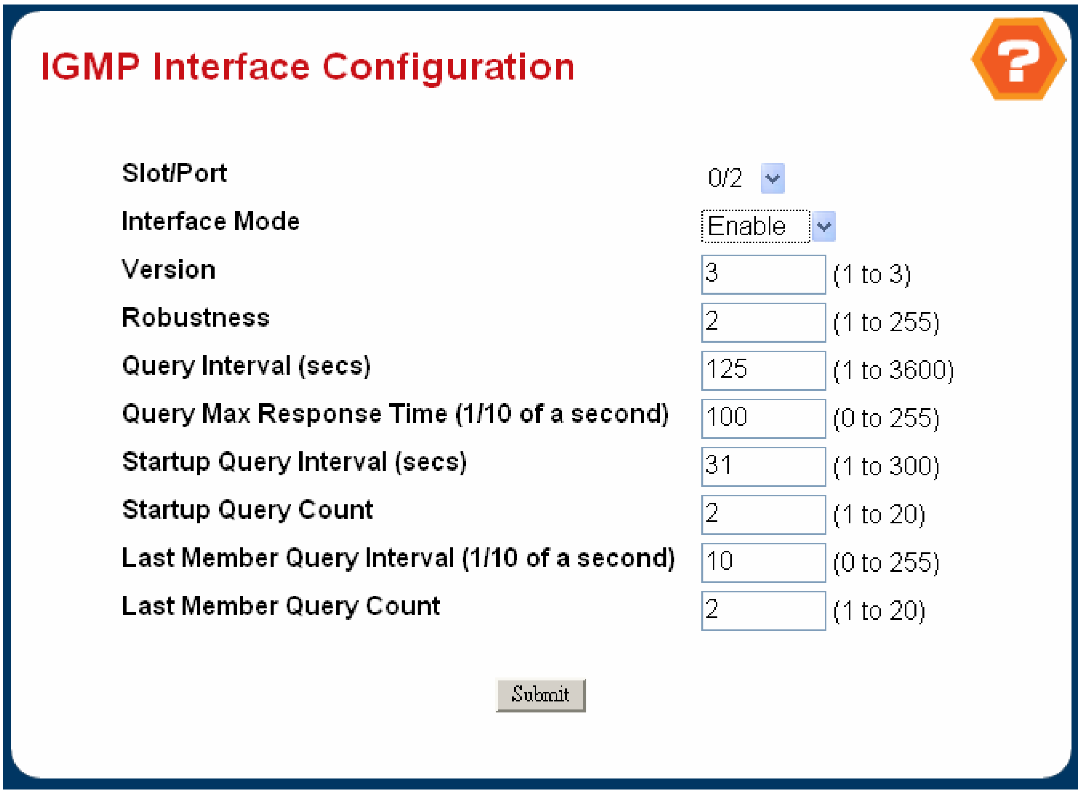
Configurable Data

- **Admin Mode** - Select enable or disable from the pulldown menu to set the administrative status of IGMP in the router to active or inactive. The default is disable.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.2.2 IGMP Interface Configuration



IGMP Interface Configuration

Slot/Port	0/2	
Interface Mode	Enable	
Version	3	(1 to 3)
Robustness	2	(1 to 255)
Query Interval (secs)	125	(1 to 3600)
Query Max Response Time (1/10 of a second)	100	(0 to 255)
Startup Query Interval (secs)	31	(1 to 300)
Startup Query Count	2	(1 to 20)
Last Member Query Interval (1/10 of a second)	10	(0 to 255)
Last Member Query Count	2	(1 to 20)

Figure 4-6-57 IGMP Interface Configuration

Selection Criteria

- **Slot/Port** - Select the slot and port for which data is to be displayed or configured from the pulldown menu. Slot 0 is the base unit. You must have configured at least one router interface before configuring or displaying data for an IGMP interface, otherwise an error message will be displayed.

Configurable Data

- **Interface Mode** - Select enable or disable from the pulldown menu to set the administrative status of IGMP on the selected interface. The default is disable.

- **Version** - Enter the version of IGMP you want to configure on the selected interface. Valid values are 1 to 2 and the default value is 2.

- **Robustness** - Enter the robustness value. This variable allows tuning for the expected packet loss on a subnet. If you expect the subnet to be lossy, you should enter a higher number for this parameter. IGMP is robust to (robustness variable-1) packet losses. Valid values are from 1 to 255. The default value is 2.

- **Query Interval** - Enter the frequency in seconds at which IGMP host-query packets are to be transmitted on this interface. Valid values are from 1 to 3600. The default value is 125.

- **Query Max Response Time** - Enter the maximum query response time to be advertised in IGMPv2 queries on this interface, in tenths of a second. The default value is 10. Valid values are from (0 to 255) .

- **Startup Query Interval** - Enter the number of seconds between the transmission of startup queries on the selected interface. The valid values are from 1 to 300. The default value is 31.

- **Startup Query Count** - Enter the number of queries to be sent on startup. The valid values are from 1 to 20. The default value is 2.

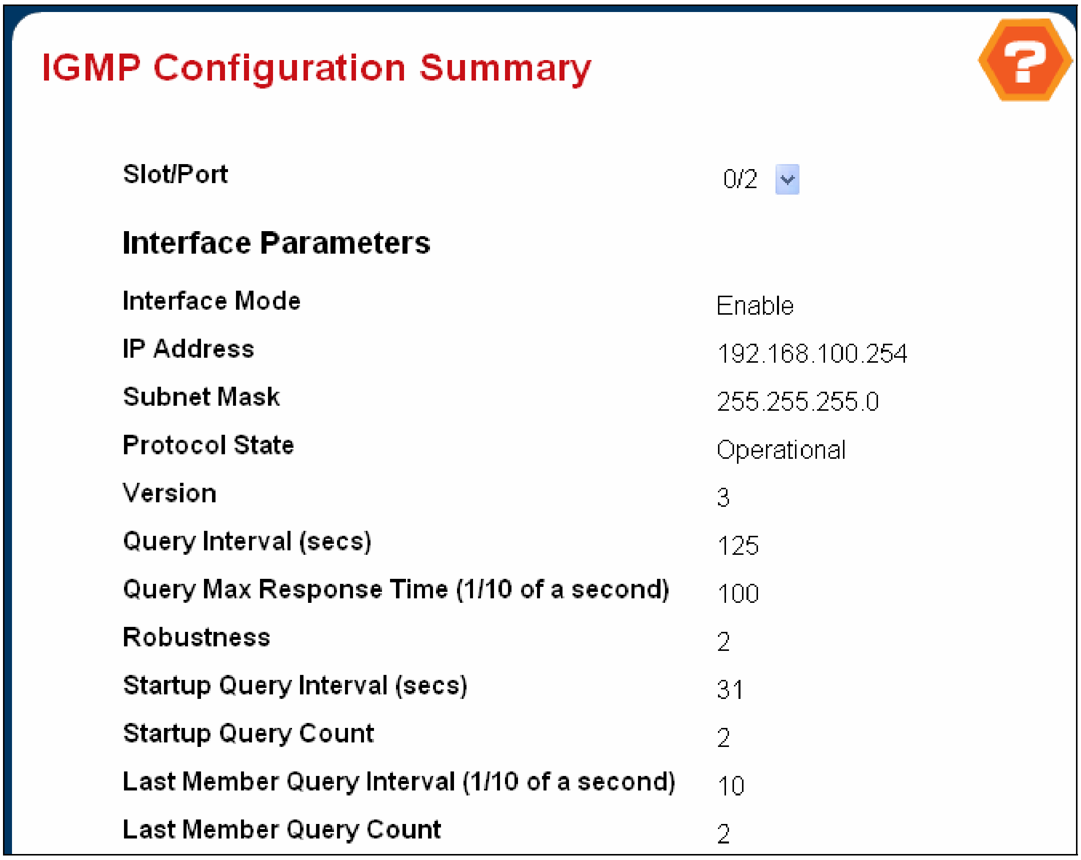
- **Last Member Query Interval** - Enter the last member query interval in tenths of a second. This the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 1. This value is not used for IGMP version 1.

- **Last Member Query Count** - Enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.2.3 IGMP Interface Configuration Summary



IGMP Configuration Summary

Slot/Port	0/2

Interface Parameters

Interface Mode	Enable
IP Address	192.168.100.254
Subnet Mask	255.255.255.0
Protocol State	Operational
Version	3
Query Interval (secs)	125
Query Max Response Time (1/10 of a second)	100
Robustness	2
Startup Query Interval (secs)	31
Startup Query Count	2
Last Member Query Interval (1/10 of a second)	10
Last Member Query Count	2

Figure 4-6-58 IGMP Configuration Summary

- **Slot/Port** - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Non-Configurable Data

- **Interface Mode** - The administrative status of IGMP on the selected interface.
- **IP Address** - The IP address of the selected interface.
- **Subnet Mask** - The subnet mask for the IP address of the selected interface.
- **Protocol State** - The operational state of IGMP on the selected interface.
- **Version** - The version of IGMP configured on the selected interface.
- **Query Interval** - The frequency at which IGMP host-query packets are transmitted on the selected interface.
- **Query Max Response Time** - The maximum query response time advertised in IGMPv2 queries sent from the selected interface.

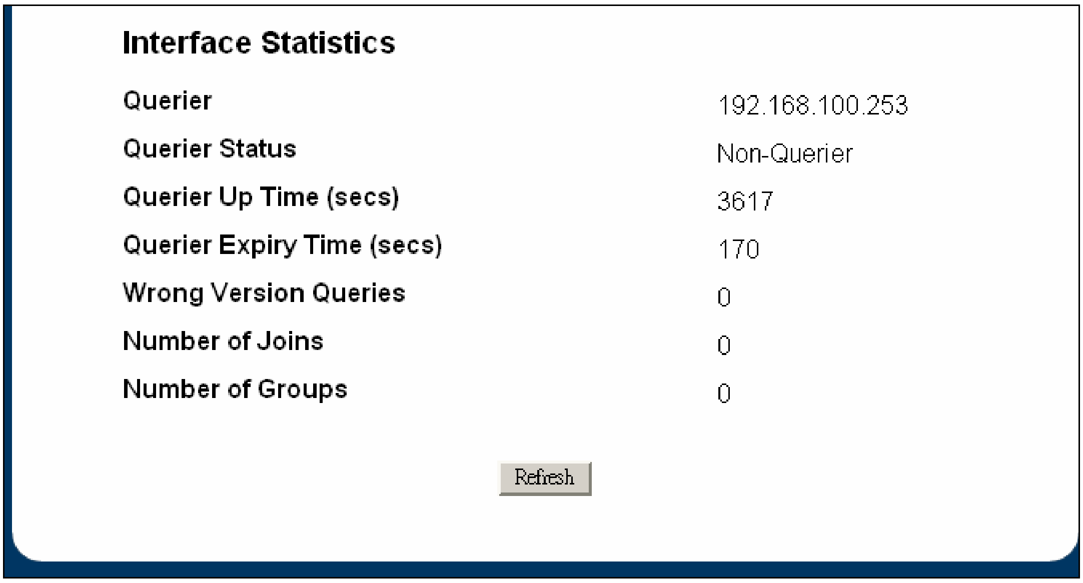
- **Robustness** - The robustness parameter for the selected interface. This variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. IGMP is robust to (robustness variable-1) packet losses.

- **Startup Query Interval** - The interval at which startup queries are sent on the selected interface.

- **Startup Query Count** - The number of queries to be sent on startup.

- **Last Member Query Interval** - The last member query interval. The last member query interval is the maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This value is not used for IGMP version 1.

- **Last Member Query Count** - The number of queries to be sent on receiving a leave group report.



Interface Statistics

Querier	192.168.100.253
Querier Status	Non-Querier
Querier Up Time (secs)	3617
Querier Expiry Time (secs)	170
Wrong Version Queries	0
Number of Joins	0
Number of Groups	0

Figure 4-6-59 IGMP Configuration Summary

- **Querier** - The address of the IGMP querier on the IP subnet to which the selected interface is attached.

- **Querier Status** - Indicates whether the selected interface is in querier or non querier mode.

- **Querier Up Time** - The time in seconds since the IGMP interface querier was last changed.

- **Querier Expiry Time** - The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this will be zero.

- **Wrong Version Queries** - The number of queries that have been received on the selected interface with an IGMP version that does not match the IGMP version configured for the interface, over the lifetime of the entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Therefore, a configuration error is indicated if any queries are received with the wrong version number.

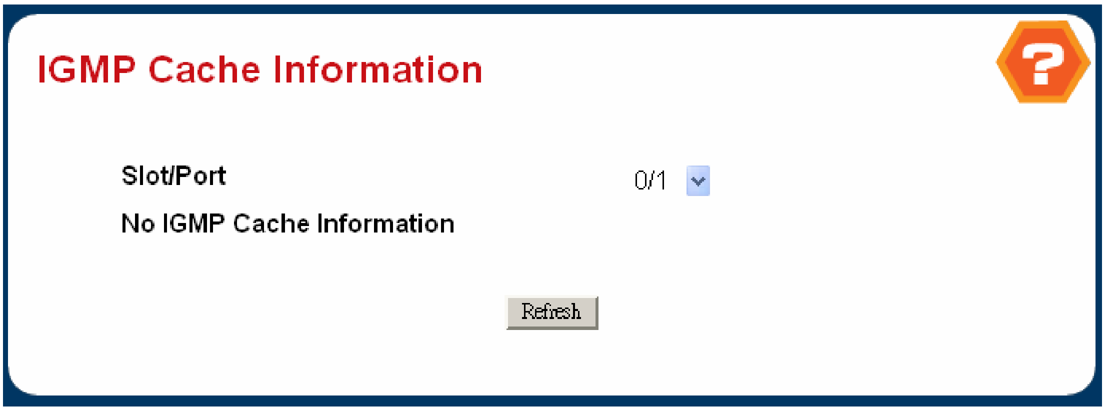
- **Number of Joins** - The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.

- **Number of Groups** - The current number of entries for the selected interface in the cache table.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.2.4 IGMP Cache Information



IGMP Cache Information

Slot/Port 0/1

No IGMP Cache Information

Figure 4-6-60 IGMP Cache Information

Selection Criteria

- **Slot/Port** - Select the Slot and port for which data is to be displayed. Slot 0 is the base unit.
- **Multicast Group IP** - Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface you will not be able to make this selection, and none of the non-configurable data will be displayed.

Non-Configurable Data

- **Last Reporter** - The IP address of the source of the last membership report received for the IP Multicast group address on the selected interface.

- **Up Time** - The time elapsed since this entry was created.

- **Expiry Time** - The minimum amount of time remaining before this entry will be aged out.

- **Version 1 Host Timer** - The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. When an IGMPv1 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 1.

- **Version 2 Host Timer** - The time remaining until the local router will assume that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. When an IGMPv2 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv1 and IGMPv3 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 2.

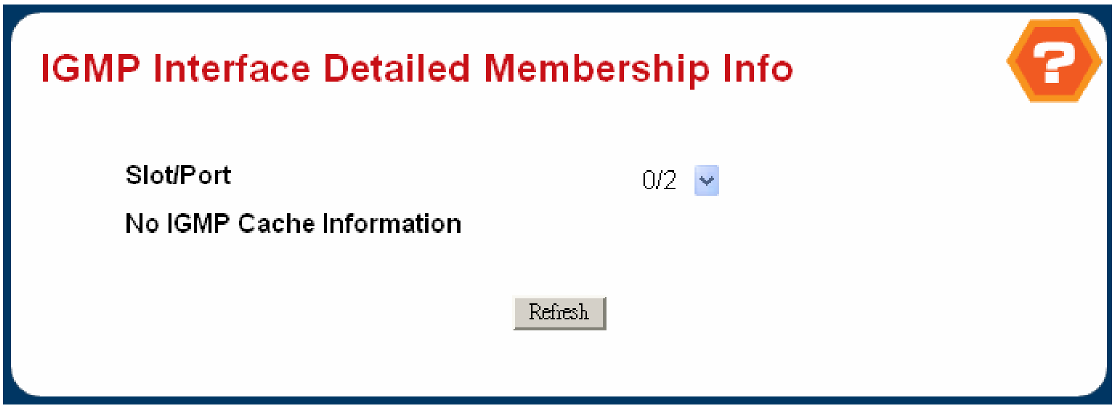
- **Compatibility** - This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.

- **Filter Mode** - The source filter mode (Include/Exclude/NA) for the specified group on this interface. When NA mode is active the field is blank

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.2.5 IGMP Interface Membership Details Info



IGMP Interface Detailed Membership Info

Slot/Port 0/2

No IGMP Cache Information

Figure 4-6-61 IGMP InterfaceDetail Membership Info

Selection Criteria

- **Slot/Port** - Select the Slot and port for which data is to be displayed. Slot 0 is the base unit.
- **Multicast Group IP** - Select the IP multicast group address for which data is to be displayed. If no group membership reports have been received on the selected interface you will not be able to make this selection, and none of the non-configurable data will be displayed.

Non-Configurable Data

- **Interface** - This parameter shows the interface on which multicast packets are forwarded.
- **Group Compatibility Mode** - This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.
- **Source Filter Mode** - The source filter mode (Include/Exclude/NA) for the specified group on this interface.
- **Source Hosts** - This parameter shows source addresses which are members of this multicast address.
- **Expiry Time** - This parameter shows expiry time interval against each source address which are members of this multicast group. This is the amount of time after which the specified source entry is aged out.

4.7.3 DVMRP

Distance Vector Multicast Routing Protocol is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. To configure DVMRP, you must specify the routing metric, probe interval, and neighbor router timeout.

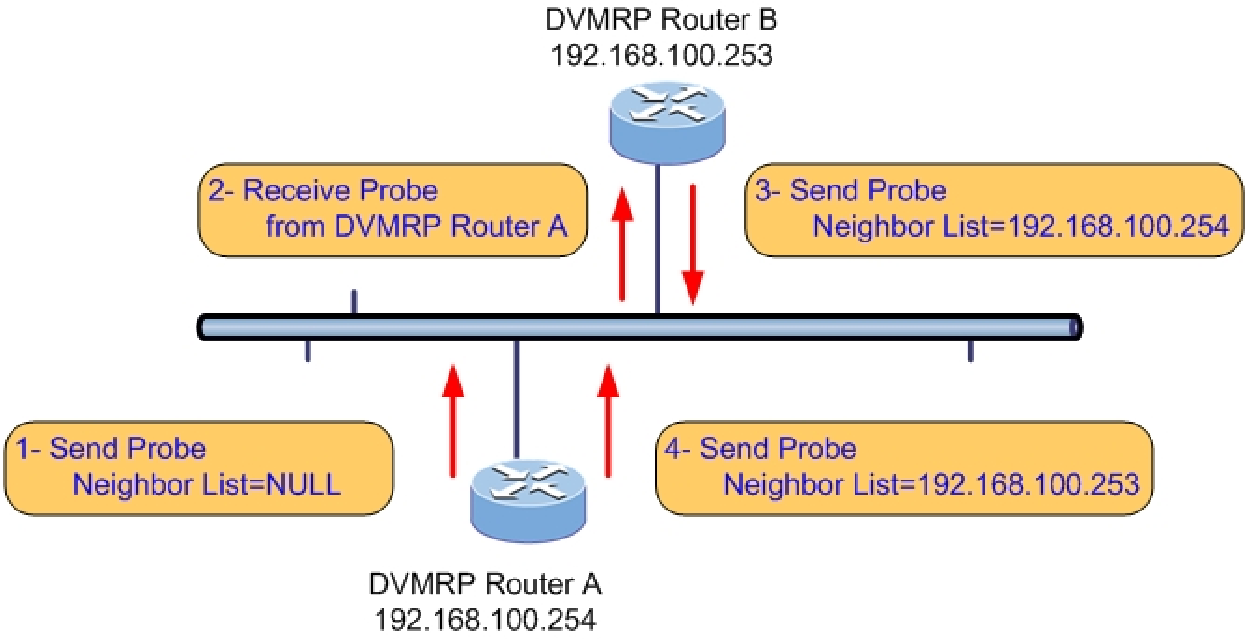
DVMRP Overview -

- Base on Distance Vector
  - Similar to RIP
  - Infinity = 32 hops
- DVMRP uses the IGMP to exchange routing datagram
  - IP Protocol 0x02 (IGMP)
  - IGMP type 0x13 (DVMRP)
- Similar to PIM DM
  - Broadcast and Prune operation
  - Uses DVMRP route table for RPF check
- Route Table
  - Build source distribution trees
  - Perform multicast forwarding (RPF checks)
  - Periodic route updates (every 60 Seconds)
- Concept of Virtual interfaces
  - Physical: Ethernet, FDDI, Token Ring
  - Tunnels: IP-in-IP tunnels
- Version Compatibility
  - V1, V2 : No support Pruning and Generation ID
  - V3.0, v3.1, v3.2 : Have support Pruning but no support Generation ID

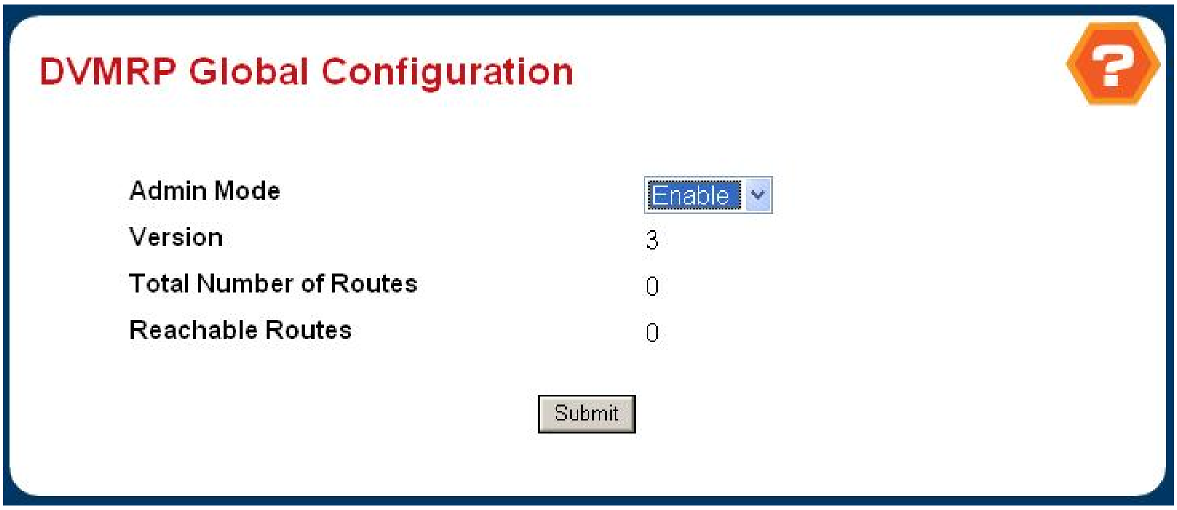
- V1, V2 : No support Pruning and Generation ID
- V3.0, v3.1, v3.2 : Have support Pruning but no support Generation ID

DVMRP Negihbor Discovery

- DVMRP Probe messages are periodically multicast to the all DVMRP Routers group address (224.0.0.4).
- Once you have received a Probe from a neighbor that contains your address in the neighbor list, your have established a two-way neighbor adjacency with this router.



4.7.3.1 DVMRP Global Configuration



DVMRP Global Configuration

Admin Mode	Enable
Version	3
Total Number of Routes	0
Reachable Routes	0

Figure 4-6-62 DVMRP Global Configuation

Configurable Data

- **Admin Mode** - Select enable or disable from the dropdown menu. This sets the administrative status of DVMRP to active or inactive. The default is disable.

Non-Configurable Data

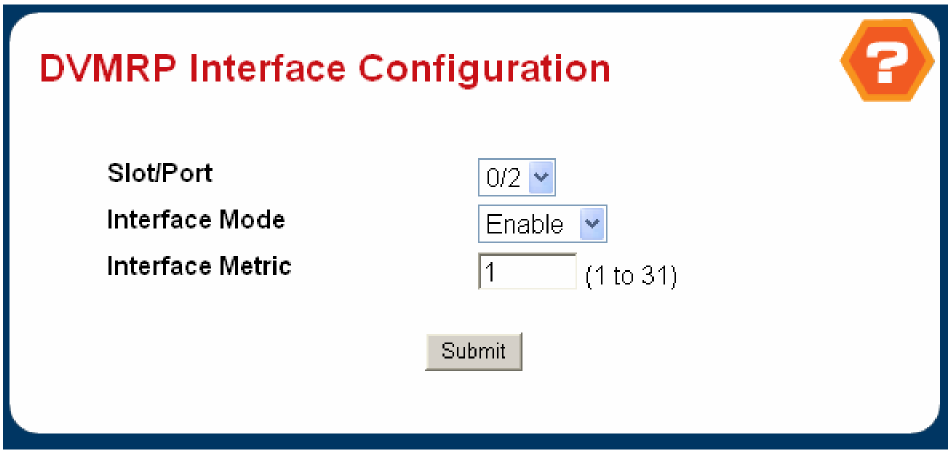
- **Version** - The current value of the DVMRP version string.
- **Total Number of Routes** - The number of routes in the DVMRP routing table.
- **Reachable Routes** - The number of routes in the DVMRP routing table that have a non-infinite metric.

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Note: Only one multicast routing protocol could be enabled at one time. That means, for example, once the PIM-DM admin mode is enabled, the user is not able to enable the DVMRP.

4.7.3.2 DVMRP Interface Configuration



DVMRP Interface Configuration

Slot/Port	0/2
Interface Mode	Enable
Interface Metric	1 (1 to 31)

Figure 4-6-63 DVMRP Interface Configuation

Selection Criteria

- **Slot/Port** - Select the interface for which data is to be configured. You must configure at least one router interface before you configure a DVMRP interface. Otherwise you will see a message telling you that no router interfaces are available, and the configuration screen will not be displayed.

Configurable Data

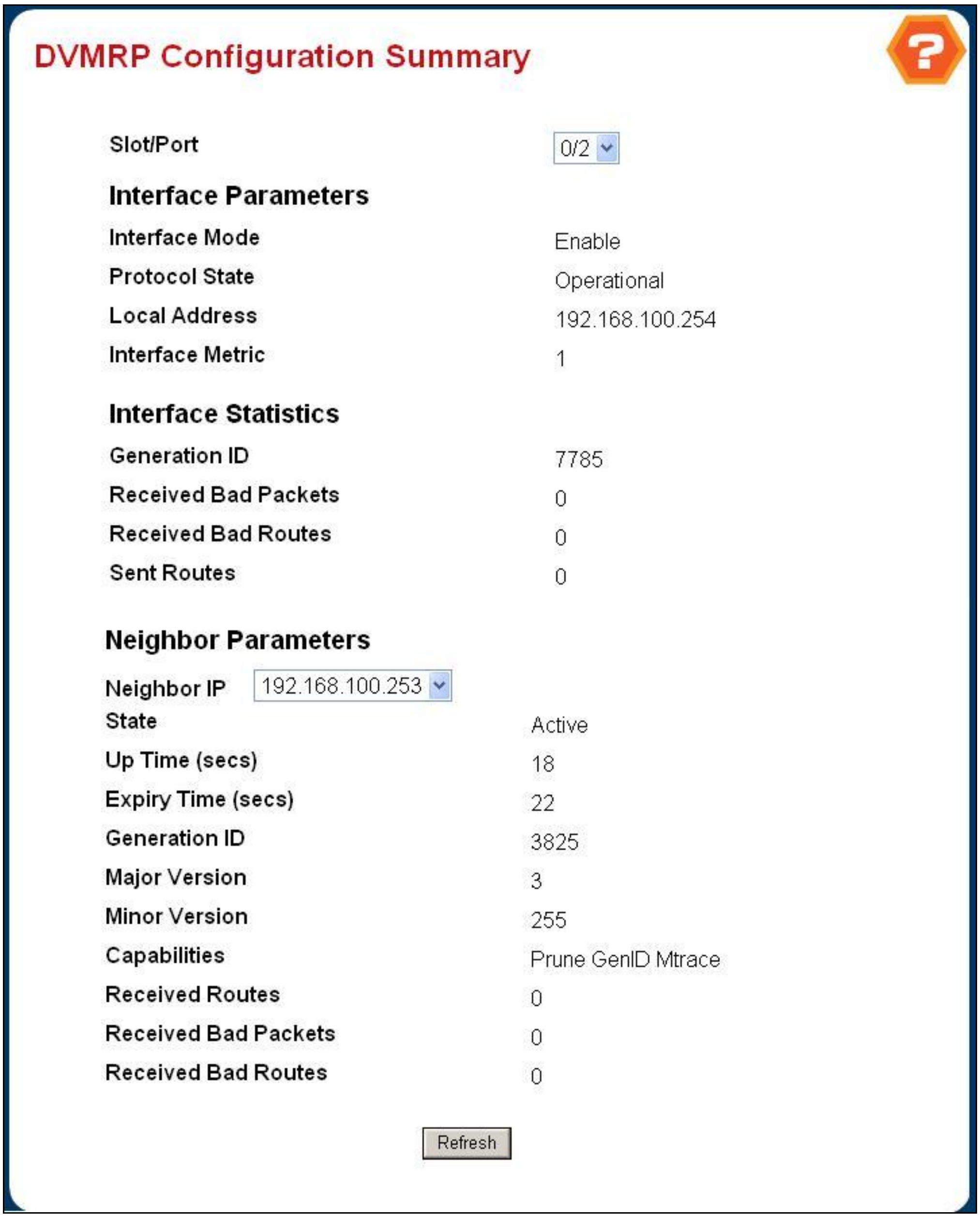
- **Interface Mode** - Select enable or disable from the pulldown menu to set the administrative mode of the selected DVMRP routing interface.

- **Interface Metric** - Enter the DVMRP metric for the selected interface. This value is sent in DVMRP messages as the cost to reach this network. Valid values are from (1 to 31).

Command Buttons

- **Submit** - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.3.3 DVMRP Configuration Summary



DVMRP Configuration Summary

Slot/Port	0/2
Interface Parameters	
Interface Mode	Enable
Protocol State	Operational
Local Address	192.168.100.254
Interface Metric	1
Interface Statistics	
Generation ID	7785
Received Bad Packets	0
Received Bad Routes	0
Sent Routes	0
Neighbor Parameters	
Neighbor IP	192.168.100.253
State	Active
Up Time (secs)	18
Expiry Time (secs)	22
Generation ID	3825
Major Version	3
Minor Version	255
Capabilities	Prune GenID Mtrace
Received Routes	0
Received Bad Packets	0
Received Bad Routes	0

Figure 4-6-64 DVMRP Configuration Summary

Selection Criteria

- **Slot/Port** - Select the interface for which data is to be displayed. You must configure at least one router interface before you can display data for a DVMRP interface. Otherwise you will see a message telling you that no router interfaces are available, and the configuration summary screen will not be displayed.

Non-Configurable Data

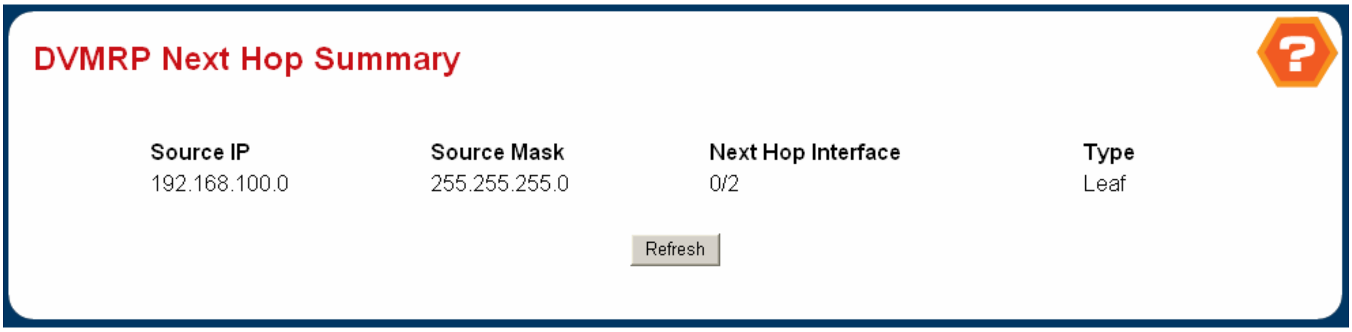
- **Interface Mode** - The administrative mode of the selected DVMRP routing interface, either enable or disable.

- **Protocol State** - The operational state of the DVMRP protocol on the selected interface, either operational or non-operational.
- **Local Address** - The IP address used as a source address in packets sent from the selected interface.
- **Interface Metric** - The metric used to calculate distance vectors for the selected interface.
- **Generation ID** - The DVMRP generation ID used by the router for the selected interface. This value is reset every time an interface is (re)started and is placed in prune messages. A change in generation ID informs the neighbor routers that any previous information about this router should be discarded.
- **Received Bad Packets** - The number of invalid packets received on the selected interface.
- **Received Bad Routes** - The number of invalid routes received on the selected interface.
- **Sent Routes** - The number of routes sent on the selected interface.
- **Neighbor IP** - The IP address of the neighbor whose information is displayed.
- **State** - The state of the specified neighbor router on the selected interface, either active or down.
- **Neighbor Uptime** - The DVMRP uptime for the specified neighbor on the selected interface. This is the time since the neighbor entry was learned.
- **Neighbor Expiry Time** - The DVMRP expiry time for the specified neighbor on the selected interface. This is the time left before this neighbor entry will age out, and is not applicable if the neighbor router's state is down.
- **Generation ID** - The DVMRP generation ID for the specified neighbor on the selected interface.
- **Major Version** - The DVMRP Major Version for the specified neighbor on the selected interface.
- **Minor Version** - The DVMRP Minor Version for the specified neighbor on the selected interface.
- **Capabilities** - The DVMRP capabilities of the specified neighbor on the selected interface.
- **Received Routes** - The number of routes received for the specified neighbor on the selected interface.
- **Received Bad Packets** - The number of invalid packets received for the specified neighbor on the selected interface.
- **Received Bad Routes** - The number of invalid routes received for the specified neighbor on the selected interface.

Command Buttons

- **Refresh** - Refresh the screen with the new data.

4.7.3.4 DVMRP Next Hop Summary



DVMRP Next Hop Summary

Source IP	Source Mask	Next Hop Interface	Type
192.168.100.0	255.255.255.0	0/2	Leaf

Figure 4-6-65 DVMRP Next Hop Summary

Non-Configurable Data

- **Source IP** - The IP address used with the source mask to identify the source network for this table entry.

- **Source Mask** - The network mask used with the source IP address.

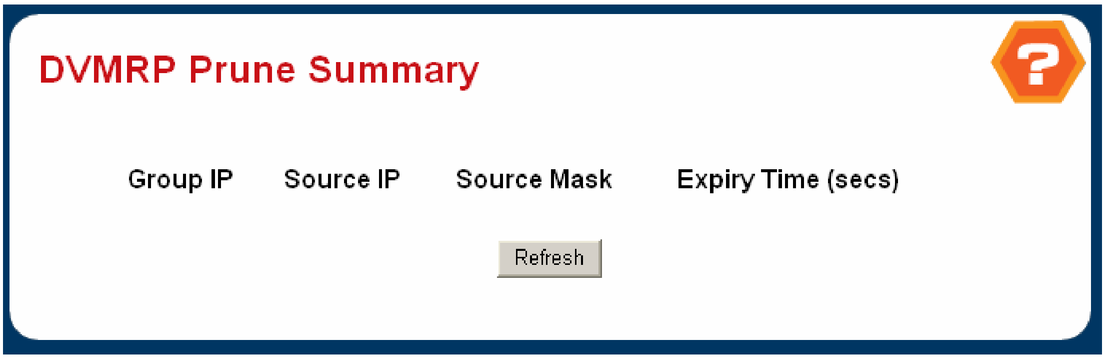
- **Next Hop Interface** - The outgoing interface for this next hop.

- **Type** - The next hop type. 'Leaf' means that no downstream dependent neighbors exist on the outgoing interface. Otherwise, the type is 'branch'.

Command Buttons

- **Refresh** - Refresh the screen with the new data

4.7.3.5 DVMRP Prune Summary



DVMRP Prune Summary

Group IP	Source IP	Source Mask	Expiry Time (secs)

Figure 4-6-66 DVMRP Prune Summary

Non-Configurable Data

- **Group IP** - The group address which has been pruned.
- **Source IP** - The address of the source or source network which has been pruned.
- **Source Mask** - The subnet mask to be combined with the source IP address to identify the source or source network which has been pruned.
- **Expiry Time** - The amount of time remaining before this prune should expire at the upstream neighbor. If no prune messages have been received from downstream neighbors, this is set to value of the default prune lifetime timer, otherwise it is set to the smallest received value or the default timer, whichever is less.

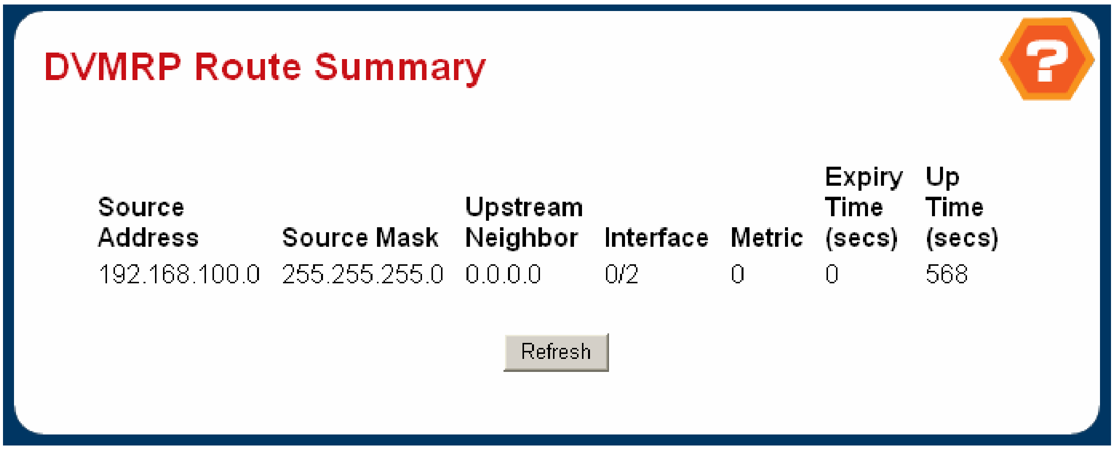
Command Buttons

- **Refresh** - Refresh the screen with the new data

Notice

- **Purning**
  - Pruning is the mechanism with which DVMRP is cutting unneeded routers out from the Truncated Broadcast Tree (TBT) in order to minimize the network resources used in carrying the multicast traffic.
  - Infinity the multicast packet (S, G) is broadcasted thru all TBT.
  - Each leaf router that has no subsequent receivers for that traffic, sends up-stream a Prune message in order to be left out of the TBT for that traffic.
  - Pruned branches of the TBT will time out (typically after 2 minutes) and traffic will once again flood down all branches of the TBT.

4.7.3.6 DVMRP Route Summary



DVMRP Route Summary

Source Address	Source Mask	Upstream Neighbor	Interface	Metric	Expiry Time (secs)	Up Time (secs)
192.168.100.0	255.255.255.0	0.0.0.0	0/2	0	0	568

Figure 4-6-67 DVMRP Route Summary

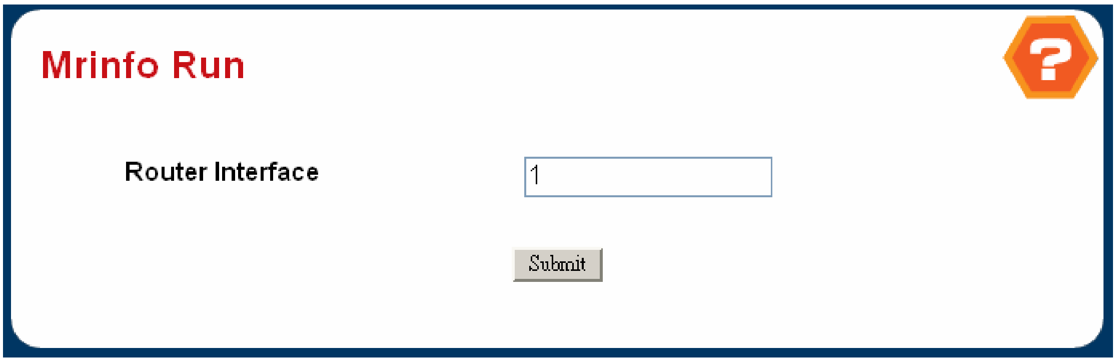
Non-Configurable Data

- **Source Address** - The network address that is combined with the source mask to identify the sources for this entry.
- **Source Mask** - The subnet mask to be combined with the source address to identify the sources for this entry.
- **Upstream Neighbor** - The address of the upstream neighbor (e.g., RPF neighbor) from which IP datagrams from these sources are received.
- **Interface** - The interface on which IP datagrams sent by these sources are received. A value of 0 typically means the route is an aggregate for which no next-hop interface exists.
- **Metric** - The distance in hops to the source subnet.
- **Expiry Time** - The minimum amount of time remaining before this entry will be aged out.
- **Up Time** - The time since the route represented by this entry was learned by the router

4.7.4 Mdebug

4.7.4.1 Mrinfo Run

Use this screen to initiate an mrinfo command. You can use the mrinfo command to find out information about neighboring multicast routers. While you initiate the query using this screen, the results are displayed on the Mrinfo Show screen.



Mrinfo Run

Router Interface: 1

Figure 4-6-68 Mrinfo Run

Configurable Data

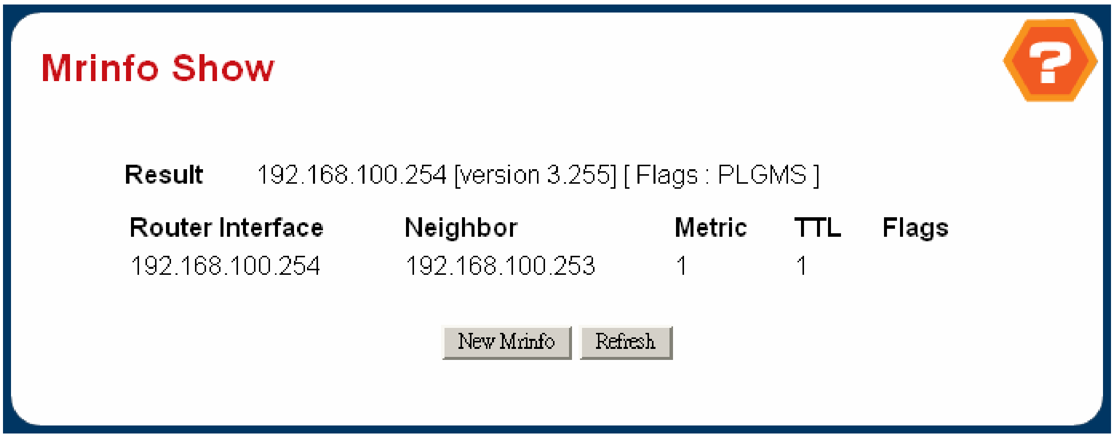
- **Router Interface** - Enter the IP address of the router interface for which you want to see the neighbor router information. If you do not enter an address the router will query itself.

Command Buttons

- **Submit** - Initiate the *mrinfo* command on the router. If the *mrinfo* command completes successfully the browser will display the Mrinfo Show screen. If the *mrinfo* command fails, you will see the Mrinfo Run screen again.

4.7.4.2 Mrinfo Show

This screen displays the results of an mrinfo command.



Mrinfo Show

Result 192.168.100.254 [version 3.255] [Flags : PLGMS]

Router Interface	Neighbor	Metric	TTL	Flags
192.168.100.254	192.168.100.253	1	1	

Figure 4-6-69 Mrinfo Show

Non-Configurable Data

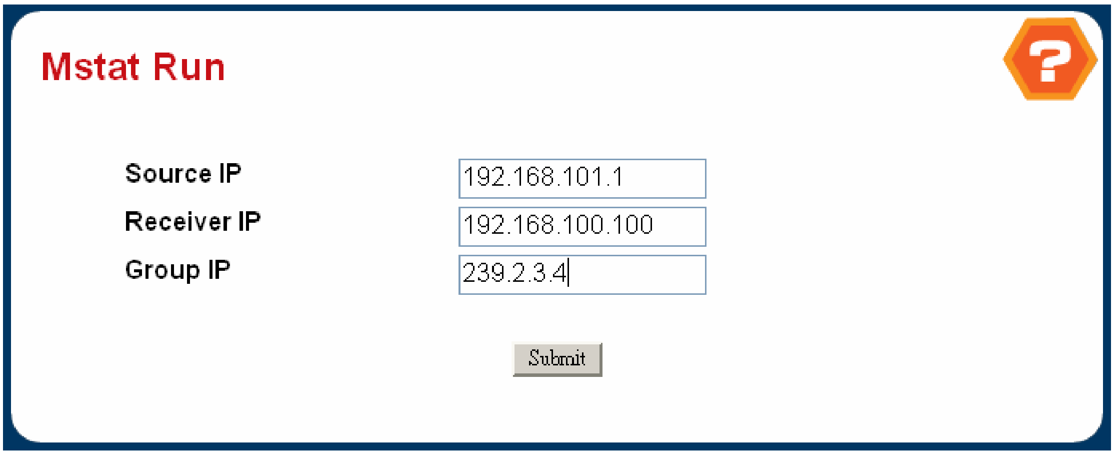
- **Router Interface** - The IP address of the router interface for which configuration information was requested.
- **Neighboring router's IP Address** - The IP address of the neighboring router.
- **Metric** - The routing metric for this router.
- **TTL Threshold** - The time-to-live threshold on this hop.
- **Flags** - The flags indicating whether the router is an IGMP querier or whether or not it has neighbors (leaf router).

Command Buttons

- **New Mrinfo** - Redirect the web browser to the Mrinfo Run screen so that you can initiate another *mrinfo* command.
- **Refresh** - Refresh the content of the screen with the latest data available on the router. Typically, it takes around 20 seconds to process the results after you have initiated the *mrinfo* command. The contents of the screen have to be refreshed to display the latest results.

4.7.4.3 Mstat Run

Use this screen to initiate an mstat command on the router. You can use the mstat command to see the hop-by-hop path taken by packets from a given multicast source to the destination. It also gives you information regarding packet rate and packet loss on the path.



Mstat Run

Source IP	192.168.101.1
Receiver IP	192.168.100.100
Group IP	239.2.3.4

Figure 4-6-70 Mstat Run

Configurable Data

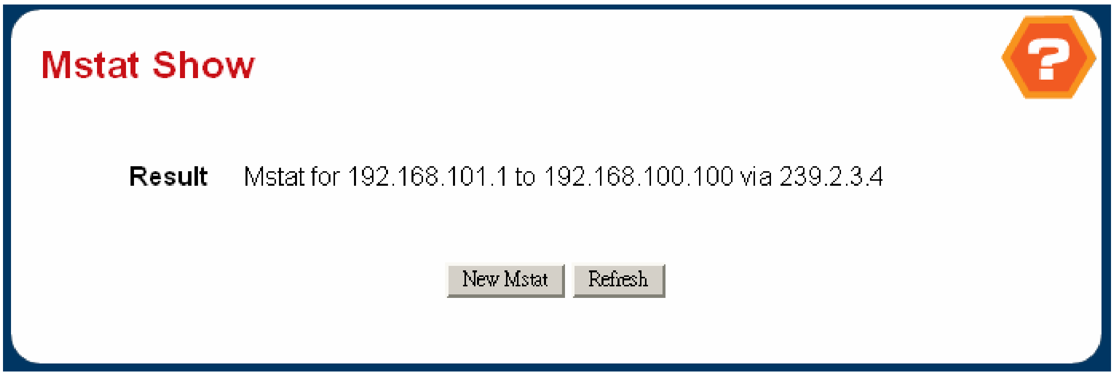
- **Source Address** - Enter the IP address of the multicast-capable source. This is the unicast address of the beginning of the path to be traced.
- **Receiver Address** - Enter the IP address of the host to which the *mstat* response will be sent by the last hop router. If a value is not entered, the IP address of the router interface through which the *mstat* will be sent is used.
- **Group Address** - Enter the multicast address of the group to be traced. If you leave this field blank, the multicast address 224.2.0.1 will be used. Valid addresses are 224.0.0.0 through 239.255.255.255.

Command Buttons

- **Submit** - Initiate the *mstat* command on the router. If the *mstat* command completes successfully the browser will display the Mstat Show screen. If the *mstat* command fails, you will see the Mstat Run screen again.

4.7.4.4 Mstat Show

This screen is used to display the results of an mstat command.



Mstat Show

Result Mstat for 192.168.101.1 to 192.168.100.100 via 239.2.3.4

Figure 4-6-71 Mstat Show

Non-Configurable Data

- This screen shows the path taken by multicast traffic between the specified IP addresses. Forward data flow is indicated by arrows pointing downward and the query path is indicated by arrows pointing upward. For each hop, both the entry and exit addresses of the router are shown if different, along with the initial TTL required for packets to be forwarded at this hop and the propagation delay across the hop. The right half of the screen displays statistics for the path in two groups. Within each group, the columns are the number of packets lost, the number of packets sent, the percentage lost, and the average packet rate at each hop. These statistics are calculated from differences between traces and from hop to hop. The first group shows the statistics for all traffic flowing out the interface at one hop and in the interface at the next hop. The second group shows the statistics only for traffic forwarded from the specified source to the specified group.

Command Buttons

- **New Mstat** - Redirect the web browser to the Mstat Run screen so that you can initiate another *mstat* command.

- **Refresh** - Refresh the content of the screen with the latest data available on the router. Typically, it takes around 20 seconds to process the results after initiating *mstat* command. You must refresh the screen to display the latest results.

4.7.4.5 Mtrace Configuration

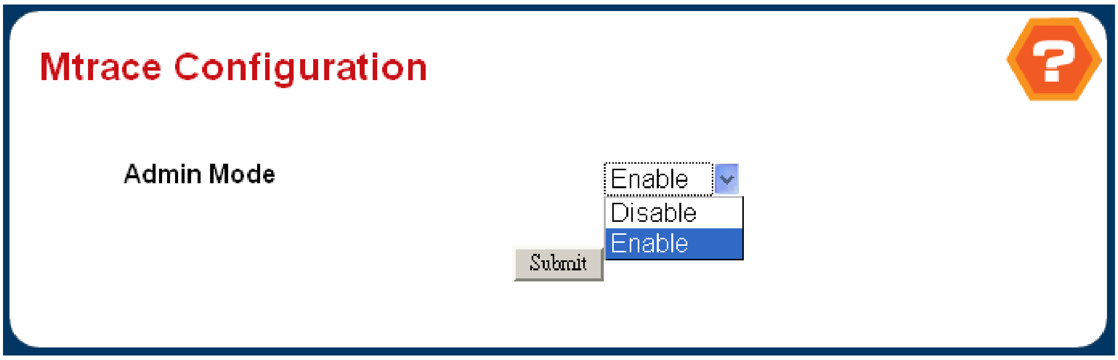


Figure 4-6-72 Mtrace Configuation

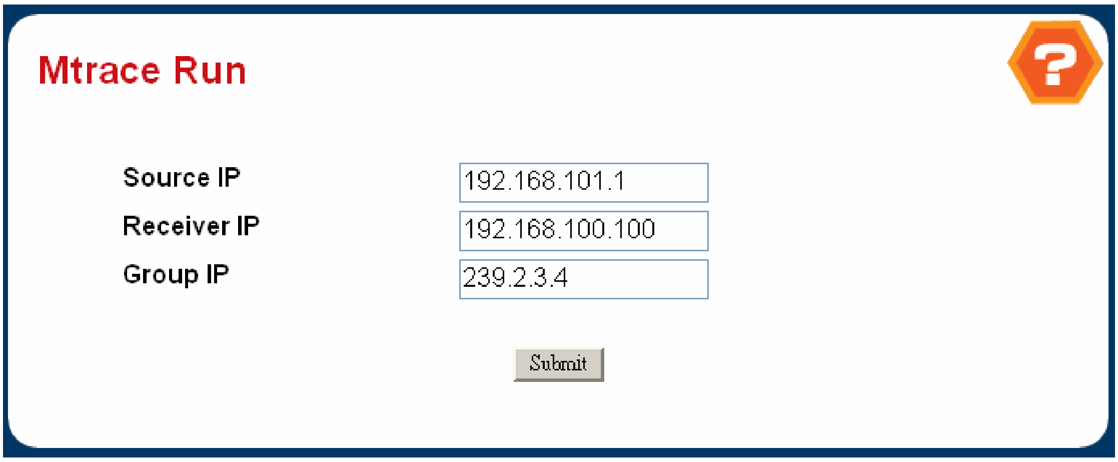
Configurable Data

- **Admin Mode** - Select enable or disable from the pulldown menu. If you select enable the router will process and forward *mtrace* requests received from other routers, otherwise received *mtrace* requests will be discarded. This field is non-configurable for read-only users.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.4.6 Mtrace Run



Mtrace Run

Source IP: 192.168.101.1

Receiver IP: 192.168.100.100

Group IP: 239.2.3.4

Figure 4-6-73 Mtrace Run

Use this screen to initiate an mtrace command on the router. You can use the mtrace command trace the path from the source to a destination branch for a multicast distribution tree.

Configurable Data

- **Source Address** - Enter the IP address of a multicast-capable source. This is the unicast address of the beginning of the path to be traced.

- **Receiver Address** - Enter the IP address of the host to which the *mtrace* response will be sent by the last hop router. If you leave this field blank, *mtrace* will use the IP address of the router interface through which the *mtrace* will be sent.

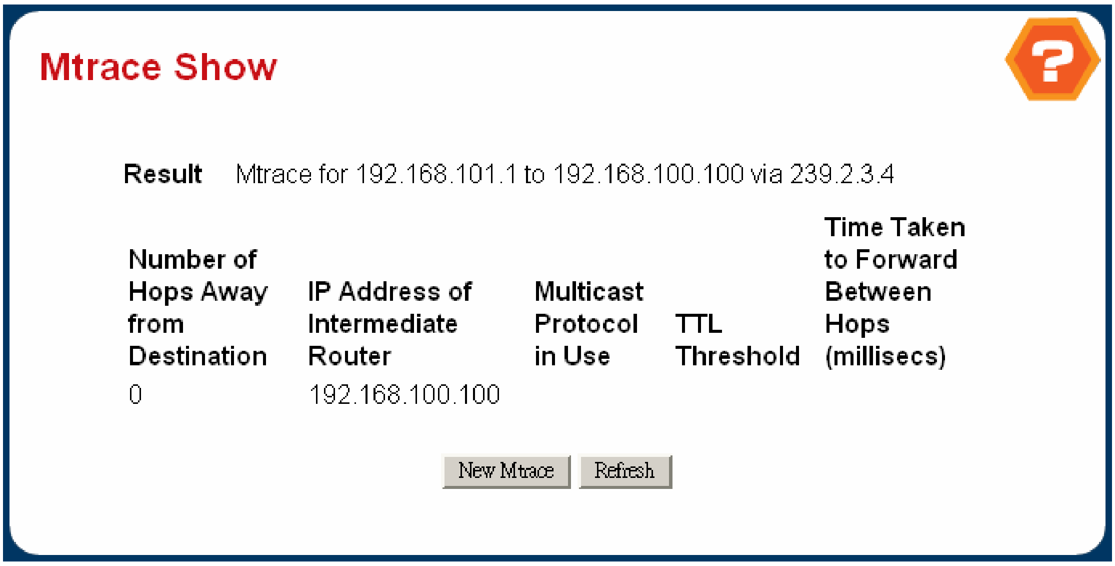
- **Group Address** - Enter the Multicast address of the group to be traced. If you do not enter a valid address, multicast address 224.2.0.1 will be used. Valid addresses are 224.0.0.0 through 239.255.255.255.

Command Buttons

- **Submit** - Initiate the *mtrace* command on the router. If the *mtrace* command completes successfully the browser will display the Mtrace Show screen. If the *mtrace* command fails, you will see the Mtrace Run screen again.

4.7.4.7 Mtrace Show

This screen displays the results of an mtrace command. The mtrace command is used to trace the path from source to a destination branch for a multicast distribution tree.



Mtrace Show

Result Mtrace for 192.168.101.1 to 192.168.100.100 via 239.2.3.4

Number of Hops Away from Destination	IP Address of Intermediate Router	Multicast Protocol in Use	TTL Threshold	Time Taken to Forward Between Hops (millisecs)
0	192.168.100.100			

Figure 4-6-74 Mtrace Show

Non-Configurable Data

- **Number of hops away from destination** - The number of hops away from the destination.
- **IP address of intermediate router** - The IP address of the intermediate router in the path being traced between source and destination for the hop number in the previous field.
- **Multicast Protocol in use** - The multicast protocol in use on this hop.
- **TTL Threshold** - The time-to-live threshold on this hop.
- **Time taken to forward between hops** - The time taken for the trace request to be forwarded from the previous hop to this hop.

Command Buttons

- **New Mtrace** - Redirect the web browser to the Mtrace Run screen so that you can initiate another *mtrace* command.
- **Refresh** - Refresh the content of the screen with the latest data available on the router. Typically, it takes around 20 seconds to process the results after initiating *mtrace* command. You must refresh the screen to display the latest results.

4.7.5 PIM-DM

Dense mode PIM initiates forwarding state in routers when a source begins to send. A source does not give any prior notifications to the network when it sends multicast datagrams to a group G. If a receiving router does not already have a forwarding entry, it creates it for the source and group G. This forwarding entry is called a (S,G) entry. It includes the following contents: source address, group address, the incoming interface, a list of outgoing interfaces, a few flags and a few timers. The incoming interface for (S,G) is determined by an RPF lookup in the unicast routing table. The (S,G) outgoing interface list contains interfaces that have PIM routers present or host members for group G.
If a router creates a (S,G) entry with an empty outgoing interface list after receiving a multicast datagram, it must trigger a PIM-Prune message toward the source S. This type of entry is called a negative cache entry. Negative cache entries can be found on leaf routers with no local group members, or on routers where prune messages were received from downstream routers that caused the outgoing interface list to become NULL.

Dense mode PIM routers send periodic Hello messages out of each interface and keep track of neighbors based on received Hello messages. The Hello message has a Holdtime field that tells the neighbor to delete neighbor information if it is not refreshed before expiration.

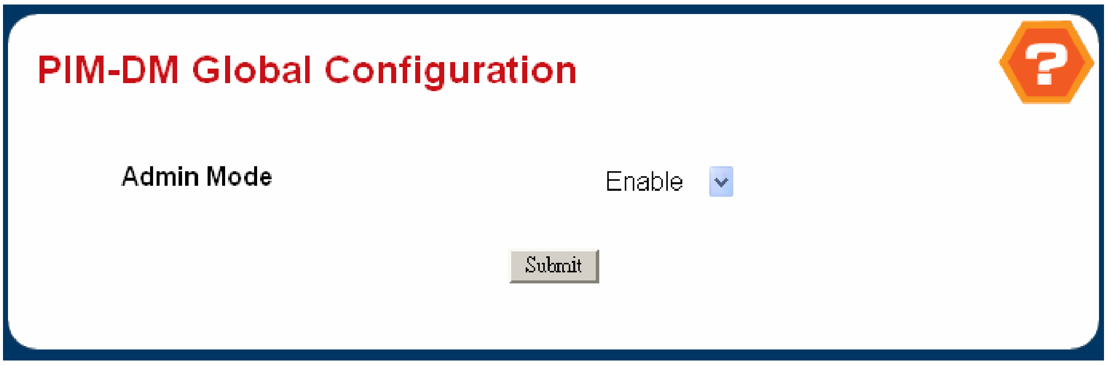
Dense-mode PIM assumes that when a source starts sending, all downstream systems want to receive multicast datagrams. Initially, multicast datagrams are flooded to all areas of the network. If some areas of the network do not have group members, dense-mode PIM will prune off the forwarding branch by setting up prune state. The prune state has an associated timer, hich on expiration will turn into forward state, allowing data to go down the branch previously in prune state.

The prune state contains source and group address information. When a new member appears in a pruned area, a router can ``graft'' toward the source for the group, turning the pruned branch into forward state. The forwarding branches form a tree rooted at the source leading to all members of the group. This tree is called a source rooted tree.

The broadcast of datagrams followed by pruning of unwanted branches is often referred to as a broadcast-and-prune cycle, typical of dense mode protocols. The broadcast-and-prune mechanism in dense mode PIM uses a technique called reverse path forwarding (RPF), in which a multicast datagram is forwarded if the receiving interface is the one used to forward unicast datagrams to the source of the datagram.

Compared with multicast routing protocols with built-in topology discovery mechanisms (e.g. DVMRP with its own RIP-like ``unicast'' routing protocol), dense mode PIM has simplified design, and is not hard-wired into a specific type of topology discovery protocol. However, such simplification does incur more overhead and cause broadcast-and-prune to occur on some links that could be avoided if sufficient topology information is available, e.g. to decide whether each interface leads to any downstream neighbors for a particular source. We chose to accept the additional overhead in favor of the simplification and flexibility gained by not depending on a specific type of topology discovery protocol.

4.7.5.1 PIM-DM Global Configuration


PIM-DM Global Configuration

Admin Mode: Enable

Figure 4-6-75 PIM-DM Global Configuration

Configurable Data

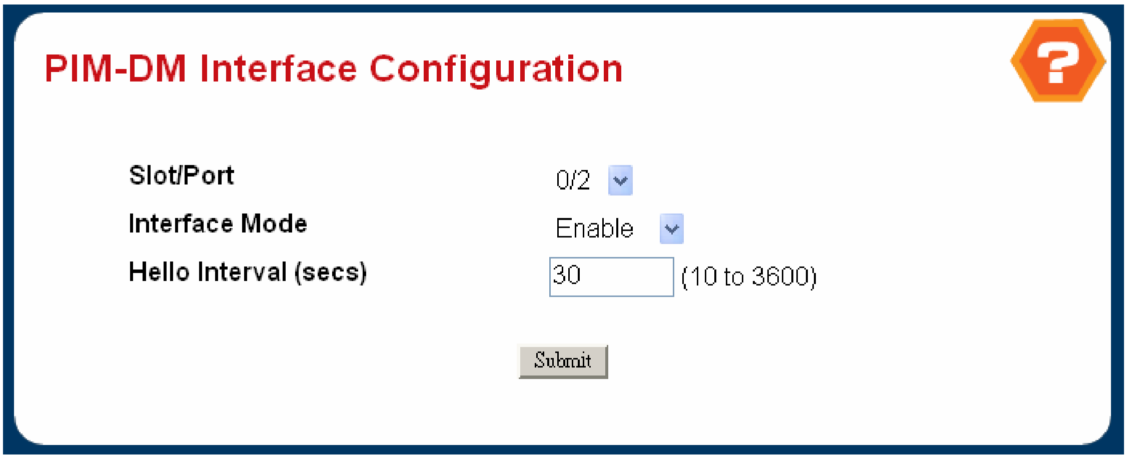
- **Admin Mode** - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM in the router. The default is disable.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Note: Only one multicast routing protocol could be enabled at one time. That means, for example, once the PIM-DM admin mode is enabled, the user is not able to enable the DVMRP.

4.7.5.2 Help for PIM-DM Interface Configuration


PIM-DM Interface Configuration

Slot/Port: 0/2

Interface Mode: Enable

Hello Interval (secs): 30 (10 to 3600)

Figure 4-6-76 PIM-DM Interface Configuation

Selection Criteria

- **Slot/Port** - Select the Slot and port for which data is to be displayed or configured. Slot 0 is the base unit. You must have configured at least one router interface before configuring or displaying data for a PIM-DM interface, otherwise an error message will be displayed.

Configurable Data

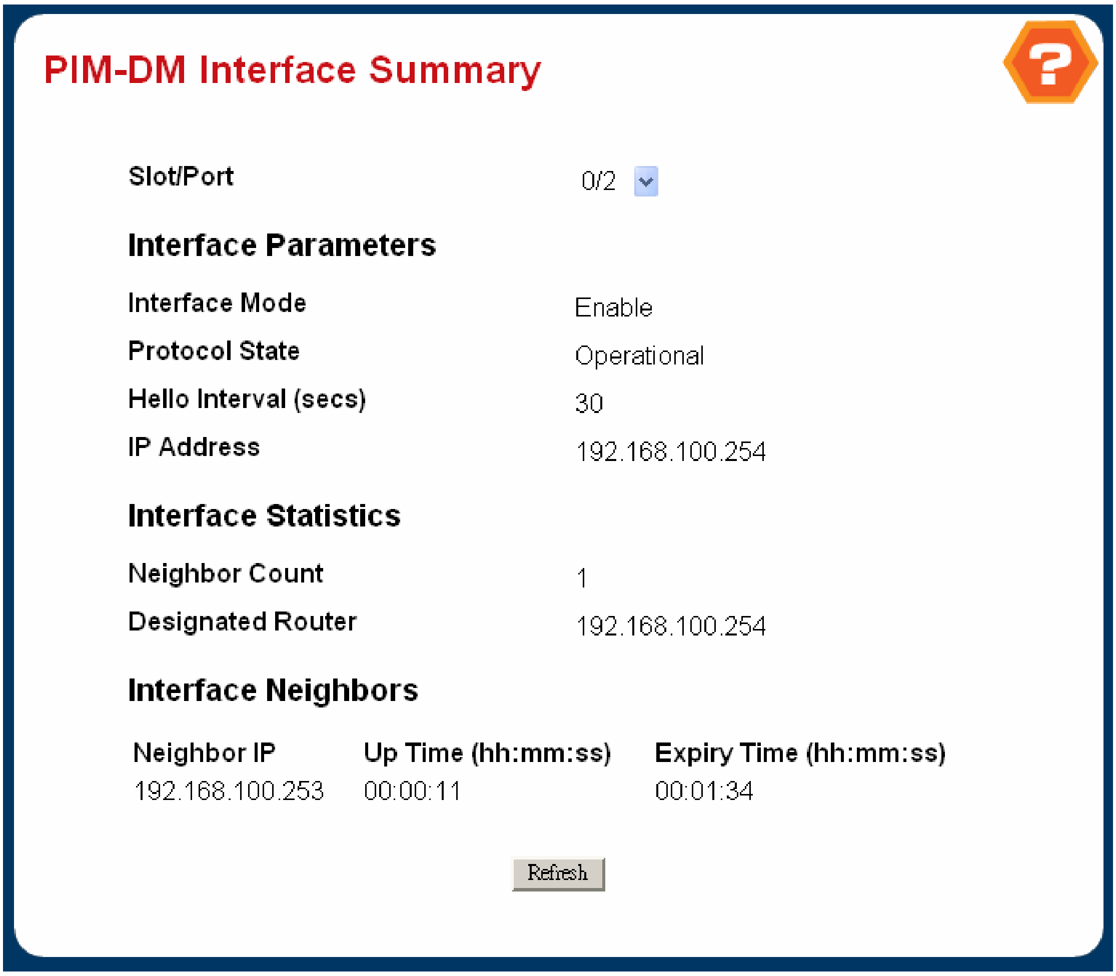
- **Interface Mode** - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM for the selected interface. The default is disable.

- **Hello Interval** - Enter the number of seconds between PIM hello messages transmitted from the selected interface. The default value is 30. Valid values are from (10 to 3600) .

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.5.3 Help for PIM-DM Interface Summary



PIM-DM Interface Summary

Slot/Port 0/2

Interface Parameters

Interface Mode Enable

Protocol State Operational

Hello Interval (secs) 30

IP Address 192.168.100.254

Interface Statistics

Neighbor Count 1

Designated Router 192.168.100.254

Interface Neighbors

Neighbor IP	Up Time (hh:mm:ss)	Expiry Time (hh:mm:ss)
192.168.100.253	00:00:11	00:01:34

Figure 4-6-77 PIM-DM Interfaces Summary

Selection Criteria

- **Slot/Port** - Select the physical interface for which data is to be displayed. There must be configured at least one router interface before displaying data for a PIM-DM interface, otherwise a message will be displayed.

Non-Configurable Data

- **Interface Mode** - Displays the administrative status of PIM-DM for the selected interface. The default is disable.
- **Protocol State** - The operational state of the PIM-DM protocol on this interface.
- **Hello Interval** - The frequency at which PIM hello messages are transmitted on the selected interface.
- **IP Address** - The IP address of the selected interface.
- **Neighbor Count** - The number of PIM neighbors on the selected interface.
- **Designated Router** - The designated router on the selected PIM interface. For point- to-point interfaces, this will be 0.0.0.0.
- **Neighbor IP** - The IP address of the PIM neighbor for which this entry contains information.
- **Uptime** - The time since this PIM neighbor (last) became a neighbor of the local router.
- **Expiry Time** - The minimum time remaining before this PIM neighbor will be aged out.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

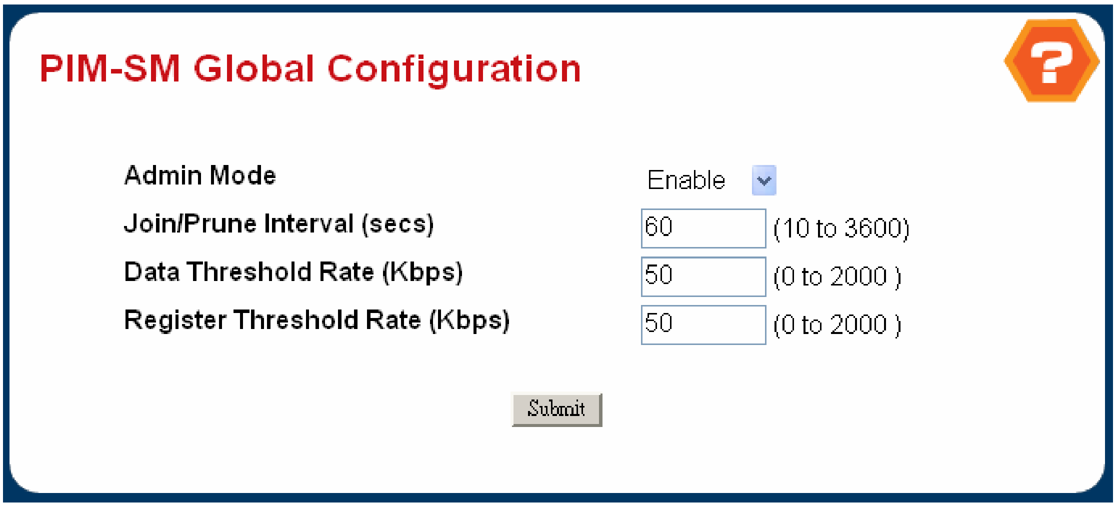
4.7.6 PIM-SM

Protocol Independent Multicast--Sparse Mode (PIM-SM)

A router receives explicit Join/Prune messages from those neighboring routers that have downstream group members. The router then forwards data packets addressed to a multicast group, G, only onto those interfaces on which explicit joins have been received. Note that all routers mentioned in this document are assumed to be PIM-SM capable, unless otherwise specified.

A Designated Router (DR) sends periodic Join/Prune messages toward a group-specific Rendezvous Point (RP) for each group for which it has active members. Each router along the path toward the RP builds a wildcard (any-source) state for the group and sends Join/Prune messages on toward the RP. We use the term route entry to refer to the state maintained in a router to represent the distribution tree. A route entry may include such fields as the source address, the group address, the incoming interface from which packets are accepted, the list of outgoing interfaces to which packets are sent, timers, flag bits, etc. The wildcard route entry's incoming interface points toward the RP; the outgoing interfaces point to the neighboring downstream routers that have sent Join/Prune messages toward the RP. This state creates a shared, RP-centered, distribution tree that reaches all group members. When a data source first sends to a group, its DR unicasts Register messages to the RP with the source's data packets encapsulated within. If the data rate is high, the RP can send source-specific Join/Prune messages back towards the source and the source's data packets will follow the resulting forwarding state and travel unencapsulated to the RP. Whether they arrive encapsulated or natively, the RP forwards the source's decapsulated data packets down the RP-centered distribution tree toward group members. If the data rate warrants it, routers with local receivers can join a source-specific, shortest path, distribution tree, and prune this source's packets off of the shared RP-centered tree. For low data rate sources, neither the RP, nor last-hop routers need join a source-specific shortest path tree and data packets can be delivered via the shared, RP-tree. Protocol Independent Multicasting - Sparse Mode (PIM-SM) Protocol Help

4.7.6.1 PIM-SM Global Configuration



PIM-SM Global Configuration

Admin Mode	Enable	
Join/Prune Interval (secs)	60	(10 to 3600)
Data Threshold Rate (Kbps)	50	(0 to 2000)
Register Threshold Rate (Kbps)	50	(0 to 2000)

Figure 4-6-78 PIM-SM Global Configuration

Configurable Data

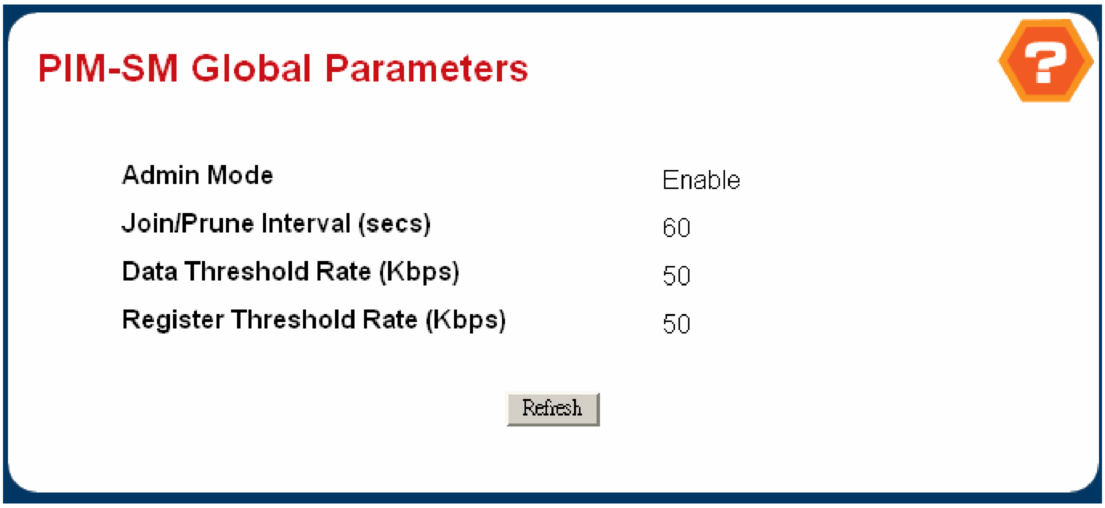
- **PIMSM Admin Mode** - Select enable or disable from the pulldown menu to set the administrative status of PIM-SM in the router. You must enable IGMP before enabling PIM-SM. The default is disable.
- **Join/Prune Interval** - Enter the interval between the transmission of PIM-SM Join/Prune messages. The valid values are from (10 to 3600 secs). The default value is 60.
- **Data Threshold Rate** - Enter the minimum source data rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. The valid values are from (0 to 2000 K bits/sec) . The default value is 50.
- **Register Threshold Rate** - Enter the minimum source data rate in K bits/second above which the Rendezvous Point router will switch to a source-specific shortest path tree. The valid values are from (0 to 2000 K bits/sec) . The default value is 50.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Note: Only one multicast routing protocol could be enabled at one time. That means, for example, once the PIM-DM admin mode is enabled, the user is not able to enable the DVMRP.

4.7.6.2 PIM-SM Global Parameters



PIM-SM Global Parameters

Admin Mode	Enable
Join/Prune Interval (secs)	60
Data Threshold Rate (Kbps)	50
Register Threshold Rate (Kbps)	50

Figure 4-6-79 PIM-SM Global Parameters

Non-Configurable Data

- **PIMSM Admin Mode** - The administrative status of PIM-SM in the router: either enable or disable.

- **Join/Prune Interval** - The interval between the transmission of PIM-SM Join/Prune messages.

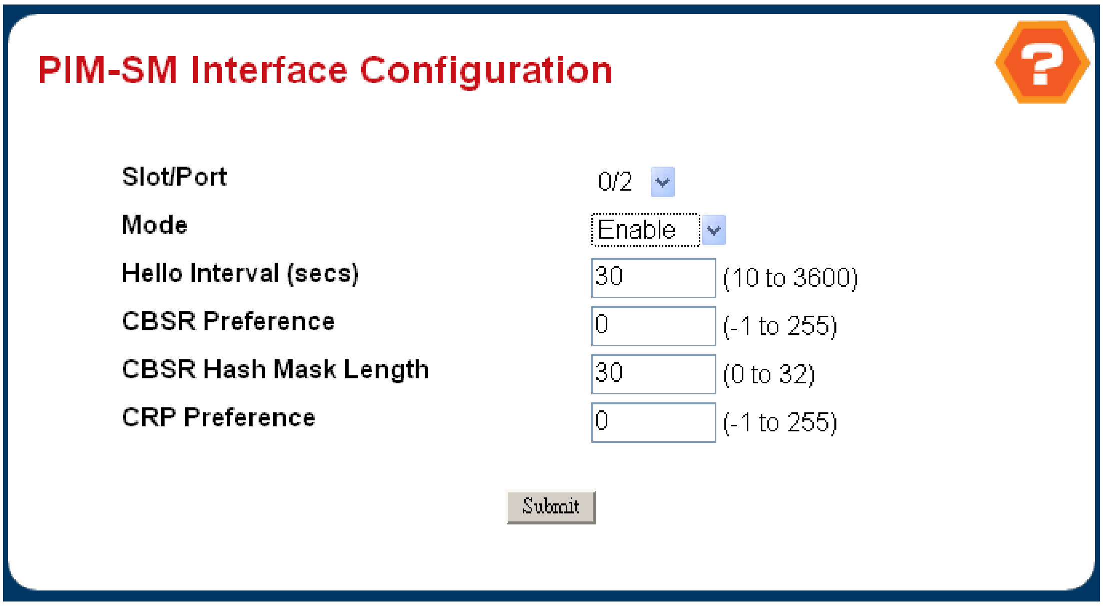
- **Data Threshold Rate** - The minimum source data rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree.

- **Register Threshold Rate** - The minimum source data rate in K bits/second above which the Rendezvous Point router will switch to a source-specific shortest path tree.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.6.3 PIM-SM Interface Configuration



PIM-SM Interface Configuration

Slot/Port	0/2	
Mode	Enable	
Hello Interval (secs)	30	(10 to 3600)
CBSR Preference	0	(-1 to 255)
CBSR Hash Mask Length	30	(0 to 32)
CRP Preference	0	(-1 to 255)

Figure 4-6-80 PIM-SM Interface Configuration

Selection Criteria

- **Slot/Port** - Select the slot and port for which data is to be displayed or configured. Slot 0 is the base unit.

Configurable Data

- **Mode** - Select enable or disable from the pulldown menu to set the administrative status of PIM-SM in the router. The default is disable.

- **Hello Interval** - Enter the time in seconds between the transmission of which PIM Hello messages on this interface. The valid values are from (10 to 3600 secs) . The default value is 30.

- **CBSR Preference** - Enter the preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface. The valid values are from (-1 to 255) The default value is 0.

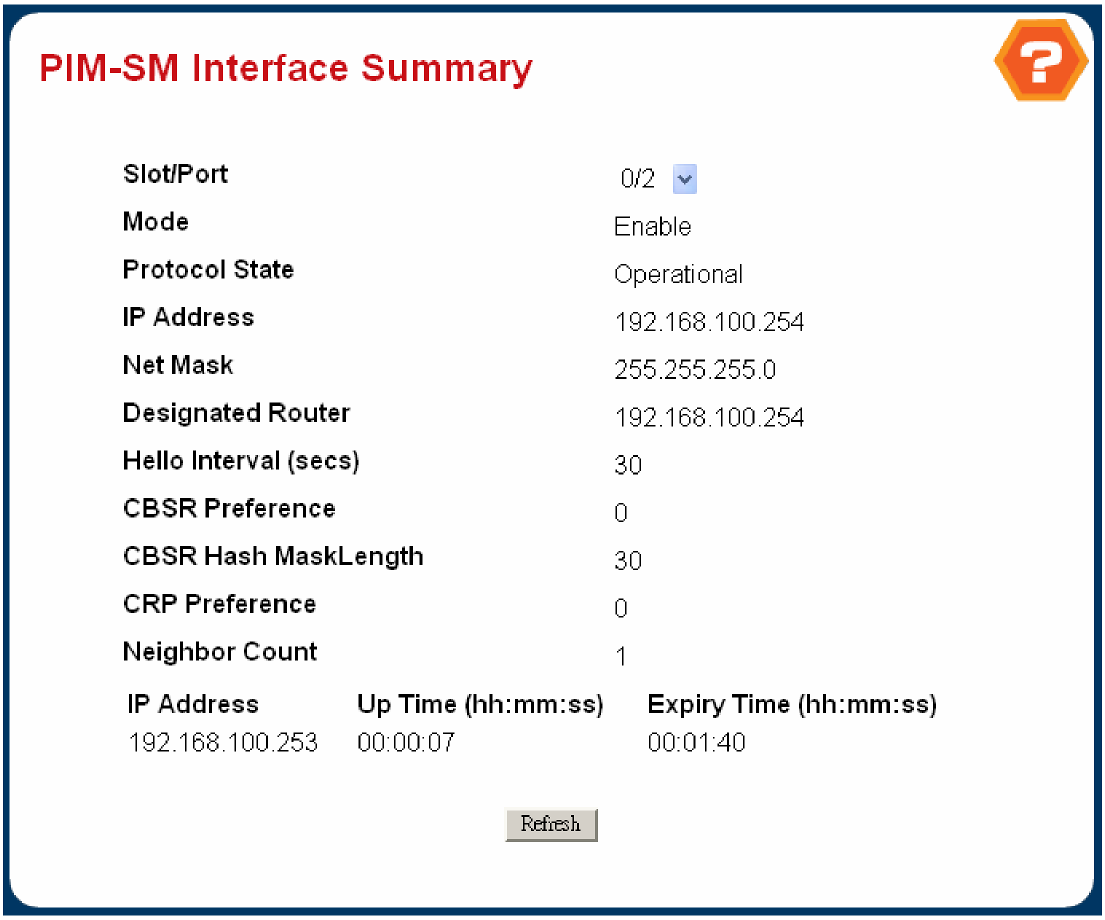
- **CBSR Hash Mask Length** - Enter the CBSR hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from (0 to 32). The default value is 30.

- **CRP Preference** - Enter the preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface. The valid values are from (-1 to 255). The default value is 0.

Command Buttons

- **Submit** - Send the updated configuration to the router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

4.7.6.4 PIM-SM Interface Summary



PIM-SM Interface Summary

Slot/Port	0/2
Mode	Enable
Protocol State	Operational
IP Address	192.168.100.254
Net Mask	255.255.255.0
Designated Router	192.168.100.254
Hello Interval (secs)	30
CBSR Preference	0
CBSR Hash MaskLength	30
CRP Preference	0
Neighbor Count	1

IP Address	Up Time (hh:mm:ss)	Expiry Time (hh:mm:ss)
192.168.100.253	00:00:07	00:01:40

Figure 4-6-81 PIM-SM Interface Summary

Selection Criteria

- **Slot/Port** - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Non-Configurable Data

- **Mode** - The administrative status of PIM-SM in the router: either enable or disable.
- **IP Address** - The IP address of the selected PIM interface.
- **Net Mask** - The network mask for the IP address of the selected PIM interface.
- **Designated Router** - The Designated Router on the selected PIM interface. For point-to- point interfaces, this object has the value 0.0.0.0.
- **Hello Interval** - The frequency at which PIM Hello messages are transmitted on the selected interface.

- **CBSR Preference** - The preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface.

- **CBSR Hash Mask Length** - The CBSR hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group.

- **CRP Preference** - The preference value for the local interface as a candidate bootstrap router. The value of -1 is used to indicate that the local interface is not a candidate BSR interface.

- **Neighbor Count** - The number of PIM neighbors on the selected interface.

- **IP Address** - The IP address of the PIM neighbor for this entry.

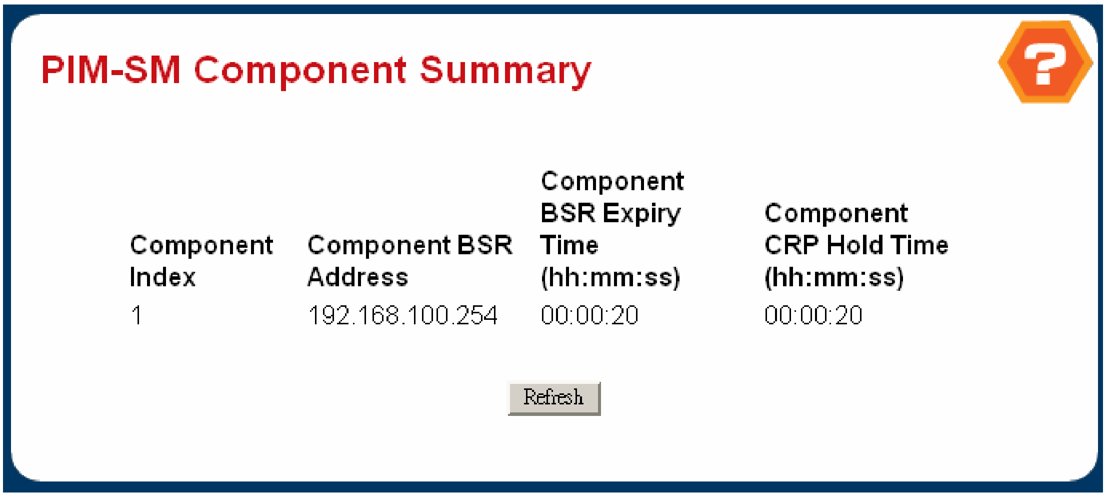
- **Up Time** - The time since this PIM neighbor (last) became a neighbor of the local router.

- **Expiry Time** - The minimum time remaining before this PIM neighbor will be aged out.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.6.5 PIM-SM Component Summary



PIM-SM Component Summary

Component Index	Component BSR Address	Component BSR Expiry Time (hh:mm:ss)	Component CRP Hold Time (hh:mm:ss)
1	192.168.100.254	00:00:20	00:00:20

Figure 4-6-82 PIM-SM Component Summary

Non-Configurable Data

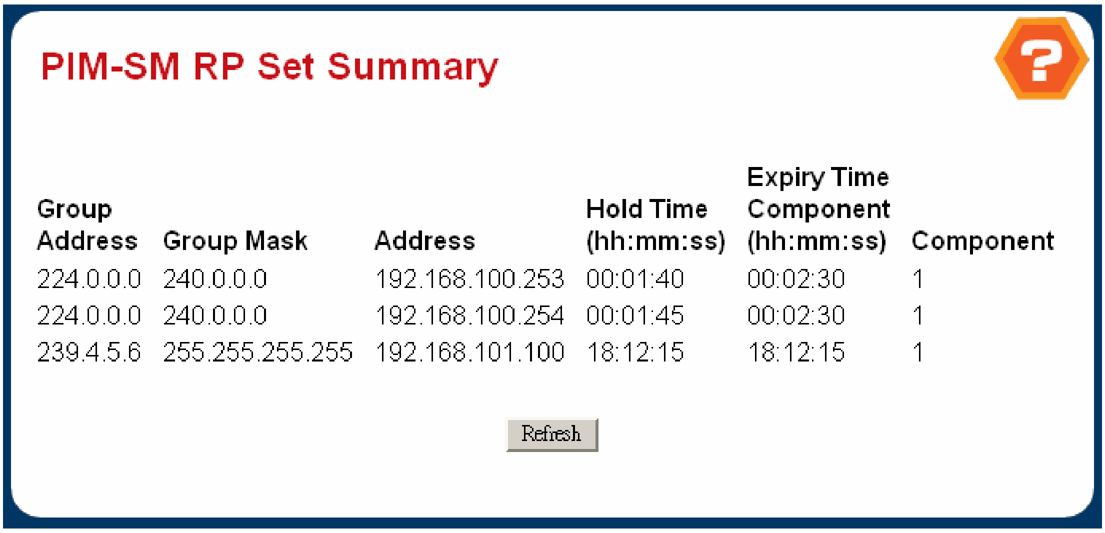
- **Component Index** - Unique number identifying the component index.

- **Component BSR Address** - Displays the IP address of the bootstrap router (BSR) for the local PIM region.
- **Component BSR Expiry Time** - Displays the minimum time remaining before the bootstrap router in the local domain will be declared.
- **Component CRP Hold Time** - The hold time of the component when it is a candidate Rendezvous Point in the local domain.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.6.6 PIM-SM RP Set Summary



PIM-SM RP Set Summary

Group Address	Group Mask	Address	Hold Time (hh:mm:ss)	Expiry Time Component (hh:mm:ss)	Component
224.0.0.0	240.0.0.0	192.168.100.253	00:01:40	00:02:30	1
224.0.0.0	240.0.0.0	192.168.100.254	00:01:45	00:02:30	1
239.4.5.6	255.255.255.255	192.168.101.100	18:12:15	18:12:15	1

Figure 4-6-83 PIM-SM RP Set Summary

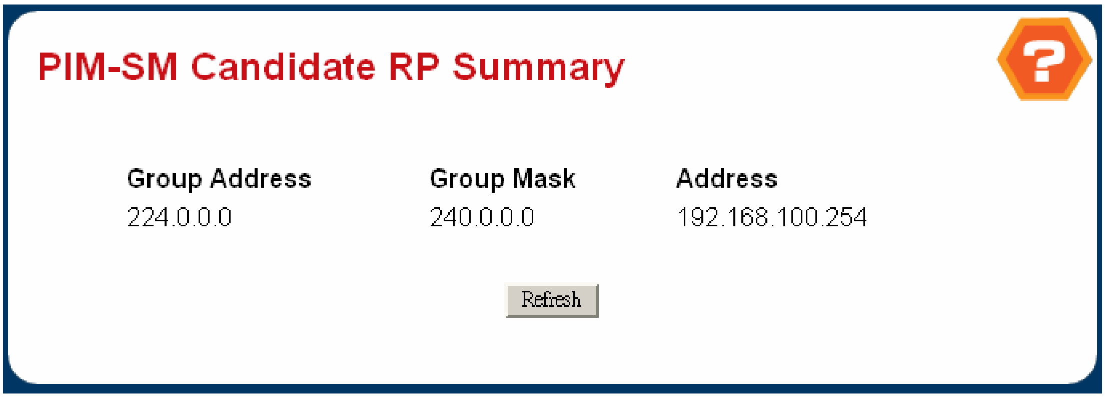
Non-Configurable Data

- **Group Address** - Displays IP multicast group address.
- **Group Mask** - Displays Multicast group address mask.
- **Address** - Displays IP address of the Candidate-RP.
- **Hold Time** - The holdtime of a Candidate-RP.If the local router is not the BSR, this value is 0.
- **Expiry Time Component** - The minimum time remaining before the Candidate-RP will be declared.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.6.7 PIM-SM Candidate RP Summary



PIM-SM Candidate RP Summary

Group Address	Group Mask	Address
224.0.0.0	240.0.0.0	192.168.100.254

Figure 4-6-84 PIM-SM Candidate RP Summary

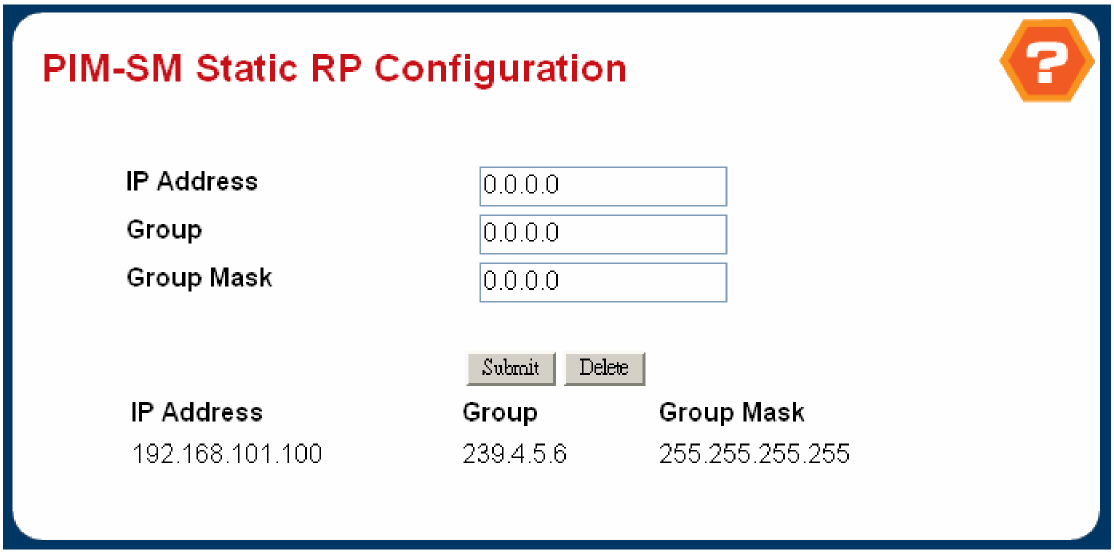
Non-Configurable Data

- **Group Address** - The group address transmitted in Candidate-RP-Advertisements.
- **Group Mask** - The group address mask transmitted in Candidate-RP-Advertisements to fully identify the scope of the group which the router will support if elected as a Rendezvous Point.
- **Address** - Displays the unicast address of the interface which will be advertised as a Candidate RP.

Command Buttons

- **Refresh** - Refresh the data on the screen with the present state of the data in the router.

4.7.6.8 PIM-SM Static RP Configuration



PIM-SM Static RP Configuration

IP Address	0.0.0.0
Group	0.0.0.0
Group Mask	0.0.0.0

IP Address	Group	Group Mask
192.168.101.100	239.4.5.6	255.255.255.255

Figure 4-6-85 PIM-SM Static RP Configuation

Configurable Data

- **IP Address** - IP Address of the RP to be created or deleted.
- **Group** - Group Address of the RP to be created or deleted.
- **Group Mask** - Group Mask of the RP to be created or deleted.

Command Buttons

- **Submit** - Attempts to create the specified static RP IP Address for the PIM-SM router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.
- **Delete** - Attempts to remove the specified static RP IP Address for the PIM-SM router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

5. COMMAND STRUCTURE

The Command Line Interface (CLI) syntax, conventions and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

5.1 Format

Commands are followed by values, parameters, or both.

Example 1

network parms <ipaddr> <netmask> [<gateway>]

- **network parms** is the command name.
- **<ipaddr> <netmask>** are the required values for the command.
- **[<gateway>]** is the optional value for the command

Example 2

snmp-server location <loc>

- **snmp-server location** is the command name.
- **<loc>** is the required parameter for the command.

Example 3

clear vlan

- **clear vlan** is the command name.

5.1.1 Command

The text in bold, non-italic font must be typed exactly as shown.

5.1.2 Parameters

Parameters are order dependent.

The text in bold italics should be replaced with a name or number. To use spaces as part of a name parameter, enclose it in double quotes like this: "System Name with Spaces".

Parameters may be mandatory values, optional values, choices, or a combination.

- **<parameter>**. The <> angle brackets indicate that a mandatory parameter must be entered in place of the brackets and text inside them.
- **[parameter]**. The [] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
- **choice1 | choice2**. The | indicates that only one of the parameters should be entered.
- The **{}** curly braces indicate that a parameter must be chosen from the list of choices.

5.1.3 Values

ipaddr This parameter is a valid IP address, made up of four decimal bytes ranging from 0 to 255. The default for all IP parameters consists of zeros (that is, 0.0.0.1). The interface IP address of 0.0.0.0 is invalid. In some cases, the IP address can also be entered as a 32-bit number.

macaddr The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

areaid Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network number of the sub-netted network may be used for the area ID.

slot/port This parameter denotes a valid slot number and a valid port number. For example, 0/1 represents slot number 0 and port number 1. The <slot/port> field is composed of a valid slot number and a valid port number separated by a forward slash (/).

logical slot/port This parameter denotes a logical slot number and logical port number assigned. This is applicable in the case of a port-channel (LAG). The operator can use the logical slot number and the logical port number to configure the port-channel.

5.1.4 Conventions

1. Network addresses are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:
2. Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.
3. Empty strings ("") are not valid user defined strings.
4. Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> or <space bar> (command completion).

Address Type	Format	Range
ipaddr	A.B.C.D	0.0.0.0 to 255.255.255.255 (decimal)
macaddr	YY:YY:YY:YY:YY:YY:	hexidecimal digit pairs

Table 4-1 Network Address Syntax

5. The value 'Err' designates that the requested value was not internally accessible. This should never happen and indicates that there is a case in the software that is not handled correctly.
6. The value of '-----' designates that the value is unknown.

5.1.5 Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point ('!') character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character '!' is recognized as a comment line and ignored by the parser. Some examples are provided below:

```
! Script file for displaying the ip interface
! Display information about interfaces
show ip interface 0/1 !Displays the information about the first interface
! Display information about the next interface
show ip interface 0/2
! End of the script file
```

6. QUICK START UP

The CLI Quick Start up details procedures to quickly become acquainted with the software.

6.1 Quick Starting the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the software locally or from a remote workstation. The device must be configured with IP information (IP address, subnet mask, and default gateway).
2. Turn the Power ON.
3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
4. When the prompt asks for operator login, execute the following steps:
   - Type the word **"admin"** in the login area. Since a number of the Quick Setup commands require administrator account rights, we suggest logging into an administrator account.
   - Do not enter a password because there is no password in the default mode.
   - Press the enter key two times.
   - The CLI User EXEC prompt will be displayed.
   - Use **"enable"** to switch to the Privileged EXEC mode from User EXEC.
   - Use **"configure"** to switch to the Global Config mode from Privileged EXEC.
   - Use **"exit"** to return to the previous mode.

6.2 System Info and System Setup

Quick Start up Software Version Information.

Command	Details
show hardware **(in Privileged EXEC)**	Allows the user to see the software version the device contains
	Machine Model (The type and number of ports the device provides.)
	For example: Machine Model…………. 24+2G 24 = 24 10/100 ports 02 = 2 Uplink ports on back of switch

Table 5-1 Quick Start up Software Version Information.

Quick Star up Physical Port Data.

Command	Details
Show port all **(in Privileged EXEC)**	Displays the Ports
	slot/port

	Type - Indicates if the port is a special type of port
	Admin Mode - Selects the Port Control Administration State
	Physical Mode - Selects the desired port speed and duplex mode
	Physical Status - Indicates the port speed and duplex mode
	Link Status - Indicates whether the link is up or down
	Link Trap - Determines whether or not to send a trap when link status changes
	LACP Mode - Displays whether LACP is enabled or disabled on this port

Table 5-2 Quick Star up Physical Port Data.

Quick Start up Account Management

Command	Details
show users **(in Privileged EXEC)**	Displays all of the users that are allowed to access the switch
	Access Mode - Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view then (Read Only). As a factory default, the ‘admin’ user has Read/Write access and the ‘guest’ user has Read Only access. There can only be one Read/Write user and up to five Read Only users.
show loginsession **(in User EXEC)**	Displays all of the login session information
users passwd <*username*> **(in Global Config)**	Allows the user to set passwords or change passwords needed to login A prompt will appear after the command is entered requesting the users old password. In the absence of an old password leave the area blank. The operator must press enter to execute the command. The system then prompts the user for a new password then a prompt to confirm the new password. If the new password and the confirmed password match a message will be displayed. User password should not be more than eight characters in length.
copy system:running-config nvram:startup-config **(in Privileged EXEC)**	This will save passwords and all other changes to the device. If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset
logout **(in User EXEC and Privileged EXEC)**	Logs the user out of the switch

Table 5-3 Quick Start up Account Management

Quick Start up IP Address

To view the network parameters the operator can access the device by the following three methods.

- Simple Network Management Protocol - SNMP
- Telnet
- Web Browser

✍ **Note:** Helpful Hint: The user should do a **"copy system:running-config nvram:startup-config"** after configuring the network parameters so that the configurations are not lost

Command	Details
show network **(in User EXEC)**	Displays the Network Configurations
	IP Address - IP Address of the interface Default IP is 0.0.0.0
	Subnet Mask - IP Subnet Mask for the interface Default is 0.0.0.0
	Default Gateway - The default Gateway for this interface Default value is 0.0.0.0
	Burned in MAC Address - The Burned in MAC Address used for in-band connectivity
	Locally Administered MAC Address - Can be configured to allow a locally administered MAC address
	MAC Address Type - Specifies which MAC address should be used for in-band connectivity
	Network Configurations Protocol Current - Indicates which network protocol is being used Default is none
	Management VLAN Id - Specifies VLAN id
	Web Mode - Indicates whether HTTP/Web is enabled.
	Java Mode - Indicates whether java mode is enabled.
network parms **(in Privileged EXEC)**	**network parms <ipaddr> *<netmask> [<gateway>]***
	IP Address range from 0.0.0.0 to 255.255.255.255
	Subnet Mask range from 0.0.0.0 to 255.255.255.255
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Table 5-4 Quick Start up IP Address

Quick Start up Uploading from Switch to Out-of-Band PC (Only XMODEM)

Command	Details
copy { ***nvram:startup-config |*** ***nvram:errorlog |*** ***nvram:msglog |*** ***nvram:traplog} <url>***	The types are: ▫ config - configuration file ▫ errorlog - error log ▫ system trace - system trace ▫ traplog - trap log The URL must be specified as: ▫ xmodem:filepath/fileName
	This starts the upload and also displays the mode of uploading and the type of upload it is and confirms the upload is taking place. **For example:** If the user is using HyperTerminal, the user must specify where the file is going to be received by the PC.

Table 5-4 Quick Start up Uploading from Switch to Out-of-Band PC (XMODEM)

Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)

Command	Details
copy <url> **{nvram:startup-config |** **system: image}**	Sets the destination (download) data type to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: xmodem:filepath/fileName
	For example: If the user is using HyperTerminal, the user must specify which file is to be sent to the switch. The Switch will restart automatically once the code has been downloaded.

Table 5-5 Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)

Quick Start up Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Start up for the IP Address.

Command	Details
copy <url> **{nvram:startup-config |** **system: image}**	Sets the destination (download) data type to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: tftp://ipAddr/filepath/fileName. The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.

Table 5-6 Quick Start up Downloading from TFTP Server

Quick Start up Factory Defaults

Command	Details

clear config	Enter yes when the prompt pops up to clear all the configurations made to the switch.
copy system:running-config nvram:startup-config	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
reload OR Cold Boot the Switch	Enter yes when the prompt pops up that asks if you want to reset the system. This is the users choice either reset the switch or cold boot the switch, both work effectively.

Table 5-7 Quick Start up Factory Defaults

7. MODE-BASED CLI

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

- User Exec Mode
- Privileged Exec Mode
- Global Config Mode
- Vlan Mode
- Interface Config Mode
- Line Config Mode
- Policy Map Mode
- Policy Class Mode
- Class Map Mode

The Command Mode table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User Exec Mode	This is the first level of access. Perform basic tasks and list system information.	(Switching) >	Enter Logout command
Privileged Exec Mode	From the User Exec Mode, enter the **enable** command.	(Switching) #	To exit this mode, enter exit or press Ctrl-Z.
VLAN Mode	From the Privileged User Exec mode, enter the **vlan database** command.	(Switching) (Vlan) #	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.
Global Config Mode	From the Privileged Exec mode, enter the **configure** command.	(Switching) (Config)#	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.
Interface Config Mode	From the Global Configuration mode, enter the **interface**	(Switching) (Interface-"if number")#	To exit to the Global Config mode enter exit. To return to user

	<slot/port> command		EXEC mode enter ctrl-Z.
Line Config Mode	From the Global Configuration mode, enter the **lineconfig** command.	(Switching) (line) #	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.
Policy Map Mode	From the Global Configuration mode, enter the **policy map <policy name> <in|out>** command.	(Switching) (Config-policy-map)#	To exit to the Global Config mode enter exit. To return to user EXEC mode enter ctrl-Z.
Policy Class Mode	From the Policy Map mode enter the **class-map <existed class-name>** command.	(Switching) (Config-policy-classmap)#	To exit to Policy Map mode enter exit. To return to User Exec mode enter ctrl-Z.
Class Map Mode	From the Global Config mode, enter the **class-map** command.	(Switching) (Config-classmap)#	To exit to Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.

Table 6-1 Command Mode

7.1 Mode-Based Topology

The CLI tree is built on a mode concept where the commands are available according to the interface. Some of the modes are depicted in the mode-based CLI Figure 12.

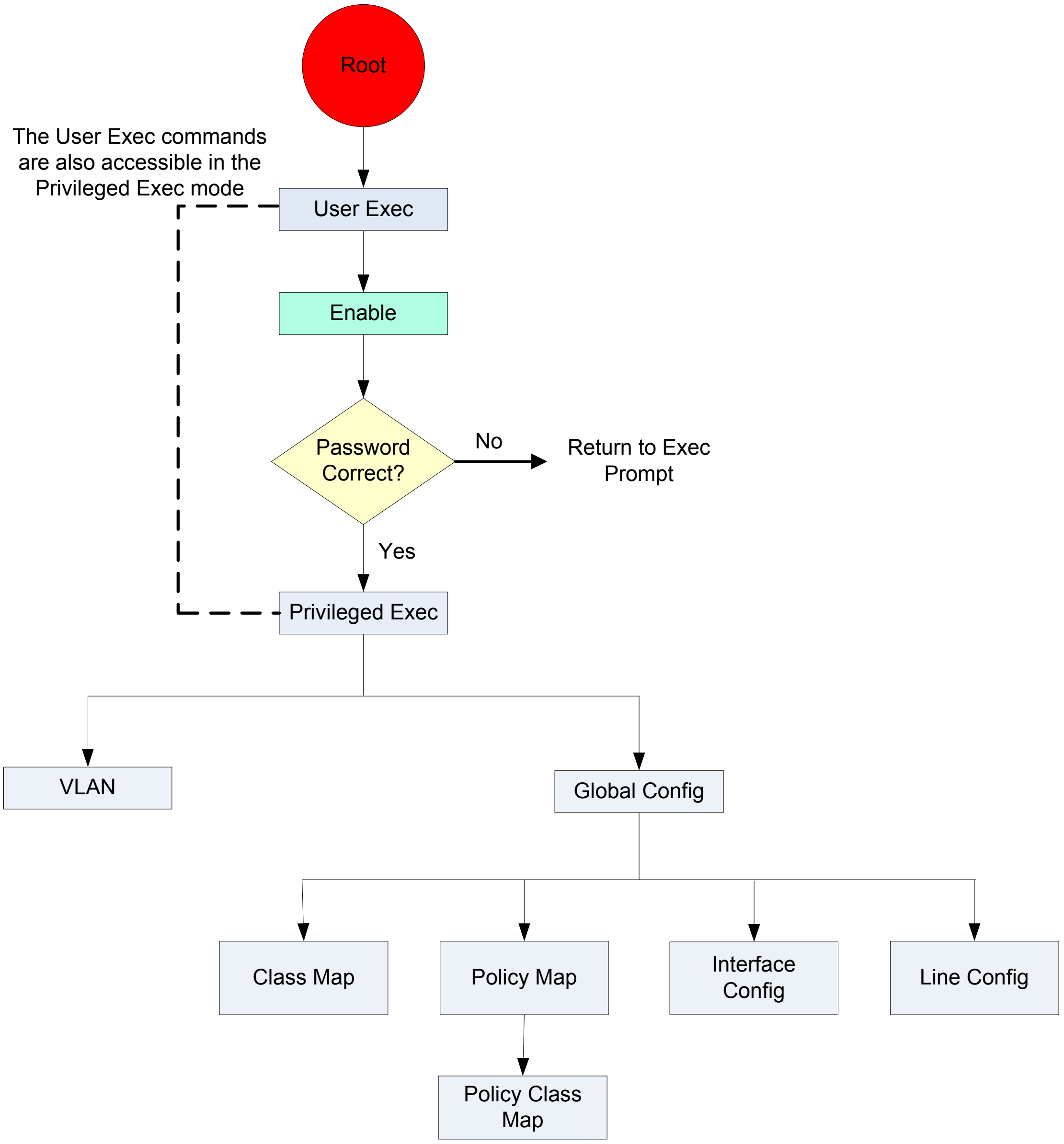


Figure 7-1 Mode-Based CLI

Accessing to all commands in the Privileged Exec mode and below is restricted through a password.

7.2 Mode-based Command Hierarchy

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands. The User Exec mode commands may also be executed in the Privileged Exec mode.

The commands available to the operator at any point in time depend upon the mode. Entering a question mark **"?"** at the CLI prompt, displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Exec Mode

When the operator logs into the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands. The command prompt shown at this level is:

```
Command Prompt: (Switching) >
```

Privileged Exec Mode

To have access to the full suite of commands, the operator must enter the Privileged Exec mode. The Privileged Exec mode requires password authentication. From Privileged Exec mode, the operator can issue any Exec command, enter the VLAN mode or enter the Global Configuration mode. The command prompt shown at this level is:

```
Command Prompt: (Switching) #
```

VLAN Mode

This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is:

```
Command Prompt: (Switching) (VLAN) #
```

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the System Configuration mode, the Physical Port Configuration mode, the Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:

```
Command Prompt: (Switching) (Config) #
```

From the Global Config mode, the operator may enter the following configuration modes:

Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface. In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands. The command prompt at this level is:

```
Command Prompt: (Switching) (Interface <slot/port>)#
```

The resulting prompt for the interface configuration command entered in the Global Configuration mode is shown below:

```
(Switching) (Config) # interface 2/1
(Switching) (Interface 2/1) #
```

Line Config Mode

This mode allows the operator to configure the console interface. The operator may configure the interface from the directly connected console or the virtual terminal used with Telnet. The command prompt at this level is:

```
Command Prompt: (Switching) (Line) #
```

Policy Map Mode

Use the policy-map <policy-name>command to access the QoS policy map configuration mode to configure the QoS policy map.

```
(Switching) (Config)# policy-map <policy-name>
```

```
Command Prompt: (Switching) (Config policy-map) #
```

Policy Class Mode

Use the class <class-name> command to access the QoS policy-classmap mode to attach/remove a diffserv class to a policy and to configure the QoS policy map.

```
(Switching) (Config-policy-map) # class <class-name>
Command Prompt: (Switching) (Config – policy-classmap) #
```

Class Map Mode:

This mode consists of class creation/deletion and matching commands. The class match commands specify layer 2, layer 3 and general match criteria. Use the class-map class-map-name commands to access the QoS class map configuration mode to configure QoS class maps.

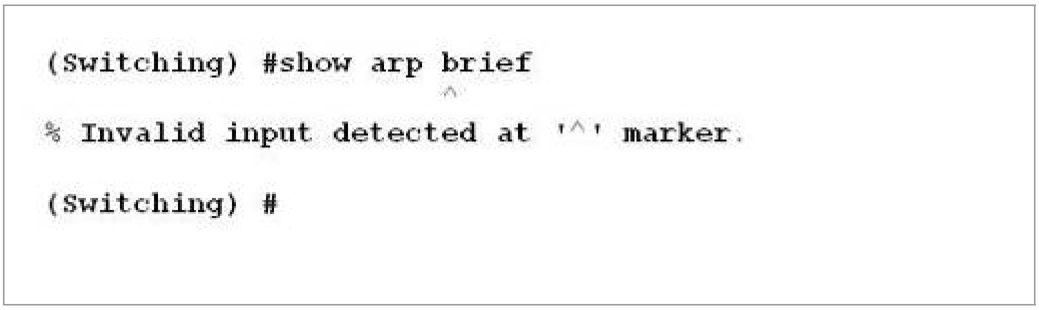
```
(Switching) (Config)# class map <class-map-name>
Command Prompt: (Switching) (Config - class) #
```

7.3 Flow of Operation

This section captures the flow of operation for the CLI:

1. The operator logs into the CLI session and enters the User Exec mode. In the User Exec mode the **“$(exec)>”** prompt is displayed on the screen.

   The parsing process is initiated whenever the operator types a command and presses <ENTER>. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, command node A has the command **"show arp brief"** but the operator attempts to execute the command **"show arpp brief"** then the output message would be **$(exec)> show arpp brief^. $%Invalid input detected at '^' marker**. If the operator has given an invalid input parameter in the command, then the message conveys to the operator an invalid input was detected. The layout of the output is depicted below:



```
(Switching) #show arp brief
                      ^
% Invalid input detected at '^' marker.

(Switching) #
```

   After all the mandatory parameters are entered, any additional parameters entered are treated as optional parameters. If any of the parameters are not recognized a syntax error message will be displayed.

2. After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.
3. For mandatory parameters, the command tree extends till the mandatory parameters make the leaf of the branch. The callback function is only invoked when all the mandatory parameters are provided. For optional parameters, the command tree extends till the mandatory parameters and the optional parameters make the leaf of the branch. However, the call back

function is associated with the node where the mandatory parameters are fetched. The call back function then takes care of the optional parameters.

4. Once the control has reached the callback function, the callback function has complete information about the parameters entered by the operator.

7.4 "No" Form of a Command

"No" is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the **"no"** form. The behavior and the support details of the **"no"** form is captured as part of the mapping sheets.

7.4.1 Support for "No" Form

Almost every configuration command has a **"no"** form. In general, use the no form to reverse the action of a command or reset a value back to the default. For example, the **"no shutdown interface”** configuration command reverses the shutdown of an interface. Use the command without the keyword no to re-enable a disabled feature or to enable a feature that is disabled by default.

7.4.2 Behavior of Command Help ("?")

The **"no"** form is treated as a specific form of an existing command and does not represent a new or distinct command. This implies that the behavior of the "?" and help text is the same for the **"no"** form:

- The help message is the same for all forms of the command. The help string may be augmented with details about the **"no"** form behavior.
- For the (no interface?) and (no inte?) cases of the **"?"**, the options displayed are identical to the case when the **"no"** token is not specified as in (interface) and (inte?).

8. CLI Commands: Base

This chapter provides detailed explanation of the Switching commands. The commands are divided into four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration Commands configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

This chapter includes the following configuration types:

- System information and statistics commands
- Management commands
- Device configuration commands
- User account management commands
- Security commands
- System utilities

8.1 System Information and Statistics Commands

8.1.1 show arp switch

This command displays connectivity between the switch and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the switch.

- **Format** show arp switch
- **Mode** Privileged EXEC
- **MAC Address** A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB
- **IP Address** The IP address assigned to each interface.
- **slot/port** A valid slot number and a valid port number.

8.1.2 show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

- **Format** show eventlog
- **Mode** Privileged EXEC
- **File** The file in which the event originated.
- **Line** The line number of the event.
- **Task Id** The task ID of the event.
- **Code** The event code.
- **Time** The time this event occurred.

✍ ***Note:*** Event log information is retained across a switch reset.

8.1.3 show hardware

This command displays inventory information for the switch.

- **Format** show hardware
- **Mode** Privileged EXEC
- **Switch Description** Text used to identify the product name of this switch.
- **Machine Type** Specifies the machine model as defined by the Vital Product Data.
- **Machine Model** Specifies the machine model as defined by the Vital Product Data.
- **Serial Number** The unique box serial number for this switch.
- **FRU Number** The field replaceable unit number.
- **Part Number** Manufacturing part number.
- **Maintenance Level** Indicates hardware changes that are significant to software.
- **Manufacturer** Manufacturer descriptor field.
- **Burned in MAC Address** Universally assigned network address.
- **Software Version** The release version number of the code currently running on the switch.
- **Operating System** The operating system currently running on the switch.
- **Network Processing Element** The type of the processor microcode.
- **Additional Packages** This displays the additional packages that are incorporated into this system, such as BGP-4, or Multicast.

8.1.4 show interface

This command displays a summary of statistics for a specific port or a count of all CPU traffic based upon the argument.

- **Format** show interface {<slot/port> | switchport}
- **Mode** Privileged EXEC

The display parameters when the argument is '<slot/port>' are as follows:

- **Packets Received Without Error** The total number of packets (including broadcast packets and multicast packets) received by the processor.
- **Packets Received With Error** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Broadcast Packets Received** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Packets Transmitted Without Error** The total number of packets transmitted out of the interface.
- **Transmit Packets Errors** The number of outbound packets that could not be transmitted because of errors.
- **Collisions Frames** The best estimate of the total number of collisions on this Ethernet segment.
- **Time Since Counters Last Cleared** The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.
- The display parameters when the argument is **'switchport'** are as follows:
- **Packets Received Without Error** The total number of packets (including broadcast packets and multicast packets)

received by the processor.

- **Broadcast Packets Received** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Packets Received With Error** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Packets Transmitted Without Error** The total number of packets transmitted out of the interface.
- **Broadcast Packets Transmitted** The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
- **Transmit Packet Errors** The number of outbound packets that could not be transmitted because of errors.
- **Address Entries Currently In Use** The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
- **VLAN Entries Currently In Use** The number of VLAN entries presently occupying the VLAN table.
- **Time Since Counters Last Cleared** The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

8.1.5 show interface ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

- **Format** show interface ethernet {<slot/port> | switchport}
- **Mode** Privileged EXEC

The display parameters when the argument is ' <slot/port>' is as follows:

Packets Received

- **Octets Received -** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.
- **Packets Received < 64 Octets -** The total number of packets (including bad packets) received that were < 64 octets in length (excluding framing bits but including FCS octets).
- **Packets Received 64 Octets -** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
- **Packets Received 65-127 Octets -** 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).
- **Packets Received 128-255 Octets -** 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).
- **Packets Received 256-511 Octets -** 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).
- **Packets Received 512-1023 Octets -** 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).
- **Packets Received 1024-1518 Octets -** 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).

- **Packets Received 1519-1522 Octets -** The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Received > 1522 Octets -** The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets Received Successfully

- **Total -** The total number of packets received that were without errors.
- **Unicast Packets Received -** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Multicast Packets Received -** The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
- **Broadcast Packets Received -** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received with MAC Errors

- **Total -** The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Jabbers Received -** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
- **Fragments/Undersize Received -** The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- **Alignment Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
- **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
- **Overruns -** The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Received Packets not forwarded

- **802.3x Pause Frames Received -** A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
- **Unacceptable Frame Type -** The number of frames discarded from this port due to being an unacceptable frame type.
- **VLAN Membership Mismatch -** The number of frames discarded on this port due to ingress filtering.
- **Total -** A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.
- **Local Traffic Frames -** The total number of frames dropped in the forwarding process because the destination address was located off of this port.
- **VLAN Viable Discards -** The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.
- **Multicast Tree Viable Discards -** The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

- **Reserved Address Discards -** The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
- **Broadcast Storm Recovery -** The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.
- **CFI Discards -** The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
- **Upstream Threshold -** The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Packets Transmitted Octets

- **Total Bytes -** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. -----
- **Packets Transmitted 64 Octets -** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
- **Packets Transmitted 65-127 Octets -** 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).
- **Packets Transmitted 128-255 Octets -** 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).
- **Packets Transmitted 256-511 Octets -** 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).
- **Packets Transmitted 512-1023 Octets -** 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).
- **Packets Transmitted 1024-1518 Octets -** 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).
- **Packets Transmitted 1519-1522 Octets -** The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
- **Max Info -** The maximum size of the Info (non-MAC) field that this port will receive or transmit.

Packets Transmitted Successfully

- **Total -** The number of frames that have been transmitted by this port to its segment.
- **Unicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Multicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
- **Broadcast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Errors

- **Total Errors -** The sum of Single, Multiple, and Excessive Collisions.
- **Tx FCS Errors -** The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of

octets

- **Oversized -** The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.
- **Underrun Errors -** The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards

- **Total Discards -** The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
- **Single Collision Frames -** A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
- **Multiple Collision Frames -** A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
- **Excessive Collisions -** A count of frames for which transmission on a particular interface fails due to excessive collisions.
- **Port Membership -** The number of frames discarded on egress for this port due to egress filtering being enabled.
- **VLAN Viable Discards -** The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Protocol Statistics

- **BPDU's received -** The count of BPDU's (Bridge Protocol Data Units) received in the spanning tree layer.
- **BPDU's Transmitted -** The count of BPDU's (Bridge Protocol Data Units) transmitted from the spanning tree layer.
- **802.3x Pause Frames Received -** A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
- **GVRP PDU's Received -** The count of GVRP PDU's received in the GARP layer.
- **GVRP PDU's Transmitted -** The count of GVRP PDU's transmitted from the GARP layer.
- **GVRP Failed Registrations -** The number of times attempted GVRP registrations could not be completed.
- **GMRP PDU's received -** The count of GMRP PDU's received in the GARP layer.
- **GMRP PDU's Transmitted -** The count of GMRP PDU's transmitted from the GARP layer.
- **GMRP Failed Registrations -** The number of times attempted GMRP registrations could not be completed.
- **STP BPDUs Transmitted -** Spanning Tree Protocol Bridge Protocol Data Units sent
- **STP BPDUs Received -** Spanning Tree Protocol Bridge Protocol Data Units received
- **RST BPDUs Transmitted -** Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
- **RSTP BPDUs Received -** Rapid Spanning Tree Protocol Bridge Protocol Data Units received
- **MSTP BPDUs Transmitted -** Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
- **MSTP BPDUs Received -** Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Dot1x Statistics

- **EAPOL Frames Received -** The number of valid EAPOL frames of any type that have been received by this authenticator.
- **EAPOL Frames Transmitted -** The number of EAPOL frames of any type that have been transmitted by this authenticator.
- **Time Since** - Counters Last Cleared The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters when the argument is **'switchport'** are as follows:

- **Octets Received -** The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
- **Total Packets Received Without Error-** The total number of packets (including broadcast packets and multicast packets) received by the processor.
- **Unicast Packets Received -** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Multicast Packets Received -** The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
- **Broadcast Packets Received -** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
- **Receive Packets Discarded -** The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
- **Octets Transmitted -** The total number of octets transmitted out of the interface, including framing characters.
- **Packets Transmitted without Errors -** The total number of packets transmitted out of the interface.
- **Unicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Multicast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
- **Broadcast Packets Transmitted -** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
- **Transmit Packets Discarded -** The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
- **Most Address Entries Ever Used -** The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
- **Address Entries in Use -** The number of Learned and static entries in the Forwarding Database Address Table for this switch.
- **Maximum VLAN Entries -** The maximum number of Virtual LANs (VLANs) allowed on this switch.
- **Most VLAN Entries Ever Used -** The largest number of VLANs that have been active on this switch since the last reboot.
- **Static VLAN Entries -** The number of presently active VLAN entries on this switch that have been created statically.
- **Dynamic VLAN Entries -** The number of presently active VLAN entries on this switch that have been created by GVRP registration.
- **VLAN Deletes -** The number of VLANs on this switch that have been created and then deleted since the last reboot.
- **Time Since** - Counters Last Cleared The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

8.1.6 show logging

This command displays the trap log maintained by the switch.

The trap log contains a maximum of 256 entries that wrap

- **Format show logging**
- **Mode Privileged EXEC**
- **Number of Traps since last reset -** The number of traps that have occurred since the last reset of this device.
- **Number of Traps since log last displayed -** The number of traps that have occurred since the traps were last displayed. Getting the traps by any method (terminal interface display, Web display, upload file from switch etc.) will result in this counter being cleared to 0.
- **Log -** The sequence number of this trap.
- **System Up Time -** The relative time since the last reboot of the switch at which this trap occurred.
- **Trap -** The relevant information of this trap.

✍ ***Note:*** Trap log information is not retained across a switch reset.

8.1.7 show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional all parameter. Alternatively, the administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

- **Format show mac-addr-table [<macaddr> | all]**
- **Mode Privileged EXEC**
- **Mac Address -** A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.slot/port. The port which this address was learned.
- **if Index -** This object indicates the ifIndex of the interface table entry associated with this port.
- **Status -** The status of this entry. The meanings of the values are:
- **Static -** The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.
- **Learned -** The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.
- **Management -** The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1 and is currently used when enabling VLANs for routing.
- **Self -** The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).
- **GMRP Learned -** The value of the corresponding was learned via GMRP and applies to Multicast.
- **Other -** The value of the corresponding instance does not fall into one of the other categories.

8.1.8 show msglog

This command displays the message log maintained by the switch. The message log contains system trace information. The trap log contains a maximum of 256 entries that wrap.

- **Format show msglog**
- **Mode Privileged EXEC**
- **Message** - The message that has been logged.

✍ ***Note:*** Message log information is not retained across a switch reset.

8.1.9 show running-config

This command is used to display the current setting of different protocol packages supported on switch. This command displays only those parameters, the values of which differ from default value. The output is displayed in the script format, which can be used to configure another switch with same configuration.

- **Format show running-config**
- **ModePrivileged EXEC**

8.1.10 show sysinfo

This command displays switch information.

- **Format show sysinfo**
- **Mode Privileged EXEC**
- **Switch Description -** Text used to identify this switch.
- **System Name -** Name used to identify the switch.
- **System Location -** Text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank.
- **System Contact -** Text used to identify a contact person for this switch. May be up to 31 alphanumeric characters. The factory default is blank.
- **System ObjectID -** The base object ID for the switch's enterprise MIB.
- **System Up Time -** The time in days, hours and minutes since the last switch reboot.
- **MIBs Supported -** A list of MIBs supported by this agent.

8.1.11 snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network.The range for name, location and contact is from 1 to 31 alphanumeric characters.

- **Default** None
- **Format snmp-server {sysname <name> | location <loc> | contact <con>}**
- **Mode Global Config**

8.2 Management VLAN Commands

8.2.1 network mgmt_vlan

This command configures the Management VLAN ID.

- **Default** 1
- **Format network mgmt_vlan <1-4094>**
- **Mode Privileged EXEC**

8.3 Dot1P Commands

8.3.1 classofservice dot1pmapping

This command maps an 802.1p priority to an internal traffic class for a device when in 'Global Config' mode. The number of available traffic classes may vary with the platform. Userpriority and trafficclass can both be the range from 0-7. The command is only available on platforms that support priority to traffic class mapping on a 'per-port' basis, and the number of available traffic classes may vary with the platform.

- **Format** **classofservice dot1pmapping <userpriority> <trafficclass>**
- **Mode** **Global Config or Interface Config**

8.3.2 show classofservice dot1pmapping

This command displays the current 802.1p priority mapping to internal traffic classes for a specific interface. The slot/port parameter is required on platforms that support priority to traffic class mapping on a 'per-port' basis.

Platforms that support priority to traffic class mapping on a per-port basis:

- **Format** **show classofservice dot1pmapping <slot/port>**

Platforms that do not support priority to traffic class mapping on a per-port basis:

- **Format** **show classofservice dot1pmapping**
- **Mode** **Privileged EXEC and User EXEC**

8.3.3 vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

- **Format** **vlan port priority all <priority>**
- **Mode** **Global Config**

8.3.4 vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0-7

- **Default** 0
- **Format** **vlan priority <priority>**
- **Mode** **Interface Config**

8.4 LAG/Port-Channel (802.3ad) Commands

8.4.1 port-channel staticcapability

This command enables the support of port-channels (static link aggregations - LAGs) on the device. By default, the static capability for all port-channels is disabled.

- **Default** Disabled
- **Format** **port-channel staticcapability**
- **Mode** **Global Config**

8.4.1.1 no port-channel staticcapability

This command disables the support of static port-channels (link aggregations - LAGs) on the device.

- **Default** Disabled
- **Format** **no port-channel staticcapability**
- **Mode** **Global Config**

8.4.2 show port-channel brief

This command displays the static capability of all port-channels (LAGs) on the device as well as a summary of individual port-channels.

- **Format** **show port-channel brief**
- **Mode** **Privileged EXEC and User EXEC**

Static Capability - This field displays whether or not the device has static capability enabled.

For each port-channel the following information is displayed:

- **Name -** This field displays the name of the port-channel.
- **Link State -** This field indicates whether the link is up or down.
- **Mbr Ports** - This field lists the ports that are members of this port-channel, in slot/port notation.
- **Active Ports -** This field lists the ports that are actively participating in this port-channel.

8.5 Management Commands

These commands manage the switch and show current management settings.

8.5.1 bridge aging-time

This command configures the forwarding database address aging timeout in seconds. In an IVL system, the [fdbid/all] parameter is required.

- **Default** 300
- **Format** **bridge aging-time <10-1,000,000> [fdbid | all]**
- **Mode** **Global Config**

Seconds - The <seconds> parameter must be within the range of 10 to 1,000,000 seconds.

Forwarding Database ID - Fdbid (Forwarding database ID) indicates which forwarding database's aging timeout is being configured. All is used to configure all forwarding database's agetime.

8.5.1.1 no bridge aging-time

This command sets the forwarding database address aging timeout to 300 seconds. In an IVL system, the [fdbid/all] parameter is required.

- **Format** **no bridge aging-time [fdbid | all]**
- **Mode** **Global Config**

Forwarding Database ID - Fdbid (Forwarding database ID) indicates which forwarding database's aging timeout is being configured. All is used to configure all forwarding database's agetime.

8.5.2 mtu

This command sets the maximum transmission unit (MTU) size (in bytes) for physical and port-channel (LAG) interfaces. For the standard implementation, the range of <mtusize> is a valid integer between 1522-9216.

- **Default** 1522
- **Format** **mtu <1522-9216>**
- **Mode** **Interface Config**

8.5.2.1 no mtu

This command sets the default maximum transmission unit (MTU) size (in bytes) for the interface.

- **Format** **no mtu**
- **Mode** **Interface Config**

8.5.3 network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

- **Default** Enabled
- **Format** **network javamode**
- **Mode** **Privileged EXEC**

8.5.3.1 no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

- **Format** **no network javamode**
- **Mode** **Privileged EXEC**

8.5.4 network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

- **Format** **network mac-address <macaddr>**
- **Mode** **Privileged EXEC**

8.5.5 network mac-type

This command specifies whether the burned in MAC address or the locally-administered MAC address is used.

- **Default** **burnedin**

- **Format** **network mac-type {local | burnedin}**
- **Mode** **Privileged EXEC**

8.5.5.1 no network mac-type

This command resets the value of MAC address to its default.

Format **no network mac-type**

Mode **Privileged EXEC**

8.5.6 network parms

This command sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.

Format **network parms <ipaddr> <netmask> [<gateway>]**

Mode **Privileged EXEC**

8.5.7 network protocol

This command specifies the network configuration protocol to be used. If you modify this value change is effective immediately.

Default **None**

Format network protocol {none | bootp | dhcp}, where bootp indicates that the switch periodically sends requests to a Bootstrap Protocol (BootP) server or a dhcp server until a response is received. none indicates that the switch should be manually configured with IP information.

Mode **Privileged EXEC**

8.5.8 remotecon maxsessions

This command specifies the maximum number of remote connection sessions that can be established. A value of 0 indicates that no remote connection can be established. The range is 0 to 5.

Default **5**

Format **remotecon maxsessions <0-5>**

Mode **Privileged EXEC**

8.5.8.1 no remotecon maxsessions

This command sets the maximum number of remote connection sessions that can be established to the default value.

- **Default** **5**
- **Format** **no remotecon maxsessions**
- **Mode** **Privileged EXEC**

8.5.9 remotecon timeout

This command sets the remote connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. A value of 0 indicates that a session remains active indefinitely. The time is a decimal value from 0 to 160.

✍ ***Note:*** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

- **Default** **5**
- **Format** **remotecon timeout <0-160>**
- **Mode** **Privileged EXEC**

8.5.9.1 no remotecon timeout

This command sets the remote connection session timeout value, in minutes, to the default.

✍ ***Note:*** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

- **Default** **5**
- **Format** **no remotecon timeout**
- **Mode** **Privileged EXEC**

8.5.10 serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default 9600

Format **serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}**

Mode **Line Config**

8.5.10.1 no serial baudrate

This command sets the communication rate of the terminal interface to 9600.

- **Format** **no serial baudrate**
- **Mode** **Line Config**

8.5.11 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

- **Default** **5**
- **Format** **serial timeout <0 - 160>**
- **Mode** **Line Config**

8.5.11.1 no serial timeout

This command sets the maximum connect time (in minutes) without console activity to 5.

- **Format** **no serial timeout**
- **Mode** **Line Config**

8.5.12 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

- **Format set prompt <prompt string>**
- **Mode Privileged EXEC**

8.5.13 show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

- **Default all**
- **Format show forwardingdb agetime [fdbid | all]**
- **Mode Privileged EXEC**

Forwarding DB ID Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.

Agetime Displays the address aging timeout for the associated forwarding database in IVL.

8.7.14 show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

- **Format show network**
- **Mode Privileged EXEC and User EXEC**
- **IP Address -** The IP address of the interface. The factory default value is 0.0.0.0
- **Subnet Mask -** The IP subnet mask for this interface. The factory default value is 0.0.0.0
- **Default Gateway -** The default gateway for this IP interface. The factory default value is 0.0.0.0
- **Burned In MAC Address -** The burned in MAC address used for in-band connectivity.
- **Locally Administered MAC Address -** If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
- **MAC Address Type -** Specifies which MAC address should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
- **Network Configuration Protocol Current -** Indicates which network protocol is being used. The options are bootp | dhcp | none.
- **Java Mode -** Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is disabled.
- **Management VLAN ID -** Specifies the management VLAN ID.

8.5.15 show remotecon

This command displays telnet settings.

- ▫ **Format show remotecon**
- ▫ **Mode Privileged EXEC and User EXEC**

Remote Connection Login Timeout (minutes) - This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. A zero means there will be no timeout. This may be specified as a number from 0 to 160. The factory default is 5.

Maximum Number of Remote Connection Sessions - This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.

Allow New Telnet Sessions - Indicates that new telnet sessions will not be allowed when set to no. The factory default value is yes.

8.5.16 show serial

This command displays serial communication settings for the switch.

- ▫ **Format show serial**
- ▫ **Mode Privileged EXEC and User EXEC**

Serial Port Login Timeout (minutes) - Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.

Baud Rate - The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory Default is 9600 baud.

Character Size - The number of bits in a character. The number of bits is always 8.

Flow Control - Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.

Stop Bits - The number of Stop bits per character. The number of Stop bits is always 1.

Parity Type - The Parity Method used on the Serial Port. The Parity Method is always None.

8.5.17 show snmpcommunity

This command displays SNMP community information.

Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Version 1 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

- ▫ **Format show snmpcommunity**
- ▫ **Mode Privileged EXEC**
- ▫ **SNMP Community Name -** The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
- ▫ **Client IP Address -** An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the

IP Address. Note: that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0

- **Client IP Mask -** A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authentic cated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0
- **Access Mode -** The access level for this community string.
- **Status -** The status of this community access entry.

8.5.18 show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

- **Format show snmptrap**
- **Mode Privileged EXEC**
- **SNMP Trap Name -** The community string of the SNMP trap packet sent to the trap manager. This may be up to 16 alphanumeric characters. This string is case sensitive.
- **IP Address -** The IP address to receive SNMP traps from this device. Enter 4 numbers between 0 and 255 separated by periods.
- **Status -** A pull down menu that indicates the receiver's status (enabled or disabled) and allows the administrator/user to perform actions on this user entry:

  Enable - send traps to the receiver

  Disable - do not send traps to the receiver.

  Delete - remove the table entry.

8.5.19 show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

- **Format show trapflags**
- **Mode Privileged EXEC**
- **Authentication Flag -** May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
- **Link Up/Down Flag -** May be enabled or disabled. The factory default is enabled. Indicates **whether link status traps will be sent. Multiple Users Flag.**
- **Multiple Users Flag -** May be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via telnet or serial port).

- **Spanning Tree Flag -** May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.
- **Broadcast Storm Flag -** May be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps will be sent.
- **DVMRP Traps -** May be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps will be sent.
- **OSPF Traps -** May be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps will be sent.
- **PIM Traps -** May be enabled or disabled. The factory default is disabled. Indicates whether PIM traps will be sent.

8.5.20 snmp-server community

This command adds (and names) a new SNMP community. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 16 case-sensitive characters.

✍ ***Note:*** Community names in the SNMP community table must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

- **Default** Two default community names: Public and Private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.
- **Format** **snmp-server community <name>**
- **Mode** **Global Config**

8.5.20.1 no snmp-server community

This command removes this community name from the table. The name is the community name to be deleted.

- **Format** **no snmp-server community <name>**
- **Mode** **Global Config**

8.5.21 snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

- **Default** **0.0.0.0**
- **Format** **snmp-server community ipaddr <ipaddr> <name>**
- **Mode** **Global Config**

8.5.21.1 no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

- **Format** **no snmp-server community ipaddr <name>**
- **Mode** **Global Config**

8.5.22 snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

- **Default** 0.0.0.0
- **Format** **snmp-server community ipmask <ipmask> <name>**
- **Mode** **Global Config**

8.5.22.1 no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

- **Format** **no snmp-server community ipmask <name>**
- **Mode** **Global Config**

8.5.23 snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

- **Default** The default private and public communities are enabled by default. The four undefined communities are disabled by default.
- **Format** **snmp-server community mode <name>**
- **Mode** **Global Config**

8.5.23.1 no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

- **Format** **no snmp-server community mode <name>**
- **Mode** **Global Config**

8.5.24 snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

- **Format** **snmp-server community ro <name>**
- **Mode** **Global Config**

8.5.25 snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

- **Format snmp-server community rw <name>**
- **Mode Global Config**

8.5.26 snmp-server enable traps

This command enables the Authentication Flag.

- **Default Enabled**
- **Format snmp-server enable traps**
- **Mode Global Config**

8.5.26.1 no snmp-server enable traps

This command disables the Authentication Flag.

- **Format no snmp-server enable traps**
- **ModeGlobal Config**

8.5.27 snmp-server enable traps bcaststorm

This command enables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

- **Default Enabled**
- **Format snmp-server enable traps bcaststorm**
- **Mode Global Config**

8.5.27.1 no snmp-server enable traps bcaststorm

This command disables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

- **Format no snmp-server enable traps bcaststorm**
- **Mode Global Config**

8.5.28 snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see 'snmp trap link-status' command).

- **Default Enabled**
- **Format snmp-server enable traps linkmode**
- **Mode Global Config**

8.5.28.1 no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

- **Format** **no snmp-server enable traps linkmode**
- **Mode** **Global Config**

8.5.29 snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or telnet) and there is an existing terminal interface session.

- **Default** **Enabled**
- **Format** **snmp-server enable traps multiusers**
- **Mode** **Global Config**

8.5.29.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

- **Format** **no snmp-server enable traps multiusers**
- **Mode** **Global Config**

8.5.30 snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

- **Default** **Enabled**
- **Format** **snmp-server enable traps stpmode**
- **Mode** **Global Config**

8.5.30.1 no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

- **Format** **no snmp-server enable traps stpmode**
- **Mode** **Global Config**

8.5.31 snmptrap

This command adds an SNMP trap name. The maximum length of name is 16 case-sensitive alphanumeric characters.

- **Default** The default name for the six undefined community names is Delete.
- **Format** **snmptrap <name> <ipaddr>**
- **Mode** **Global Config**

8.5.31.1 no snmptrap

This command deletes trap receivers for a community.

- **Format** **no snmptrap <name> <ipaddr>**
- **Mode** **Global Config**

8.5.32 snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

- **Format** **snmptrap ipaddr <name> <ipaddrold> <ipaddrnew>**
- **Mode** **Global Config**

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

8.5.33 snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

- **Format** **snmptrap mode <name> <ipaddr>**
- **Mode** **Global Config**

8.5.33.1 no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are inactive (not able to receive traps).

- **Format** **no snmptrap mode <name> <ipaddr>**
- **Mode** **Global Config**

8.5.34 telnet

This command regulates new telnet sessions. If sessions are enabled, new telnet sessions can be established until there are no more sessions available. If sessions are disabled, no new telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends it.

- **Default** **Enabled**
- **Format** **telnet**
- **Mode** **Privileged EXEC**

8.5.34.1 no telnet

This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

- **Format** **no telnet**
- **Mode** **Privileged EXEC**

8.6 Device Configuration Commands

8.6.1 addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot and port number of a configured port-channel.

- **Format** **addport <logical slot/port>**
- **Mode** **Interface Config**

Note: Before adding a port to a port-channel, set the physical mode of the port. See 'speed' command.

8.6.2 auto-negotiate

This command enables automatic negotiation on a port. The default value is enable.

- **Format** **auto-negotiate**
- **Mode** **Interface Config**

8.6.2.1 no auto-negotiate

This command disables automatic negotiation on a port.

- **Format** **no auto-negotiate**
- **Mode** **Interface Config**

8.6.3 auto-negotiate all

This command enables automatic negotiation on all ports. The default value is enable.

- **Format** **auto-negotiate all**
- **Mode** **Global Config**

8.6.3.1 no auto-negotiate all

This command disables automatic negotiation on all ports.

- **Format** **no auto-negotiate all**
- **Mode** **Global Config**

8.6.4 delete interface

This command deletes an existing port-channel (LAG) from the configuration. The interface is a logical slot and port for a configured port-channel. The all option removes all configured port-channels (LAGs).

- **Format** **delete interface { <logical slot/port> | all}**
- **ModeInterface Config**

8.6.5 deleteport

This command deletes the port from the port-channel (LAG). The interface is a logical slot and port number of a configured port-channel.

- **Format** **deleteport <logical slot/port>**
- **Mode** **Interface Config**

8.6.6 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF.

The <vlanid> parameter must identify a valid VLAN.

Up to 100 static MAC filters may be created.

- **Format** **macfilter <macaddr> <vlanid>**
- **Mode** **Global Config**

8.6.6.1 no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter <macaddr> <vlanid>**
- **Mode** **Global Config**

8.6.7 macfilter adddest

This command adds the interface to the destination filter set for the MAC filter with the given <macaddr> andVLAN of <vlanid>.

The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter adddest <macaddr> <vlanid>**
- **Mode** **Interface Config**

8.6.7.1 no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>.

The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter adddest <macaddr> <vlanid>**
- **Mode** **Interface Config**

8.6.8 macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter adddest all <macaddr> <vlanid>**
- **Mode** **Global Config**

8.6.8.1 no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter adddest all <macaddr> <vlanid>**
- **Mode** **Global Config**

8.6.9 macfilter addsrc

This command adds the interface to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter addsrc <macaddr> <vlanid>**
- **Mode** **Interface Config**

8.6.9.1 no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **no macfilter addsrc <macaddr> <vlanid>**
- **Mode** **Interface Config**

8.6.10 macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC addressf <macaddr> and <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

- **Format** **macfilter addsrc all <macaddr> <vlanid>**
- **Mode** **Global Config**

8.6.10.1 no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of

<vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The <vlanid> parameter must identify a valid VLAN.

- ▫ **Format** **no macfilter addsrc all <macaddr> <vlanid>**
- ▫ **Mode** **Global Config**

8.6.11 monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). The first slot/port is the source monitored port and the second slot/port is the destination probe port. If this command is executed while port monitoring is enabled, it will have the effect of changing the probe and monitored port values.

- ▫ **Format** **monitor session source <slot/port> destination <slot/port>**
- ▫ **Mode** **Global Config**

8.6.11.1 no monitor session

This command removes the monitor session (port monitoring) designation from both the source probe port and the destination monitored port and removes the probe port from all VLANs. The port must be manually re-added to any desired VLANs.

- ▫ **Format** **no monitor session**
- ▫ **Mode** **Global Config**

8.6.12 monitor session mode

This command configures the monitor session (port monitoring) mode to enable. The probe and monitored ports must be configured before monitor session (port monitoring) can be enabled. If enabled, the probe port will monitor all traffic received and transmitted on the physical monitored port. It is not necessary to disable port monitoring before modifying the probe and monitored ports.

- ▫ **Default** **Disabled**
- ▫ **Format** **monitor session mode**
- ▫ **Mode** **Global Config**

8.6.12.1 no monitor session mode

This command sets the monitor session (port monitoring) mode to disable.

- ▫ **Format** **no monitor session mode**
- ▫ **Mode** **Global Config**

8.6.13 port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

- ▫ **Default** **Disabled**
- ▫ **Format** **port lacpmode**
- ▫ **Mode** **Interface Config**

8.6.13.1 no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

- **Format** **no port lacpmode**
- **Mode** **Interface Config**

8.6.14 port lacpmode all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

- **Format** **port lacpmode all**
- **Mode** **Global Config**

8.6.14.1 no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

- **Format** **no port lacpmode all**
- **Mode** **Global Config**

8.6.15 port-channel

This command configures a new port-channel (LAG) and generates a logical slot and port number for it. Display this number using the "show port-channel".

✍ ***Note:*** Before including a port in a port-channel, set the port physical mode. See **'speed'** command.

- **Format** **port-channel <name>**
- **Mode** **Global Config**

8.6.16 port-channel adminmode

This command enables a port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

- **Format** **port-channel adminmode {<logical slot/port> | all}**
- **Mode** **Global Config**

8.6.16.1 no port-channel adminmode

This command disables a port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

- **Format** **no port-channel adminmode {<logical slot/port> | all}**
- **Mode** **Global Config**
-

8.6.17 port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

- **Default** **Enabled**
- **Format** **port-channel linktrap {<logical slot/port> | all}**
- **Mode** **Global Config**

8.6.17.1 no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

- **Format** **no port-channel linktrap {<logical slot/port> | all}**
- **Mode** **GlobalConfig**

8.6.18 port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel, and name is an alphanumeric string up to 15 characters. This command is used to modify the name that was associated with the port-channel when it was created.

- **Format** **port-channel name {<logical slot/port> | all} <name>**
- **Mode** **Global Config**

8.6.19 protocol group

This command attaches a <vlanid> to the protocol-based VLAN identified by <groupid>. A group may only be associated with one VLAN at a time; however the VLAN association can be changed.

- **Default** **none**
- **Format** **protocol group <groupid> <vlanid>**
- **Mode** **VLAN database**

8.6.19.1 no protocol group

This command removes the <vlanid> from this protocol-based VLAN group that is identified by this <groupid>.

- **Format** **no protocol group <groupid> <vlanid>**
- **Mode** **VLAN database**

8.6.20 protocol vlan group

This command adds the physical <slot/port> interface to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

- **Default** **none**
- **Format** **protocol vlan group <groupid>**
- **Mode** **Interface Config**

8.6.20.1 no protocol vlan group

This command removes the <interface> from this protocol-based VLAN group that is identified by this <groupid>. If <all> is selected, all ports will be removed from this protocol group.

- **Format** **no protocol vlan group <groupid>**
- **Mode** **Interface Config**

8.6.21 protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

- **Default** **none**
- **Format** **protocol vlan group all <groupid>**
- **Mode** **Global Config**

8.6.21.1 no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this <groupid>.

- **Format** **no protocol vlan group all <groupid>**
- **Mode** **Global Config**

8.6.22 set garp timer join

This command sets the GVRP join time per port and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group.
This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds)

- **Default** 20 centiseconds (0.2 seconds)
- **Format** **set garp timer join <10-100>**
- **Mode** **Interface Config**

8.6.22.1 no set garp timer join

This command sets the GVRP join time per port and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

- **Format** **no set garp timer join**
- **Mode** **Interface Config**

8.6.23 set garp timer join all

This command sets the GVRP join time for all ports and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group.

This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds)

- **Default** 20 centiseconds (0.2 seconds)
- **Format** **set garp timer join all <10-100>**
- **Mode** **Global Config**

8.6.23.1 no set garp timer join all

This command sets the GVRP join time for all ports and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

- **Format** **no set garp timer join all**
- **Mode** **Global Config**

8.6.24 set garp timer leave

This command sets the GVRP leave time per port. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service time is 20 to 600 (centiseconds).

- **Default** 60 centiseconds (0.6 seconds)
- **Format** **set garp timer leave <20-600>**
- **Mode** **Interface Config**

Note: This command has an effect only when GVRP is enabled.

8.6.24.1 no set garp timer leave

This command sets the GVRP leave time per port to 60 centiseconds (0.6 seconds).

- **Format** **no set garp timer leave**
- **Mode** **Interface Config**

Note: This command has an effect only when GVRP is enabled.

8.6.25 set garp timer leave all

This command sets the GVRP leave time for all ports. Leave time is the time to wait after receiving an unregister request for a

VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service time is 20 to 600 (centiseconds).

✍ ***Note:*** This command has an effect only when GVRP is enabled.

- **Default** 60 centiseconds (0.6 seconds)
- **Format** **set garp timer leave all <20-600>**
- **Mode** **Global Config**

8.6.25.1 no set garp timer leave all

This command sets the GVRP leave time for all ports to the default 60 centiseconds (0.6 seconds).

✍ ***Note:*** This command has an effect only when GVRP is enabled.

- **Format** **no set garp timer leave all**
- **Mode** **Global Config**

8.6.26 set garp timer leaveall

This command sets how frequently Leave All PDUs are generated per port. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds).

✍ ***Note:*** This command has an effect only when GVRP is enabled.

- **Default** 1000 centiseconds (10 seconds)
- **Format** **set garp timer leaveall <200-6000>**
- **ModeInterface Config**

8.6.26.1 no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated per port to 1000 centiseconds (10 seconds).

✍ ***Note:*** This command has an effect only when GVRP is enabled.

- **Format** **no set garp timer leaveall**
- **Mode** **Interface Config**

8.6.27 set garp timer leaveall all

This command sets how frequently Leave All PDUs are generated for all ports. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds).

✍ ***Note:*** This command has an effect only when GVRP is enabled.

- **Default** 1000 centiseconds (10 seconds)
- **Format** **set garp timer leaveall all <200-6000>**
- **Mode** **Global Config**

8.6.27.1 no set garp timer leaveall all

This command sets how frequently Leave All PDUs are generated for all ports to 1000 centiseconds (10 seconds).

✍ ***Note:*** This command has an effect only when GVRP is enabled.

- **Format** **no set garp timer leaveall all**
- **Mode** **Global Config**

8.6.28 set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system. The default value is disable.

- **Format** **set gmrp adminmode**
- **Mode** **Privileged EXEC**

8.6.28.1 no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

- **Format** **no set gmrp adminmode**
- **Mode** **Privileged EXEC**

8.6.29 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and portchannel (LAG) membership is removed from an interface that has GARP enabled.

- **Default** Disabled
- **Format** **set gmrp interfacemode**
- **Mode** **Interface Config**

8.6.29.1 no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and portchannel (LAG) membership is removed from an interface that has GARP enabled.

- **Format** **no set gmrp interfacemode**
- **Mode** **Interface Config**

8.6.30 set gmrp interfacemode all

This command enables GARP Multicast Registration Protocol on all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and portchannel (LAG) membership is removed from an interface that has GARP enabled.

- **Default** Disabled
- **Format** **set gmrp interfacemode all**
- **Mode** **Global Config**

8.6.30.1 no set gmrp interfacemode all

This command disables GARP Multicast Registration Protocol on a selected interface.

- **Format** **no set gmrp interfacemode all**
- **Mode** **Global Config**

8.6.31 set gvrp adminmode

This command enables GVRP.

- **Default** Disabled
- **Format** **set gvrp adminmode**
- **Mode** **Privileged EXEC**

8.6.31.1 no set gvrp adminmode

This command disables GVRP.

- **Format** **no set gvrp adminmode**
- **Mode** **Privileged EXEC**

8.6.32 set gvrp interfacemode

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

- **Default** **Disabled**
- **Format** **set gvrp interfacemode**
- **Mode** **Interface Config**

8.6.32.1 no set gvrp interfacemode

This command disables GVRP (GARP VLAN Registration Protocol) for a specific port. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

- **Format** **no set gvrp interfacemode**
- **ModeInterface Config**

8.6.33 set gvrp interfacemode all

This command enables GVRP (GARP VLAN Registration Protocol) for all ports.

- **Default Disabled**
- **Format set gvrp interfacemode all**
- **Mode Global Config**

8.6.33.1 no set gvrp interfacemode all

This command disables GVRP (GARP VLAN Registration Protocol) for all ports. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

- **Format no set gvrp interfacemode all**
- **Mode Global Config**

8.6.34 show description

This command displays the port description information for one or all interfaces.

- **Format show description {<slot/port> | all}**
- **Mode Privileged EXEC and User EXEC**

8.6.35 show garp

This command displays Generic Attributes Registration Protocol (GARP) information.

- **Format show garp**
- **Mode Privileged EXEC and User EXEC**
- **GMRP Admin Mode -** This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
- **GVRP Admin Mode -** This displays the administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

8.6.36 show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

- **Format show gmrp configuration {<slot/port> | all}**
- **Mode Privileged EXEC and User EXEC**
- **Interface -** This displays the slot/port of the interface that this row in the table describes.
- **Join Timer -** Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
- **Leave Timer -** Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to

assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

- **LeaveAll Timer -** This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
- **Port GMRP Mode -** Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.
- **Port GVRP Mode -** Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

8.6.37 show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

- **Format show gvrp configuration {<slot/port> | all}**
- **Mode Privileged EXEC and User EXEC**
- **Interface -** This displays the slot/port of the interface that this row in the table describes.
- **Join Timer -** Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
- **Leave Timer -** Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
- **LeaveAll Timer -** This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
- **Port GMRP Mode -** Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.
- **Port GVRP Mode -** Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

8.6.38 show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled. Status information is only displayed when IGMP Snooping is enabled.

- **Format show igmpsnooping**
- **Mode Privileged EXEC**
- **Admin Mode -** This indicates whether or not IGMP Snooping is active on the switch.
- **Query Interval Time -** This displays the IGMP Query Interval Time. This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured
- **Max Response Time -** This displays the amount of time the switch will wait after sending a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
- **Multicast Router Present Expiration Time -** If a query is not received on an interface within this amount of time, the interface is removed from the list of interfaces with multicast routers attached. This value may be configured.
- **Interfaces Enabled for IGMP Snooping -** This is the list of interfaces on which IGMP Snooping is enabled. The following status values are only displayed when IGMP Snooping is enabled.
- **Multicast Control Frame Count -** This displays the number of multicast control frames that are processed by the CPU.

8.6.39 show mac-address-table gmrp

This command displays the GARP Multicast Registration Protocol (GMRP) entries in the Multicast Forwarding Database (MFDB) table.

- **Format show mac-address-table gmrp**
- **Mode Privileged EXEC**
- **Mac Address -** A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
- **Type -** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
- **Description -** The text description of this multicast table entry.
- **Interfaces -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

8.6.40 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

- **Format show mac-address-table igmpsnooping**
- **ModePrivileged EXEC**
- **Mac Address -** A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
- **Type -** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are

added to the table as a result of a learning process or protocol.

- **Description -** The text description of this multicast table entry.
- **Interfaces -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

8.6.41 show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional all parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

- **Format show mac-address-table multicast [<macaddr> | all]**
- **Mode Privileged EXEC**
- **Mac Address -** A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
- **Type -** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
- **Component -** The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
- **Description -** The text description of this multicast table entry.
- **Interfaces -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
- **Forwarding Interfaces -** The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

8.6.42 show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If <all> is selected, all the Static MAC Filters in the system are displayed. If a macaddr is entered, a vlan must also be entered and the Static MAC Filter information will be displayed only for that MAC address and VLAN.

- **Format show mac-address-table static {<macaddr> <vlanid> | all}**
- **Mode Privileged EXEC**
- **MAC Address -** Is the MAC Address of the static MAC filter entry.
- **VLAN ID -** Is the VLAN ID of the static MAC filter entry.
- **Source Port(s) -** Indicates the source port filter set's slot and port(s).
- **Destination Port(s) -** Indicates the destination port filter set's slot and port(s).

8.6.43 show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

- **Format show mac-address-table staticfiltering**
- **Mode Privileged EXEC**

- **Mac Address -** An unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
- **Type -** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
- **Description -** The text description of this multicast table entry.
- **Interfaces -** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

8.6.44 show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

- **Format show mac-address-table stats**
- **Mode Privileged EXEC**
- **Total Entries -** This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.
- **Most MFDB Entries Ever Used -** This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
- **Current Entries** - This displays the current number of entries in the Multicast Forwarding Database table.

8.6.45 show monitor

This command displays the Port monitoring information for the system.

- **Format show monitor**
- **Mode Privileged EXEC**
- **Port Monitor Mode** indicates whether the Port Monitoring feature is enabled or disabled. The possible values are enable and disable.
- **Probe Port slot/port** is the slot/port that is configured as the probe port. If this value has not been configured, **'Not Configured'** will be displayed.
- **Monitored Port slot/port** is the slot/port that is configured as the monitored port. If this value has not been configured, **'Not Configured'** will be displayed.

8.6.46 show port

This command displays port information.

- **Format show port {<slot/port> | all}**
- **Mode Privileged EXEC**
- **slot/port -** The physical slot and physical port.
- **Type -** If not blank, this field indicates that this port is a special type of port. The possible values are:

  Mon - this port is a monitoring port. Look at the Port Monitoring screens to find out more information.

  Lag - this port is a member of a port-channel (LAG).

  Probe - this port is a probe port.

- **Admin Mode -** Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.
- **Physical Mode -** Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate.
- The factory default is Auto.
- **Physical Status -** Indicates the port speed and duplex mode.
- **Link Status -** Indicates whether the Link is up or down.
- **Link Trap -** This object determines whether or not to send a trap when link status changes. The factory default is enabled.
- **LACP Mode -** Displays whether LACP is enabled or disabled on this port.

8.6.47 show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated Group.

- **Format show port protocol {<groupid> | all}**
- **Mode Privileged EXEC**
- **Group Name -** This field displays the group name of an entry in the Protocol-based VLAN table.
- **Group ID -** This field displays the group identifier of the protocol group.
- **Protocol(s) -** This field indicates the type of protocol(s) for this group.
- **VLAN -** This field indicates the VLAN associated with this Protocol Group.
- **Interface(s) -** This field lists the slot/port interface(s) that are associated with this Protocol Group.

8.6.48 show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

- **Format show port-channel {<logical slot/port> | all}**
- **Mode Privileged EXEC**
- **Logical slot/port -** The logical slot and the logical port.
- **Name -** The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
- **Link State -** Indicates whether the Link is up or down.
- **Admin Mode -** May be enabled or disabled. The factory default is enabled.
- **Link Trap Mode -** This object determines whether or not to send a trap when link status changes. The factory default is enabled.
- **STP Mode -** The Spanning Tree Protocol Administrative Mode associated with the port or portchannel (LAG). The possible values are:
- **Disable -** Spanning tree is disabled for this port.
- **Enable -** Spanning tree is enabled for this port.
- **Mbr Ports -** A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
- **Port Speed -** Speed of the port-channel port.

- **Type -**This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. The possible values of this field are Static, indicating that the port-channel is statically maintained; and Dynamic, indicating that the port-channel is dynamically maintained.
- **Active Ports -** This field lists the ports that are actively participating in the port-channel (LAG).

8.6.49 show storm-control

This command displays switch configuration information.

- **Format show storm-control**
- **Mode Privileged EXEC**
- **Broadcast Storm Recovery Mode -** May be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode -** May be enabled or disabled. The factory default is disabled.

8.6.50 show vlan

This command displays detailed information, including interface information, for a specific VLAN.

- **Format show vlan <vlanid>, where the ID is a valid VLAN identification number**
- **Mode Privileged EXEC and User EXEC**
- **VLAN ID -** There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
- **VLAN Name -** A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.
- **VLAN Type -** Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
- **slot/port -** Indicates by slot id and port number which port is controlled by the fields on this line. It is possible to set the parameters for all ports by using the selectors on the top line.
- **Current** - Determines the degree of participation of this port in this VLAN. The permissible values are:

  Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

  Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

  Autodetect - Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
- **Configured -** Determines the configured degree of participation of this port in this VLAN. The permissible values are:

  Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

  Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

  Autodetect - Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the

IEEE 802.1Q standard.

- **Tagging -** Select the tagging behavior for this port in this VLAN.

  Tagged - specifies to transmit traffic for this VLAN as tagged frames.

  Untagged - specifies to transmit traffic for this VLAN as untagged frames.

8.6.51 show vlan brief

This command displays a list of all configured VLANs.

- **Format show vlan brief**
- **Mode Privileged EXEC and User EXEC**
- **VLAN ID -** There is a VLAN Identifier (vlanid)associated with each VLAN. The range of the VLAN ID is 1 to 4094.
- **VLAN Namev -** A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.
- **VLAN Type -** Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

8.6.52 show vlan port

This command displays VLAN port information.

- **Format show vlan port {<slot/port> | all}**
- **Mode Privileged EXEC and User EXEC**
- **slot/port -** Indicates by slot id and port number which port is controlled by the fields on this line. It is possible to set the parameters for all ports by using the selectors on the top line.
- **Port VLAN ID -** The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
- **Acceptable Frame Types -** Specifies the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
- **Ingress Filtering -** May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
- **GVRP -** May be enabled or disabled.
- **Default Priority -** The 802.1p priority assigned to tagged packets arriving on the port.

8.6.53 shutdown

This command disables a port.

- **Default** **Enabled**
- **Format** **shutdown**
- **Mode** **Interface Config**

8.6.53.1 no shutdown

This command enables a port.

- **Format** **no shutdown**
- **Mode** **Interface Config**

8.6.54 shutdown all

This command disables all ports.

- **Default** **Enabled**
- **Format** **shutdown all**
- **Mode** **Global Config**

8.6.54.1 no shutdown all

This command enables all ports.

- **Format** **no shutdown all**
- **Mode** **Global Config**

8.6.55 snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See 'snmpserverenable traps linkmode' command.

- **Format** **snmp trap link-status**
- **Mode** **Interface Config**

8.6.55.1 no snmp trap link-status

This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See 'snmpserver enable traps linkmode' command).

- **Format** **no snmp trap link-status**
- **Mode** **Interface Config**

8.6.56 snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see "snmpserver enable traps linkmode").

- **Format** **snmp trap link-status all**
- **Mode** **Global Config**

8.6.56.1 no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see "snmpserver enable traps linkmode").

- **Format** **no snmp trap link-status all**
- **Mode** **Global Config**

8.6.57 spanning-tree

This command sets the STP mode for a specific port-channel (LAG). This is the value specified for STP Mode on the Port Configuration Menu. 802.1D mode is the default. The interface is a logical slot and port for a configured port-channel. The all option sets all configured port-channels (LAGs) with the same option.

- **Format** **spanning-tree {<logical slot/port> | all} {off | 802.1d | fast}**
- **ModeGlobal Config**

The mode is one of the following:

802.1d	IEEE 802.1D-compliant STP mode is used
fast	Fast STP mode is used
off	STP is turned off

8.6.58 spanning-tree bpdumigrationcheck

This command enables BPDU migration check on a given interface. The all option enables BPDU migration check on all interfaces.

- **Format** **spanning-tree bpdumigrationcheck {<slot/port> | all}**
- **Mode** **Global Config**

8.6.58.1 no spanning-tree bpdumigrationcheck

This command disables BPDU migration check on a given interface. The all option disables BPDU migration check on all interfaces.

- **Format** **no spanning-tree bpdumigrationcheck {<slot/port> | all}**
- **Mode** **Global Config**

8.6.59 description

This command sets the description information for the interface. The description is an alphanumeric string of up to 64 characters. To use spaces as part of a description, enclose it in double quotes like: "Port 1 connect to Ln 1"

- **Format** **description <description>**

- **ModeInterface Config**

8.6.60 speed

This command sets the speed and duplex setting for the interface.

- **Format** **speed {{100 | 10} {half-duplex | full-duplex} | 1000 fullduplex}**
- **ModeInterface Config**

Acceptable values are:

100h	100BASE-T half-duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	100BASE-T full duplex

8.6.61 speed all

This command sets the speed and duplex setting for all interfaces.

- **Format** **speed all {{100 | 10} {half-duplex | full-duplex} | 1000 fullduplex}**
- **Mode** **Global Config**

Acceptable values are:

100h	100BASE-T half-duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	100BASE-T full duplex

8.6.62 storm-control broadcast

This command enables broadcast storm recovery mode. If the mode is enabled, broadcast storm recovery with high and low thresholds is implemented.

The threshold implementation follows a percentage pattern. If the broadcast traffic on any Ethernet port exceeds the high threshold percentage (as represented in "Broadcast Storm Recovery Thresholds" table) of the link speed, the switch discards the broadcasts traffic until the broadcast traffic returns to the low threshold percentage or less. The full implementation is depicted in the "Broadcast Storm Recovery Thresholds" table.

- **Format** **storm-control broadcast**
- **Mode** **Global Config**

Link Speed	High	Low
10M	**20**	**10**
100M	**5**	**2**
1000M	**5**	**2**

Table 7-1 Broadcast Storm Recovery Thresholds

8.6.62.1 no storm-control broadcast

This command disables broadcast storm recovery mode.

The threshold implementation follows a percentage pattern. If the broadcast traffic on any Ethernet port exceeds the high threshold percentage (as represented in "Broadcast Storm Recovery Thresholds" table) of the link speed, the switch discards the broadcasts traffic until the broadcast traffic returns to the low threshold percentage or less. The full implementation is depicted in the "Broadcast Storm Recovery Thresholds" table.

- **Format** **no storm-control broadcast**
- **Mode** **Global Config**

Link Speed	High	Low
10M	20	10
100M	5	2
1000M	5	2

8.6.63 storm-control flowcontrol

This command enables 802.3x flow control for the switch.

- **Default** **Disabled**
- **Format** **storm-control flowcontrol**
- **Mode** **Global Config**

Note: This command only applies to full-duplex mode ports.

8.6.63.1 no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

- **Format** **no storm-control flowcontrol**
- **Mode** **Global Config**

8.6.64 vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4094.

- **Format** **vlan <2-4094>**
- **Mode** **VLAN database**

8.6.64.1 no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4094.

- **Format no vlan <2-4094>**
- **Mode VLAN database**

8.6.65 vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

- **Default Admit All**
- **Format vlan acceptframe {vlanonly | all}**
- **ModeInterface Config**

8.6.65.1 no vlan acceptframe

This command sets the frame acceptance mode per interface to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

- **Format vlan acceptframe {vlanonly | all}**
- **Mode Interface Config**

8.6.66 vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

- **Default Disabled**
- **Format vlan ingressfilter**
- **Mode Interface Config**

8.6.66.1 no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

- **Format no vlan ingressfilter**
- **Mode Interface Config**

8.6.67 vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4094.

- **Format vlan makestatic <2-4094>**
- **Mode VLAN database**

8.6.68 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 16 characters, and the ID is a valid VLAN identification number. ID range is 1- 4094.

- **Default** The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.
- **Format** **vlan name <2-4094> <name>**
- **Mode** **VLAN database**

8.6.68.1 no vlan name

This command sets the name of a VLAN to a blank string. The VLAN ID is a valid VLAN identification number. ID range is 1-4094.

- **Format** **no vlan name <2-4094>**
- **Mode** **VLAN database**

8.6.69 vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

- **Format** **vlan participation {exclude | include | auto} <1-4094>**
- **Mode** **Interface Config**
- **Participation options are:**
- **include -** The interface is always a member of this VLAN. This is equivalent to registration fixed.
- **exclude -** The interface is never a member of this VLAN. This is equivalent to registration forbidden.
- **auto -** The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

8.6.70 vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

- **Format** **vlan participation all {exclude | include | auto} <1-4094>**
- **Mode** **Global Config**

Participation options are:

- **include -** The interface is always a member of this VLAN. This is equivalent to registration fixed.
- **Exclude -** The interface is never a member of this VLAN. This is equivalent to registration forbidden.
- **Auto -** The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

8.6.71 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

- **Default** **Admit All**

- **Format** **vlan port acceptframe all {vlanonly | all}**
- **Mode** **Global Config**

8.6.71.1 no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

- **Format** **no vlan port acceptframe all {vlanonly | all}**
- **Mode** **Global Config**

8.6.72 vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

- **Default** **Disabled**
- **Format** **vlan port ingressfilter all**
- **Mode** **Global Config**

8.6.72.1 no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

- **Format** **no vlan port ingressfilter all**
- **Mode** **Global Config**

8.6.73 vlan port pvid all

This command changes the VLAN ID for all interfaces.

- **Default** **1**
- **Format** **vlan port pvid all <1-4094>**
- **Mode** **Global Config**

8.6.73.1 no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

- **Format** **no vlan port pvid all <1-4094>**
- **Mode** **Global Config**

8.6.74 vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

- **Format** **vlan port tagging all <1-4094>**
- **Mode** **Global Config**

8.6.74.1 no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

- **Format** **no vlan port tagging all <1-4094>**
- **Mode** **Global Config**

8.6.75 vlan protocol group

- This command adds protocol-based VLAN group to the system. The <groupName> is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

  Format **vlan protocol group <groupname>**
- **Mode** **Global Config**

8.6.76 vlan protocol group add protocol

This command adds the <protocol> to the protocol-based VLAN identified by <groupid>. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are ip, arp, and ipx.

- **Default** **none**
- **Format** **vlan protocol group add protocol <groupid> <protocol>**
- **Mode** **Global Config**

8.6.76.1 no vlan protocol group add protocol

This command removes the <protocol> from this protocol-based VLAN group that is identified by this <groupid>. The possible values for protocol are ip, arp, and ipx.

- **Format** **no vlan protocol group add protocol <groupid> <protocol>**
- **Mode** **Global Config**

8.6.77 vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this <groupid>.

- **Format** **vlan protocol group remove <groupid>**
- **Mode** **Global Config**

8.6.78 vlan pvid

This command changes the VLAN ID per interface.

- **Default** **1**
- **Format** **vlan pvid <1-4094>**
- **Mode** **Interface Config**

8.6.78.1 no vlan pvid

This command sets the VLAN ID per interface to 1.

- **Format** **no vlan pvid <1-4094>**
- **Mode** **Interface Config**

8.6.79 vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

- **Format** **vlan tagging <1-4094>**
- **Mode** **Interface Config**

8.6.79.1 no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

- **Format** **no vlan tagging <1-4094>**
- **Mode** **Interface Config**

8.7 User Account Management Commands

These commands manage user accounts.

8.7.1 disconnect

This command closes a telnet session.

- **Format** **disconnect {<sessionID> | all}**
- **Mode** **Privileged EXEC**

8.7.2 show loginsession

This command displays current telnet and serial port connections to the switch.

- **Format** **show loginsession**
- **Mode** **Privileged EXEC**
- **ID** **Login Session ID**
- **User Name -** The name the user will use to login using the serial port or Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. Two users are included as the factory default, **'admin'** and **'guest'**.
- **Connection From -** IP address of the telnet client machine or EIA-232 for the serial port connection.
- **Idle Time -** Time this session has been idle.
- **Session Time -** Total time this session has been connected.

8.7.3 show users

This command displays the configured user names and their settings. This command is only available for users with readwrite privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

- **Format** **show users**
- **Mode** **Privileged EXEC**
- **User Name -** The name the user will use to login using the serial port, Telnet or Web. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. Two users are included as the factory default, **'admin'** and **'guest'.**
- **Access Mode -** Shows whether the operator is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the 'admin' user has Read/Write access and the 'guest' has Read Only access. There can only be one Read/Write user and up to five Read Only users.
- **SNMPv3 AccessMode** - This field displays the SNMPv3 Access Mode. If the value is set to Read-Write, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
- **SNMPv3 Authentication -** This field displays the authentication protocol to be used for the specified login user.
- **SNMPv3 Encryption -** This field displays the encryption protocol to be used for the specified login user.

8.7.4 users name

This command adds a new user (account) if space permits. The account <username> can be up to eight characters in length. The name may be comprised of alphanumeric characters as well as the dash ('-') and underscore ('_'). The <username> is not case-sensitive.

Six user names can be defined.

- **Format** **users name <username>**
- **Mode** **Global Config**

8.7.4.1 no users name

This command removes an operator.

- **Format** **no users name <username>**
- **Mode** **Global Config**

✍ ***Note:*** The 'admin' user account cannot be deleted.

8.7.5 users passwd

This command is used to change a password. The password should not be more than eight alphanumeric characters in length. If a user is authorized for authentication or encryption is enabled, the password must be at least eight alphanumeric characters in length. The username and password are not case sensitive when a password is changed, a prompt will ask for the former password. If none, press enter.

- **Default** **No Password**
- **Format** **users passwd <username>**
- **Mode** **Global Config**

8.7.5.1 no users passwd

This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

- **Format** **no users passwd <username>**
- **Mode** **Global Config**

8.7.6 users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are readonly or readwrite. The <username> is the login user name for which the specified access mode will apply.

- **Default** **readwrite for 'admin' user; readonly for all other users**
- **Format** **users snmpv3 accessmode <username> {readonly | readwrite}**
- **Mode** **Global Config**

8.7.6.1 no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified login user as readwrite for the 'admin' user; readonly for all other users. The <username> is the login user name for which the specified access mode will apply.

- **Format** **no users snmpv3 accessmode <username>**
- **Mode** **Global Config**

8.7.7 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are none, md5 or sha. If md5 or sha are specified, the user login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The <username> is the login user name associated with the authentication protocol.

- **Default** **no authentication**
- **Format** **users snmpv3 authentication <username> {none | md5 | sha}**
- **Mode** **Global Config**

8.7.7.1 no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified login user to none. The <username> is the login user name for which the specified authentication protocol will be used.

- **Format** **users snmpv3 authentication <username>**
- **Mode** **Global Config**

8.7.8 users snmpv3 encryption

This command specifies the encryption protocol to be used for the specified login user. The valid encryption protocols are des or none.

If des is specified, the required key may be specified on the command line. The key may be up to 16 characters long. If the des protocol is specified but a key is not provided, the user will be prompted for the key. When using the des protocol, the user login password is also used as the snmpv3 encryption password and therefore must be at least eight characters in length.

If none is specified, a key must not be provided. The <username> is the login user name associated with the specified encryption.

- **Default** **no encryption**
- **Format** **users snmpv3 encryption <username> {none | des [key]}**
- **Mode** **Global Config**

8.7.8.1 no users snmpv3 encryption

This command sets the encryption protocol to none. The <username> is the login user name for which the specified encryption protocol will be used.

- **Format** **no users snmpv3 encryption <username>**
- **Mode** **Global Config**

8.8 System Utilities

This section describes system utilities.

8.8.1 clear config

This command resets the configuration to the factory defaults without powering off the switch. The switch is automatically reset when this command is processed. You are prompted to confirm that the reset should proceed.

- **Format** **clear config**
- **Mode** **Privileged EXEC**

8.8.2 clear counters

This command clears the stats for a specified <slot/port> or for all the ports or for the entire switchbased upon the argument.

Format **clear counters [{<slot/port> | all}]**

Mode **Privileged EXEC**

8.8.3 clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

- **Format** **clear igmpsnooping**
- **Mode** **Privileged EXEC**

8.8.4 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

- **Format** **clear pass**
- **Mode** **Privileged EXEC**

8.8.5 clear port-channel

This command clears all port-channels (LAGs).

- **Format** **clear port-channel**

- **Mode** **Privileged EXEC**

8.8.6 clear traplog

This command clears the trap log.

- **Format** **clear traplog**
- **Mode** **Privileged EXEC**

8.8.7 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

- **Format** **clear vlan**
- **Mode** **Privileged EXEC**

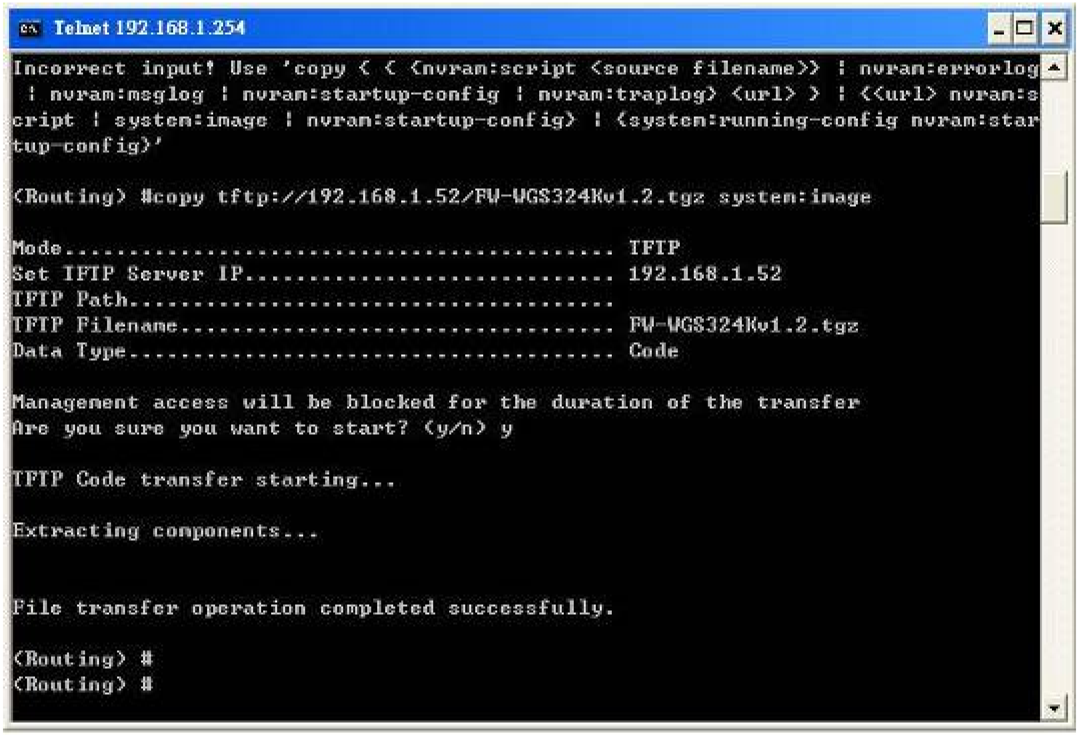
8.8.8 copy

This command uploads and downloads to/from the switch. Local URLs can be specified using tftp or xmodem. The following can be specified as the source file for uploading from the switch: startup configuration **(nvram:startup-config)**, error log **(nvram:errorlog)**, message log **(nvram:msglog)** and trap log **(nvram:traplog)**. A URL is specified for the destination.
The command can also be used to download the startup configuration or code image by specifying the source as a URL and destination as **nvram:startup-config** or .**system:image** respectively.
The command can be used to the save the running configuration to **nvram** by specifying the source as **system:running-config** and the destination as **nvram:startup-config**
The command can also be used to download **ssh** key files as **nvram:sshkey-rsa**, nvram:sshkey-rsa2, and **nvram:sshkey-dsa** and http secure-server certificates as **nvram:sslpem-root**, **nvram:sslpemserver**, **nvram:sslpem-dhweak**, and **nvram:sslpem-dhstrong**.

- **Default** none
- **Format** **copy nvram:startup-config <url>**

```
copy nvram:errorlog <url>
copy nvram:msglog <url>
copy nvram:traplog <url>
copy <url> nvram:startup-config
copy <url> system:image
copy system:running-config nvram:startup-config
copy <url> nvram:sslpem-root
copy <url> nvram:sslpem-server
copy <url> nvram:sslpem-dhweak
copy <url> nvram:sslpem-dhstrong
copy <url> nvram:sshkey-rsa1
copy <url> nvram:sshkey-rsa2
copy <url> nvram:sshkey-dsa
```

- **Mode** **Privileged EXEC**



```
Incorrect input! Use 'copy < < <nvram:script <source filename>> | nvram:errorlog
 | nvram:msglog | nvram:startup-config | nvram:traplog> <url> > | <<url> nvram:s
cript | system:image | nvram:startup-config> | <system:running-config nvram:star
tup-config>'

(Routing) #copy tftp://192.168.1.52/FW-WGS324Kv1.2.tgz system:image

Mode........................................... TFTP
Set TFTP Server IP............................. 192.168.1.52
TFTP Path......................................
TFTP Filename.................................. FW-WGS324Kv1.2.tgz
Data Type...................................... Code

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP Code transfer starting...

Extracting components...


File transfer operation completed successfully.

(Routing) #
(Routing) #
```

8.8.9 logout

This command closes the current telnet connection or resets the current serial connection.

✍ ***Note:*** Save configuration changes before logging out.

- **Format** **logout**
- **Mode** **Privileged EXEC**

8.8.10 ping

This command checks if another computer is on the network which is listening for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

- **Format** **ping <ipaddr>**
- **Mode** **Privileged EXEC and User EXEC**

8.8.11 reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

- **Format** **reload**
- **Mode** **Privileged EXEC**

9. CLI COMMANDS: QUALITY OF SERVICE

This chapter provides a detailed explanation of the Quality of Service (QOS) commands. The following QOS CLI commands are available in the software QOS Package.

The commands are divided into these different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

9.1 CLI Commands: Access Control List

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

9.1.1 show ip access-lists

This command displays an Access Control List (ACL) and all of the rules that are defined for the ACL. The <accesslistnumber> is the number used to identify the ACL.

- **Format show ip access-lists <accesslistnumber>**
- **Mode Privileged EXEC and User EXEC**
- **Rule Number -** This displays the number identifier for each rule that is defined for the ACL.
- **Action -** This displays the action associated with each rule. The possible values are Permit or Deny.
- **Protocol -** This displays the protocol to filter for this rule.
- **Source IP Address -** This displays the source IP address for this rule.
- **Source IP Mask -** This field displays the source IP Mask for this rule.
- **Source Ports -** This field displays the source port range for this rule.
- **Destination IP Address -** This displays the destination IP address for this rule.
- **Destination IP Mask -** This field displays the destination IP Mask for this rule.
- **Destination Ports -** This field displays the destination port range for this rule.
- **Service Type Field Match -** This field indicates whether an IP DSCP, IP Precedence, or IP TOS match condition is specified for this rule.
- **Service Type Field Value -** This field indicates the value specified for the Service Type Field Match (IP DSCP, IP Precedence, or IP TOS).

9.2 Configuration Commands

9.2.1 access-list

This command creates an Access Control List (ACL) that is identified by the parameter <accesslistnumber>. The ACL number is an integer from 1 to 199. The range 1 to 99 is for normal ACL List and 100 to 199 is for extended ACL List. The ACL rule is created with the option of permit or deny. The protocol to filter for an ACL rule is specified by giving the protocol to be used like cmp, igmp, ip, tcp, udp. The command specifies a source ipaddress and source mask for match condition of the ACL rule specified by the srcip and srcmask parameters.The source layer 4 port match condition for the ACL rule are specified by the port value parameter.The <startport> and <endport> parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the destination port range.The <portvalue> parameter uses a single keyword notation and currently has the values of domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www. Each of these values translates into its equivalent port number, which is used as both the start and end of a port range. The command specifies a destination ipaddress and destination mask for match condition of the ACL rule specified by the dstip and dstmask parameters.The command specifies the TOS for an ACL rule depending on a match of precedence or DSCP values using the parameters tos, tosmask ,dscp.

- **Default** none
- **Format** **access-list {(<1-99> {deny | permit} <srcip> <srcmask>) | ({<100-199> {deny | permit} {evry | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask> [{eq {<portkey> | <portvalue>} | range <startport> <endport>}] <dstip> <dstmask> [{eq {<portkey> | <portvalue>} | range <startport> <endport>}] [precedence <precedence>] [tos <tos> <tosmask>] [dscp <dscp>]}})}**
- **Mode** **Global Config**

9.2.1.1 no access-list

This command deletes an ACL that is identified by the parameter <accesslistnumber> from the system.

- **Format** **no access-list <accesslistnumber>**
- **Mode** **Global Config**

9.2.2 ip access-group

This command attaches a specified access-control list to an interface.

- **Default** none
- **Format** **ip access-group <accesslistnumber> [in | out]**
- **Mode** **Interface Config**

9.2.3 ip access-group all

This command attaches a specified access-control list to all interfaces.

- **Default** none
- **Format** **ip access-group all <accesslistnumber> [in | out]**
- **Mode** **Global Config**

9.3 CLI Commands: Differentiated Services

This chapter contains the CLI commands used for the QOS Differentiated Services (DiffServ) package.

The user configures DiffServ in several stages by specifying:

1. Class

- creating and deleting classes
- defining match criteria for a class. Note: The only way to remove an individual match criterion from an existing class

definition is to delete the class and re-create it.

2. Policy

- creating and deleting policies
- associating classes with a policy
- defining policy statements for a policy/class combination

3. Service

- adding and removing a policy to/from a directional (i.e., inbound, outbound) interface

Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

Packet processing begins by testing the match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

Note that the type of class - all, any, or acl - has a bearing on the validity of match criteria specified when defining the class. A class type of 'any' processes its match rules in an ordered sequence; additional rules specified for such a class simply extend this list. A class type of 'acl' obtains its rule list by interpreting each ACL rule definition at the time the Diffserv class is created. Differences arise when specifying match criteria for a class type 'all', since only one value for each non-excluded match field is allowed within a class definition. If a field is already specified for a class, all subsequent attempts to specify the same field fail, including the cases where a field can be specified multiple ways through alternative formats. The exception to this is when the 'exclude' option is specified, in which case this restriction does not apply to the excluded fields.

The following class restrictions are imposed by the DiffServ design:

- nested class support limited to:
  - 'any' within 'any'
  - 'all' within 'all'
  - no nested 'not' conditions
  - no nested 'acl' class types
  - each class contains at most one referenced class
- hierarchical service policies not supported in a class definition
- access list matched by reference only, and must be sole criterion in a class
  - i.e., ACL rules copied as class match criteria at time of class creation, with class type 'any'
  - implicit ACL 'deny all' rule also copied
  - no nesting of class type 'acl'

Regarding nested classes, referred to here as class references, a given class definition can contain at most one reference to another class, which can be combined with other match criteria. The referenced class is truly a reference and not a copy, since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes otherwise the change is rejected. A class reference may be removed from a class definition.

The user can display summary and detailed information for classes, policies and services. All configuration information is accessible via the CLI, Web, and SNMP user interfaces.

9.3.1 diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

- **Format** **diffserv**
- **Mode** **Global Config**

9.3.1.1 no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

- **Format** **no diffserv**
- **Mode** **Global Config**

9.4 Class Commands

The 'class' command set is used in DiffServ to define:

- **Traffic Classification -** Specify Behavior Aggregate (BA), based on DSCP, and Multi-Field (MF) classes of traffic (name, match criteria)
- **Service Levels -** Specify the BA forwarding classes / service levels. Conceptually, DiffServ is a twolevel hierarchy of classes: 1. Service/PHB, 2. Traffic Class

This set of commands consists of class creation/deletion and matching, with the class match commands specifying layer 3, layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic belonging to the class.

Note that once a class match criterion is created for a class, it cannot be changed or deleted - the entire class must be deleted and re-created.

The CLI command root is **class-map**.

9.4.1 class-map

This command defines a new DiffServ class of type match-all, match-any or match-access-group. The **<classname>** parameter is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class (Note: the class name 'default' is reserved and must not be used here).

When used without any match condition, this command enters the class-map mode. The **<classname>** is the name of an existing DiffServ class (note: the class name 'default' is reserved and is not allowed here)

The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.

The class type of **match-any** indicates only one of the match criteria must be true for a packet to belong to the class; multiple matching criteria are evaluated in a sequential order, with the highest precedence awarded to the first criterion defined for the class.

The class type of **match-access-group** indicates the individual class match criteria are evaluated based on an access list (ACL). The **<aclid>** parameter is an integer specifying an existing ACL number (refer to the appropriate ACL documentation for the valid ACL number range). A **match-access-group** class type copies its set of match criteria from the current rule definition of the specified ACL number. All elements of a single ACL Rule are treated by DiffServ as a grouped set, similar to class type all.

For any class, at least one class match condition must be specified for the class to be considered valid.

✍ ***Note:*** The class match conditions are obtained from the referenced access list at the time of class creation. Thus, any subsequent changes to the referenced ACL definition do not affect the DiffServ class. To pick up the latest ACL definition, the DiffServ class must be deleted and re-created.

This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

✍ ***Note:*** The CLI mode is changed to Class-Map Config when this command is successfully executed.

- **Format** **class-map [{match-all | match-any | match-access-group <aclid>}] <classmapname>**
- **Mode** **Global Config**

9.4.1.1 no class-map

This command eliminates an existing DiffServ class. The <classname> is the name of an existing DiffServ class (note: the class name 'default' is reserved and is not allowed here). This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, this deletion attempt shall fail.

- **Format** **no class-map <classname>**
- **Mode** **Global Config**

9.4.2 class-map rename

This command changes the name of a DiffServ class. The <classname> is the name of an existing DiffServ class. The <newclassname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class (Note: the class name 'default' is reserved and must not be used here).

- **Default** **None**
- **Format** **class-map rename <classname> <newclassname>**
- **Mode** **Global Config**

9.4.3 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. The optional [not] parameter has the effect of negating this match condition for the class (i.e., none of the packets are considered to belong to the class).

- **Default** **None**
- **Format** **match [not] any**
- **Mode** **Class-Map Config**

9.4.4 match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The <refclassname> is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

✍ ***Note:*** There is no [not] option for this match command.

- **Default** **None**

- **Format** **match class-map <refclassname>**
- **Mode** **Class-Map Config**

Restrictions - The class types of both **<classname>** and **<refclassname>** must be identical (i.e., any vs. any, or all vs. all). A class type of acl is not supported by this command. Cannot specify **<refclassname>** the same as **<classname>** (i.e., self-referencing of class name not allowed).

At most one other class may be referenced by a class.

Any attempt to delete the **<refclassname>** class while still referenced by any **<classname>** shall fail.

The combined match criteria of **<classname>** and **<refclassname>** must be an allowed combination based on the class type. Any subsequent changes to the **<refclassname>** class match criteria must maintain this validity, or the change attempt shall fail.

The total number of class rules formed by the complete reference class chain (includes both predecessor and successor classes) must not exceed a platform-specific maximum.

In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

9.4.4.1 no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The <refclassname> is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition. Note: there is no [not] option for this match command.

- **Default** **None**
- **Format** **no match class-map <refclassname>**
- **Mode** **Class-Map Config**

9.4.5 match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The **<macaddr>** parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The **<macmask>** parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all destination MAC addresses except for what is specified here).

- **Default** **None**
- **Format** **match [not] destination-address mac <macaddr> <macmask>**
- **Mode** **Class-Map Config**

9.4.6 match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The <ipaddr> parameter specifies an IP address. The <ipmask> parameter specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all destination IP addresses except for what is specified here).

- **Default** **None**
- **Format** **match [not] dstip <ipaddr> <ipmask>**

- **Mode** **Class-Map Config**

9.4.7 match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

To specify the match condition as a single keyword, the value for **<portkey>** is one of the supported port name keywords. The currently supported **<portkey>** values are: **domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.** Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

To specify the match condition using a numeric range notation, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all destination layer 4 port numbers except for the one specified here).

- **Default** **None**
- **Format** **match [not] dstl4port {<portkey> | <0-65535> [<0-65535>]}**
- **Mode** **Class-Map Config**

9.4.8 match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked). The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all IP DSCP values except for what is specified here). The **<dscpval>** value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**

✍ ***Note:*** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

✍ ***Note:*** To specify a match on all DSCP values, use the match [not] ip tos <tosbits> <tosmask> command with **<tosbits>** set to 0 and **<tosmask>** set to 03 (hex).

- **Default** **None**
- **Format** **match [not] ip dscp <dscpval>**
- **Mode** **Class-Map Config**

9.4.9 match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked).

The precedence value is an integer from 0 to 7. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all IP Precedence values except for what is specified here).

✍ ***Note:*** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

✍ ***Note:*** To specify a match on all Precedence values, use the match [not] ip tos <tosbits> <tosmask> command with <tosbits> set to 0 and <tosmask> set to 1F (hex).

- **Default** **None**
- **Format** **match [not] ip precedence <0-7>**
- **Mode** **Class-Map Config**

9.4.10 match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of **<tosbits>** is a two-digit hexadecimal number from 00 to ff. The value of **<tosmask>** is a two-digit hexadecimal number from 00 to ff. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all IP Precedence values except for what is specified here). The **<tosmask>** denotes the bit positions in **<tosbits>** that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a **<tosbits>** value of a0 (hex) and a **<tosmask>** of a2 (hex).

✍ ***Note:*** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

✍ ***Note:*** In essence, this the "free form" version of the IP DSCP/Precedence/TOS match specification in that the user has complete control of specifying which bits of the IP Service Type field are checked.

- **Default** **None**
- **Format** **match [not] ip tos <tosbits> <tosmask>**
- **Mode** **Class-Map Config**

9.4.11 match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for **<protocol-name>** is one of the supported protocol name keywords. The currently supported values are: **icmp, igmp, ip, tcp, udp**.

Note that a value of **ip** is interpreted to match all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Note: This command does not validate the protocol number value against the current list defined by IANA.

The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all IP Protocol numbers except for the one specified here).

- ▫ **Default None**
- ▫ **Format match [not] protocol {<protocol-name> | <0-255>}**
- ▫ **Mode Class-Map Config**

9.4.12 match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The **<address>** parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The **<macmask>** parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all source MAC addresses except for what is specified here).

- ▫ **Default None**
- ▫ **Format match [not] source-address mac <address> <macmask>**
- ▫ **Mode Class-Map Config**

9.4.13 match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The **<ipaddr>** parameter specifies an IP address. The **<ipmask>** parameter specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous. The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all source IP addresses except for what is specified here).

- ▫ **Default None**
- ▫ **Format match [not] srcip <ipaddr> <ipmask>**
- ▫ **Mode Class-Map Config**

9.4.14 match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

To specify the match condition as a single keyword notation, the value for <portkey> is one of the supported port name keywords (listed below).

The currently supported **<portkey>** values are: **domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

To specify the match condition as a range, rwo layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first. The optional [not] parameter has the effect of negating this match condition for the class (i.e., match all source layer 4 ports except for those within the range specified here).

The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all source layer 4 port numbers except for the one specified here).

- ▫ **Default None**

- **Format** **match [not] srcl4port {<portkey> | <0-65535> [<0-65535>]}**
- **Mode** **Class-Map Config**

9.4.15 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field of a packet. The VLAN ID is an integer from 1 to 4094. The optional **[not]** parameter has the effect of negating this match condition for the class (i.e., match all VLAN Identifier values except for what is specified here).

- **Default** **None**
- **Format** **match [not] vlan <1-4094>**
- **Mode** **Class-Map Config**

9.5 Policy Commands

The 'policy' command set is used in DiffServ to define:

- **Traffic Conditioning** Specify traffic conditioning actions (policing, marking, shaping) to apply to traffic classes
- **Service Provisioning** Specify bandwidth and queue depth management requirements of service levels (EF, AF, etc.)

The policy commands are used to associate a traffic class, which was defined by the class command set, with one or more QoS policy attributes. This association is then assigned to an interface in a particular direction to form a service. The user specifies the policy name when the policy is created.

The DiffServ CLI does not necessarily require that users associate only one traffic class to one policy. In fact, multiple traffic classes can be associated with a single policy, each defining a particular treatment for packets that match the class definition. When a packet satisfies the conditions of more than one class, preference is based on the order in which the classes were added to the policy, with the foremost class taking highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes. Note that the only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is policy-map.

9.5.1 bandwidth kbps

This command identifies a minimum amount of bandwidth to be reserved for the specified class instance within the named policy using an absolute rate notation. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295.

Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

Note: The bandwidth kbps and percent commands are alternative ways to specify the same bandwidth policy attribute.

- **Format** **bandwidth kbps <1-4294967295>**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type -** Out

- **Incompatibilities -** Expedite (all forms)

9.5.2 bandwidth percent

This command identifies a minimum amount of bandwidth to be reserved for the specified class instance within the named policy using a relative rate notation. The committed information rate is specified as a percentage of total link capacity and is an integer from 1 to 100.

Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

✍ ***Note:*** The bandwidth kbps and percent commands are alternative ways to specify the same bandwidth policy attribute.

- **Format** **bandwidth percent <1-100>**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type -** Out
- **Incompatibilities -** Expedite (all forms)

9.5.3 class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The **<classname>** is the name of an existing DiffServ class. Note that this command causes the specified policy to create a reference to the class definition.

✍ ***Note:*** The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

- **Format** **class <classname>**
- **Mode** **Policy-Map Config**

9.5.3.1 no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. **<classname>** is the names of an existing DiffServ class. Note that this command removes the reference to the class definition for the specified policy.

- **Format** **no class <classname>**
- **Mode** **Policy-Map Config**

9.5.4 expedite kbps

This command identifies the maximum guaranteed amount of bandwidth to be reserved for the specified class instance within the named policy using an absolute rate notation. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The optional committed burst size is specified in kilobytes (KB) as an integer from 1 to 128, with a default of 4.

✍ ***Note:*** The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

✍ ***Note:*** The expedite kbps and percent commands are alternative ways to specify the same expedite policy attribute.

- **Format** **expedite kbps <1-4294967295> [1-128]**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type -** Out
- **Incompatibilities -** Bandwidth (all forms), Shape Peak

9.5.5 expedite percent

This command identifies the maximum guaranteed amount of bandwidth to be reserved for the specified class instance within the named policy using a relative rate notation. The committed information rate is specified as a percentage of total link capacity and is an integer from 1 to 100. The optional committed burst size is specified in kilobytes (KB) as an integer from 1 to 128, with a default of 4.

✍ ***Note:*** The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

✍ ***Note:*** The expedite kbps and percent commands are alternative ways to specify the same expedite policy attribute.

- **Format** **expedite percent <1-100> [1-128]**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.
- **Policy Type -** Out
- **Incompatibilities -** Bandwidth (all forms), Shape Peak

9.5.6 mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value. The **<dscpval>** value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**

- **Format** **mark ip-dscp <dscpval>**
- **Mode** **Policy-Class-Map Config**
- **Policy Type -** In
- **Incompatibilities -** Mark IP Precedence, Police (all forms)

9.5.7 mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

- **Format** **mark ip-precedence <0-7>**
- **Mode** **Policy-Class-Map Config**
- **Policy Type -** In
- **Incompatibilities -** Mark IP DSCP, Police (all forms)

9.5.8 police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and nonconform. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a **<dscpval>** value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

- **Format** **police-simple {<1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscptransmit <0-63> | transmit}]}**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.
- **Policy Type -** In
- **Incompatibilities -** Mark IP DSCP, Mark IP Precedence

9.5.9 police-single-rate

This command is used to establish the traffic policing style for the specified class. The single-rate form of the police command uses a single data rate and two burst sizes, resulting in three outcomes: conform, exceed and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) as an integer from 1 to 128. The exceeding burst size is specified in kilobytes (KB) as an integer from 1 to 128. Note that the exceeding burst size must be equal to or greater than the conforming burst size.

For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or transmit. In this singlerate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a **<dscpval>** value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4,**

cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

- **Format police-single-rate {<1-4294967295> <1-128> <1-128> conformaction {drop | set-prec-transmit <0-7> | set-dscp-transmit <0- 63> | transmit} exceed-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit}]}**
- **Mode Policy-Class-Map Config**
- **Restrictions -** Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.
- **Policy Type -** In
- **Incompatibilities -** Mark IP DSCP, Mark IP Precedence

9.5.10 police-two-rate

This command is used to establish the traffic policing style for the specified class. The two-rate form of the police command uses two data rates and two burst sizes, resulting in three outcomes: conform, exceed and violate. The first two data parameters are the conforming data rate and burst size. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295, while the conforming burst size is specified in kilobytes (KB) as an integer from 1 to 128. The next two data parameters are the peak data rate and burst size. The peak data rate is specified in kilobits-persecond (Kbps) as an integer from 1 to 4294967295, while the peak burst size is specified in kilobytes (KB) as an integer from 1 to 128. Note that the peak data rate must be equal to or greater than the conforming data rate.

For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a **<dscpval>** value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.**

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

- **Format police-two-rate {<1-4294967295> <1-128> <1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} exceed-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | transmit}]}**
- **Mode Policy-Class-Map Config**
- **Restrictions -** Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.
- **Policy Type -** In
- **Incompatibilities -** Mark IP DSCP, Mark IP Precedence

9.5.11 policy-map

This command establishes a new DiffServ policy. The <policyname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to either the inbound or outbound traffic direction as indicated by the {in | out} parameter.

✍ ***Note:*** The policy type dictates which of the individual policy attribute commands are valid within the policy definition.

✍ ***Note:*** The CLI mode is changed to Policy-Map Config when this command is successfully executed.

- **Format** **policy-map <policyname> {in | out}**
- **Mode** **Global Config**

9.5.11.1 no policy-map

This command eliminates an existing DiffServ policy. The <policyname> parameter is the name of an existing DiffServ policy. This command may be issued at any time; if the policy is currently referenced by one or more interface service attachments, this deletion attempt shall fail.

- **Format** **no policy-map <policyname>**
- **Mode** **Global Config**

9.5.12 policy-map rename

This command changes the name of a DiffServ policy. The **<policyname>** is the name of an existing DiffServ class. The **<newpolicyname>** parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

- **Format** **policy-map rename <policyname> <newpolicyname>**
- **Mode** **Global Config**

9.5.13 randomdrop

This command changes the active queue depth management scheme from the default tail drop to RED. The first two data parameters are the average queue depth minimum and maximum threshold values specified in bytes. The minimum threshold is an integer from 1 to 250000. The maximum threshold is an integer from 1 to 500000, but it must be equal to or greater than the minimum threshold. The third data parameter is the maximum drop probability and is an integer from 0 to 100. It indicates the percentage likelihood that a packet will be dropped when the average queue depth reaches the maximum threshold value. The remaining parameters are all optional. The fourth data parameter is the sampling rate, indicating the period at which the queue is sampled for computing the average depth. Expressed in microseconds, the sampling rate is an integer from 0 to 1000000, with a default of 0 (meaning per-packet sampling). The last parameter is the decay exponent, which determines how quickly the average queue length calculation decays over time, with a higher number producing a faster rate of decay. This value is an integer from 0 to 16, with a default of 9.

✍ ***Note:*** The last two parameters, namely sampling rate and decay exponent, are hierarchically specified in this command.

That is, in order to provide a value for the decay exponent <0-16>, the user is required to also specify a sampling rate **<0-1000000>** for proper command interpretation.

- **Format** **randomdrop <1-250000> <1-500000> <0-100> [<0-1000000> [<0-16>]]**
- **Mode** **Policy-Class-Map Config**
- **Policy Type -** Out

9.5.14 shape bps-average

This command is used to establish average rate traffic shaping for the specified class, which limits transmissions for the class to the committed information rate, with excess traffic delayed via queuing. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295.

✍ ***Note:*** Queue depth management defaults to tail drop, but the randomdrop command can be used to change to a RED scheme.

- **Format** **shape bps-average <1-4294967295>**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** This shaping rate must not exceed the maximum link data rate of the interface to which the policy is applied.
- **Policy Type -** Out

9.5.15 shape bps-peak

This command is used to establish peak rate traffic shaping for the specified class, which allows transmissions for the class to exceed the committed information rate by sending excess traffic with the understanding that it could be dropped by a downstream network element. Two rate parameters are used, a committed information rate and a peak information rate. Each of these rates is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The peak rate must be specified as equal to or greater than the committed rate.

✍ ***Note:*** Queue depth management defaults to tail drop, but the randomdrop command can be used to change to a RED scheme.

- **Format** **shape bps-peak <1-4294967295> <1-4294967295>**
- **Mode** **Policy-Class-Map Config**
- **Restrictions -** Neither of the shaping rate parameters is allowed to exceed the maximum link data rate of the interface to which the policy is applied.
- **Policy Type -** Out
- **Incompatibilities -** Expedite (all forms)

9.6 Service Commands

The 'service' command set is used in DiffServ to define:

- **Traffic Conditioning** Assign a DiffServ traffic conditioning policy (as specified by the policy commands) to an interface in the incoming direction
- **Service Provisioning** Assign a DiffServ service provisioning policy (as specified by the policy commands) to an interface in the outgoing direction

The service commands attach a defined policy to a directional interface. Only one policy may be assigned at any one time to an interface in a particular direction. The policy type (in, out) must match the interface direction to which it is attached.

This set of commands consists of service addition/removal.

The CLI command root is **service-policy**

9.6.1 service-policy

This command attaches a policy to an interface in a particular direction. The command can be used in the **Interface Config** mode to attach a policy to a specific interface. Alternatively, the command can be used in the **Global Config** mode to attach this policy to all system interfaces. The direction value is either in or out. The **<policyname>** parameter is the name of an existing DiffServ policy, whose type must match the interface direction. Note that this command causes a service to create a reference to the policy.

✍ ***Note:*** This command effectively enables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

Note: This command shall fail if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition such that it would result in a violation of said interface capabilities shall cause the policy change attempt to fail.

- **Format** **service-policy {in | out} <policymapname>**
- **Modes** **Global Config (for all system interfaces)**

  Interface Config (for a specific interface)
- **Restrictions** Only a single policy may be attached to a particular interface in a particular direction at any one time.

9.6.1.1 no service-policy

This command detaches a policy from an interface in a particular direction. The command can be used in the Interface Config mode to detach a policy from a specific interface. Alternatively, the command can be used in the Global Config mode to detach this policy from all system interfaces to which it is currently attached. The direction value is either in or out. The **<policyname>** parameter is the name of an existing DiffServ policy. Note that this command causes a service to remove its reference to the policy.

✍ ***Note:*** This command effectively disables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

- **Format** **no service-policy {in | out} <policymapname>**
- **Modes** **Global Config (for all system interfaces)**

Interface Config (for a specific interface)

9.7 Show Commands

The 'show' command set is used in DiffServ to display configuration and status information for:

- **Classes**
- **Policies**
- **Services**

This information can be displayed in either summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled; it is suppressed otherwise.

There is also a 'show' command for general DiffServ information that is available at any time.

9.7.1 show class-map

This command displays all configuration information for the specified class. The <classname> is the name of an existing DiffServ class.

- **Format show class-map [<classname>]**
- **Mode Privileged EXEC and User EXEC**

If the Class Name is specified the following fields are displayed:

- **Class Name -** The name of this class.
- **Class Type -** The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.
- **Match Criteria -** The Match Criteria fields will only be displayed if they have been configured. They will be displayed in the order entered by the user. These are evaluated in accordance with the class type. The possible Match Criteria fields are: Class of Service, Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, Source Layer 4 Port, Source MAC Address, and VLAN.
- **Values -** This field displays the values of the Match Criteria.
- **Excluded -** This field indicates whether or not this Match Criteria is excluded.

If the Class Name is not specified, this command displays a list of all defined DiffServ classes. The following fields are displayed:

- **Class Name -** The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
- **Class Type -** The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match.For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.
- **ACL Number -** The ACL number used to define the class match conditions at the time the class was created. This field is

only meaningful if the class type is acl. (Note that the contents of the ACL may have changed since this class was created.)

- **Ref Class Name -** The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

9.7.2 show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

- **Format show diffserv**
- **Mode Privileged EXEC**
- **DiffServ Admin mode -** The current value of the DiffServ administrative mode.
- **Class Table Size -** The current number of entries (rows) in the Class Table.
- **Class Table Max -** The maximum allowed entries (rows) for the Class Table.
- **Class Rule Table Size -** The current number of entries (rows) in the Class Rule Table.
- **Class Rule Table Max -** The maximum allowed entries (rows) for the Class Rule Table.
- **Policy Table Size -** The current number of entries (rows) in the Policy Table.
- **Policy Table Max -** The maximum allowed entries (rows) for the Policy Table.
- **Policy Instance Table Size -** The current number of entries (rows) in the Policy Instance Table.
- **Policy Instance Table Max -** The maximum allowed entries (rows) for the Policy Instance Table.
- **Policy Attribute Table Size -** The current number of entries (rows) in the Policy Attribute Table.
- **Policy Attribute Table Max -** The maximum allowed entries (rows) for the Policy Attribute Table.
- **Service Table Size -** The current number of entries (rows) in the Service Table.
- **Service Table Max -** The maximum allowed entries (rows) for the Service Table.

9.7.3 show policy-map

This command displays all configuration information for the specified policy. The <policyname> is the name of an existing DiffServ policy.

- **Format how policy-map [<policyname>]**
- **Mode Privileged EXEC**

If the Policy Name is specified the following fields are displayed:

- **Policy Name -** The name of this policy.
- **Type -** The policy type, namely whether it is an inbound or outbound policy definition.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

- **Class Name -** The name of this class.
- **Mark CoS -** Denotes the class of service value that is set in the 802.1p header of outbound packets. This is not displayed if the mark cos was not specified.
- **Mark IP DSCP -** Denotes the mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified using the police-two-rate command, or if policing is in use for the class under this

policy.

- **Mark IP Precedence -** Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if precedence is not specified using police-tworate command, or if either mark DSCP or policing is in use for the class under this policy.
- **Policing Style -** This field denotes the style of policing, if any, used (simple, single rate, or two rate).
- **Committed Rate (Kbps) -** This field displays the committed rate, used in simple policing, single-rate policing, and two-rate policing.
- **Committed Burst Size (KB) -** This field displays the committed burst size, used in simple policing, single-rate policing, and two-rate policing.
- **Excess Burst Size (KB) -** This field displays the excess burst size, used in single-rate policing.
- **Peak Rate (Kbps) -** This field displays the peak rate, used in two-rate policing.
- **Peak Burst Size (KB) -** This field displays the peak burst size, used in two-rate policing.
- **Conform Action -** The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
- **Conform DSCP Value -** This field shows the DSCP mark value if the conform action is markdscp.
- **Conform IP Precedence Value -** This field shows the IP Precedence mark value if the conform action is markprec.
- **Exceed Action -** The current setting for the action taken on a packet considered to exceed to the policing parameters. This is not displayed if policing not in use for the class under this policy.
- **Exceed DSCP Value -** This field shows the DSCP mark value if this action is markdscp.
- **Exceed IP Precedence Value -** This field shows the IP Precedence mark value if this action is markprec.
- **Non-Conform Action -** The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
- **Non-Conform DSCP Value -** This field displays the DSCP mark value if this action is markdscp.
- **Non-Conform IP Precedence Value -** This field displays the IP Precedence mark value if this action is markprec.
- **Bandwidth -** This field displays the minimum amount of bandwidth reserved in either percent or kilobits-per-second.
- **Expedite Burst Size (KBytes) -** This field displays the maximum guaranteed amount of bandwidth reserved in either percent or kilobits-per-second format.
- **Shaping Average -** This field is displayed if average shaping is in use. Indicates whether average or peak rate shaping is in use, along with the parameters used to form the traffic shaping criteria, such as CIR and PIR. This is not displayed if shaping is not configured for the class under this policy.
- **Shape Committed Rate (Kbps) -** This field is displayed if average or peak rate shaping is in use. It displays the shaping committed rate in kilobits-per-second.
- **Shape Peak Rate (Kbps) -** This field is displayed if peak rate shaping is in use. It displays the shaping peak rate in kilobits-per-second.
- **Random Drop Minimum Threshold -** This field displays the RED minimum threshold.This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Maximum Threshold -** This field displays the RED maximum threshold. This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Maximum Drop Probability -** This field displays the RED maximum drop probability. This is not displayed if the queue depth management scheme is not RED.

- **Random Drop Sampling Rate -** This field displays the RED sampling rate. This is not displayed if the queue depth management scheme is not RED.
- **Random Drop Decay Exponent -** This field displays the RED decay exponent. This is not displayed if the queue depth management scheme is not RED.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

- **Policy Name -** The name of this policy. (Note that the order in which the policies are displayed is not necessarily the same order in which they were created.)
- **Policy Type -** The policy type, namely whether it is an inbound or outbound policy definition.
- **Class Members -** List of all class names associated with this policy.

9.7.4 show diffserv service

This command displays policy service information for the specified interface and direction. The **<slot/port>** parameter specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

- **Format show diffserv service <slot/port> {in | out}**
- **Mode Privileged EXEC**
- **DiffServ Admin Mode -** The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
- **Interface -** The slot number and port number of the interface (slot/port).
- **Direction -** The traffic direction of this interface service, either in or out.
- **Operational Status -** The current operational status of this DiffServ service interface.
- **Policy Name -** The name of the policy attached to the interface in the indicated direction.
- **Policy Details -** Attached policy details, whose content is identical to that described for the show policy-map <policymapname> command (content not repeated here for brevity).

9.7.5 show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The direction parameter is optional; if specified, only services in the indicated direction are shown, otherwise service information is shown for both directions, where applicable.

- **Format show diffserv service brief [in | out]**
- **Mode Privileged EXEC**
- **DiffServ Mode -** The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Interface - The slot number and port number of the interface (slot/port).

Direction - The traffic direction of this interface service, either in or out.

OperStatus - The current operational status of this DiffServ service interface.

Policy Name - The name of the policy attached to the interface in the indicated direction.

9.7.6 show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The <slot/port> parameter specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

✍ **Note:** This command is only allowed while the DiffServ administrative mode is enabled.

- **Format show policy-map interface <slot/port> <in | out>**
- **Interface -** The slot number and port number of the interface (slot/port).
- **Direction -** The traffic direction of this interface service, either in or out.
- **Operational Status -** The current operational status of this DiffServ service interface.
- **Policy Name -** The name of the policy attached to the interface in the indicated direction.
- **Interface Offered Octets/Packets -** A cumulative count of the octets/packets offered to this service interface in the specified direction before the defined DiffServ treatment is applied.
- **Interface Discarded Octets/Packets -** A cumulative count of the octets/packets discarded by this service interface in the specified direction for any reason due to DiffServ treatment.
- **Interface Sent Octets/Packets -** A cumulative count of the octets/packets forwarded by this service interface in the specified direction after the defined DiffServ treatment was applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element.

The following information is repeated for each class instance within this policy:

- **Class Name -** The name of this class instance.
- **In Offered Octets/Packets -** A count of the octets/packets offered to this class instance before the defined DiffServ treatment is applied. Only displayed for the 'in' direction.
- **In Discarded Octets/Packets -** A count of the octets/packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class. Only displayed for the 'in' direction.
- **Tail Dropped Octets/Packets -** A count of the octets/packets discarded due to tail dropping from a transmission queue, typically due to the effects of traffic shaping. These counts may not be supported on all platforms. Only displayed for the 'out' direction.
- **Random Dropped Octets/Packets -** A count of the octets/packets discarded due to WRED active queue depth management, typically due to the effects of traffic shaping. These counts are only applicable for a class instance whose policy attributes includes random dropping, and may not be supported on all platforms. Only displayed for the 'out' direction.
- **Shape Delayed Octets/Packets -** A count of the octets/packets that were delayed due to traffic shaping. These counts are only applicable for a class instance whose policy attributes includes shaping, and may not be supported on all platforms. Only displayed for the 'out' direction.
- **Sent Octets/Packets -** A count of the octets/packets forwarded for this class instance after the defined DiffServ treatment was applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element. Only displayed for the 'out' direction.

✍ **Note:** None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

9.7.7 show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction. The direction parameter indicates the interface direction of interest.

This command enables or disables the route reflector client. A route reflector client relies on a route reflector to re-advertise its routes to the entire AS. The possible values for this field are enable and disable.

- **Format** **show service-policy [in | out]**
- **Mode** **Privileged EXEC**

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

- **Interface -** The slot number and port number of the interface (slot/port).
- **Dir -** The traffic direction of this interface service, either in or out.
- **Operational Status -** The current operational status of this DiffServ service interface.
- **Offered Packets -** A count of the total number of packets offered to all class instances in this service before their defined DiffServ treatment is applied. These are overall per-interface perdirection counts.
- **Discarded Packets -** A count of the total number of packets discarded for all class instances in this service for any reason due to DiffServ treatment. These are overall per-interface perdirection counts.
- **Sent Packets -** A count of the total number of packets forwarded for all class instances in this service after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element. These are overall per-interface per-direction counts.
- **Policy Name -** The name of the policy attached to the interface.

✍ ***Note:*** None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

9.8 Rate-Limiting Commands

9.8.1 rate-limiting

This command is used to set the bandwidth of a specified interface. The type of rate limiting is specific to either the inbound or outbound traffic direction as indicated by the **{ingress | egress}** parameter. The **<limit>** parameter defines the value of bandwidth in megabit-per-second (Mbps). The granularity of bandwidth for the 10/100 interface is 1 Mbps and for the gigabit interface is 8 Mbps.

- **Format** **rate-limiting {ingress | egress} <limit>**
- **Mode** **Interface Config**

9.8.1.1 no rate-limiting

This command removes the bandwidth limitation of specified interface.

- **Format** **no rate-limiting {ingress | egress}**
- **Mode** **Interface Config**

9.8.2 show rate-limiting

This command displays the bandwidth of limiting in both ingress and egress direction for one or all interface

- **Format** **show rate-limiting {<slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

10. CLI COMMANDS: SECURITY

10.1 Security Commands

This section describes commands used for configuring security settings for login users and port users.

10.1.1 authentication login

This command creates an authentication login list. The **<listname>** is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method "local" is set as the first method.

When the optional parameters "Option1", "Option2" and/or "Option3" are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list os first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are **local**, **radius** and **reject**.

The value of **local** indicates that the user's locally stored ID and password are used for authentication. The value of **radius** indicates that the user's ID and password will be authenticated using the RADIUS server. The value of **reject** indicates that the user is never authenticated.

To authenticate a user, the authentication methods in the user's login will be attempted in order until an authentication attempt succeeds or fails.

Note that the default login list included with the default configuration can not be changed.

- **Format** **authentication login <listname> [method1 [method2 [method3]]]**
- **Mode** **Global Config**

10.1.1.1 no authentication login

This command deletes the specified authentication login list. The attempt to delete will fail if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the nonconfigured user for any component
- The login list is the default login list included with the default configuration and was not created using 'authentication login'. The default login list cannot be deleted.
- **Format** **no authentication login <listname>**
- **Mode** **Global Config**

10.1.2 clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

- **Format** **clear dot1x statistics {<slot/port> | all}**
- **Mode** **Privileged EXEC**

10.1.3 clear radius statistics

This command is used to clear all RADIUS statistics.

- **Format clear radius statistics**
- **Mode Privileged EXEC**

10.1.4 dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

- **Format dot1x defaultlogin <listname>**
- **Mode Global Config**

10.1.5 dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

- **Format dot1x initialize <slot/port>**
- **Mode Privileged EXEC**

10.1.6 dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The <user> parameter must be a configured user and the **<listname>** parameter must be a configured authentication login list.

- **Format dot1x login <user> <listname>**
- **Mode Global Config**

10.1.7 dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The <count> value must be in the range 1 - 10.

- **Default 2**
- **Format dot1x max-req <count>**
- **Mode Interface Config**

10.1.7.1 no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant to the default value, i.e. 2.

- **Format no dot1x max-req**
- **Mode Interface Config**

10.1.8 dot1x port-control

This command sets the authentication mode to be used on the specified port. . The control mode may be one of the following.

- **force-unauthorized:** The authenticator PAE unconditionally sets the controlled port to unauthorized.
- **force-authorized:** The authenticator PAE unconditionally sets the controlled port to authorized.
- **auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.
- **Default auto**
- **Format dot1x port-control {force-unauthorized | force-authorized | auto}**
- **Mode Interface Config**

10.1.8.1 no dot1x port-control

This command sets the authentication mode to be used on the specified port to 'auto'.

- **Format no dot1x port-control**
- **Mode Interface Config**

10.1.9 dot1x port-control All

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.

- **force-unauthorized:** The authenticator PAE unconditionally sets the controlled port to unauthorized.
- **force-authorized:** The authenticator PAE unconditionally sets the controlled port to authorized.
- **auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.
- **Default auto**
- **Format dot1x port-control all {force-unauthorized | force-authorized | auto}**
- **Mode Global Config**

10.1.9.1 no dot1x port-control All

This command sets the authentication mode to be used on all ports to 'auto'.

- **Format no dot1x port-control all**
- **Mode Global Config**

10.1.10 dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

- **Format dot1x re-authenticate <slot/port>**
- **Mode Privileged EXEC**

10.1.11 dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

- **Default Disabled**
- **Format dot1x re-authentication**

- **Mode** **Interface Config**

10.1.11.1 no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

- **Format** **no dot1x re-authentication**
- **Mode** **Interface Config**

10.1.12 dot1x system-auth-control

This command is used to enable the dot1x authentication support on the switch. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

- **Default** **Disabled**
- **Format** **dot1x system-auth-control**
- **Mode** **Global Config**

10.1.12.1 no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

- **Format** **no dot1x system-auth-control**
- **Mode** **Global Config**

10.1.13 dot1x timeout

- This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported.
  reauth-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
- **quiet-period:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
- **tx-period:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
- **supp-timeout:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
- **server-timeout:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.
- **Default** **reauth-period:** 3600 seconds
  quiet-period: 60 seconds
  tx-period: 30 seconds
  supp-timeout: 30 seconds
  server-timeout: 30 seconds

- **Format dot1x timeout {{reauth-period <seconds>} | {quiet-period <seconds>} | {tx-period <seconds>} | {supp-timeout <seconds>} | {server-timeout <seconds>}}**
- **Mode Interface Config**

10.1.13.1 no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

- **Format no dot1x timeout {reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}**
- **Mode Interface Config**

10.1.14 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The <user> parameter must be a configured user.

- **Format dot1x user <user> {<slot/port> | all}**
- **Mode Global Config**

10.1.14.1 no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

- **Format no dot1x user <user> {<slot/port> | all}**
- **Mode Global Config**

10.1.15 radius accounting mode

This command is used to enable the RADIUS accounting function.

- **Default Disabled**
- **Format radius accounting mode**
- **Mode Global Config**

10.1.15.1 no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

- **Format no radius accounting mode**
- **Mode lobal Config**

10.1.16 radius server host

This command is used to configure the RADIUS authentication and accounting server. If the 'auth' token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the no form of the command. If the optional <port> parameter is used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.

If the 'acct' token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional <port> parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

- **Format** **radius server host {auth | acct} <ipaddr> [<port>]**
- **Mode** **lobal Config**

10.1.16.1 no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The **<ipaddr>** parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

- **Format** **no radius server host {auth | acct} <ipaddress>**
- **Mode** **Global Config**

10.1.17 radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the 'auth' or 'acct' token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

- **Format** **radius server key {auth | acct} <ipaddr>**
- **Mode** **Global Config**

10.1.18 radius server msgauth

This command enables the message authenticator attribute for a specified server.

- **Default** **radius server msgauth <ipaddr>**
- **Mode** **Global Config**

10.1.19 radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

- **Format** **radius server primary <ipaddr>**

- **Mode** **Global Config**

10.1.20 radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

- **Default** **10**
- **Format** **radius server retransmit <retries>**
- **Mode** **Global Config**

10.1.20.1 no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, i.e. 10.

- **Format** **no radius server retransmit**
- **Mode** **Global Config**

10.1.21 radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

- **Default** **6**
- **Format** **radius server timeout <seconds>**
- **Mode** **Global Config**

10.1.21.1 no radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received, to the default value, i.e. 6.

- **Format** **no radius server timeout**
- **Mode** **Global Config**

10.1.22 show accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

- **Format** **show accounting [statistics <ipaddr>]**
- **Mode** **Privileged EXEC**

If the optional token 'statistics <ipaddr>' is not included, then only the accounting mode and the RADIUS accounting server details are displayed.

- **Mode** **Enabled or disabled**
- **IP Address -** The configured IP address of the RADIUS accounting server
- **Port -**The port in use by the RADIUS accounting server
- **Secret Configured -** Yes or No

If the optional token 'statistics <ipaddr>' is included, the statistics for the configured RADIUS accounting server are displayed.

The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

- **Accounting Server IP Address -** IP Address of the configured RADIUS accounting server
- **Round Trip Time -** The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
- **Requests -** The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
- **Retransmission -** The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
- **Responses -** The number of RADIUS packets received on the accounting port from this server.
- **Malformed Responses -** 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.
- **Bad Authenticators -** The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
- **Pending Requests -** The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
- Timeouts - The number of accounting timeouts to this server.
- **Unknown Types -** The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
- **Packets Dropped -** The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

10.1.23 show authentication

This command displays the ordered authentication methods for all authentication login lists.

- **Format** **show authentication**
- **Mode** **Privileged EXEC**
- **Authentication Login List -** This displays the authentication login listname.
- **Method 1 -** This displays the first method in the specified authentication login list, if any.
- **Method 2 -** This displays the second method in the specified authentication login list, if any.
- **Method 3 -** This displays the third method in the specified authentication login list, if any.

10.1.24 show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user "default" will appear in the user column.

- **Format** **show authentication users <listname>**
- **Mode** **Privileged EXEC**
- **User -** This field displays the user assigned to the specified authentication login list.
- **Component -** This field displays the component (User or 802.1x) for which the authentication login list is assigned.

10.1.25 show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

- **Format show dot1x [{summary {<slot/port> | all}} | {detail <slot/port>} | {statistics <slot/port>}]**
- **Mode Privileged EXEC**

If none of the optional parameters are used, the global dot1x configuration summary is displayed.

- **Administrative mode -** Indicates whether authentication control on the switch is enabled or disabled.

If the optional parameter 'summary {<slot/port> | all}' is used, the dot1x configuration for the specified port or all ports are displayed.

- **Port -**The interface whose configuration is displayed.
- **Control Mode -** The configured control mode for this port. Possible values are force-unauthorized / force-authorized/ auto
- **Operating Control Mode -** The control mode under which this port is operating. Possible values are authorized/ unauthorized
- **Reauthentication Enabled -** Indicates whether re-authentication is enabled on this port.
- **Key Transmission Enabled -** Indicates if the key is transmitted to the supplicant for the specified port

If the optional parameter 'detail <slot/port>' is used, the detailed dot1x configuration for the specified port are displayed.

- **Port -** The interface whose configuration is displayed.
- **Protocol Version -** The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
- **PAE Capabilities -** The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
- **Authenticator PAE State -** Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
- **Backend Authentication State -** Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
- **Quiet Period -** The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
- **Transmit Period -** The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
- **Supplicant Timeout -** The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
- **Server Timeout -** The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
- **Maximum Requests -** The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
- **Reauthentication Period -** The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
- **Reauthentication Enabled -** Indicates if reauthentication is enabled on this port. Possible values are True or False.
- **Key Transmission Enabled -** Indicates if the key is transmitted to the supplicant for the specified port. Possible values

are True or False.

- **Control Direction -** Indicates the control direction for the specified port or ports. Possible values are both or in.

If the optional parameter 'statistics <slot/port>' is used, the dot1x statistics for the specified port are displayed.

- **Port -** The interface whose statistics are displayed.
- **EAPOL Frames Received -** The number of valid EAPOL frames of any type that have been received by this authenticator.
- **EAPOL Frames Transmitted -** The number of EAPOL frames of any type that have been transmitted by this authenticator.
- **EAPOL Start Frames Received -** The number of EAPOL start frames that have been received by this authenticator.
- **EAPOL Logoff Frames Received -** The number of EAPOL logoff frames that have been received by this authenticator.
- **Last EAPOL Frame Version -** The protocol version number carried in the most recently received EAPOL frame.
- **Last EAPOL Frame Source -** The source MAC address carried in the most recently received EAPOL frame.
- **EAP Response/Id Frames Received -** The number of EAP response/identity frames that have been received by this authenticator.
- **EAP Response Frames Received -** The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
- **EAP Request/Id Frames Transmitted -** The number of EAP request/identity frames that have been transmitted by this authenticator.
- **EAP Request Frames Transmitted -** The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
- **Invalid EAPOL Frames Received -** The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
- **EAP Length Error Frames Received -** The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

10.1.26 show dot1x users

This command displays 802.1x port security user information for locally configured users.

- **Format show dot1x users <slot/port>**
- **Mode Privileged EXEC**
- **User -** Users configured locally to have access to the specified port.

10.1.27 show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items will be displayed.

- **Format show radius [servers]**
- **Mode Privileged EXEC**
- **Primary Server IP Address -** Indicates the configured server currently in use for authentication
- **Number of configured servers -** The configured IP address of the authentication server
- **Max number of retransmits -** The configured value of the maximum number of times a request packet is retransmitted
- **Timeout Duration -** The configured timeout value, in seconds, for request re-transmissions

- **Accounting Mode -** Yes or No

If the optional token 'servers' is included, the following information regarding the configured RADIUS servers is displayed.

- **IP Address -** IP Address of the configured RADIUS server
- **Port -**The port in use by this server
- **Type -** Primary or secondary
- **Secret Configured -** Yes / No

10.1.28 show radius statistics

This command is used to display the statistics for RADIUS or configured server . To show the confifured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

- **Format show radius statistics [ipaddr]**
- **Mode Privileged EXEC**

If ip address is not specified than only Invalis Server Address filed is displayed. Otherwise other listed fields are displayed.

- **Invalid Server Addresses -** The number of RADIUS Access-Response packets received from unknown addresses.
- **Server IP Address**
- **Round Trip Time -** The time interval, in hundredths of a second, between the most recent Access-Reply/ Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
- **Access Requests -** The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
- **Access Retransmission -** The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
- **Access Accepts -** The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.
- **Access Rejects -** The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
- **Access Challenges -** The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.
- **Malformed Access Responses -** 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 unknown types are not included as malformed access responses.
- **Bad Authenticators -** The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
- **Pending Requests -** The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
- **Timeouts -** The number of authentication timeouts to this server.
- **Unknown Types -** The number of RADIUS packets of unknown types, which were received from this server on the authentication port.
- **Packets Dropped -** The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

10.1.29 show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

- **Format** **show users authentication**
- **Mode** **Privileged EXEC**
- **User -** This field lists every user that has an authentication login list assigned.
- **System Login -** This field displays the authentication login list assigned to the user for system login.
- **802.1x Port Security -** This field displays the authentication login list assigned to the user for 802.1x port security.

10.1.30 users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

- **Format users defaultlogin <listname>**
- **Mode Global Config**

10.1.31 users login

This command assigns the specified authentication login list to the specified user for system login. The **<user**> must be a configured **<user>** and the **<listname>** must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note that the login list associated with the 'admin' user can not be changed to prevent accidental lockout from the switch.

- **Format** **users login <user> <listname>**
- **Mode** **Global Config**

10.2 Secure Shell (SSH) Commands

The commands in this section is not supported currently

10.2.1 ip ssh

This command is used to enable SSH.

- **Default** **Disabled**
- **Format** **ip ssh**
- **Mode** **Privileged EXEC**

10.2.1.1 no ip ssh

This command is used to disable SSH.

- **Format** **no ip ssh**
- **Mode** **Privileged EXEC**

10.2.2 ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

- **Default** 1 and 2
- **Format** **ip ssh protocol [1] [2]**
- **Mode** **Privileged EXEC**

10.2.3 show ip ssh

This command displays the ssh settings.

- **Format** **show ip ssh**
- **Mode** **Privileged EXEC**
- **Administrative Mode -** This field indicates whether the administrative mode of SSH is enabled or disabled.
- **Protocol Level -** The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
- **Connections -** This field specifies the current ssh connections.

10.3 HTTP Commands

The commands in this section is not supported currently

10.3.1 ip http secure-port

This command is used to set the sslt port where port can be 1-65535 and the default is port 443.

- **Default** **443**
- **Format** **ip http secure-port <portid>**
- **Mode** **Privileged EXEC**

10.3.1.1 no ip http secure-port

This command is used to reset the sslt port to the default value.

- **Format** **no ip http secure-port**
- **Mode** **Privileged EXEC**

10.3.2 ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

- **Default** **SSL3 and TLS1**
- **Format** **ip http secure-protocol [SSL3] [TLS1]**
- **Mode** **Privileged EXEC**

10.3.2.1 no ip http secure-protocol

This command is used to remove protocol levels (versions) for secure HTTP.

- **Format** **no ip http secure-protocol [SSL3] [TLS1]**
- **Mode** **Privileged EXEC**

10.3.3 ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

- **Default Disabled**
- **Format ip http secure-server**
- **Mode Privileged EXEC**

10.3.3.1 no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

- **Format ip http secure-server**
- **Mode Privileged EXEC**

10.3.4 ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Disabling the Web interface takes effect immediately. All interfaces are effected.

- **Default enabled**
- **Format ip http server**
- **Mode Privileged EXEC**

10.3.4.1 no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

- **Default enabled**
- **Format no ip http server**
- **Mode Privileged EXEC**

10.3.5 show ip http

This command displays the http settings for the switch.

- **Format show ip http**
- **Mode Privileged EXEC**
- **Secure-Server Administrative Mode -** This field indicates whether the administrative mode of secure HTTP is enabled or disabled.
- **Secure Protocol Level -** The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
- **Secure Port -** This field specifies the port configured for SSLT.
- **HTTP Mode -** This field indicates whether the HTTP mode is enabled or disabled.

10.4 MAC Lock Commands

10.4.1 mac-lock

This command adds the specified MAC address with **<vlanid>** to a specified interface. The **<macaddr>** parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The **<vlanid>** parameter must identify a valid VLAN.

- **Format** **mac-lock <vlanid> <macaddr>**
- **Mode** **Interface Config**

10.4.1.1 no mac-lock

This command removes the MAC address with the MAC address of <macaddr> and VLAN of <vlanid> locked by the specified interface.

- **Format** **mac-lock <vlanid> <macaddr>**
- **Mode** **Interface Config**

10.4.2 show mac-lock

This command displays the vlan id and mac addresses that are locked at the specified interface for one or all interfaces.

- **Format** **show mac-lock {<slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

11. CLI COMMANDS: SWITCHING

11.1 Spanning Tree Commands

This section provides detailed explanation of the spanning tree commands. The commands are divided into two functional groups:

- **Show commands** display spanning tree settings, statistics, and other information.
- **Configuration Commands** configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.

11.1.1 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter "brief" is not included in the command. The following details are displayed.

- **Format show spanning-tree [brief]**
- **Mode Privileged EXEC and User EXEC**
- **Bridge Priority -** Configured value.
- **Bridge Identifier**
- **Time Since Topology Change -** in seconds
- **Topology Change Count -** Number of times changed.
- **Topology Change -** Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
- **Designated Root**
- **Root Path Cost -** Value of the Root Path Cost parameter for the common and internal spanning tree.
- **Root Port Identifier**
- **Root Port Max Age -** Derived value
- **Root Port Bridge Forward Delay -** Derived value
- **Hello Time -** Configured value
- Bridge Hold Time - Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)
- **CST Regional Root**
- **Regional Root Path Cost**
- **Associated FIDs -** List of forwarding database identifiers currently associated with this instance.
- **Associated VLANs -** List of VLAN IDs currently associated with this instance.

When the "brief" optional parameter is included, this command displays spanning tree settings for the bridge. In this case, the following details are displayed.

- **Bridge Priority** - Configured value.
- **Bridge Identifier**
- **Bridge Max Age -** Configured value.
- **Bridge Hello Time -** Configured value.
- **Bridge Forward Delay -** Configured value.

- **Bridge Hold Time -** Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

11.1.2 show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. The following details are displayed on execution of the command.

- **Format show spanning-tree interface <slot/port>**
- **Mode Privileged EXEC and User EXEC**
- **Port mode -** Enabled or disabled.
- **Port Up -** Time Since Counters Last Cleared Time since port was reset, displayed in days, hours, minutes, and seconds.
- **STP BPDUs -** Transmitted Spanning Tree Protocol Bridge Protocol Data Units sent
- **STP BPDUs Received -** Spanning Tree Protocol Bridge Protocol Data Units received.
- **RST BPDUs Transmitted -** Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
- **RST BPDUs Received -** Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
- **MSTP BPDUs Transmitted -** Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
- **MSTP BPDUs Received -** Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

11.1.3 show spanning-tree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance. The instance **<mstid>** is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

- **Format show spanning-tree mst detailed <mstid>**
- **Mode Privileged EXEC and User EXEC**
- **MST Instance ID**
- **MST Bridge Priority**
- **Time Since Topology Change -** in seconds
- **Topology Change Count -** Number of times the topology has changed for this multiple spanning tree instance.
- **Topology Change in Progress -** Value of the Topology Change parameter for the multiple spanning tree instance
- **Designated Root -** Identifier of the Regional Root for this multiple spanning tree instance.
- **Root Path Cost -** Path Cost to the Designated Root for this multiple spanning tree instance
- **Root Port Identifier -** Port to access the Designated Root for this multiple spanning tree instance
- **Associated FIDs -** List of forwarding database identifiers associated with this instance.
- **Associated VLANs -** List of VLAN IDs associated with this instance.

11.1.4 show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance **<mstid>** is a number that corresponds to the desired existing multiple spanning tree instance. The <slot/port> is the desired switch port.

- **Format show spanning-tree mst port detailed <mstid> <slot/port>**
- **Mode Privileged EXEC and User EXEC**
- **MST Instance ID**

- **Port Identifier**
- **Port Priority**
- **Port Forwarding State -** Current spanning tree state of this port
- **Port Role**
- **Port Path Cost -** Configured value of the Internal Port Path Cost parameter
- **Designated Root -** The Identifier of the designated root for this port.
- **Designated Port Cost -** Path Cost offered to the LAN by the Designated Port
- **Designated Bridge Bridge** - Identifier of the bridge with the Designated Port.
- **Designated Port Identifier -** Port on the Designated Bridge that offers the lowest cost to the LAN

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. In this case, the following are displayed.

- **Port Identifier -** The port identifier for this port within the CST.
- **Port Priority -** The priority of the port within the CST.
- **Port Forwarding State -** The forwarding state of the port within the CST.
- **Port Role -** The role of the specified interface within the CST.
- **Port Path Cost -** The configured path cost for the specified interface.
- **Designated Root -** Identifier of the designated root for this port within the CST.
- **Designated Port Cost -** Path Cost offered to the LAN by the Designated Port.
- **Designated Bridge -** The bridge containing the designated port
- **Designated Port Identifier -** Port on the Designated Bridge that offers the lowest cost to the LAN
- **Topology Change Acknowledgement -** Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
- **Hello Time -** The hello time in use for this port.
- **Edge Port -** The configured value indicating if this port is an edge port.
- **Edge Port Status -** The derived value of the edge port status. True if operating as an edge port; false otherwise.
- **Point To Point MAC Status -** Derived value indicating if this port is part of a point to point link.
- **CST Regional Root -** The regional root identifier in use for this port.
- **CST Port Cost -** The configured path cost for this port.

11.1.5 show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter <mstid> indicates a particular MST instance. The parameter {<slot/port> | all} indicates the desired switch port or all ports.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then the status summary is displayed for one or all ports within the common and internal spanning tree.

- **Format** **show spanning-tree mst port summary <mstid> {<slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**
- **MST** **Instance ID -** The MST instance associated with this port.
- **Slot/Port -** The interface being displayed
- **Type -** Currently not used.

- **STP State -** The forwarding state of the port in the specified spanning tree instance
- **Port Role -** The role of the specified port within the spanning tree.
- **Link Status -** The operational status of the link. Possible values are "Up" or "Down".
- **Link Trap -** The link trap configuration for the specified interface.

11.1.6 show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

- **Format show spanning-tree mst summary**
- **Mode Privileged EXEC and User EXEC**
- **MST Instance ID List - List of multiple spanning trees IDs currently configured.**
- **For each MSTID:**

  Associated FIDs - List of forwarding database identifiers associated with this instance.

  Associated VLANs - List of VLAN IDs associated with this instance.

11.1.7 show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

- **Format show spanning-tree summary**
- **Mode Privileged EXEC and User EXEC**
- **Spanning Tree Adminmode -** Enabled or disabled.
- **Spanning Tree Version -** Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter
- **Configuration Name -** Configured name.
- **Configuration Revision Level -** Configured value.
- **Configuration Digest Key -** Calculated value.
- **Configuration Format Selector -** Configured value.
- **MST Instances -** List of all multiple spanning tree instances configured on the switch

11.1.8 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID.

- **Format show spanning-tree vlan <vlanid>**
- **Mode Privileged EXEC and User EXEC**
- **VLAN Identifier**
- **Associated Instance -** Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree

11.1.9 spanning-tree

This command sets the spanning-tree operational mode to enabled.

- **Default** **Disabled**
- **Format** **spanning-tree**
- **Mode** **Global Config**

11.1.9.1 no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

- **Format** **no spanning-tree**
- **Mode** **Global Config**

11.1.10 spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The <name> is a string of at most 32 characters.

- **Default** The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.
- **Format** **spanning-tree configuration name <name>**
- **Mode** **Global Config**

11.1.10.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

- **Format** **no spanning-tree configuration name**
- **Mode** **Global Config**

11.1.11 spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

- **Default** **0**
- **Format** **spanning-tree configuration revision <0-65535>**
- **Mode** **Global Config**

11.1.11.1 no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, i.e. 0.

- Format no spanning-tree configuration revision
- Mode Global Config

11.1.12 spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

- **Format** **spanning-tree edgeport**
- **Mode** **Interface Config**

11.1.12.1 no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

- **Format** **no spanning-tree edgeport**
- **Mode** **Interface Config**

11.1.13 spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. The Force Protocol Version can be one of the following:

- **802.1d -** ST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1d functionality supported)
- **802.1w -** RST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1w functionality supported)
- **802.1s -** MST BPDUs are transmitted (IEEE 802.1s functionality supported)
- **Default** **802.1s**
- **Format** **spanning-tree forceversion <802.1d | 802.1w | 802.1s>**
- **Mode** **Global Config**

11.1.13.1 no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value, i.e. 802.1s.

- **Format** **no spanning-tree forceversion**
- **Mode** **Global Config**

11.1.14 spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

- **Default** **15**
- **Format** **spanning-tree forward-time <4-30>**
- **Mode** **Global Config**

11.1.14.1 no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, i.e. 15.

- **Format** **no spanning-tree forward-time**
- **Mode** **Global Config**

11.1.15 spanning-tree hello-time

This command sets the Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 10 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

- **Default** **2**

- **Format** **spanning-tree hello-time <1-10>**
- **Mode** **Global Config**

11.1.15.1 no spanning-tree hello-time

This command sets the Hello Time parameter for the common and internal spanning tree to the default value, i.e. 2.

- **Format** **no spanning-tree hello-time**
- **Mode** **Global Config**

11.1.16 spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)".

- **Default** **20**
- **Format** **spanning-tree max-age <6-40>**
- **Mode** **Global Config**

11.1.16.1 no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, i.e. 20.

- **Format** **no spanning-tree max-age**
- **Mode** **Global Config**

11.1.17 spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

- **Default** **cost : auto**
- **port-priorty : 128**
- **Format** **spanning-tree mst <mstid> {cost {<1-200000000> | auto} | port-priority <0-240>}**
- **Mode** **Interface Config**

11.1.17.1 no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree to the respective default values. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default

CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. a pathcost value based on the Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. 128.

- **Format** **no spanning-tree mst <mstid> {cost | port-priority}**
- **Mode** **Interface Config**

11.1.18 spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The instance <mstid> is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by this switch is 4.

- **Format** **spanning-tree mst instance <mstid>**
- **Mode** **Global Config**

11.1.18.1 no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

- **Format** **no spanning-tree mst instance <mstid>**
- **Mode** **Global Config**

11.1.19 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value again is a number within a range of 0 to 61440. The twelve least significant bits will be masked according to the 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

- **Default** **32768**
- **Format** **spanning-tree mst priority <mstid> <0-61440>**
- **Mode** **Global Config**

11.1.19.1 no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value, i.e. 32768. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, i.e. 32768.

- **Format** **spanning-tree mst priority <mstid>**
- **Mode** **Global Config**

11.1.20 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID.

- **Format** **spanning-tree mst vlan <mstid> <vlanid>**
- **Mode** **Global Config**

11.1.20.1 no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID.

- **Format** **no spanning-tree mst vlan <mstid> <vlanid>**
- **Mode** **Global Config**

11.1.21 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

- **Default** **Disabled**
- **Format** **spanning-tree port mode**
- **Mode** **Interface Config**

11.1.21.1 no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

- **Format** **no spanning-tree port mode**
- **Mode** **Interface Config**

11.1.22 spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

- **Default** **Disabled**
- **Format** **spanning-tree port mode all**
- **Mode** **Global Config**

11.1.22.1 no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

- **Format** **no spanning-tree port mode all**
- **Mode** **Global Config**

12. CLI COMMANDS: Routing

This chapter describes the routing commands available in the FASTPATH CLI.

The Routing Commands chapter contains the following sections:

The commands in this chapter are in one of three functional groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

12.1 Address Resolution Protocol (ARP) Commands

This section describes the commands you use to configure ARP and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

12.1.1 arp

This command creates an ARP entry. The value for <ipaddress> is the IP address of a device on a subnet attached to an existing routing interface. <macaddr> is a unicast MAC address for that device.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

- **Format** **arp <ipaddress> <macaddr>**
- **Mode** **Global Config**

12.1.2 no arp

This command deletes an ARP entry. The value for <arpentry> is the IP address of the interface. The value for <ipaddress> is the IP address of a device on a subnet attached to an existing routing interface. <macaddr> is a unicast MAC address for that device.

- **Format** **no arp <ipaddress> <macaddr>**

- **Mode** **Global Config**

12.1.3 ip proxy-arp

This command enables proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

- **Default** **enabled**
- **Format** **ip proxy-arp**
- **Mode** **Interface Config**

12.1.4 no ip proxy-arp

This command disables proxy ARP on a router interface.

- **Format** **no ip proxy-arp**
- **Mode** **Interface Config**

12.1.5 arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

- **Format** **arp cachesize <platform specific integer value>**
- **Mode** **Global Config**

12.1.6 no arp cachesize

This command configures the default ARP cache size.

- **Format** **no arp cachesize**
- **Mode** **Global Config**

12.1.7 arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out.

- **Default** **enable**
- **Format** **arp dynamicrenew**
- **Mode** **Priviledge EXEC**

12.1.8 no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

- **Format** **no arp dynamicrenew**
- **Mode** **Privileged EXEC**

12.1.9 arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

- **Format** **arp purge <ipaddr>**
- **Mode** **Privileged EXEC**

12.1.10 arp resptime

This command configures the ARP request response timeout.

The value for <seconds> is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for <seconds> is between 1-10 seconds.

- **Default** **l**
- **Format** **arp resptime <1-10>**
- **Mode** **Global Config**

12.1.11 no arp resptime

This command configures the default ARP request response timeout.

- **Format** **no arp resptime**
- **Mode** **Global Config**

12.1.12 arp retries

This command configures the ARP count of maximum request for retries.

The value for <retries> is an integer, which represents the maximum number of request for retries. The range for <retries> is an integer between 0-10 retries.

- **Default** **4**
- **Format** **arp retries <0-10>**
- **Mode** **Global Config**

12.1.13 no arp retries

This command configures the default ARP count of maximum request for retries.

- **Format** **no arp retries**

- **Mode** **Global Config**

12.1.14 arp timeout

This command configures the ARP entry ageout time.

The value for <seconds> is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for <seconds> is between 15-21600 seconds.

- **Default** **1200**
- **Format** **arp timeout <15-21600>**
- **Mode** **Global Config**

12.1.15 no arp timeout

This command configures the default ARP entry ageout time.

- **Format** **no arp timeout**
- **Mode** **Global Config**

12.1.16 clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the gateway keyword is specified, the dynamic entries of type gateway are purged as well.

- **Format** **clear arp-cache [gateway]**
- **Mode** **Privileged EXEC**

12.1.17 show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the show arp results in conjunction with the show arp switch results.

- **Format** **show arp**
- **Mode** **Privileged EXEC**

Age Time (seconds)	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time (seconds)	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.

Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry.

IP Address	Is the IP address of a device on a subnet attached to an existing routing interface.
MAC Address	Is the hardware MAC address of that device.
Interface	Is the routing slot/port associated with the device ARP entry.
Type	Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.
Age	This field displays the current age of the ARP entry since last refresh (in hh:mm:ss format

12.1.18 show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

- **Format** **show arp brief**
- **Mode** **Privileged EXEC**

Age Time (seconds)	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time (seconds)	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

12.1.19 show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

- **Format** **show arp switch**
- **Mode** **Privileged EXEC**

IP Address	Is the IP address of a device on a subnet attached to the switch.
MAC Address	Is the hardware MAC address of that device.
Interface	Is the routing slot/port associated with the device's ARP entry.

12.2 IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

12.2.1 routing

This command enables IPv4 and IPv6 routing for an interface. You can view the current value for this function with the **show ip brief** command. The value is labeled as "Routing Mode."

- **Default** **disabled**
- **Format** **routing**
- **Mode** **Interface Config**

12.2.2 no routing

This command disables routing for an interface.

You can view the current value for this function with the **show ip brief** command. The value is labeled as "Routing Mode."

- **Format** **no routing**
- **Mode** **Interface Config**

12.2.3 ip routing

This command enables the IP Router Admin Mode for the master switch.

- **Format** **ip routing**
- **Mode** **Global Config**

12.2.4 no ip routing

This command disables the IP Router Admin Mode for the master switch.

- **Format** **no ip routing**
- **Mode** **Global Config**

12.2.5 ip address

This command configures an IP address on an interface. You can also use this command to configure one or more secondary IP addresses on the interface.The value for <ipaddr> is the IP Address of the interface. The value for <subnetmask> is a 4-digit dotted-decimal number which represents the subnet mask of the interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command changes the label IP address in **show ip interface**.

- **Format** **ip address <ipaddr> <subnetmask> [secondary]**
- **Mode** **Interface Config**

12.2.6 no ip address

This command deletes an IP address from an interface. The value for <ipaddr> is the IP Address of the interface. The value for <subnetmask> is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface.

- **Format** **no ip address <ipaddr> <subnetmask> [secondary]**
- **Mode** **Interface Config**

12.2.7 ip route

This command configures a static route. The <ipaddr> parameter is a valid IP address, and <subnetmask> is a valid subnet mask. The <nexthopip> parameter is a valid IP address of the next hop router. The optional <preference> parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called "administrative distance") of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

Enable ip routing globally.

Enable ip routing for the interface.

Confirm that the associated link is also up.

- **Default** **preference-1**

- **Format** **ip route *<ipaddr> <subnetmask> [<nexthopip>][<preference>*]**
- **Mode** **Global Config**

12.2.8 no ip route

This command deletes a single next hop to a destination static route. If you use the <nexthopip> parameter, the next hop is deleted. If you use the <preference> value, the preference value of the static route is reset to its default.

- **Format** **no ip route <ipaddr> <subnetmask> [{<nexthopip> | <preference>}]**
- **Mode** **Global Config**

12.2.9 ip route default

This command configures the default route. The value for <nexthopip> is a valid IP address of the next hop router. The <preference> is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

- **Default** **preference—1**
- **Format** **ip route default *<nexthopip*> [*<preference*>]**
- **Mode** **Global Config**

12.2.10 no ip route default

This command deletes all configured default routes. If the optional <nexthopip> parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

- **Format** **no ip route default [*{<nexthopip*> | *<preference>}*]**
- **Mode** **Global Config**

12.2.11 ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ip route distance** command.

- **Default 1**

- **Format ip route distance <1-255>**
- **Mode Global Config**

12.2.12 no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

- **Format no ip route distance**
- **Mode Global Config**

12.2.13 ip forwarding

This command enables forwarding of IP frames.

- **Default enabled**
- **Format ip forwarding**
- **Mode Global Config**

12.2.14 no ip forwarding

This command disables forwarding of IP frames.

- **Format no ip forwarding**

Mode Global Config

12.2.15 ip netdirbcast

This command enables the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

- **Default disabled**
- **Format ip netdirbcast**
- **Mode Interface Config**

12.2.16 no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

- **Format** **no ip netdirbcast**

  Mode **Interface Config**

12.2.17 ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation.

FASTPATH software currently does not fragment IP packets.

Packets forwarded in hardware ignore the IP MTU.
Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.
OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the **ip ospf mtu-ignore** command.)

✍ ***Note:*** The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (See “mtu” on page 17.) must take into account the size of the Ethernet header.

- **Default** **1500 bytes**
- **Format** **ip mtu <68-1500>**
- **Mode** **Interface Config**

12.2.18 no ip mtu

This command resets the ip mtu to the default value.

- **Format** **no ip mtu <mtu>**
- **Mode** **Interface Config**

12.2.19 encapsulation

This command configures the link layer encapsulation type for the packet. The encapsulation type can be ethernet or snap.

- **Default** **ethernet**
- **Format** **encapsulation {ethernet | snap}**
- **Mode** **Interface Config**

✍ ***Note:*** Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

12.2.20 show ip brief

This command displays all the summary information of the IP.

- **Format** **show ip brief**
- **Modes** **Privileged EXEC**
  User EXEC
- **Default** **Time to Live**

The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.

Routing Mode Shows whether the routing mode is enabled or disabled.

IP Forwarding Mode Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.

Maximum Next Hops Shows the maximum number of next hops the packet can travel.

12.2.21 show ip interface

This command displays all pertinent information about the IP interface.

Format **show ip interface <slot/port>**

Modes **Privileged EXEC**
User EXEC

Primary IP Address Displays the primary IP address and subnet masks for the interface.
This value appears only if you configure it.

Secondary IP Address Displays one or more secondary IP addresses and subnet masks for the interface.
This value appears only if you configure it.

Routing Mode Is the administrative mode of router interface participation.
The possible values are **enable** or **disable**. This value was configured into the unit.

Administrative Mode Is the administrative mode of the specified interface. The possible values of this field are

enable or **disable**. This value was configured into the unit.

Routing Configuration Displays whether Routing Configuration is **enabled** or **disabled** on the system.

Interface Configuration Status Displays whether the Interface Configuration is **enabled** or **disabled** on the system.

Forward Net Directed Broadcasts Displays whether forwarding of network-directed broadcasts is **enabled** or **disabled**. This value was configured into the unit.

Proxy ARP Displays whether Proxy ARP is enabled or disabled on the system.

Local Proxy ARP Displays whether Local Proxy ARP is enabled or disabled on the interface.

Active State Displays whether the interface is **active** or **inactive**. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Data Rate Is an integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

MAC Address Is the burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons

Encapsulation Type Is the encapsulation type for the specified interface.
The types are: Ethernet or SNAP.

IP MTU Displays the maximum transmission unit (MTU) size of a frame, in bytes.

Example: show ip interface

```
(Routing) # show ip interface 0/2

Routing Configuration.............................. Enable
Interface Configuration Status................. Enable
Forward Net Directed Broadcasts............ Disable
Proxy ARP.................................... ……..Enable
Local Proxy ARP............................... …..Disable
Active State............................................ Active
Link Speed Data Rate............................ 100 Full
MAC Address.......................................... 00:10:4B:D2:17:83
Encapsulation Type................................ Ethernet
IP MTU.................................................. 1500
```

12.2.22 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

- **Format** **show ip interface brief**
- **Modes** **Privileged EXEC**

User EXEC

Interface Valid slot and port number separated by forward slashes.

IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are **Enable** or **Disable**.
MultiCast Fwd	Indicates the multicast forwarding administrative mode on the interface. Possible values are **Enable** or **Disable**.

12.2.23 show ip route

This command displays the routing table. The <ip-address> specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The <mask> specifies the subnet mask for the given <ip-address>. When you use the longer-prefixes keyword, the <ip-address> and <mask> pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the <protocol> parameter to specify the protocol that installed the routes. The value for <protocol> can be connected, ospf, rip, static, or bgp. Use the all parameter to display all routes including best and non-best routes. If you do not use the all parameter, the command only displays the best route.

✍ ***Note:*** If you use the connected keyword for <protocol>, the all option is not available because there are no best or non-best connected routes.

- ▫ **Format** **show ip route[{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]**
- ▫ **Mode** **Privileged EXEC**
  User EXEC

Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The **show ip route** command displays the routing tables in the following format:

Code	IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

The columns for the routing table display the following information:

Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are

	preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination
Interface	The outgoing router interface to use when forwarding traffic to the next destination

12.2.24 show ip route summary

Use this command to display the routing table summary. Use the optional all parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

- **Format** **show ip route summary [*all*]**
- **Mode** **Privileged EXEC**
  User EXEC

Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by BGP protocol.
OSPF Routes	Total number of routes installed by OSPF protocol.
Total Routes	Total number of routes in the routing table.

12.2.25 show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

- **Format** **show ip route preferences**
- **Modes** **Privileged EXEC**
  User EXEC

Local	This field displays the local route preference value.
Static	This field displays the static route preference value.
OSPF Intra	This field displays the OSPF Intra route preference value.
OSPF Inter	This field displays the OSPF Inter route preference value.
OSPF Ext T1	This field displays the OSPF External Type-1 route preference value.

OSPF Ext T2	This field displays the OSPF External Type-2 route preference value.
OSPF NSSA T1	This field displays the OSPF NSSA Type-1 route preference value.
OSPF NSSA T2	This field displays the OSPF NSSA Type-2 route preference value.
RIP	This field displays the RIP route preference value.
BGP4	This field displays the BGP-4 route preference value.

✍***Note:*** The configuration of NSSA preferences is not supported in this release.

12.2.26 show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

- **Format** **show ip stats**
- **Modes** **Privileged EXEC**

  User EXEC

12.3 Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

12.3.1 ip irdp

This command enables Router Discovery on an interface.

- **Default** **disabled**
- **Format** **ip irdp**
- **Mode** **Interface Config**

12.3.1.1 no ip irdp

This command disables Router Discovery on an interface.

- **Format** **no ip irdp**
- **Mode** **Interface Config**

12.3.2 ip irdp address

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for <ipaddr> are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

- **Default** **224.0.0.1**

- **Format ip irdp address <ipaddr>**
- **Mode Interface Config**

12.3.2.1 no ip irdp address

This command configures the default address used to advertise the router for the interface.

- **Format no ip irdp address**
- **Mode Interface Config**

12.3.3 ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of <maxadvertinterval> to 9000 seconds.

- **Default 3 * maxinterval**
- **Format ip irdp holdtime <maxadvertinterval-9000>**
- **Mode Interface Config**

12.3.3.1 no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

- **Format no ip irdp holdtime**
- **Mode Interface Config**

12.3.4 ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

- **Default 600**
- **Format ip irdp maxadvertinterval <*4-1800*>**
- **Mode Interface Config**

12.3.4.1 no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

- **Format no ip irdp maxadvertinterval**
- **Mode Interface Config**

12.3.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

- **Default 0.75 * maxadvertinterval**
- **Format ip irdp minadvertinterval <3-maxadvertinterval>**

- **Mode** **Interface Config**

12.3.5.1 no ip irdp minadvertinterval

This command sets the default minimum time to the default.

- **Format** **no ip irdp minadvertinterval**
- **Mode** **Interface Config**

12.3.6 ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

- **Default** **0**
- **Format** **ip irdp preference <-2147483648 to 2147483647>**
- **Mode** **Interface Config**

12.3.6.1 no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

- **Format** **no ip irdp preference**
- **Mode** **Interface Config**

12.3.7 show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

- **Format** **show ip irdp {<slot/port> | all}**
- **Modes** **Privileged EXEC**
  User EXEC

Interface	Shows the <slot/port> that matches the rest of the information in the row.
Ad Mode	Displays the advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Advertise Address	Displays the IP address to which the interface sends the advertisement.
Max Int	Displays the maximum advertise interval, which is the maximum time, in sec onds, allowed between sending router advertisements from the interface.
Min Int	Displays the minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	Displays the amount of time, in seconds, that a system should keep the router advertisement before discarding it.

Preference	Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

12.4 Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

12.4.1 vlan routing

This command creates routing on a VLAN. The <vlanid> value has a range from 1 to 4094.

Format **vlan routing <vlanid>**

Mode **VLAN Config**

12.4.1.1 no vlan routing

This command deletes routing on a VLAN. The <vlanid> value has a range from 1 to 4094.

Format **no vlan routing <vlanid>**

Mode **VLAN Config**

12.4.2 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format **show ip vlan**

Modes **Privileged EXEC**
User EXEC

MAC Address used by Routing VLANs	Is the MAC Address associated with the internal-bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	Is the identifier of the VLAN.
Logical Interface	Shows the logical slot/port associated with the VLAN routing interface.
IP Address	Displays the IP Address associated with this VLAN.
Subnet Mask	Indicates the subnet mask that is associated with this VLAN

12.5 Virtual Router Redundancy Protocol Commands

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

12.5.1 ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router. Default none

- **Format** **ip vrrp**
- **Mode** **Global Config**

12.5.1.1 no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

- **Format** **no ip vrrp**

Mode **Global Config**

12.5.2 ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface. The parameter <vrid>is the **virtual router ID**, which has an integer value range from **1 to 255**.

- **Format** **ip vrrp <vrid>**
- **Mode** **Interface Config**

12.5.2.1 no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, <vrid>, is an integer value that ranges from **1 to 255**.

- **Format** **no ip vrrp <vrid>**
- **Mode** **Interface Config**

12.5.3 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter <vrid> is the virtual router ID which has an integer value ranging from **1 to 255**.

- **Default** **disabled**
- **Format** **ip vrrp <vrid> mode**
- **Mode** **Interface Config**

12.5.3.1 no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

- **Format** **no ip vrrp <vrid> mode**
- **Mode** **Interface Config**

12.5.4 ip vrrp ip

This command sets the virtual router IP address value for an interface. The value for <ipaddr> is the IP address which is to be configured on that interface for VRRP. The parameter <vrid> is the virtual router ID which has an integer value range from 1 to

255. You can use the optional [secondary] parameter to designate the IP address as a secondary IP address.

- **Default none**
- **Format ip vrrp <vrid> ip <ipaddr> [secondary]**
- **Mode Interface Config**

12.5.4.1 no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

- **Format no ip vrrp <vrid> <ipaddress> secondary**
- **Mode Interface Config**

12.5.5 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter {none | simple} specifies the authorization type for virtual router configured on the specified interface. The parameter [key] is optional, it is only required when authorization type is simple text password. The parameter <vrid> is the virtual router ID which has an integer value ranges from 1 to 255.

- **Default no authorization**
- **Format ip vrrp <vrid> authentication {none | simple <key>}**
- **Mode Interface Config**

12.5.5.1 no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

- **Format no ip vrrp <vrid> authentication**
- **Mode Interface Config**

12.5.6 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. The parameter <vrid> is the virtual router ID, which is an integer from 1 to 255

- **Default enabled**
- **Format ip vrrp <vrid> preempt**
- **Mode Interface Config**

12.5.6.1 no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

- **Format no ip vrrp <vrid> preempt**
- **Mode Interface Config**

12.5.7 ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface. The priority of the interface is a priority integer from 1 to 254. The parameter <vrid> is the virtual router ID which has an integer value ranges from 1 to 255.

- **Default** **100**
- **Format** **ip vrrp <vrid> priority <1-254>**
- **Mode** **Interface Config**

12.5.7.1 no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

- **Format** **no ip vrrp <vrid> priority**
- **Mode** **Interface Config**

12.5.8 ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

- **Default** **1**
- **Format** **ip vrrp <vrid> timers advertise <1-255>**
- **Mode** **Interface Config**

12.5.8.1 no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface.

- **Format** **no ip vrrp <vrid> timers advertise**
- **Mode** **Interface Config**

12.5.9 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

- **Format** **show ip vrrp interface stats <slot/port> <vrid>**
- **Modes** **Privileged EXEC**
User EXEC

Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	Represents the protocol configured on the interface.
State Transitioned to Master	Represents the total number of times virtual router state has changed to MASTER.
Advertisement Received	Represents the total number of VRRP advertisements received by this virtual router.
Advertisement Interval	Represents the total number of VRRP advertisements received for which advertisement

Errors	interval is different than the configured value for this virtual router.
Authentication Failure	Represents the total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	Represents the total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	Represents the total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	Represents the total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	Represents the total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	Represents the total number of VRRP packets received with packet length less than length of VRRP header.

12.5.10 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring.

This command takes no options.

▫ **Format** **show ip vrrp**

▫ **Modes** **Privileged EXEC**
User EXEC

VRRP Admin Mode	Displays the administrative mode for VRRP functionality on the switch.
Router Checksum Errors	Represents the total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	Represents the total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	Represents the total number of VRRP packets received with invalid VRID for this virtual router.

12.5.11 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

- ▫ **Format** **show ip vrrp interface <slot/port> <vrid>**
- ▫ **Modes** **Privileged EXEC**
  User EXEC

IP Address	This field represents the configured IP Address for the Virtual router.
VMAC address	Represents the VMAC address of the specified router.
Authentication type	Represents the authentication type for the specific virtual router.
Priority	Represents the priority value for the specific virtual router.
Advertisement interval	Represents the advertisement interval for the specific virtual router.
Pre-Empt Mode	Is the preemption mode configured on the specified virtual router.
Administrative Mode	Represents the status (Enable or Disable) of the specific router.
State	Represents the state (Master/backup) of the virtual router.

12.5.12 show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

- ▫ **Format** **show ip vrrp interface brief**
- ▫ **Modes** **Privileged EXEC**
  User EXEC

Interface	Valid slot and port number separated by forward slashes.
VRID	Represents the router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Represents whether the virtual router is enabled or disabled.
State	Represents the state (Master/backup) of the virtual router

12.6 DHCP and BOOTP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

12.6.1 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

- ▫ **Default** **disabled**
- ▫ **Format** **bootpdhcprelay cidoptmode**

- **Mode Global Config**

12.6.1.1 no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

- **Format no bootpdhcprelay cidoptmode**
- **Mode Global Config**

12.6.2 bootpdhcprelay enable

This command enables the forwarding of relay requests for BootP/DHCP Relay on the system.

- **Default disabled**
- **Format bootpdhcprelay enable**
- **Mode Global Config**

12.6.2.1 no bootpdhcprelay enable

This command disables the forwarding of relay requests for BootP/DHCP Relay on the system.

- **Format no bootpdhcprelay enable**
- **Mode Global Config**

12.6.3 bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The <hops> parameter has a range of 1 to 16.

- **Default 4**
- **Format bootpdhcprelay maxhopcount <1-16>**
- **Mode Global Config**

12.6.3.1 no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

- **Format no bootpdhcprelay maxhopcount**
- **Mode Global Config**

12.6.4 bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

- **Default 0**
- **Format bootpdhcprelay minwaittime <0-100>**

- **Mode** **Global Config**

12.6.4.1 no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

- **Format** **no bootpdhcprelay minwaittime**
- **Mode** **Global Config**

12.6.5 bootpdhcprelay serverip

This command configures the server IP Address for BootP/DHCP Relay on the system. The <ipaddr> parameter is an IP address in a 4-digit dotted decimal format.

- **Default** **0.0.0.0**
- **Format** **bootpdhcprelay serverip <ipaddr>**
- **Mode** **Global Config**

12.6.5.1 no bootpdhcprelay serverip

This command configures the default server IP Address for BootP/DHCP Relay on the system.

- **Format** **no bootpdhcprelay serverip**
- **Mode** **Global Config**

12.6.6 show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

- **Format** **show bootpdhcprelay**
- **Modes** **Privileged EXEC**
  User EXEC

Maximum Hop Count	Is the maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	Is the minimum wait time.
Admin Mode	Represents whether relaying of requests is enabled or disabled.
Server IP Address	Is the IP Address for the BootP/DHCP Relay server.
Circuit Id Option Mode	Is the DHCP circuit Id option which may be enabled or disabled.
Requests Received	Is the number or requests received.
Requests Relayed	Is the number of requests relayed.
Packets Discarded	Is the number of packets discarded.

12.7 Open Shortest Path First (OSPF) Commands

This section describes the commands you use to view and configure OSPF, which is a link-state routing protocol that you use to route traffic within a network.

12.7.1 router ospf

Use this command to enter Router OSPF mode.

- **Format** **router ospf**
- **Mode** **Global Config**

12.7.2 enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

- **Default** **enabled**
- **Format** **enable**
- **Mode** **Router OSPF Config**

no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

- **Format** **no enable**
- **Mode** **Router OSPF Config**

12.7.3 ip ospf

This command enables OSPF on a router interface.

- **Default** **disabled**
- **Format** **ip ospf**
- **Mode** **Interface Config**

no ip ospf

This command disables OSPF on a router interface.

- **Format** **no ip ospf**
- **Mode** **Interface Config**

12.7.4 1583compatibility

This command enables OSPF 1583 compatibility.

NOTE: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

- **Default** **enabled**
- **Format** **1583compatibility**
- **Mode** **Router OSPF Config**

no 1583compatibility

This command disables OSPF 1583 compatibility.

- **Format** **no 1583compatibility**
- **Mode** **Router OSPF Config**

12.7.5 area default-cost (OSPF)

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215.

- **Format** **area <areaid> default-cost <1-16777215>**
- **Mode** **Router OSPF Config**

12.7.6 area nssa (OSPF)

This command configures the specified areaid to function as an NSSA.

- **Format** **area <areaid> nssa**
- **Mode** **Router OSPF Config**

no area nssa

This command disables nssa from the specified area id.

- **Format** **no area <areaid> nssa**
- **Mode** **Router OSPF Config**

12.7.7 area nssa default-info-originate (OSPF)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

- **Format** **area <areaid> nssa default-info-originate [<metric>] [{comparable | non-comparable}]**
- **Mode** **Router OSPF Config**

no area nssa default-info-originate (OSPF)

This command disables the default route advertised into the NSSA.

- **Format** **no area <areaid> nssa default-info-originate [<metric>] [{comparable | non-comparable}]**
- **Mode** **Router OSPF Config**

12.7.8 area nssa no-redistribute (OSPF)

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

- **Format** **area <areaid> nssa no-redistribute**
- **Mode** **Router OSPF Config**

no area nssa no-redistribute (OSPF)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

- **Format** **no area <areaid> nssa no-redistribute**
- **Mode** **Router OSPF Config**

12.7.9 area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

- **Format** **area <areaid> nssa no-summary**
- **Mode** **Router OSPF Config**

no area nssa no-summary (OSPF)

This command disables nssa from the summary LSAs.

- **Format** **no area <areaid> nssa no-summary**
- **Mode** **Router OSPF Config**

12.7.10 area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of always causes the router to assume the role of the translator the instant it becomes a border router and a value of candidate causes the router to participate in the translator election process when it attains border router status.

- **Format** **area <areaid> nssa translator-role {always | candidate}**
- **Mode** **Router OSPF Config**

no area nssa translator-role (OSPF)

This command disables the nssa translator role from the specified area id.

- **Format** **no area <areaid> nssa translator-role {always | candidate}**
- **Mode** **Router OSPF Config**

12.7.11 area nssa translator-stab-intv (OSPF)

This command configures the translator <stabilityinterval> of the NSSA. The <stabilityinterval> is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

- **Format** **area <areaid> nssa translator-stab-intv <stabilityinterval>**
- **Mode** **Router OSPF Config**

no area nssa translator-stab-intv (OSPF)

This command disables the nssa translator's <stabilityinterval> from the specified area id.

- **Format** **no area <areaid> nssa translator-stab-intv <stabilityinterval>**
- **Mode** **Router OSPF Config**

12.7.12 area range (OSPF)

This command creates a specified area range for a specified NSSA. The <ipaddr> is a valid IP address. The <subnetmask> is a valid subnet mask. The LSDB type must be specified by either **summarylink** or **nssaexternallink**, and the advertising of the area range can be allowed or suppressed.

- **Format** **area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise]**
- **Mode** **Router OSPF Config**

no area range

This command deletes a specified area range. The <ipaddr> is a valid IP address. The <subnetmask> is a valid subnet mask.

- **Format** **no area <areaid> range <ipaddr> <subnetmask>**
- **Mode** **Router OSPF Config**

12.7.13 area stub (OSPF)

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

- **Format** **area <areaid> stub**
- **Mode** **Router OSPF Config**

no area stub

This command deletes a stub area for the specified area ID.

- **Format** **no area <areaid> stub**

- **Mode Router OSPF Config**

12.7.14 area stub no-summary (OSPF)

This command configures the Summary LSA mode for the stub area identified by <areaid>. Use this command to prevent LSA Summaries from being sent.

- **Default disabled**
- **Format area <areaid> stub no-summary**
- **Mode Router OSPF Config**

no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by <areaid>.

- **Format no area <areaid> stub no-summary**
- **Mode Router OSPF Config**

12.7.15 area virtual-link (OSPF)

This command creates the OSPF virtual interface for the specified <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

- **Format area <areaid> virtual-link <neighbor>**
- **Mode Router OSPF Config**

no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

- **Format no area <areaid> virtual-link <neighbor>**
- **Mode Router OSPF Config**

12.7.16 area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor. The value for <type> is either none, simple, or encrypt. The [key] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified.The default value for authentication type is none. Neither the default password key nor the default key id are configured.

- **Default none**
- **Format area <areaid> virtual-link <neighbor> authentication {none | {simple <key>} | {encrypt <key> <keyid>}}**

- **Mode Router OSPF Config**

no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

- **Format no area <areaid> virtual-link <neighbor> authentication**
- **Mode Router OSPF Config**

12.7.17 area virtual-link dead-interval (OSPF)

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

- **Default 40**
- **Format area <areaid> virtual-link <neighbor> dead-interval <seconds>**
- **Mode Router OSPF Config**

no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

- **Format no area <areaid> virtual-link <neighbor> dead-interval**
- **Mode Router OSPF Config**

12.7.18 area virtual-link hello-interval (OSPF)

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor. The range for <seconds> is 1 to 65535.

- **Default 10**
- **Format area <areaid> virtual-link <neighbor> hello-interval <1-65535>**
- **Mode Router OSPF Config**

no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

- **Format no area <areaid> virtual-link <neighbor> hello-interval**
- **Mode Router OSPF Config**

12.7.19 area virtual-link retransmit-interval (OSPF)

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

- **Default 5**
- **Format area <areaid> virtual-link <neighbor> retransmit-interval <seconds>**
- **Mode Router OSPF Config**

no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

- **Format no area <areaid> virtual-link <neighbor> retransmit-interval**
- **Mode Router OSPF Config**

12.7.20 area virtual-link transmit-delay (OSPF)

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600 (1 hour).

- **Default 1**
- **Format area <areaid> virtual-link <neighbor> transmit-delay <seconds>**
- **Mode Router OSPF Config**

no area virtual-link transmit-delay

This command resets the default transmit delay for the OSPF virtual interface to the default value.

- **Format no area <areaid> virtual-link <neighbor> transmit-delay**
- **Mode Router OSPF Config**

12.7.21 default-information originate (OSPF)

This command is used to control the advertisement of default routes.

- **Default metric—unspecified type—2**
- **Format default-information originate [always] [metric <0-16777214>] [metric-type {1 | 2}]**
- **Mode Router OSPF Config**

no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

- **Format no default-information originate [metric] [metric-type]**
- **Mode Router OSPF Config**

12.7.22 default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

- **Format** **default-metric <1-16777214>**
- **Mode** **Router OSPF Config**

no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

- **Format** **no default-metric**
- **Mode** **Router OSPF Config**

12.7.23 distance ospf (OSPF)

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2. The <preference> range is 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

- **Default** **intra—8**
  inter—10
  type-1—13
  type-2—50
- **Format** **distance ospf {intra | inter | type1 | type2} <preference>**
- **Mode** **Router OSPF Config**

no distance ospf

This command sets the default route preference value of OSPF in the router. The type of OSPF can be intra, inter, type-1, or type-2.

- **Format** **no distance ospf {intra | inter | type1 | type2}**
- **Mode** **Router OSPF Config**

12.7.24 distribute-list out (OSPF)

Use this command to specify the access list to filter routes received from the source protocol.

- **Format** **distribute-list <1-199> out {rip | bgp | static | connected}**
- **Mode** **Router OSPF Config**

no distribute-list out

Use this command to specify the access list to filter routes received from the source protocol.

- **Format** **no distribute-list <1-199> out {rip | bgp | static | connected}**

- **Mode Router OSPF Config**

12.7.25 exit-overflow-interval (OSPF)

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs.

When set to 0, the router will not leave Overflow State until restarted. The range for seconds is 0 to 2147483647 seconds.

- **Default 0**
- **Format exit-overflow-interval <seconds>**
- **Mode Router OSPF Config**

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

- **Format no exit-overflow-interval**
- **Mode Router OSPF Config**

12.7.26 external-lsdb-limit (OSPF)

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.

- **Default - 1**
- **Format external-lsdb-limit <limit>**
- **Mode Router OSPF Config**

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

- **Format no external-lsdb-limit**
- **Mode Router OSPF Config**

12.7.27 ip ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The <areaid> is an IP address, formatted as a 4-digit dotted-decimal number or a decimal value in the range of <0-4294967295>. The <areaid> uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

- **Format ip ospf areaid <areaid>**

- **Mode** **Interface Config**

12.7.28 ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface. The value of <type> is either none, simple or encrypt. The [key] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. If the type is encrypt a <keyid> in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

- **Default** **none**
- **Format** **ip ospf authentication {none | {simple <key>} | {encrypt <key> <keyid>}}**
- **Mode** **Interface Config**

no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

- **Format** **no ip ospf authentication**
- **Mode** **Interface Config**

12.7.29 ip ospf cost

This command configures the cost on an OSPF interface. The <cost> parameter has a range of 1 to 65535.

- **Default** **10**
- **Format** **ip ospf cost <1-65535>**
- **Mode** **Interface Config**

no ip ospf cost

This command configures the default cost on an OSPF interface.

- **Format** **no ip ospf cost**
- **Mode** **Interface Config**

12.7.30 ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface. The value for <seconds> is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range for seconds is from 1 to 2147483647.

- **Default** **40**
- **Format** **ip ospf dead-interval <seconds>**
- **Mode** **Interface Config**

no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

- **Format** **no ip ospf dead-interval**
- **Mode Interface Config**

12.7.31 ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values range from 1 to 65535.

- **Default** **10**
- **Format** **ip ospf hello-interval <seconds>**
- **Mode** **Interface Config**

no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

- **Format** **no ip ospf hello-interval**
- **Mode** **Interface Config**

12.7.32 ip ospf priority

This command sets the OSPF priority for the specified router interface. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

- **Default** **1, which is the highest router priority.**
- **Format** **ip ospf priority <0-255>**
- **Mode** **Interface Config**

no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

- **Format** **no ip ospf priority**
- **Mode** **Interface Config**

12.7.33 ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. The retransmit interval is specified in seconds. The value for <seconds> is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

- **Default** **5**
- **Format** **ip ospf retransmit-interval <0-3600>**

- **Mode Interface Config**

no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

- **Format no ip ospf retransmit-interval**
- **Mode Interface Config**

12.7.34 ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for <seconds> range from 1 to 3600 (1 hour).

- **Default 1**
- **Format ip ospf transmit-delay <1-3600>**
- **Mode Interface Config**

no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

- **Format no ip ospf transmit-delay**
- **Mode Interface Config**

12.7.35 ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

- **Default enabled**
- **Format ip ospf mtu-ignore**
- **Mode Interface Config**

no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

- **Format no ip ospf mtu-ignore**
- **Mode Interface Config**

12.7.36 router-id (OSPF)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <ipaddress> is a configured value.

- **Format** **router-id <ipaddress>**
- **Mode** **Router OSPF Config**

12.7.37 redistribute (OSPF)

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

- **Default** **metric—unspecified**
  type—2
  tag—0
- **Format** **redistribute {rip | bgp | static | connected} [metric <016777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]**
- **Mode** **Router OSPF Config**

no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

- **Format** **no redistribute {rip | bgp | static | connected} [metric] [metric-type] [tag] [subnets]**
- **Mode** **Router OSPF Config**

12.7.38 maximum-paths (OSPF)

This command sets the number of paths that OSPF can report for a given destination where maxpaths is platform dependent.

- **Default** **4**
- **Format** **maximum-paths <maxpaths>**
- **Mode** **Router OSPF Config**

no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

- **Format** **no maximum-paths**
- **Mode** **Router OSPF Config**

12.7.39 timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

- **Default** **delay-time—5**
  hold-time—10
- **Format** **timers spf <delay-time> <hold-time>**
- **Mode** **Router OSPF Config**

12.7.40 trapflags (OSPF)

This command enables OSPF traps.

- **Default** **enabled**
- **Format** **trapflags**
- **Mode** **Router OSPF Config**

no trapflags

This command disables OSPF traps.

- **Format** **no trapflags**
- **Mode** **Router OSPF Config**

12.7.41 show ip ospf

This command displays information relevant to the OSPF router.

- **Format** **show ip ospf**
- **Mode** **Privileged EXEC**

NOTE: Some of the information below displays only if you enable OSPF and configure certain features.

Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
ASBR Mode	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).
RFC 1583 Compatibility	Reflects whether 1583 compatibility is enabled or disabled. This is a configured value.
ABR Status	Shows whether the router is an OSPF Area Border Router.
Exit Overflow Interval	Shows the number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the

link-state database.

New LSAs Originated Shows the number of new link-state advertisements that have been originated.

LSAs Received Shows the number of link-state advertisements received determined to be new instantiations.

External LSDB Limit Shows the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.

Default Metric Default value for redistributed routes.

Default Route Advertise Indicates whether the default routes received from other source protocols are advertised or not

Always Shows whether default routes are always advertised.

Metric Shows the metric for the advertised default routes. If the metric is not configured, this field is blank.

Metric Type Shows whether the routes are External Type 1 or External Type 2.

Maximum Paths Shows the maximum number of paths that OSPF can report for a given destination.

Redistributing This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.

Source Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.

Metric Shows the metric of the routes being redistributed.

Metric Type Shows whether the routes are External Type 1 or External Type 2.

Tag Shows the decimal value attached to each external route.

Subnets For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Distribute-List Shows the access list used to filter redistributed routes.

12.7.42 show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

- **Format** **show ip ospf abr**
- **Modes** **Privileged EXEC**
  User EXEC

Type	The type of the route to the destination. It can be either: ▫ **intra** — Intra-area route ▫ **inter** — Inter-area route
Router ID	Router ID of the destination
Cost	Cost of using this route
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

12.7.43 show ip ospf area

This command displays information about the area. The <areaid> identifies the OSPF area that is being displayed.

- **Format** **show ip ospf area <areaid>**
- **Modes** **Privileged EXEC**
  User EXEC

AreaID	Is the area id of the requested OSPF area
External Routing	Is a number representing the external routing capabilities for this area.
Spf Runs	Is the number of times that the intra-area route table has been calculated using this area's link-state database
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Import Summary LSAs	Shows whether to import summary LSAs.
OSPF Stub Metric Value	Shows the metric value of the stub area. This field displays only if the area is a configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA.

Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.

Redistribute into NSSA	Shows whether to redistribute information into the NSSA
Default Information Originate	Shows whether to advertise a default route into the NSSA
Default Metric	Shows the metric value for the default route advertised into the NSSA.
Default Metric Type	Shows the metric type for the default route advertised into the NSSA.
Translator Role	Shows the NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	Shows the amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

12.7.44 show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

- **Format show ip ospf asbr**
- **Modes Privileged EXEC**
- **User EXEC**

Type	The type of the route to the destination. It can be either: ▫ **intra** — Intra-area route ▫ **inter** — Inter-area route
Router ID	Router ID of the destination
Cost	Cost of using this route
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

12.7.45 show ip ospf database

This command displays information about the link state database when OSPF is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional <areaid> parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display. Use asbrsummary to show the autonomous system boundary router (ASBR) summary LSAs. Use external to display the external LSAs. Use network to display the network LSAs. Use nssaexternal to display NSSA external LSAs. Use router to display router LSAs. Use summary to show the LSA database summary information. Use <lsid> to specify the link state ID (LSID). The value of <lsid> can be an IP address or an integer in the range of 0-4294967295. Use adv-router to show the LSAs that are restricted by the advertising router. Use self-originate to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.

- **Format** **show ip ospf [<areaid>] database [{asbr-summary | external | network | nssa-external | router | summary}] [<lsid>] [{advrouter [<rtrid>] | self-originate}]**
- **Modes** **Privileged EXEC**
  User EXEC

For each link-type and area, the following information is displayed.

Link Id	Is a number that uniquely identifies an LSA that a router originates from all other self originated LSA's of the same LS type.
Adv Router	The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.
Age	Is a number representing the age of the link state advertisement in seconds.
Sequence	Is a number that represents which LSA is more recent.
Checksum	Is the total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

12.7.46 show ip ospf database database-summary

Use this command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

- **Format** **show ip ospf database database-summary**
- **Modes** **Privileged EXEC**
  User EXEC

Router	Total number of router LSAs in the OSPF link state database.
Network	Total number of network LSAs in the OSPF link state database.

Summary Net	Total number of summary network LSAs in the database.
Summary ASBR	Number of summary ASBR LSAs in the database.
Type-7 Ext	Total number of Type-7 external LSAs in the database.
Self-Originated Type-7	Total number of self originated AS external LSAs in the OSPFv3 link state database.
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.
Subtotal	Number of entries for the identified area.
Total	Number of entries for all areas.

12.7.48 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

▫ **Format** **show ip ospf interface {<slot/port> | loopback <loopback-id>}**

▫ **Modes** **Privileged EXEC**
User EXEC

IP Address	Represents the IP address for the specified interface.
Subnet Mask	A mask of the network and host portion of the IP address for the OSPF inter face.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	Represents the OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgement Interval for the specified interface.
Transit Delay Interval	A number representing the OSPF Transit Delay for the specified interface.

Authentication Type	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.

The information below will only be displayed if OSPF is enabled.

OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Metric Cost	The cost of the OSPF interface.

12.7.49 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

▫ **Format** **show ip ospf interface brief**

▫ **Modes** **Privileged EXEC**
User EXEC

Interface	Valid slot and port number separated by forward slashes.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	Represents the OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Retransmit Delay Interval	A number representing the OSPF Transit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgement Interval for the specified

interface.

12.7.50 show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

- **Format** **show ip ospf interface stats <slot/port>**
- **Modes** **Privileged EXEC**
- **User EXEC**

OSPF Area ID The area id of this OSPF interface.

Area Border Router Count The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.

AS Border Router Count The total number of Autonomous System border routers reachable within this area.

Area LSA Count The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

IP Address The IP address associated with this OSPF interface

OSPF Interface Events The number of times the specified OSPF interface has changed its state, or an error has occurred

Virtual Events The number of state changes or errors that occurred on this virtual link.

Neighbor Events The number of times this neighbor relationship has changed state, or an error has occurred.

External LSA Count The number of external (LS type 5) link-state advertisements in the link-state database.

Sent Packets The number of OSPF packets transmitted on the interface.

Received Packets The number of valid OSPF packets received on the interface.

Discards The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.

Bad Version The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.

Source Not On Local Subnet The number of received packets discarded because the source IP address is not within a subnet configured on a local interface.

(NOTE: This field only applies to OSPFv2.)

Virtual Link Not Found The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.

Area Mismatch The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.

Invalid Destination Address The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses

Wrong Authentication Type The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface. (NOTE: This field only applies to OSPFv2.)

Authentication Failure The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.

(NOTE: This field only applies to OSPFv2.)

No Neighbor at Source Address The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.

NOTE: Does not apply to Hellos.

Invalid OSPF Packet Type The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.

Table 9 lists the number of OSPF packets of each type sent and received on the interface.

Packet Type	Sent	Received
Hello	6960	6960
Database Description	3	3
LS Request	1	1
LS Update	141	42
LS Acknowledgement	40	135

Table 9. Type of OSPF Packets Sent and Received on the Interface

12.7.51 show ip ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The <ip-address> is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

▫ **Format** **show ip ospf neighbor [interface <slot/port>] [<ip-address>]**

▫ **Modes** **Privileged EXEC**

▫ **User EXEC**

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Router ID Shows the 4-digit dotted-decimal number of the neighbor router.

Priority Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

IP Address Shows the IP address of the neighbor

Interface Shows the interface of the local router in slot/port format

State Shows the state of the neighboring routers. Possible values are:

Down- initial state of the neighbor conversation - no recent information has been received from the neighbor.

Attempt - Neighbor no recent information has been received from the neighbor but a more concerted effort should be made to contact the

Init - an Hello packet has recently been seen from the neighbor, but bidirec tional communication has not yet been established.

2 way - communication between the two routers is bidirectional.

Exchange start - the first step in creating an adjacency between the two neigh boring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.

Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the

Exchange state

Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs

Dead Time Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display:

Interface Valid slot and port number separated by forward slashes.

Neighbor IP Address Shows the IP address of the neighbor router

Interface Index Shows the interface ID of the neighbor router

Area ID Shows the area ID of the OSPF area associated with the interface

Options An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Router Priority Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

Dead Timer Due Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

State Shows the state of the neighboring routers.

Events The number of times this neighbor relationship has changed state, or an error has occurred.

Retransmission Queue Length Is an integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

12.7.52 show ip ospf range

This command displays information about the area ranges for the specified <areaid>. The <areaid> identifies the OSPF area whose ranges are being displayed.

▫ **Format** **show ip ospf range <areaid>**

▫ **Modes** **Privileged EXEC**

User EXEC

Area ID	The area id of the requested OSPF area.
IP Address	An IP Address which represents this area range.
Subnet Mask	A valid subnet mask for this area range.
Lsdb Type	The type of link advertisement associated with this area range.
Advertisement	The status of the advertisement. Advertisement has two possible settings: **enabled** or **disabled**.

12.7.53 show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

- **Format** **show ip ospf statistics**
- **Modes** **Privileged EXEC**

  User EXEC

Delta T	How long ago the SPF ran. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds since the SPF run.
SPF Duration	How long the SPF took in milliseconds.
Reason	The reason the SPF was scheduled. Reason codes are as follows: ▫ **R** - a router LSA has changed ▫ **N** - a network LSA has changed ▫ **SN** - a type 3 network summary LSA has changed ▫ **SA** - a type 4 ASBR summary LSA has changed ▫ **X** - a type 5 or type 7 external LSA has changed

12.7.54 show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

- **Format** **show ip ospf stub table**
- **Modes** **Privileged EXEC**

  User EXEC

Area ID	Is a 32-bit identifier for the created stub area
Type of Service	Is the type of service associated with the stub metric. FASTPATH only sup ports Normal TOS.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas

12.7.55 show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The <areaid> parameter identifies the area and the <neighbor> parameter identifies the neighbor's Router ID.

- **Format** **show ip ospf virtual-link <areaid> <neighbor>**
- **Modes** **Privileged EXEC**
  User EXEC

Area ID	The area id of the requested OSPF area
Neighbor Router ID	The input neighbor Router ID
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Iftransit Delay Interval	The configured transit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The configured authentication type of the OSPF virtual interface.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

12.7.56 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

- **Format** **show ip ospf virtual-link brief**
- **Modes** **Privileged EXEC**
  User EXEC

Area Id	The area id of the requested OSPF area.
Neighbor	The neighbor interface of the OSPF virtual interface.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transit Delay	The configured transit delay for the OSPF virtual interface.

12.8 Routing Information Protocol (RIP) Commands

This section describes the commands you use to view and configure RIP, which is a distance-vector routing protocol that you use to route traffic within a small network.

12.8.1 router rip

Use this command to enter Router RIP mode.

- **Format** **router rip**
- **Mode** **Global Config**

12.8.2 enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

- **Default** **enabled**
- **Format** **enable**
- **Mode** **Router RIP Config**

no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

- **Format** **no enable**
- **Mode** **Router RIP Config**

12.8.3 ip rip

This command enables RIP on a router interface.

- **Default** **disabled**
- **Format** **ip rip**
- **Mode** **Interface Config**

no ip rip

This command disables RIP on a router interface.

- **Format** **no ip rip**
- **Mode** **Interface Config**

12.8.4 auto-summary

This command enables the RIP auto-summarization mode.

▫ **Default** **disabled**

▫ **Format** **auto-summary**

▫ **Mode** **Router RIP Config**

no auto-summary

This command disables the RIP auto-summarization mode.

▫ **Format** **no auto-summary**

▫ **Mode** **Router RIP Config**

12.8.5 default-information originate (RIP)

This command is used to control the advertisement of default routes.

▫ **Format** **default-information originate**

▫ **Mode** **Router RIP Config**

no default-information originate (RIP)

This command is used to control the advertisement of default routes.

▫ **Format** **no default-information originate**

▫ **Mode** **Router RIP Config**

12.8.6 default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

▫ **Format** **default-metric <0-15>**

▫ **Mode** **Router RIP Config**

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

▫ **Format** **no default-metric**

▫ **Mode** **Router RIP Config**

12.8.7 distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

▫ **Default** **15**

▫ **Format** **distance rip <1-255>**

▫ **Mode** **Router RIP Config**

no distance rip

This command sets the default route preference value of RIP in the router.

- **Format** **no distance rip**
- **Mode** **Router RIP Config**

12.8.8 distribute-list out (RIP)

This command is used to specify the access list to filter routes received from the source protocol. Default 0

- **Format** **distribute-list <1-199> out {ospf | bgp | static | connected}**
- **Mode** **Router RIP Config**

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

- **Format** **no distribute-list <1-199> out {ospf | bgp | static | connected}**
- **Mode** **Router RIP Config**

12.8.9 ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface. The value of <type> is either none, simple, or encrypt. The value for authentication key [key] must be 16 bytes or less. The [key] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of <type> is encrypt, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

- **Default** **none**
- **Format** **ip rip authentication {none | {simple <key>} | {encrypt <key> <keyid>}}**
- **Mode** **Interface Config**

no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

- **Format** **no ip rip authentication**
- **Mode** **Interface Config**

12.8.10 ip rip receive version

This command configures the interface to allow RIP control packets of the specified version(s) to be received.

The value for <mode> is one of: rip1 to receive only RIP version 1 formatted packets, rip2 for RIP version 2, both to receive packets from either format, or none to not allow any RIP control packets to be received.

- **Default** **both**
- **Format** **ip rip receive version {rip1 | rip2 | both | none}**

- **Mode** **Interface Config**

no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

- **Format** **no ip rip receive version**
- **Mode** **Interface Config**

12.8.11 ip rip send version

This command configures the interface to allow RIP control packets of the specified version to be sent.

The value for <mode> is one of: rip1 to broadcast RIP version 1 formatted packets, rip1c (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, rip2 for sending RIP version 2 using multicast, or none to not allow any RIP control packets to be sent.

- **Default** **rip2**
- **Format** **ip rip send version {rip1 | rip1c | rip2 | none}**
- **Mode** **Interface Config**

no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

- **Format** **no ip rip send version**
- **Mode** **Interface Config**

12.8.12 hostroutesaccept

This command enables the RIP hostroutesaccept mode.

- **Default** **enabled**
- **Format** **hostroutesaccept**
- **Mode** **Router RIP Config**

no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

- **Format** **no hostroutesaccept**
- **Mode** **Router RIP Config**

12.8.13 split-horizon

This command sets the RIP split horizon mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

- **Default** **simple**
- **Format** **split-horizon {none | simple | poison}**
- **Mode** **Router RIP Config**

no split-horizon

This command sets the default RIP split horizon mode.

- **Format** **no split-horizon**
- **Mode** **Router RIP Config**

12.8.14 redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match <match-type> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

- **Default** **metric—not-configured**
  match—internal
- **Format for OSPF as source protocol**
  redistribute ospf [metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]
- **Format for other source protocol**
  redistribute {bgp | static | connected} [metric <0-15>]
- **Mode** **Router RIP Config**

no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

- **Format** **no redistribute {ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]**
- **Mode** **Router RIP Config**

12.8.15 show ip rip

This command displays information relevant to the RIP router.

- **Format** **show ip rip**
- **Modes** **Privileged EXEC**
  User EXEC

RIP Admin Mode	Enable or disable.

Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. The default is enable.
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.
Default Metric	Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)
Default Route Advertise	The default route.

12.8.16 show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

▫ **Format** **show ip rip interface brief**

▫ **Modes** **Privileged EXEC**
User EXEC

Interface	Valid slot and port number separated by forward slashes.
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are **none, RIP-1, RIP-1c, RIP-2**.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are **none, RIP-1, RIP-2, Both**
RIP Mode	RIP administrative mode of router RIP operation; enable activates, disable deactivates it.
Link State	The mode of the interface (up or down).

12.8.17 show ip rip interface

This command displays information related to a particular RIP interface.

- **Format** **show ip rip interface <slot/port>**
- **Modes** **Privileged EXEC**

  User EXEC

Interface	Valid slot and port number separated by forward slashes. This is a configured value.
IP Address	The IP source address used by the specified RIP interface. This is a configured value.
Send version	The RIP version(s) used when sending updates on the specified interface. The types are **none, RIP-1, RIP-1c, RIP-2**. This is a configured value.
Receive version	The RIP version(s) allowed when receiving updates from the specified interface. The types are **none, RIP-1, RIP-2, Both**. This is a configured value.
Both RIP Admin Mode	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
Link State	Indicates whether the RIP interface is up or down. This is a configured value.
Authentication Type	The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.
Default Metric	A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value. The following information will be invalid if the link state is down.
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

13 CLI COMMANDS: IP Multicast

This chapter provides a detailed explanation of the IP Multicast commands. The following IP Multicast CLI commands are available in the switch's Multicast module.

Note: The command in this chapter are applied only for Layer 3 Series.

13.1 Multicast Commands

The following commands are used to configure IP Multicast.

13.1.1 ip mcast boundary

This command adds an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable. <groupipaddr> is a group IP address and <mask> is a group IP mask.

- **Format** **ip mcast boundary <groupipaddr> <mask>**
- **Mode** **Interface Config**

no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable. <groupipaddr> is a group IP address and <mask> is a group IP mask.

- **Format** **no ip mcast boundary <groupipaddr> <mask>**
- **Mode** **Interface Config**

13.1.2 ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active . For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

- **Default** **disabled**
- **Format** **ip multicast**
- **Mode** **Global Config**

no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive . For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

- **Format** **no ip multicast**

- **Mode Global Config**

13.1.3 ip multicast staticroute

This command creates a static route which is used to perform RPF checking in multicast packet forwarding. The combination of the <sourceipaddr> and the <mask> fields specify the network IP address of the multicast packet source. The <groupipaddr> is the IP address of the next hop toward the source. The <metric> is the cost of the route entry for comparison with other routes to the source network and is a value in the range of 0 and 255. The current incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

- **Default none**
- **Format ip multicast staticroute <sourceipaddr> <mask> <rpfipaddr> <met-ric> <unit/slot/port>**
- **Mode Global Config**

no ip multicast staticroute

This command deletes a static route in the static mcast table. The <sourceipaddr> is the IP address of the multicast packet source.

- **Format no ip multicast staticroute <sourceipaddr>**
- **Mode Global Config**

13.1.4 ip multicast ttl-threshold

This command applies the given <ttlthreshold>to a routing interface. The <ttlthreshold> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. The value for <ttlthreshold>has range from 0 to 255.

- **Default 1**
- **Format ip multicast ttl-threshold <ttlvalue>**
- **Mode Interface Config**

no ip multicast ttl-threshold

This command applies the default <ttlthreshold>to a routing interface. The <ttlthreshold> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

- **Format no ip multicast ttl-threshold**
- **Mode Interface Config**

13.1.5 mrinfo

This command is used to query the neighbor information of a multicast-capable router specified by [ipaddr]. The default value is the IP address of the system at which the command is issued. The mrinfo command can take up to 2 minutes to complete. Only one mrinfo command may be in process at a time. The results of this command will be available in the results buffer pool which can be displayed by using "show mrinfo".

- **Default** **none**
- **Format** **mrinfo [<ipaddr>]**
- **Mode** **Privileged EXEC**

13.1.6 mstat

This command is used to find the IP Multicast packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command will be available in the results buffer pool which can be displayed by using the command “show mstat” on page 255. If a debug command is already in progress, a message is displayed and the new request fails.

The <source> is the IP address of the remote multicast-capable source. The [receiver] is the IP address of the receiver. The default value is the IP address of the system at which the command is issued. The [group] is a multicast address of the group to be displayed. The default value is 224.2.0.1(the group used for the multicast backbone).

Note: The group and receiver IP addresses can be entered in any order.

- **Default** none
- **Format** **mstat <source> [<group/receiver >] [<group/receiver>]**
- **Mode** **Privileged EXEC**

13.1.7 mtrace

This command is used to find the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command are available in the results buffer pool which can be displayed by using the command “show mtrace” on page 255.

The <source> is the IP address of the remote multicast-capable source. The [receiver] is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The [group] is the multicast address of the group to be displayed. The default value is 224.2.0.1(the group used for the multicast backbone). If a debug command is already in execution, a message is displayed and the new request fails.

Note: The group and destination IP addresses can be entered in any order.

- **Default** **none**
- **Format** **mtrace <sourceipaddr> [<group/destination>] [<group/destina-tion >]**
- **Mode** **Privileged EXEC**

13.1.8 show ip mcast

This command displays the system-wide multicast information.

- **Format** **show ip mcast**
- **Modes** **Privileged EXEC User EXEC**

Admin Mode	This field displays the administrative status of multicast. This is a configured value.
Protocol State	This field indicates the current state of the multicast protocol. Possible values are Operational or Non-Operational.
Table Max Size	This field displays the maximum number of entries allowed in the multicast table.
Number Of Packets For Which Source Not Found	This displays the number of packets for which the source is not found.
Number Of Packets	For Which Group Not Found This displays the number of packets for which the group is not found.
Protocol	This field displays the multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP. Entry Count This field displays the number of entries in the multicast table.
Highest Entry Count	This field displays the highest entry count in the multicast table.

13.1.9 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

- **Format** **show ip mcast boundary {<unit/slot/port> | all}**
- **Modes** **Privileged EXEC User EXEC**

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
Group Ip	The group IP address
Mask	The group IP mask

13.1.10 show ip mcast interface

This command displays the multicast information for the specified interface.

- **Format** **show ip mcast interface <unit/slot/port>**
- **Modes** **Privileged EXEC User EXEC**

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
TTL	This field displays the time-to-live value for this interface.

13.1.11 show ip mcast mroute

This command displays a summary or all the details of the multicast table.

- **Format** **show ip mcast mroute {detail | summary}**
- **Modes** **Privileged EXEC User EXEC**

If the “detail” parameter is specified, the following fields are displayed:

Source IP Addr	This field displays the IP address of the multicast data source.
Group IP Addr	This field displays the IP address of the destination of the multicast packet.
Expiry Time	This field displays the time of expiry of this entry in seconds.
Up Time	This field displays the time elapsed since the entry was created in seconds.
RPF Neighbor	This field displays the IP address of the RPF neighbor.
Flags	This field displays the flags associated with this entry.

If the “summary” parameter is specified, the following fields are displayed:

Source IP Addr	This field displays the IP address of the multicast data source.
Group IP Addr	This field displays the IP address of the destination of the multicast packet
Protocol	This field displays the multicast routing protocol by which this entry was created.
Incoming Interface	This field displays the interface on which the packet for this source/group arrives
Outgoing Interface	List This field displays the list of outgoing interfaces on which this packet is forwarded.

13.1.12 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given <groupipaddr>.

- **Format** **show ip mcast mroute group <groupipaddr> {detail |summary}**
- **Modes** **Privileged EXEC User EXEC**

Source IP Addr	This field displays the IP address of the multicast data source.

Group IP Addr	This field displays the IP address of the destination of the multicast packet.
Protocol	This field displays the multicast routing protocol by which this entry was created.
Incoming Interface	This field displays the interface on which the packet for this group arrives.
Outgoing Interface List	This field displays the list of outgoing interfaces on which this packet is forwarded.

13.1.13 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given **<sourceipaddr> or <sourceipaddr> [<groupipaddr>] pair.**

▫ **Format** **show ip mcast mroute source <sourceipaddr> {summary | <groupi-paddr>}**

▫ **Modes** **Privileged EXEC User EXEC**

If the detail parameter is specified the follow fields are displayed:

Source IP Addr	This field displays the IP address of the multicast data source.
Group IP Addr	This field displays the IP address of the destination of the multicast packet.
Expiry Time	This field displays the time of expiry of this entry in seconds.
Up Time	This field displays the time elapsed since the entry was created in seconds.
RPF Neighbor	This field displays the IP address of the RPF neighbor.
Flags	This field displays the flags associated with this entry.

If the summary parameter is specified the follow fields are displayed:

Source IP Addr	This field displays the IP address of the multicast data source.
Group IP Addr	This field displays the IP address of the destination of the multicast packet.
Protocol	This field displays the multicast routing protocol by which this entry was created.
Interface	This field displays the interface on which the packet for this source arrives.
Outgoing Interface List	This field displays the list of outgoing interfaces on which this packet is forwarded.

13.1.14 show ip mcast mroute static

This command displays all the static routes configured in the static mcast table if is specified or displays the static route associated with the particular <sourceipaddr>.

- **Format show ip mcast mroute static [<sourceipaddr>]**
- **Modes Privileged EXEC User EXEC**

Source Address	This field displays the IP address of the multicast packet source.
Source Mask	This field displays the mask applied to the IP address of the multicast packet source.
RPF Address	This field displays the IP address to be used as RPF for the given source and mask.
Metric	This field displays the metric value corresponding to the source address.
Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.

13.1.15 show mrinfo

This command is used to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a "mrinfo [ipaddr]" command. The results subsequent to the completion of the latest "mrinfo" will be available in the bufferpool after a maximum duration of two minutes after the completion of the ‘show mrinfo’ command. A subsequent issue ‘mrinfo’ will overwrite the contents of the buffer pool with fresh results.

- **Default none**
- **Format show mrinfo**
- **Mode Privileged EXEC**

Router Interface	The IP address of this neighbor
Neighbor	The neighbor associated with the router interface
Metric	The metric value associated with this neighbor
TTL	The TTL threshold associated with this neighbor
Flags	Status of the neighbor

13.1.16 show mstat

This command is used to display the results of packet rate and loss information from the results buffer pool of the router, subsequent to the execution/completion of a ‘mstat <source> [group] [receiver]’ command. Within two minutes of the completion of the ‘mstat’ command, the results will be available in the buffer pool. The next issuing of "mstat" would overwrite the buffer pool with fresh results.

- ▫ **Default none**
- ▫ **Format show mstat**
- ▫ **Mode Privileged EXEC**

13.1.17 show mtrace

This command is used to display results of multicast trace path from the results buffer pool of the router, subsequent to the execution/completion of a "mtrace <source> [group] [receiver]" command. The results subsequent to the completion of the "mtrace" will be available in the buffer pool within 2 minutes and thereafter. A subsequent "mtrace" command would overwrite the results in the buffer pool.

- ▫ **Default noneFormat show mtrace**
- ▫ **Modes Privileged EXEC User EXEC**

Hops Away From Destination	The ordering of intermediate routers between the source and the destination
Intermediate Router Address	The address of the intermediate router at the specified hop distance
Mcast Protocol In Use	The multicast routing protocol used for the out interface of the specified intermediate router.
TTL Threshold	The Time-To-Live threshold of the out interface on the specified intermediate router.
Time Elapsed Between Hops (msecs)	The time between arrival at one intermediate router to the arrival at the next.

13.2 Distance Vector Multicast Routing Protocol (DVMRP) Commands

This section provides a detailed explanation of the DVMRP commands. The commands are divided into the following different groups:

◆Show commands are used to display device settings, statistics and other information.

◆Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

13.2.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

- ▫ **Default disabled**
- ▫ **Format ip dvmrp**
- ▫ **Mode Global Config**

no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive. IGMP must be enabled before DVMRP can be enabled.

- ▫ **Format no ip dvmrp**
- ▫ **Mode Global Config**

13.2.2 ip dvmrp metric

This command configures the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 63.

- ▫ **Default 1**
- ▫ **Format ip dvmrp metric <metric>**
- ▫ **Mode Interface Config**

no ip dvmrp metric

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

- ▫ **Format no ip dvmrp metric**
- ▫ **Mode Interface Config**

13.2.3 ip dvmrp trapflags

This command enables the DVMRP trap mode.

- ▫ **Default disabled**

- **Format** **ip dvmrp trapflags**
- **Mode** **Global Config**

no ip dvmrp trapflags

This command disables the DVMRP trap mode.

- **Format** **no ip dvmrp trapflags**
- **Mode** **Global Config**

13.2.4 show ip dvmrp

This command displays the system-wide information for DVMRP.

- **Format** **show ip dvmrp**
- **Modes** **Privileged EXEC User EXEC**

Admin Mode	This field indicates whether DVMRP is enabled or disabled. This is a configured value.
Version String	This field indicates the version of DVMRP being used.
Number of Routes	This field indicates the number of routes in the DVMRP routing table.
Reachable Routes	This field indicates the number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
Interface Mode	This field indicates the mode of this interface. Possible values are **Enabled** and **Disabled**.
State	This field indicates the current state of DVMRP on this interface. Possible values are **Operational** or **Non-Operational**.

13.2.5 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

- **Format** **show ip dvmrp interface <unit/slot/port>**
- **Modes** **Privileged EXEC User EXEC**

Interface Mode	This field indicates whether DVMRP is enabled or disabled on the specified interface. This is a configured value.
Metric	This field indicates the metric of this interface. This is a configured value.
Local Address	This is the IP Address of the interface. This Field is displayed only when DVMRP is operational on the interface.
Generation ID	This is the Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Received Bad Packets	This is the number of invalid packets received.
Received Bad Routes	This is the number of invalid routes received
Sent Routes	This is the number of routes that have been sent on this interface.

13.2.6 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

- **Format** **show ip dvmrp neighbor**
- **Modes** **Privileged EXEC User EXEC**

IfIndex	This field displays the value of the interface used to reach the neighbor.
Nbr IP Addr	This field indicates the IP Address of the DVMRP neighbor for which this entry contains information.
State	This field displays the state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	This field indicates the time since this neighboring router was learned
Expiry Time	This field indicates the time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.
Generation ID	This is the Generation ID value for the neighbor.
Major Version	This shows the major version of DVMRP protocol of neighbor.
Minor Version	This shows the minor version of DVMRP protocol of neighbor.

Capabilities	This shows the capabilities of neighbor.
Received Routes	This shows the number of routes received from the neighbor.
Rcvd Bad Pkts	This field displays the number of invalid packets received from this neighbor.
Rcvd Bad Routes	This field displays the number of correct packets received with invalid routes.

13.2.7 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

- **Format** **show ip dvmrp nexthop**
- **Modes** **Privileged EXEC User EXEC**

Source IP	This field displays the sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	This field displays the IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.
Next Hop Interface	This field displays the interface in unit/slot/port format for the outgoing interface for this next hop.
Type	This field states whether the network is a LEAF or a BRANCH.

13.2.8 show ip dvmrp prune

This command displays the table listing the router’s upstream prune information.

- **Format** **show ip dvmrp prune**
- **Mode** **Privileged EXEC and User EXEC**

Group IP	This field identifies the multicast Address that is pruned.
Source IP	This field displays the IP Address of the source that has pruned.
Source Mask	This field displays the network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.
Expiry Time (secs)	This field indicates the expiry time in seconds. This is the time remaining for this prune to age out.

13.2.9 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

▫ **Format** **show ip dvmrp route**

▫ **Mode** **Privileged EXEC and User EXEC**

Source Address	This field displays the multicast address of the source group.
Source Mask	This field displays the IP Mask for the source group.
Upstream Neighbor	This field indicates the IP Address of the neighbor which is the source for the packets for a specified multicast address.
Interface	This field displays the interface used to receive the packets sent by the sources.
Metric	This field displays the distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time(secs)	This field indicates the expiry time in seconds. This is the time remaining for this route to age out.
Up Time(secs)	This field indicates the time when a specified route was learnt, in seconds.

13.3 Internet Group Management Protocol (IGMP) Commands

This section provides a detailed explanation of the IGMP commands. The commands are divided into the following different groups:

◆Show commands are used to display device settings, statistics and other information.

◆Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

13.3.1 ip igmp

This command sets the administrative mode of IGMP in the router to active.

- **Default disabled**
- **Format ip igmp**
- **Mode Global Config**

no ip igmp

This command sets the administrative mode of IGMP in the router to inactive.

- **Format no ip igmp**
- **Mode Global Config**

13.3.2 ip igmp version

This command configures the version of IGMP for an interface. The value for <version> is either 1, 2 or 3.

- **Default 3**
- **Format ip igmp version <version>**
- **Mode Interface Config**

no ip igmp version

This command resets the version of IGMP for this interface. The version is reset to the default value.

- **Format no ip igmp version**
- **Mode Interface Config**

13.3.3 set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time on the system. This is the amount of time in seconds that a switch will wait for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

- **Default 0**
- **Format set igmp mcrtrexpiretime <0-3600>**
- **Mode Global Config**

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time on the system to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.

- **Format no set igmp mcrtrexpiretime**
- **Mode Global Config**

13.3.4 ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface. The range for <count> is 1 to 20.

- **Format ip igmp last-member-query-count <count>**
- **Mode Interface Config**

no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

- **Format no ip igmp last-member-query-count**
- **Mode Interface Config**

13.3.5 igmp last-member-query-interval

This command configures the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface. The range for <seconds> is 0 to 255 tenths of a second.

- **Default 10 tenths of a second (1 second)**
- **Format ip igmp last-member-query-interval <seconds>**
- **Mode Interface Config**

no ip igmp last-member-query-interval

This command resets the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value.

- **Format no ip igmp last-member-query-interval**
- **Mode Interface Config**

13.3.6 ip igmp query-interval

This command configures the query interval for the specified interface. This is the frequency at which IGMP Host-Query packets are transmitted on this interface. The range for <queryinterval> is 1 to 3600 seconds.

- **Default 125 seconds**
- **Format ip igmp query-interval <seconds>**
- **Mode Interface Config**

no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

- **Format** **no ip igmp query-interval**
- **Mode** **Interface Config**

13.3.7 ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second. The range for <maxresptime> is 0 to 255 tenths of a second.

- **Default** **100**
- **Format** **ip igmp query-max-response-time <seconds>**
- **Mode** **Interface Config**

no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

- **Format** **no ip igmp query-max-response-time**
- **Mode** **Interface Config**

13.3.8 ip igmp robustness

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The range for <robustness> is 1 to 255.

- **Default** **2**
- **Format** **ip igmp robustness <robustness>**
- **Mode** **nterface Config**

no ip igmp robustness

This command sets the robustness value to default.

- **Format** **no ip igmp robustness**
- **Mode** **Interface Config**

13.3.9 ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface. The range for <count> is 1 to 20.

- **Default** **2**
- **Format** **ip igmp startup-query-count <count>**
- **Mode** **nterface Config**

no ip igmp startup-query-count (only for Layer 3 Series)

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

- **Format** **no ip igmp startup-query-count**
- **Mode** **Interface Config**

13.3.10 ip igmp startup-query-interval

This command sets the interval between General Queries sent by a Querier on startup on the interface. The time interval value is in seconds. The range for <interval> is 1 to 300 seconds.

- **Default** **31**
- **Format** **ip igmp startup-query-interval <interval>**
- **Mode** **Interface Config**

no ip igmp startup-query-interval

This command resets the interval between General Queries sent by a Querier on startup on the interface to the default value.

- **Format** **no ip igmp startup-query-interval**
- **Mode** **Interface Config**

13.3.11 set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on a particular interface or VLAN. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

- **Default** **260 seconds**
- **Format** **set igmp groupmembershipinterval <vlanId> <2-3600>**
- **Mode** **Interface Config Vlan Mode**

no set igmp groupmembershipinterval

This command sets the IGMPv3 Group Membership Interval time (on the interface or the VLAN) to the default value.

- **Format** **no set igmp groupmembershipinterval**
- **Mode** **Interface ConfigVlan Mode**

13.3.12 set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds.

- ▫ **Default 10 seconds**
- ▫ **Format set igmp maxresponse <1-3599>**
- ▫ **Mode Global Config Interface Config Vlan Mode**

no set igmp maxresponse

This command sets the IGMP Maximum Response time (on the interface or VLAN) to the default value.

- ▫ **Format no set igmp maxresponse**
- ▫ **Mode Global ConfigInterface Config Vlan Mode**

13.3.13 set igmp mrouter interface

This command configures a selected interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs. Default disable

- ▫ **Format set igmp mrouter interface**
- ▫ **Mode Interface Config**

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

- ▫ **Format no set igmp mrouter interface**
- ▫ **Mode Interface Config**

.

13.3.14 set igmp mrouter

This command configures the VLAN ID(<vlanId>) that has the multicast router mode enabled.

- ▫ **Format set igmp mrouter <vlanId>**
- ▫ **Mode Interface Config**

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (<vlanId>).

- ▫ **Format no set igmp mrouter <vlanId>**
- ▫ **Mode Interface Config**

13.3.15 show ip igmp

This command displays the system-wide IGMP information.

- **Format** **show ip igmp**
- **Modes** **Privileged EXEC User EXEC**

IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value.
Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational.

13.3.16 show ip igmp groups

This command displays the registered multicast groups on the interface. If "detail" is specified this command displays the registered multicast groups on the interface in detail.

- **Format** **show ip igmp groups <unit/slot/port> [detail]**
- **Mode** **Privileged EXEC**

If detail is not specified, the following fields are displayed:

IP Address	This displays the IP address of the interface participating in the multicast group.
Subnet Mask	This displays the subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.

Groups	This displays the list of multicast groups that are registered on this interface.

If detail is specified, the following fields are displayed:

Multicast IP Address	This displays the IP Address of the registered multicast group on this interface.
Last Reporter	This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	This displays the time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	This displays the amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	This displays the time remaining until the local router will assume that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	This displays the time remaining until the local router will assume that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

13.3.17 show ip igmp interface

This command displays the IGMP information for the interface.

- **Format** **show ip igmp interface <unit/slot/port>**
- **Modes** **Privileged EXEC User EXEC**

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value.
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
IGMP Version	This field indicates the version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.

Query Interval This field indicates the frequency at which IGMP Host-Query packets are transmitted on this interface. This is a configured value.

Query Max Response Time This field indicates the maximum query response time advertised in IGMPv2 queries on this interface. This is a configured value.

Robustness This field displays the tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface. This is a configured value.

Startup Query Interval This value indicates the interval between General Queries sent by a Querier on startup. This is a configured value.

Startup Query Count This value is the number of Queries sent out on startup, separated by the Startup Query Interval. This is a configured value.

Last Member Query Interval This value indicates the Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This is a configured value.

Last Member Query Count This value is the number of Group-Specific Queries sent before the router assumes that there are no local members. This is a configured value.

13.3.18 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

- **Format** **show ip igmp interface membership <multiipaddr> [detail]**
- **Mode** **Privileged EXEC**

Interface Valid unit, slot and port number separated by forward slashes.

Interface IP This displays the IP address of the interface participating in the multicast group.

State This displays whether the interface has IGMP in Querier mode or Non-Querier mode.

Group Compatibility Mode The group compatibility mode (v1, v2 or v3) for the specified group on this interface.

Source Filter Mode The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If detail is specified, the following fields are displayed:

Interface	Valid unit, slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
Source Hosts	This displays the list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP Address. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	This displays the amount of time remaining to remove this entry before it is aged out. This is “----” for IGMPv1 and IGMPv2 Membership Reports.

13.3.19 show ip igmp interface stats

This command displays the IGMP statistical information for the given interface. The statistics are only displayed when the interface is enabled for IGMP.

- **Format** **show ip igmp interface stats <unit/slot/port>**
- **Modes** **Privileged EXEC User EXEC**

Querier Status	This field indicates the status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	This field displays the IP Address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	This field indicates the time since the interface Querier was last changed.
Querier Expiry Time	This field displays the amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	This field indicates the number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	This field displays the number of times a group membership has been added on this interface.
Number of Groups	This field indicates the current number of membership entries for this interface

13.4 Protocol Independent Multicast – Dense Mode (PIM-DM) Commands

This section provides a detailed explanation of the PIM-DM commands. The commands are divided into the following different groups:

◆Show commands are used to display device settings, statistics and other information.

◆ Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

13.4.1 ip pimdm

This command enables the administrative mode of PIM-DM in the router.

▫ **Default** **disabled**

▫ **Format** **ip pimdm**

▫ **Mode** **Global Config**

no ip pimdm

This command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

▫ **Format** **no ip pimdm**

▫ **Mode** **Global Config**

13.4.2 ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to enabled.

▫ **Default** **disabled**

▫ **Format** **ip pimdm mode <unit/slot/port>**

▫ **Mode** **Interface Config**

no ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to disabled.

▫ **Format** **no ip pimdm mode <unit/slot/port>**

▫ **Mode** **Interface Config**

13.4.3 ip pimdm query-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

▫ **Default** **30**

▫ **Format** **ip pimdm query-interval <seconds>**

▫ **Mode** **Interface Config**

no ip pimdm query-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

- **Format** **no ip pimdm query-interval**
- **Mode** **Interface Config**

13.4.4 show ip pimdm

This command displays the system-wide information for PIM-DM.

- **Format** **show ip pimdm**
- **Mode** **Privileged EXEC and User EXEC**

PIM-DM Admin Mode	This field indicates whether PIM-DM is enabled or disabled. This is a configured value.
Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
Interface Mode	This field indicates whether PIM-DM is enabled or disabled on this interface. This is a configured value.
State	This field indicates the current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

13.4.5 show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

- **Format** **show ip pimdm interface <unit/slot/port>**
- **Mode** **Privileged EXEC and User EXEC**

Interface Mode	This field indicates whether PIM-DM is enabled or disabled on the specified interface. This is a configured value.
PIM-DM Interface Hello Interval	This field indicates the frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

13.4.6 show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

- **Format** **show ip pimdm interface stats {<unit/slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

Interface	Valid unit, slot and port number separated by forward slashes.
IP Address	This field indicates the IP Address that represents the PIM-DM interface.
Nbr Count	This field displays the neighbor count for the PIM-DM interface.
Hello Interval	This field indicates the time interval between two hello messages sent from the router on the given interface.
Designated Router	This indicates the IP Address of the Designated Router for this interface.

13.4.7 show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

- **Format** **show ip pimdm neighbor {<unit/slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

Neighbor Address	This field displays the IP Address of the neighbor on an interface.
Interface	Valid unit, slot and port number separated by forward slashes.
Up Time	This field indicates the time since this neighbor has become active on this interface.
Expiry Time	This field indicates the expiry time of the neighbor on this interface.

13.4.8 show ip pimdm componenttable

This command displays the table containing objects to a PIM domian.

- **Format** **show ip pimdm componenttable**
- **Mode** **Privileged EXEC and User EXEC**

13.5 Protocol Independent Multicast - Sparse Mode(PIM-SM) Commands

This section provides a detailed explanation of the PIM-SM commands. The commands are divided into the following different groups:

◆Show commands are used to display device settings, statistics and other information.

◆Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

13.5.1 ip pimsm cbsrpreference

This command is used to configure the CBSR preference for a particular PIM-SM interface. The range of CBSR preference is –1 to 255.

▫ **Default 0**

▫ **Format ip pimsm cbsrpreference <-1-255>**

▫ **Mode Interface Config**

no ip pimsm cbsrpreference

This command is used to reset the CBSR preference for a particular PIM-SM interface to the default value.

▫ **Format no ip pimsm cbsrpreference**

▫ **Mode Interface Config**

13.5.2 ip pimsm cbsrhashmasklength

This command is used to configure the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid range is 0 - 32. The default value is 30.

▫ **Default 30**

▫ **Format ip pimsm cbsrhashmasklength <0-32>**

▫ **Mode Interface Config**

no ip pimsm cbsrhashmasklength

This command is used to reset the CBSR hash mask length for a particular PIM-SM interface to the default value.

▫ **Format no ip pimsm cbsrhashmasklength**

▫ **Mode Interface Config**

13.5.3 ip pimsm crppreference

This command is used to configure the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface. The valid values are from (-1 to 255), and the value of -1 is used to indicate that the local interface is not a Candidate RP interface.

The active router interface, with the highest IP Address and crppreference greater than -1, is chosen as the CRP for the router. The default value is 0.In the CRP advertisements sent to the bootstrap router (BSR), the router interface advertises itself as the CRP for the group range 224.0.0.0 mask 240.0.0.0.

▫ **Default 0**

▫ **Format ip pimsm crppreference <-1-255>**

▫ **Mode Interface Config**

no ip pimsm crppreference

This command is used to reset the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface to the default value.

▫ **Format no ip pimsm crppreference**

▫ **Mode Interface Config**

13.5.4 ip pimsm message-interval

This command is used to configure the global join/prune interval for PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 10 to 3600.

▫ **Default 60**

▫ **Format ip pimsm message-interval <10-3600>**

▫ **Mode Global Config**

no ip pimsm message-interval

This command is used to reset the global join/prune interval for PIM-SM router to the default value.

▫ **Format no ip pimsm message-interval**

▫ **Mode Global Config**

13.5.5 ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled.

▫ **Default disabled**

▫ **Format ip pimsm**

▫ **Mode Global Config**

no ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to disabled. IGMP must be enabled before PIM-SM can be enabled.

▫ **Format no ip pimsm**

- **Mode** **Global Config**

13.5.6 ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to enabled.

- **Default** **disabled**
- **Format** **ip pimsm mode**
- **Mode** **Interface Config**

no ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to disabled.

- **Format** **no ip pimsm mode**
- **Mode** **Interface Config**

13.5.7 ip pimsm query-interval

This command configures the transmission frequency of hello messages in seconds between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

- **Default** **30**
- **Format** **ip pimsm query-interval <10-3600>**
- **Mode** **Interface Config**

no ip pimsm query-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

- **Format** **no ip pimsm query-interval**
- **Mode** **Interface Config**

13.5.8 ip pimsm spt-threshold

This command is used to configure the Threshold rate for the RP router to switch to the shortest path. The rate is specified in Kilobytes per second. The possible values are 0 to 2000.

- **Default** **50**
- **Format** **ip pimsm spt-threshold <0-2000>**
- **Mode** **Global Config**

no ip pimsm spt-threshold

This command is used to reset the Threshold rate for the RP router to switch to the shortest path to the default value.

- **Format** **no ip pimsm spt-threshold**

- **Mode** **Global Config**

13.5.9 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM). Default disabled

- **Format** **ip pim-trapflags**
- **Mode** **Global Config**

no ip pim-trapflags

This command disables the PIM trap mode.

- **Format** **no ip pim-trapflags**
- **Mode** **Global Config**

13.5.10 ip pimsm staticrp

This command is used to create RP IP address for the PIM-SM router. The parameter <ipaddress> is the IP address of the RP. The parameter <groupaddress> is the group address supported by the RP. The parameter <groupmask> is the group mask for the group address.

- **Default** **disabled**
- **Format** **ip pimsm staticrp <ipaddress> <groupaddress> <groupmask>**
- **Mode** **Global Config**

no ip pimsm staticrp

This command is used to delete RP IP address for the PIM-SM router. The parameter <ipaddress> is the IP address of the RP. The parameter <groupaddress> is the group address supported by the RP. The parameter <groupmask> is the group mask for the group address.

- **Format** **no ip pimsm staticrp <ipaddress> <groupaddress> <groupmask>**
- **Mode** **Global Config**

13.5.11 ip pimsm register-rate-limit

This command the register threshold rate for PIM-SM..

- **Default** **disabled**
- **Format** **ip pimsm register-rate-limit <0-2000>**
- **Mode** **Global Config**

13.5.12 show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

- **Format** **show ip pimsm rphash <groupaddress>**
- **Mode** **Privileged EXEC and User EXE**

CRP IP Address	This field displays the IP address of the RP.
Group Mask	This field displays the group mask for the group address.

13.5.13 show ip pimsm staticrp

This command displays the static RP information for the PIM-SM router.

- **Format** **show ip pimsm staticrp**
- **Mode** **Privileged EXEC and User EXE**

CRP IP Address	This field displays the IP address of the RP.
Group Address	This field displays the group address supported by the RP.
Group Mask	This field displays the group mask for the group address..

13.5.14 show ip pimsm

This command displays the system-wide information for PIM-SM.

- **Format** **show ip pimsm**
- **Mode** **Privileged EXEC and User EXEC**

PIM-SM Admin Mode	This field indicates whether PIM-SM is enabled or disabled. This is a configured value.
Join/Prune Interval (secs)	This field shows the interval at which periodic PIM-SM **Join/Prune messages are to be sent.** This is a configured value.
Data Threshold Rate (K bits/sec)	This field shows the data threshold rate for the PIM-SM router. This is a configured value.
Register Threshold Rate (K bits/sec)	This field indicates the threshold rate for the RP router to switch to the shortest path. This is a configured value.

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
Interface Mode	This field indicates whether PIM-SM is enabled or disabled on the interface. This is a configured value.
Protocol State	This field indicates the current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

13.5.15 show ip pimsm componenttable

This command displays the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

- **Format** **show ip pimsm componenttable**
- **Mode** **Privileged EXEC and User EXEC**

Component Index	This field displays a number which uniquely identifies the component.
Component BSR Address	This field displays the IP address of the bootstrap router (BSR) for the local PIM region.
Component BSR Expiry Time	This field displays the minimum time remaining before the BSR in the local domain will be declared down.
Component CRP Hold Time	This field displays the hold time of the component when it is a candidate.

13.5.16 show ip pimsm interface

This command displays the interface information for PIM-SM on the specified interface.

- **Format** **show ip pimsm interface <unit/slot/port>**
- **Mode** **Privileged EXEC and User EXEC**

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
IP Address	This field indicates the IP address of the specified interface.
Subnet Mask	This field indicates the Subnet Mask for the IP address of the PIM interface.
Mode	This field indicates whether PIM-SM is enabled or disabled on the specified interface. This is a configured value. By default it is disabled.

Hello Interval	This field indicates the frequency at which PIM hello messages are transmitted on this interface. This is a configured value. By default, the value is 30 seconds.
CBSR Preference	This field shows the preference value for the local interface as a candidate bootstrap router. This is a configured value.
CRP Preference	This field shows the preference value as a candidate rendezvous point on this interface.
CBSR Hash Mask Length	This field shows the hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. The value is used in the hash algorithm for selecting the RP for a particular group.

13.5.17 show ip pimsm interface stats

This command displays the statistical information for PIM-SM on the specified interface.

- **Format** **show ip pimsm interface stats {<unit/slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
IP Address	This field indicates the IP Address that represents the PIM-SM interface.
Subnet Mask	This field indicates the Subnet Mask of this PIM-SM interface.
Designated Router	This indicates the IP Address of the Designated Router for this interface.
Neighbor Count	This field displays the number of neighbors on the PIM-SM interface.

13.5.18 show ip pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

- **Format** **show ip pimsm neighbor {<unit/slot/port> | all}**
- **Mode** **Privileged EXEC and User EXEC**

Unit/Slot/Port	Valid unit, slot and port number separated by forward slashes.
IP Address	This field displays the IP Address of the neighbor on an interface.
Up Time	This field indicates the time since this neighbor has become active on this interface

Expiry Time	This field indicates the expiry time of the neighbor on this interface.

13.5.19 show ip pimsm rp

This command displays the PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific <groupaddress> <groupmask> provided in the command. The information in the table is displayed for each IP multicast group.

- **Format** **show ip pimsm rp {<groupaddress> <groupmask> | candidate | all}**
- **Mode** **Privileged EXEC and User EXEC**

Group Address	This field specifies the IP multicast group address.
Group Mask	This field specifies the multicast group address subnet mask.
Address	This field displays the IP address of the Candidate-RP.
Hold Time	This field displays the hold time of a Candidate-RP.
Expiry Time	This field displays the minimum time remaining before the Candidate-RP will be declared down.
Component	This field displays a number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.

13.5.20 show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

- **Format** **show ip pimsm rphash <groupaddress>**
- **Mode** **Privileged EXEC and User EXE**

CRP IP Address	This field displays the IP address of the RP.
Group Mask	This field displays the group mask for the group address.

14. SWITCH OPERATION

14.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This in-formation comes from the learning process of Ethernet Switch.

14.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

14.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

14.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

14.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

15. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

The Link LED is not lit

Solution:

Check the cable connection and remove duplex mode of the Ethernet Switch

Some stations cannot talk to other stations located on the other port

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

Performance is bad

Solution:

Check the full duplex status of the Ethernet Switch. If the Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

Why the Switch doesn't connect to the network

Solution:

- Check the LNK/ACT LED on the switch
- Try another port on the Switch
- Make sure the cable is installed properly
- Make sure the cable is the right type
- Turn off the power. After a while, turn on power again

APPENDEX A

A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

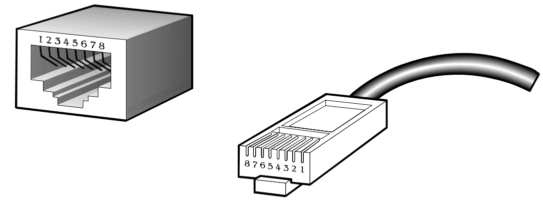
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

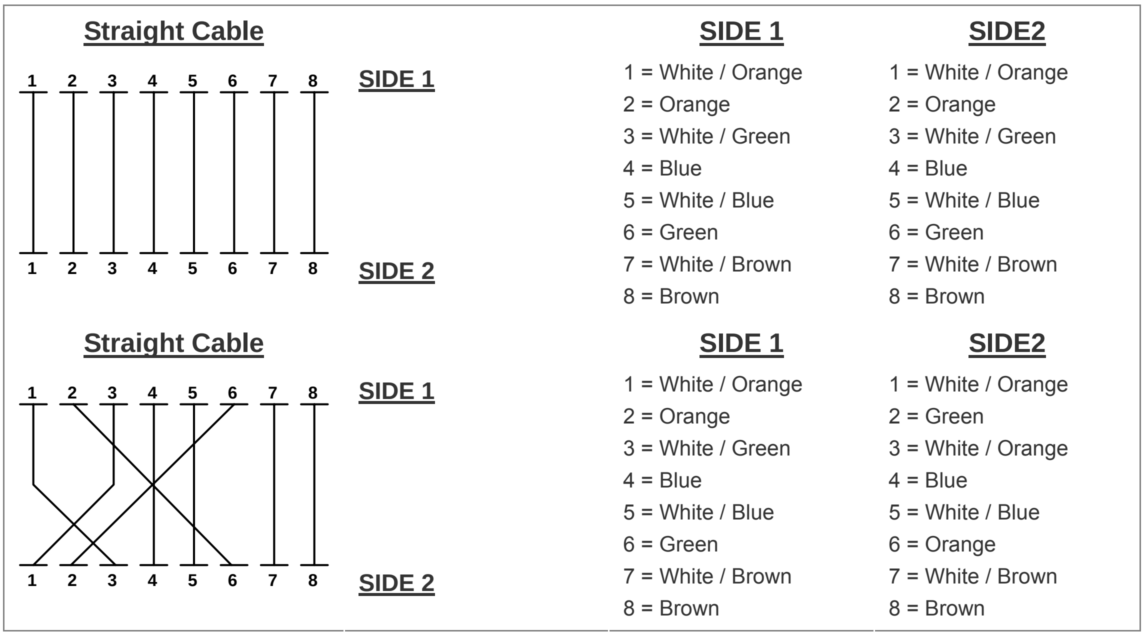
RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:



Straight Cable

SIDE 1	SIDE2
1 = White / Orange	1 = White / Orange
2 = Orange	2 = Orange
3 = White / Green	3 = White / Green
4 = Blue	4 = Blue
5 = White / Blue	5 = White / Blue
6 = Green	6 = Green
7 = White / Brown	7 = White / Brown
8 = Brown	8 = Brown

Straight Cable

SIDE 1	SIDE2
1 = White / Orange	1 = White / Orange
2 = Orange	2 = Green
3 = White / Green	3 = White / Orange
4 = Blue	4 = Blue
5 = White / Blue	5 = White / Blue
6 = Green	6 = Orange
7 = White / Brown	7 = White / Brown
8 = Brown	8 = Brown

Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

GLOSSARY

Bandwidth Utilization

The percentage of packets received over time as compared to overall bandwidth.

BOOTP

Boot protocol used to load the operating system for devices connected to the network.

Distance Vector Multicast Routing Protocol (DVMRP)

A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Broadcasting (RPB).

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment such that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Group Attribute Registration Protocol

See Generic Attribute Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end-stations with multicast groups. GMRP requires that any participating network devices or end-stations comply with the IEEE 802.1p standard.

ICMP Router Discovery

ICMP Router Discovery message is an alternative router discovery method that uses a pair of ICMP messages on multicast links. It eliminates the need to manually configure router addresses and is independent of any specific routing protocol.

Internet Control Message Protocol (ICMP)

Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is elected “querier” and assumes the responsibility of keeping track of group membership.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is directly related to the hardware interface for network devices and passes traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services no attached host has registered for, or forwards them to all ports contained within the designated multicast VLAN group.

Open Shortest Path First (OSPF)

OSPF is a link state routing protocol that functions better over a larger network such as the Internet, as opposed to distance vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobtrusively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Routing Information Protocol (RIP)

The RIP protocol attempts to find the shortest route to another device by minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Simple Network Management Protocol (SNMP)

The application protocol offering network management services in the Internet suite of protocols.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol, a standard protocol for point-to-point connections using serial lines.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or back-up linked network systems. Spanning-tree detects and directs data along the shortest path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.